Impact Assessment (IA)

Title: Data (Use and Access) Act

IA number: DSIT001(EAND)-24-DTT

RPC reference number: RPC-DSIT-5358(1)

Lead department or agency: Department for Science, Innovation and Technology

Other departments or agencies: Department for Business and Trade, Home Office, Digital Cabinet Office, Department of Health and Social Care, HM Treasury, Department for Energy Security and Net Zero, The Information Commissioner's Office, Ministry of Justice

Date: 30 October 2024

Stage: Enactment

Source of intervention: Domestic

Type of measure: Primary Legislation

Contact for enquiries: datapolicyanalysis@dsit.gov.uk

RPC opinion: Fit for purpose: green rated

Summary: intervention and options

Cost of preferred (or more likely) option

(in 2024 prices, millions)

Item	Cost
Total Net Present Social Value	10,604
Business Net Present Value	4,967
Net cost to business per year	-281
Business Impact Target Status	Not applicable

What is the problem under consideration? Why is government action or intervention necessary?

Harnessing the power of data for economic growth, supporting a modern digital government, and improving people's lives were key government commitments laid out in the King's Speech.

The nature of several data-related innovations and complexity of the current regulatory regime means that firms, public sector organisations and consumers are not able to take full advantage of the benefits that could be available to them through effective use of data and data sharing. As

a result, the market fails and benefits are not realised. It is necessary for Government intervention to allow for the realisation of all benefits derived from more effective data use.

What are the policy objectives of the action or intervention and the intended effects?

The proposals aim to:

- Harness the power of data for economic growth by giving a statutory footing to three innovative uses of data: Smart Data, Digital Verification Services, and the National Underground Asset Register
- Support a modern digital government by enabling more and better digital public services, such as an electronic register of births and deaths and applying information standards to health and care suppliers
- Update the UK's data laws to; help scientists make use of data for research; make public interest data sharing and re-use easier; support the safe deployment of new technology; future proof the legislation where appropriate; improve the law enforcement regime - while maintaining high standards of protection
- Modernise and strengthen the ICO, with a more modern regulatory structure, and new, stronger powers
- Establish a Data Preservation Process for coroners to support their investigations into children’s deaths
- Establish a framework for further regulations that will allow researchers access to data relating to online safety held by tech companies
- Provide Ofgem with greater flexibility in their process for choosing the next holder of the Smart Meter Communications Licence

What policy options have been considered, including any alternatives to regulation?

DSIT have considered a total of four policy options, which vary in the degree of change to the current UK data policy regime, these are outlined below:

Option 0: do nothing

This is the scenario in which no changes are made to the current legislation. All analysis carried out is compared to this baseline scenario.

Option 1: do minimum

Updating and simplifying the UK’s data protection framework while focusing on protecting individuals’ data rights and generating societal, scientific, and economic benefits.

Option 2: do intermediate

The do intermediate option encapsulates moderate policy changes to the current regime aiming to resolve most aspects of the market failures. It also incorporates key reforms which aim to address those set out in the King's Speech including Smart data, National Underground Asset Register (NUAR), Digital identity, and the Information Commissioner's Office (ICO) reforms.

Option 3: do maximum

Those measures in the do intermediate with additional data protection reforms.

Is this measure likely to impact international trade and investment?

Yes

Are any of these organisations in scope?

Micro: Yes

Small: Yes

Medium: Yes

Large: Yes

What is the CO_2 equivalent change in greenhouse gas emissions?

(million tonnes $C0_2$ equivalent)

Traded: Not applicable

Non-traded: Not applicable

Will the policy by reviewed?

It will be reviewed.

If applicable, set review date: within 5 years

I have read the Impact Assessment, and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible: Alex Rubin

Date: 04/09/2024

Summary: analysis and evidence – policy option 1

Data (Use and Access) Act

Description

To enable new innovative uses of data to be safely developed and deployed; to improve people's lives by making public services work better by reforming data sharing and standards; to help scientists and researchers make more life enhancing discoveries by improving our data laws; and ensure personal data is well protected by giving the Information Commissioner's

Office stronger powers and a more modern structure; and to make targeted updates to data protection legislation.

Full economic assessment

Price base per year	PV base year	Time period	Net benefit (present value (PV)) (£million) Low	Net benefit present value (PV)) (£million) High	Net benefit present value (PV)) (£million) Best
2024	2024	10	3,170	20,138	10,604

Costs

Estimate	Total transition (constant price) Years (£million)	Average annual (excluding transition) (constant price) (£million)	Total cost (present value) (£million)
Low	765	54	1,208
High	2,501	108	3,267
Best estimate	1,363	76	1,959

Description and scale of key monetised costs by ‘main affected groups’

There will be direct costs to both private and public sector organisations. The assessment provides monetised estimates for these where evidence is sufficient. These estimates include the up-front costs of familiarisation for UK businesses and public organisations including the Information Commissioner's Office. The assessment also estimates the monetised costs for Law Enforcement Agencies (LEAs) of introducing the ability to actively review automated decisions. Also included are the estimated costs to asset owners to conduct data transformation and refresh activities as well as familiarisation and administrative costs to comply with NUAR legislation. There will also be indirect costs as a result of the primary legislation designed to increase the interoperability of Digital Identity and Smart Data schemes. As these reforms are enabling, we have provided an overview of the potential scale of costs and detailed estimates will follow with secondary legislation. X

Other key non-monetised costs by ‘main affected groups’

A qualitative assessment is provided for both direct and indirect costs where evidence is currently not available. These include the costs to LEAs of changes to public sector data handling regulations, the costs to government departments of making data sharing easier and the costs of improving interoperability of data systems across the NHS. The costs of creating innovative Smart Data and Digital Identity schemes are also qualitatively assessed. An assessment on the potential impacts to data subjects trust of the package of reforms has also been included.

Benefits

Estimate	Total transition (constant price) Years (£million)	Average annual (excluding transition) (constant price) (£million)	Total cost (present value) (£million)
Low	0	796	6,437
High	0	2,973	21,34688
Best estimate	0	1,732	12,562

Description and scale of key monetised benefits by ‘main affected groups’

Monetised estimates of direct benefits include the compliance cost savings expected to be experienced by UK business as a result of changes to compliance activities especially for firms that carry out research and development and use AI. The monetary benefit of the reforms to the ICO and LEAs that are currently required to keep logs of the number of processing activities that they carry out is also estimated. The reforms are also expected to increase data use by UK businesses which indirectly will have a quantifiable impact on UK firm-level productivity. The cost savings to owners of underground assets through utility strike avoidance, back office efficiencies and on site efficiencies of the NUAR proposals are also included.

Other key non-monetised benefits by ‘main affected groups’

Where evidence is currently unavailable, we have provided a qualitative review of other anticipated benefits of the reforms. These include the benefits to law enforcement and intelligence services of introducing a ‘legal professional privilege’ exemption and removing the need to notify the ICO of data transfers. We also qualitatively assess the benefits of the oversight regime for the police use of biometrics and overt surveillance, the creation of Smart Data and Digital Identity schemes.

Key assumptions/sensitivities/risks

Discount rate: 3.5%

Where assumptions have been made in the economic modelling, we have made sure to test these either using a confidence band approach or Monte Carlo analysis.

Business case assessment (Option 1)

Costs (£million)	Benefits (£million)	Net (£million)
26	307	-281

Score for Business Impact Target (qualifying provisions only)

Not applicable

Contents

a. List of all recommended policies
b. Impact of preferred option (2024 prices, 2024 PV)
c. EU Adequacy Monte-Carlo Analysis
d. List of ICO guidance updates
e. Gravity trade modelling
f. List of additional measure in the Do maximum option.
g. Measures added via amendment during passage of the DUA Bill and included in the Bill at Royal Assent

Executive Summary

Context

1. As set out in the Kings Speech, the government has prioritised harnessing the power of data for economic growth, supporting a modern digital government, and improving people's lives.
2. This act contains measures that start delivering on the Government's commitment to better serve the British public through science and technology.
3. This impact assessment provides:
    a. An outline of the existing regulatory framework and market failures
    b. The proposed policy options and preferred package of reforms in overcoming these failures.
    c. The cost benefit analysis of the preferred package of reforms, comprising of:
        i. Direct costs and benefits
        ii. Indirect costs and benefits
        iii. Wider impacts
        iv. Trade modelling
        v. In depth analysis of the impact of these reforms on small and micro businesses and specific sectors within the UK economy
    d. An overview of all risks and assumptions associated with the modelling.
    e. An outline of all future monitoring and evaluation activities
4. Many of the policies included in the Act have been designed by other government departments alongside Department for Science, Innovation and Technology (DSIT), including, Department for Business and Trade (DBT), Home Office, Department for Energy Security and Net Zero (DESNZ) and Department of Health and Social Care (DHSC). Where this is the case, analysis has been provided directly by these departments and has been referenced accordingly. There are also reforms included in the Act which are enabling secondary legislation impact assessments. We have highlighted where this is the case and ensured that the analysis provided is representative of this, in line with Better Regulation Unit (BRU) and Regulatory Policy Committee (RPC) guidelines.

Rationale and approach

5. The Act will harness the power of data for economic growth. First, it gives a statutory footing to three innovative uses of data that will accelerate innovation, investment and productivity across the UK:
    a. Smart Data Schemes, which empower customers to make more informed choices and provide businesses with a greater opportunity to innovate by increasing the portability of

their data. Open Banking is the only active example of a regime that is comparable to a 'Smart Data scheme' – but needs a legislative framework to put it on a permanent footing, from which it can grow and expand.

b. By empowering consumers to access their data within new sectors, the aim is also to encourage similar economic growth as demonstrated in Open Banking across the economy. This is crucial in markets where customer engagement is low, or where businesses hold more information and data than the customer.

c. Digital Verification Services will help people and businesses to make the most of identity-checking technologies with confidence and peace of mind. Digital verification services will save people time and money by providing convenient and reliable options to prove things about themselves as they go about their everyday lives.

d. They will also enable smoother, cheaper and more secure online transactions. Digital verification services will lessen the everyday burdens on businesses by reducing costs, time and data leakage.

e. The National Underground Asset Register (NUAR) is a new digital map that is revolutionising the way we install, maintain, operate and repair the pipes and cables buried beneath our feet. NUAR gives planners and excavators standardised, secure, instant access to the data they need, when they need it, to carry out their work efficiently, effectively and safely.

f. Banning sexually explicit deepfakes includes new offences which criminalise the creating, or requesting the creation of, a purported intimate image (deepfake) of another person aged 18 or over without the adult's consent or reasonable belief in consent of creating or requesting the creation of a purported intimate image of an adult without consent or reasonable belief in consent.

g. Producing reports on the use of copyright works in the development of AI systems, and an impact assessment on the policy options considered in the AI and copyright consultation, will help inform policy decisions on AI and copyright.

6. The complexity of the current regulatory regime means that businesses and consumers are not able to take full advantage of the benefits that are available to them through effective use of data and data sharing. As a result, the market fails, and benefits are not realised. Furthermore, information asymmetry exists for UK businesses that are unaware of the benefits that increased data sharing can lead to. Therefore, it is necessary for Government intervention to allow for the realisation of all benefits that can be derived from more effective data use.

a. DSIT set out many of these areas in the King's Speech. The reforms aim at achieving the following objectives: Enabling more market competition and introduction of innovative services for consumers and firms through Smart Data schemes.

b. Supporting the creation and adoption of secure and trusted digital identity products and services from certified providers to help with things like moving house, pre-employment checks, and buying age restricted goods and services.

c. Creating a new digital map to revolutionise the way data can be transmitted through pipes and cables to allow secure, instant access.

d. Help scientists and researchers make more life enhancing discoveries by improving the UK's data laws.

e. Delivering better public services through better data sharing, including in public health, law enforcement, and national security

f. Improving regulation through the reform of the Information Commissioner's Office

g. Maintain high standards of protection while making some data laws clearer and more conducive to the safe development of new technologies.

h. Establishment of a Data Preservation Process that can allow access to information as part of investigations into a child's death where needed.

7. From the evidence gathered and in line with analytical guidelines, we shortlisted down to a set of four options. The three options alongside the status-quo/do nothing option all seek to harness the power of data for economic growth, support a modern digital government, and improve people's lives. The range of options includes continuing with the current data protection regime, making minor changes to address some market failures, or implementing more substantial reforms to modernise and digitalise government services. The current framework has limitations that restrict the potential benefits of data use. The minor changes aim to resolve specific issues with a generally positive reception from stakeholders, while the more moderate reforms seek to address a broader range of challenges, incorporating key recommendations from recent policy discussions.

Findings

8. We estimate the total net present value of the preferred package of reforms to be between £3.2 billion and £18.8 billion over 10 years in 2024 prices.

Table 1: Estimated NPV of preferred option

Estimate	Net Benefit (Present Value (PV)) (£million)
Low	3,170.0
High	20,138.3
Best estimate	10,603.9

9. Some of the measures assessed are enabling only and given the uncertainty over the contents of the secondary legislation, will be assessed more fully at that stage (scenario 2 in the RPC's primary legislation guidance). The impacts of these secondary measures are either indirect or unquantifiable at this stage. Usually where this is the case, an impact assessment would present two EANDCBs. However, in this case they are the same and therefore the EANDCB figures presented here cover the set of policies as a whole.

10. The Data (Use and Access) Act is classified as a quantifying regulatory provision. Many of the reforms included in the Act are pro-competition in nature. However, there are some proposals that do not qualify under these exemptions including the DHSC and Digital Identity measures. A breakdown of the competitive nature of the Act can be found later in the Impact Assessment.

11. We have ensured our analysis is robust and proportionate. We have quantified costs and benefits of the Data (Use and Access) Act where possible, and otherwise provided qualitative analysis. Any evidence gaps will feature in our monitoring and evaluation plan.

12. A breakdown of the NPV of the costs and benefits we have monetised can be found in the table below.

Table 2: Estimated Net Present Value (NPV) of preferred option over 10 years in 2024 prices (£million)

Net

Estimates	Low	High	Medium
Total NPV	3,170.0	20,138.3	10,603.9

Costs

Estimates	Low	High	Medium
Total transitional	765.1	2,501.0	1,363.3
Average annual	53.9	108.0	76.3
Total cost	1,207.8	3,267.4	1,958.5

Benefits

Estimates	Low	High	Medium
Total transitional	0.0	0.0	0.0
Average annual	795.8	2,973.0.8	1732.3
Total cost	6,437.4	21,346.1	12562.4

13. Where evidence is currently unavailable or where reforms will be followed up with secondary legislation impact assessments, we have provided detailed non-monetised qualitative analysis of the expected direct and indirect costs and benefits. These include a deep dive into the impacts on consumer trust and privacy as well as public sector and law enforcement use of data.

Impact on Trade

14. It is recognised that there will be some implications on trade as a result of the policy reforms as part of the act. The below provides a summary of the impacts on trade for the measures in the Act and further details can be found in the respective impact assessments.

15. Increasing market competition can lead to higher efficiency both domestically and boosted competitiveness internationally. By furthering the UK's leading approach towards data portability with initiatives such as Smart Data, we can expect to see further opportunity to extend the UK's tech leadership, and by providing an opportunity for international firms to

expand into the UK, attracting further foreign direct investment while increasing competition for domestic firms with knock-on benefits for customers.

16. Implementation of digital verification schemes is expected to bring beneficial impacts to international trade through reducing friction by facilitating remote ID verification checks, which is very commonly required whilst trading internationally, and helping to streamline business processes. The legal framework will also support the Government's wider work internationally to enable identity verification across borders to be secure and trusted.

17. Cross-border data transfers are a key facilitator of international trade, particularly for digitised services. Transfers underpin business transactions and financial flows. They also help streamline supply chain management and allow business to scale and trade globally.[1] We have conducted analysis that looks at the potential of the proposed data reforms to enable more trade between countries. The analysis however includes analytical caveats which mean that the results should be treated as merely indicative of the range and scale, rather than a granular and detailed account of the impacts. For this reason, we have decided to report these results separately to the total NPV of the package of reforms.

18. Moving to a system which allows personal data to be transferred more pragmatically via data adequacy regulations and alternative transfer mechanisms (ATMs) is expected to lower transaction costs and increase cross-border data flows. Using a business-level approach that assesses the direct cost of using standard contractual clauses (SCCs) we estimate the trade that is currently suppressed, due to this cost acting as a non-tariff barrier between UK businesses and the Rest of the World. This benefit is estimated to have an annual benefit of between £51m and £100m.

19. EU Adequacy decisions are adopted through a unilateral, EU process managed by the European Commission. EU Adequacy decisions do not require an 'adequate' country to have the same rules, and the Government's position is that the proposals within the Act are aligned with the EU's criteria to allow the UK to preserve its adequacy status allowing the free flow of personal data from Europe to the UK.

20. It is recognised that data transfers are integral for EU and UK organisations and if an EU Adequacy decision was not available, EU businesses would have to implement and comply with alternative transfer mechanisms to transfer personal data to the UK. Therefore, we have estimated the economic impact that UK businesses would face if Adequacy with the EU was to be discontinued or suspended as a result of this Act. We have updated our modelling assumptions and estimations of any changes to this agreement. As a result, we estimate the impact of Adequacy with the EU being lost on top of these measures to be between £190 and £460 [OBJ]million in one-off SCC costs and an annual cost of between £210 million and £420 million in lost export revenue when taking a micro approach to modelling. The analysis does not attempt to assign probabilities but simply estimates the impact in the event of loss of EU Adequacy. The trade impacts are the direct reduction in UK-EU trade and the impact may be larger when accounting for interactions with onward supply chains with trade with third countries. As there is uncertainty in both the likelihood and timing of any decision, the impact is not included in the net present value or other measures in the summary of the IA. The impacts

[1] International data transfers: building trust, delivering growth and firing up innovation, DSIT, 2021

have been uprated and discounted as if the decision was made presently, a conservative assumption. The impacts are presented for the purposes of transparency.

21. We do not anticipate there being any direct implications for trade. NUAR will primarily change the costs for domestic activities. However, as the reforms will directly benefit owners of underground assets through reduced utility strikes, back office efficiencies and enabling better data sharing, it could over time make the utility and telecoms sector in the UK a more attractive place for inward investment, compared to other economies which have not yet taken action to improve data sharing in this manner. This could include the attractiveness of investing in new developments or major projects given the data contained and made available in NUAR will help reduce risk of project overruns and delays. As these benefits are speculative at this stage, they have not been quantified.

Summary of costs and benefits

Benefits

Benefits	Monetised/ non-monetised	Direct/ Indirect
Compliance cost savings	Monetised	Direct
Reform of the ICO	Monetised	Direct
Productivity benefits	Monetised	Indirect
Creation of innovative and secure Smart Data Schemes (DBT)	Non-Monetised	Indirect
Increased Interoperability and Trust of Digital Identity Systems	Monetised for four example use cases	Indirect
Increased Interoperability and Trust of Digital Identity Systems	OBJ	Indirect
Privacy, trust and individual data rights	Non-Monetised	Indirect
Delivery of better public services	Non-Monetised	Indirect
Improved Customer Outcomes	Non-Monetised	Indirect
Improved Interoperability across Health and Social Care Systems	Non-Monetised	Indirect
Improved Interoperability across Health and Social Care Systems	Non-Monetised	Direct
Improved Interoperability across Health and Social Care Systems	Monetised	Indirect
Improved Interoperability across Health and Social Care Systems	Monetised	Direct
Enhance the work of the UK intelligence services and Law Enforcement Agencies (HO)	Monetised	Direct
Enhance the work of the UK intelligence services and Law Enforcement Agencies (HO)	Non-Monetised	Direct
Enhance the work of the UK intelligence services and Law Enforcement Agencies (HO)	Non-Monetised	Indirect
Operationalise the National Underground Asset register	Monetised	Direct
Operationalise the National Underground Asset register	Monetised	Indirect
Operationalise the National Underground Asset register	Non-Monetised	Indirect
Facilitate Researchers' Access to Online Safety Data	Non-Monetised	Indirect
Direct marketing	Monetised	Direct
Direct marketing	Non-Monetised	Direct
Strengthen the Criminal Law	Non-Monetised	Direct
Producing reports and an IA on AI Copyright	Non-monetised	Indirect

Costs

Costs	Monetised/ non-monetised	Direct/ Indirect
Familiarisation costs	Monetised	Direct
Reform of the ICO	Monetised	Direct
Enhance the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO)	Monetised but not included in calcs	Direct
Enhance the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO)	Monetised	Indirect
Enhance the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO)	Non-monetised	Direct
Creation of innovative and secure Smart Data Schemes (DBT)	Non-Monetised	Indirect
Increased Interoperability and Trust of Digital Identity Systems	Monetised for four example use cases	Indirect
Increased Interoperability and Trust of Digital Identity Systems	Non-Monetised	
Delivery of better public services	Non-Monetised	Indirect
Improved Interoperability across Health and Social Care Systems	Non-Monetised	Indirect
Improved Interoperability across Health and Social Care Systems	Monetised	Direct
Operationalise the National Underground Asset Register	Monetised	Direct
Operationalise the National Underground Asset Register	Monetised	Indirect
Operationalise the National Underground Asset Register	Non-Monetised	Indirect
Facilitate Researchers' Access to Online Safety Data	Non-Monetised	Direct
Increased flows throughout the Criminal Justice System	Monetised	Direct
Producing reports and an IA on AI Copyright	Non-monetised	Direct

Wider impacts

Wider impacts	Monetised/ non-monetised	Direct/ Indirect
Impact on Competition	Non-Monetised	Indirect
Impact on Equalities	Non-Monetised	Indirect
Impact on Individuals	Non-Monetised	Indirect
Environmental Impacts	Non-Monetised	Indirect
National Security Impacts	Non-Monetised	Indirect

Differential impact by sector and organisation size

22. Our modelling confirms that benefits and costs from these reforms will not fall equally across the economy and society. A breakdown of how the NUAR[2], Smart Data[3], Digital Identity[4] and

[2] DSIT: NUAR Impact Assessment, 2024
[3] DBT: Regulatory Powers for Smart Data Impact Assessment, 2024
[4] DSIT: Digital Identities De Minimis Assessment, 2024

Interoperability of Health Care Systems[5] measures are expected to impact different sectors and organisation sizes can be found in their respective impact assessments.

23. Small and Micro Firms (SMFs) are included in the legislation for mandatory participation in **Smart Data** schemes to ensure the schemes' effectiveness across various sectors. Exempting SMFs could undermine the objectives of future schemes, such as providing comprehensive consumer information, as seen in the example of fuel pricing. However, the legislation requires consideration of the potential impact on SMFs, with options to mitigate disproportionate risks, such as third-party data collection or fee adjustments. The specific participation requirements and thresholds will be determined during the secondary legislation stage, with smaller businesses expected to participate voluntarily if benefits outweigh costs.

24. We expect the data protection reforms to have asymmetric distributional impacts on different organisations/ sectors as a result of differing levels and types of data use[6], while in the case of several non-data protection measures, other differences including for example, firms in some sectors are more likely to have processes and privacy frameworks in place already than others.

25. Where we have been able to provide monetised estimates, the analysis is detailed and robust however some assumptions have had to have been made in areas where evidence is lacking. We have therefore ensured that we have carried out sufficient sensitivity analysis and testing to make sure that we accounted for these potential risks.

26. Given the estimated scale and scope of the project we intend to complete a Post Implementation Review (PIR),[7] within 5 years of implementation. This will provide us with the opportunity to review whether the Act has met the intended objectives highlighted in this impact assessment. In order to be able to successfully measure these impacts we will also ensure that we invest in the monitoring of all key statistics that have fed into this IA with focus on the evidence gaps we have identified.

[5] DHSC: Open Data Architecture Information Standards Impact Assessment, 2024
[6] Different sectors use data differently, e.g. in 2024, the sector most likely to say they share personal data with other organisations was Finance and Insurance (41%). DSIT: UK Business Data Survey (2024)
[7] Producing post-implementation reviews: principles of best practice, BEIS (2021)

Problem under consideration and the issue being addressed

27. The current UK General Data Protection Regulation (UK GDPR) provides an important regulatory framework for access, use and re-use of personal data that protects the rights of individuals. It also provides rules that facilitate data sharing in ways that are accountable, lawful, fair and secure. The government is committed to maintaining high standards of data protection so that people have confidence in the use of their personal data.

28. Smart Data could address various market issues, but current incentives and powers are inadequate to implement it effectively. The UK GDPR provides data portability rights but lacks the robust standards and secure sharing needed for Smart Data. Low consumer engagement across markets leads to problems like the 'loyalty penalty', low switching rates, poor satisfaction, and subscription traps, especially for vulnerable consumers. Trust in using personal data is also low, and some consumers use insecure methods like 'screen scraping', which poses risks. Restricted data access is increasingly seen as a barrier to market entry, making intervention necessary to address these challenges.

29. Identity proofing methods that rely on physical documents are costly, inefficient, and prone to fraud. Digital identities could improve and streamline this process, but the current system is inadequate. There is a gap in communication between digital identity providers and users, with a lack of standards for interoperability and insufficient trust. In the 2019 Call for Evidence, respondents highlighted the need for government intervention to establish these standards, create mechanisms for organisations to demonstrate compliance, and enable verification against government-held data.

30. Data access and availability can also support industry in other ways. Over 4 million kilometres of underground energy, water, and telecoms infrastructure suffer around 60,000 accidental strikes each year, costing industry and government £2.4 billion annually (2021 prices). Current legislation requires asset owners to share data with excavators but doesn’t specify how, leading to inefficiencies. With over 700 asset owners, this results in repeated requests and inconsistent data formats. Government intervention is needed to reform legislation and establish a sustainable data sharing service that ensures secure, efficient access to underground asset data while managing commercial interests and legal liabilities.

31. In the health sector, despite 2012 legislation for data standards, adoption is low (around 42%) and not keeping up with necessary changes. Health and social care providers struggle to access or share care information in real-time. The Health and Care Act 2022 made compliance with information standards mandatory for providers, aiming to improve interoperability. However, current powers don't compel IT suppliers to adopt these standards. This act seeks to address this by requiring IT suppliers in England's health and care system to meet specified information standards. Helping the adoption of digital identities, enabling economic gains in the digital economy while protecting against harms and enhancing privacy.

32. While the Online Safety Act 2023 (OSA) will improve the availability of data for researchers through transparency reporting in particular, in the absence of this legislation there are no provisions to provide researchers with direct access to data. This data could significantly enhance research that benefits society, such as improving public understanding of online safety

and reducing online harm in the UK. However, since platforms are not currently required to share this data, there is a clear need for government intervention to address this issue and ensure that data protection laws facilitate access to valuable information for scientific research.

33. Some businesses also view data as a liability, particularly where personal data is concerned, and take steps to curtail access and usage, implying a level of strategic over-compliance arising from uncertainty. This may come at significant opportunity cost. For example, 92% of UK businesses do not transfer data internationally, of which 10% of businesses give concerns around legal risks and uncertainty as a reason.[8] Alongside this, fewer than 10% of UK businesses use customer relationship management software to collect, store, and share customer information within their businesses,[9] meaning that most businesses do not have an easy way of using data to gain customer insights.

34. From an international perspective, "uncertainty regarding legal privacy regimes" was listed across 19 OECD countries as a main barrier to transborder data flows, followed by "Incompatibility of legal regimes" by 16 countries[10] and the overall estimated compliance cost to UK businesses of using transfer mechanisms inherited from the EU for rest of world personal data transfers is estimated at about £360m annually.[11]

35. The OECD[12] highlights that achieving the benefits available from data use requires employing data-governance frameworks that incorporate whole-of-government approaches and are coherent across areas, sectors and ideally countries. Work by Frontier Economics which was published in March 2021[13] identified a number of interrelated barriers to greater use and sharing of data in the economy, including a lack of knowledge (about potential uses of, and benefits from, data), high perceived risks (regulatory, commercial reputational), high upfront costs and misaligned incentives.

36. UK businesses identify many benefits of the UK GDPR[14] and the Data Protection Act 2018 (DPA 2018) for example in 2021, of the businesses that were shown to collect digitised personal data, 58% agreed that the introduction of the GDPR had led to increased awareness of data protection at a senior level.[15] However, the current regime can also be complex to interpret and apply, especially for small and medium businesses.[16] The 2024 UK Business Data Survey found that smaller businesses were less likely than large businesses to have someone whose role includes leading on data protection, and were less likely to say they find the regulatory guidance published by the ICO clear and easy to understand[17]. Such complexity is understood to be a barrier to compliance and lead to uncertainty, and potential over- or under-compliance (through strategy or error).[18] There is also evidence that the current regime may

[8] UK Business Data Survey (2024)
[9] ONS (2018) E-commerce and ICT activity Statistical bulletins, Table 25; this is even lower for micro-sized firms.
[10] OECD: Digital Economy Outlook 2020, fig 6.4
[11] Published DSIT estimate, from RoW Adequacy Umbrella IA.
[12] Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies, OECD (2019)
[13] Increasing access to data held across the economy , Frontier Economics, 2021
[14] Until the end of 2020 the EU GDPR applied in the UK. Since then, the applicable legislation in the UK has been the UK GDPR. For simplicity we typically refer to the UK GDPR throughout, but where evidence relates to the earlier GDPR we refer to this as the GDPR.
[15] UK Business Data Survey (2021)
[16] The European Commission's (2020) evaluation of the GDPR identified challenges for organisations, in particular SMEs.
17 UK Business Data Survey (2024)
[18] Christensen et al.(2013) The Impact of the Data Protection Regulation in the E.U. To note, this is a forecast of the proposed GDPR rather than an ex-post impact evaluation.

reduce firm-level innovation, business creation and employment,[19] decrease investment in emerging technology firms,[20] and negatively impact data-driven industries.

37. Regulation 22 of the PEC Regulations prohibits the transmission, by means of electronic mail, of unsolicited communications to individual subscribers. Currently regulation 22 of the PEC Regulations provides for one exception. It allows anyone (companies, charities, or other organisations) to send electronic marketing communications to an individual (recipient) without their explicit consent, if their contact details were collected during the sale of a product or service, or negotiations of a sale. The direct marketing materials benefiting from this exception may only concern similar products and services and the individual recipient must be offered a simple means of opting out of receiving marketing communications, both at the time the contact details are collected and in all subsequent communication sent. Both safeguards are aimed at limiting an individual's exposure to spam and nuisance communications. This exception is commonly known as the 'soft opt-in'.

38. This measure creates an exception from the prohibition for direct marketing carried out by a charity for charitable purposes. The current exception does not enable charities to send direct marketing messages to individuals in order to fundraise or promote campaigns, which is a core activity for some charities in helping them to deliver their charitable purpose(s). The government engaged with stakeholders, listening to the concerns raised by the sector over the difficulties it has experienced through covid and cost of living situation and has taken steps to support charities resilience.

39. There has been a significant rise in the ease in the accessibility of technology used to create purported intimate images ("intimate deepfakes"), and in their prevalence online without the consent of the person depicted. A purported intimate image could include a photo or video (or any hyper-realistic image) of someone engaged in sexual acts, or where the most intimate parts of the body are exposed or covered with underwear, or where the person is using the toilet, as defined in section 66D (5) to 66D (9) in the Sexual Offences Act 2003.

    a. Under section 66B of the Sexual Offences Act 2003, the law already captures situations where intimate images including deepfakes are shared without consent or reasonable belief in consent. Likewise, the criminal law already covers the creation of intimate images of children as this it already captures the making of indecent images. This includes making deepfake images of children (i.e. those under the age of 18) in section 1 of the Protection of Children Act, 1978.

    b. However, there is currently no criminal offence banning the creating or requesting of intimate image deepfakes of an adult without consent or reasonable belief in consent. This behaviour can cause harm to the individuals depicted and forms part of a wider harmful and misogynistic behaviour.

    c. The Government committed in its manifesto to banning sexually explicit deepfakes. The measure assessed in this IA will fulfil that commitment by introducing the new offences of

[19] Christensen et al.(2013) The Impact of the Data Protection Regulation in the E.U.
[20] Jia et al. (2018) found that GDPR negatively affected venture capital investment in digital technology firms.

creating or requesting the creation of a purported intimate image of an adult without consent or reasonable belief in consent.

40. Producing reports on the use of copyright works in the development of AI systems, and an impact assessment on the policy options considered in the AI and copyright consultation, will help inform policy decisions on AI and copyright.

Rationale for intervention

41. The complexity of the current regulatory regime means that firms and consumers are not able to take full advantage of the benefits that are available to them through effective use of data and data sharing. There are six market failures across different sectors of the economy that have been identified as a result of the complexity of the UK's current data regime.

    a. **Externalities** occur when the production or consumption of a good incurs costs or benefits on a third-party outside of the transaction. A data externality is an effect that arises from the disclosure of personal data.[21] In the data market, a negative externality occurs when the disclosure of personal data by some consumers leads to an excessive privacy loss for other consumers. The use of the disclosed personal data by businesses or organisations for activities such as targeted advertising, leads to a loss of privacy for those who consider the data to be private information. A positive externality can occur when data collected by one party is freely accessed by others and this generates positive external benefits for re-users.[22]

    b. **Public goods**, where the delivery and efficiency of public services is inefficient as a result of limited data sharing. The complexity of the regulation delays the sharing of data between public services. Also, public sector services lack the necessary framework to use data efficiently and this leads to public goods being under-utilised. The government can create open access data to provide the right framework to help improve the utilisation of public goods. [23]

    c. **Information asymmetry** refers to when one party in a transaction has more information than the other. In the data market, businesses such as online platforms that provide search engines or targeted advertising, have better and more information on the services markets they cover compared to the users of the platforms. The consumers are unaware of whether the platforms use the information to maximise social welfare via increased efficiency or to maximise their own profits.

    d. **Imperfect information**, where UK businesses have incomplete information regarding the regulations around data sharing and therefore choose not to share data to minimise risk. A further example is when consumers are unaware of how much personal data businesses collect and how businesses process personal data. Also includes areas where better sharing of data enables efficiencies.

    e. **Market power** refers to when the power is concentrated into too few businesses or organisations. In data markets that lack competition the complexity of the regulation deters new entrants and limits firms with relatively less power from achieving the additional benefits of effective data use. Firms with market dominance can expand into complementary data markets, at a relatively low marginal cost rather than share data with complementary firms, this may deter new entrants into complementary markets.

    f. **Network failure** refers to when a good or service whose value increases as the number of users increases fails to raise its value due to a lack of users. The data network effect is

[21] The Economics of Privacy: A Primer Especially for Policymakers, Bank of Japan, 2021
[22] Business-to-Business data sharing: An Economic and Legal Analysis, JRC Digital Economy Working Paper, 2020
[23] "Creating and governing social value from data" - Diane Coyle and Stephanie Diepeveen, 2021

when a product's value grows as a result of more usage via the accretion of data.[24] In terms of data network failure, the complexity of the regulations has resulted in insufficient cooperation between UK businesses to combine datasets through data sharing and benefit from economies of scope.

42. The table below highlights the specific market failures that are present in certain parts of the UK's data processes, policies and current protection regime.

Table 3: Summary of the market failures in data markets

[24] https://www.nfx.com/post/truth-about-data-network-effects

Market	Externalities	Public goods	Information asymmetry	Imperfect information	Market power	Network Failure
Smart Data[25]			✓	✓	✓	✓
Digital Identity Schemes[26]			✓	✓		
The National Underground Asset Register (NUAR)[27]	✓	✓		✓		
Using data to improve public services (including DHSC CDDO and HO initiatives)	✓	✓		✓	✓	
Data use for science and research (including AI)	✓	✓		✓		
Online Safety: Researcher Access to Data[28]	✓		✓			
Processing/ Re-use of data			✓	✓		
Privacy and Electronic communications	✓					
Data subject rights			✓	✓		
International data transfers	✓			✓		
The Information Commissioner's Office (ICO)			✓			
Smart meter data (DESNZ)		✓				
Direct marketing	✓	✓				
Copyright works and artificial intelligence systems			✓			

43. The market currently fails at different levels of the data value chain. The table above explores where the market failures exist.

44. Government intervention in the form of new legislation or changes to existing legislation will help overcome these market failures. Reform options have been designed specifically to

[25] More information on the rationale for intervention in the Smart Data market can be found in the Smart Data final Impact Assessment 2024 - DBT
[26] More information on the rationale for intervention in the Digital Identity market can be found in the Digital Identity De Minimis Assessment - DSIT, 2024
[27] More information on the NUAR measures can be found in the NUAR final Impact Assessment 2024
[28] DSIT: Researchers' Access to Data Impact Assessment, 2024

remedy market failure in specific industries and sectors as well as UK data policy more generally. These areas have been set out in the King's Speech[29]

a. **Smart Data initiatives**, there is a failure of existing regulation to enable easy and secure data mobility. Many markets currently face low levels of consumer engagement. Consumers are unable to navigate these markets easily resulting in negative outcomes such as the 'loyalty penalty', low switching rates, poor satisfaction. These negative outcomes are further exacerbated for vulnerable consumers who may have further inabilities to access and engage. Alongside low consumer engagement is a lack of trust and empowerment to utilise their own data in markets, increasing their cost of informed decision making. While already sharing data, some customers are currently using less secure methods, such as 'screen scraping', which can lead to direct harm if this data is mishandled. Evidence also shows that in digital markets there is increasing concern that access to data is a significant barrier to entry. Intervention is therefore necessary to help address the issues arising in these markets and to alleviate wider market failures. The Smart Data amendments in the House of Commons were intended to ensure that Smart Data schemes function optimally, and to ensure the Part 1 regulation-making powers are as clear as possible. This will further assist in addressing the market failures mentioned above. The section 11 amendments specifically allow for regulations to provide for a greater range of Smart Data scheme models regarding fee charging. This means Smart Data schemes can be designed with a fee structure that is tailored to the needs of the markets corresponding to each sector. More detail can be found on Smart Data rationales in the Smart Data Impact Assessment.[30]

b. An emergent marketplace in **Digital Identities** already exists, with more and more businesses and citizens preferring to verify information about themselves without needing paper documents. However, current identity proofing methods can be expensive, inefficient, and vulnerable to fraud. Digital identities can strengthen and simplify the process, however, the current landscape lacks standards which will enable interoperability and does not yet command trust. In the 2019 Digital Identity Call for Evidence,[31] respondents noted that the market required the government to step in and set these standards, create mechanisms to allow organisations to prove they follow them, and to enable checks against government-held data. More information on this market failure can be found in the Digital identity and attributes De Minimis Assessment.[32]

c. Currently, there are over 4 million kilometres of underground energy, water, and telecoms pipes and cables, suffering approximately 60,000 accidental strikes each year, costing the industry and government £2.4 Billion annually (2021 prices). Establishing a new sustainable data-sharing service, **National Underground Asset Register** (NUAR), is necessary to provide secure and efficient access to underground asset data, balance commercial interests, and manage legal liabilities. Existing laws require asset owners to share data on these assets with excavators but do not specify the method of sharing. As a result, 700+ asset owners have to respond to numerous requests, and excavators must contact multiple owners, receiving data in varying formats and timelines. Government intervention through legislative reform is essential to standardize data sharing, thereby resolving these issues.

[29] The King's Speech 2024, GOV.uk, 2024
[30] Smart Data Impact Assessment, DBT (2024)
[31] Digital Identity: Call for Evidence Response, DSIT, 2020
[32] Digital identity and attributes De Minimis Assessment, DSIT, 2024

d. In the **health care sector**, the fragmented IT vendor market for health and social care has resulted in suboptimal levels of interoperability, hindering the efficient exchange of information across systems. This lack of interoperability creates significant challenges for healthcare providers and patients, and the market has failed to address these issues on its own. Government intervention is necessary to set standards, promote competition, and ensure consistent and secure data sharing. By doing so, the government can overcome key market failures, such as economic externalities, coordination failures, and imperfect competition, to improve patient outcomes, reduce costs, and support innovation in healthcare technology.

e. The provision for registering births, still births and deaths is contained in the **Births and Deaths Registration Act 1953 (BDRA) and the Registration of Births and Deaths Regulations 1987**. In 2009 the registration online system (RON) was introduced allowing registrars to register births and deaths electronically. Even though all birth and death information are held electronically, registrars are still required to also hold a record of the events in paper registers. Removing the requirement for paper registers, requires a change of legislation. This would introduce efficiencies and result in savings to public expenditure as well as the support of government digital initiatives. Allowing the RON system to be the only birth and death register removes duplication and simplifies the process. It also introduces savings for the Home Office by removing the cost of providing registers, associated resources, postage costs and loose leaf, watermarked, registration paper. Moving away from paper registers will also reduce the risk of criminals gaining access to blank stock to create false identities.

f. The direct marketing measure backs the third sector in reaching out to more potential donors, potentially helping them boost their finances, which in turn could have valuable societal benefits. It will enable charities to engage with supporters in order to fundraise and promote campaigns.

g. In the case of purported intimate images, the rationale for intervention relates to equity, ensuring that the criminal law adequately provides justice to victims, and reducing their distress and invasions of privacy.

h. There is currently information asymmetry in the data licensing market as owners of copyright works have difficulty monitoring how their data is used in AI training. One of the **AI and copyright** issues that will be explored in the reports is the disclosure of information by developers of AI systems about their use of copyright works to develop AI systems, and how they access copyright works for that purpose (for example, by means of web crawlers).

Table 4: How the legislation would overcome each market failure

Market Failure	Policy Intervention
Externalities	Implement legislation that makes it easier for personal data to be used in science and research while also providing consumers with the optimum level of privacy protection.
Public Goods	Implement legislation that makes it easier for personal data to be exchanged between public sector bodies. Introduce frameworks that encourage data use in the public sector.

Information Asymmetry	Simplify the legislation regarding data exchange and data use. Provide clarification of the rules around using personal data to benefit businesses and their consumers.
Imperfect Information	Simplify the legislation regarding data exchange and data use. Provide clarification of the rules around using personal data to benefit businesses and their consumers.
Market Power	Implement legislation that encourages competition through increased data sharing and reduces the compliance requirements.
Network Failure	Implement legislation that encourages cooperation and increased data sharing.

45. The issues with the current data regime that have been outlined above require a range of reforms to be corrected. The introduction of new guidance would not solve the complexity issue of the current regime because the scale of change needed is too large to be covered by guidance. It would be inefficient to solely produce guidance in an attempt to simplify the current regime. For example, even if existing legislative mechanisms were used to oblige health and adult social care providers to purchase information technology products and services with appropriate technical features, this would be insufficient to bring the wholesale change to the IT supplier market that is needed, particularly in the timeframe required to push forward the digitisation in health and social care.

46. The full scope of the issues could also not be addressed by relying solely on changes to the Information Commissioner's Office, as many of the market failures need legislative change for them to be corrected. As a result of this, we explored policy options targeted at specific sectors and market failures to overcome these issues.

    a. The UK has three data protection regimes. Most personal data are governed by the UK General Data Protection Regulation (UK GDPR) and its accompanying provisions in Part 2 DPA 2018. Law enforcement processing has its own bespoke regime (Part 3 DPA 2018) which reflects the operational nature of the processing carried out by Law Enforcement Agencies (LEAs). The third regime governs processing of personal data by the UK's Intelligence Services (Part 4 DPA 2018) and reflects the national security sensitivities as well as the other forms of oversight outside data protection governing the intelligence services.

    b. The Home Office has responsibility for law-enforcement and intelligence services data processing. The Act will update the Data Protection Act 2018 (DPA 2018). It will contribute to reducing the risk from terrorism to the UK and UK interest overseas[33] and will restore confidence in the criminal justice system[34] (CJS) when it comes to data protection.

    c. As the DPA 2018 is recent and largely works well, the reforms will provide updates to the existing legislation rather than fully re-writing it. This will prevent undue burden on users/businesses and maintain international confidence in our data protection standards. Most of the changes aim to simplify/clarify the existing law, which in turn will provide users with the confidence needed to encourage data exchange effectively (both domestically and

[33] Home Office Outcome Delivery Plan: 2021 to 2022 - GOV.UK (www.gov.uk)
[34] People's priorities | Horizon

internationally). Effective data exchange is important for economic and law enforcement relationships.

d. The Home Office has two overarching aims:

   i. Firstly, to empower the police to use new technologies, like biometrics, within a strict legal framework which maintains public trust.

   ii. Secondly, to facilitate the effective flow and use of personal data for law enforcement and national security purposes to enhance the work of the UK Intelligence Services and Law Enforcement Agencies (LEAs) in the interest of public security.

e. Intervention is necessary as improving UK data laws will continue to deliver effective data exchange, which is good for business and public security. The measures being introduced will drive efficiencies and encourage better data cooperation. The amendments prevent undue burden on users and businesses and reduce the potential impact on the Adequacy decisions. The amendments will simplify and clarify the existing law, which in turn will provide users with the confidence needed to encourage data exchange effectively (both domestically and internationally). Effective data exchange is important for economic and law enforcement relationships.

f. In developing these proposals, the Home Office have engaged extensively with operational partners, taking as the starting point changes that support improved operational outcomes whilst maintaining public confidence and simplifying existing law (for example, using consistent language) where appropriate.

g. The UK is ranked second in the world for **science and research**[35], and made up 13.4% of highly cited research publications worldwide in 2020[36]. Data is key to a wide range of research activities across many sectors, and this is reflected in the UK GDPR. The existing legislation provides specific allowances in relation to processing for research purposes, however, the laws around personal data use for "research purposes" are complex and the current regulatory landscape has proven difficult for scientists to navigate, making it harder to establish legal certainty for vital and innovative research. This highlights how the market fails because scientists have incomplete information about personal data use and how the data value chain suffers a market failure at the collection stage. Furthermore, through the consultation process we identified that some aspects of the existing framework can place unnecessary barriers to researchers, slowing down or even stopping their progress. The barriers researchers face restricts the realisation of societal benefits from effective data use. This shows how the data value chain suffers a market failure at the impact stage.

h. When used responsibly, data-driven **artificial intelligence (AI) systems** have the potential to bring substantial benefits to the lives of consumers and businesses. The development of AI and machine learning applications is contingent on data, and places specific demands on its collection, curation and use. The market failures discussed all have an effect on the current development of AI. Consumers may not be aware of their rights when subjected to

[35] The AD Scientific Index, 2024
[36] International Comparison of UK Research Base (BEIS, 2022)

automated decision making reflecting the information gaps. Uncertainty regarding these data requirements could raise barriers to realising these benefits.

i. The **Online Safety researchers' access to data** provision will improve understanding of online safety issues and position the UK as a leader in research and innovation. While the Online Safety Act 2023 (OSA) will improve the availability of data for researchers through transparency reporting in particular, in the absence of this legislation there are no provisions to provide researchers with direct access to data. Ofcom will be able to require the largest providers to publish a broad range of information through transparency reports, but Ofcom is unlikely to require companies to publish the kind of user data required to conduct online safety research. The online safety impact of these proposed interventions could be broad. Eligible independent researchers will be able to carry out research into online safety issues that may include illegal activity, harmful content, damaging behaviours, and issues relating to free speech. This additional research is likely to help to address the limited information currently prevailing in this area and contribute to the evidence base for future online safety interventions.

j. The **re-use of personal data** can provide economic and societal benefits through facilitating innovation. The market currently fails as a result of the information gaps around the re-use of personal data at several levels of the data value chain. Clarity on when personal data can lawfully be reused is important at multiple levels of the data value chain: data subjects benefit from transparency at the collection stage, data controllers benefit from certainty during the publication stage, and society benefits from unlocking the opportunities of re-use at the impact stage of the data value chain. The UK GDPR sets out rules for when further processing of personal data is considered compatible with the purpose for which it was collected, in recognition of the value of re-use of data in certain circumstances and where safeguards are in place. In the consultation, the government identified areas of uncertainty and therefore is able to set out proposals to improve clarity in the legislation and as a result facilitate innovative re-use of data.

k. The **Privacy and Electronic Communications Regulations 2003** (PEC Regulations) is complementary to the UK GDPR and the DPA. PEC Regulations prohibits an organisation from storing or gaining access to information that is held in the equipment of an individual (such as computers and mobile phones), unless one of three exceptions apply (such as the user's consent). From consultation we know that organisations have found that the ability to collect data in order to improve services/ websites is difficult to obtain when relying on consent, and individuals find the number of consent request pop-ups a source of annoyance and routinely accept the terms without reading them.

l. The government has highlighted its ambition for the UK to harness the power of data for economic growth and the importance of the data economy to boosting trade[37]. Currently a number of barriers to **international data transfers** exist, including a lack of alignment in legal frameworks, transfer tools and data adequacy regulations. The complexity of the regulations has contributed to information gaps for data controllers which have restricted the international transfers of data. This market failure has an impact at all levels of the data value chain. The government needs to intervene to achieve its ambition of helping domestic businesses to connect more easily with foreign markets, while attracting

[37] King's Speech 2024: background briefing notes, (HMG, 2024)

investment from abroad by businesses that rightly have confidence in the responsible use of data within the UK.

m. There are many opportunities to build on the lessons learned from COVID-19 pandemic in relation to the power of using personal data responsibly **in the public interest**, and the benefits of collaboration between the public and private sectors. There are currently some challenges to do this effectively, including: data infrastructure that is not interoperable; legal and cultural barriers to data sharing; inconsistent data capability in the workforce; and financial disincentives that discourage investment. Government intervention is needed to create a joined-up and interoperable data ecosystem for the public sector that will address the limitations outlined above, whilst ensuring high levels of public trust.

n. **In order for the ICO to perform its function as an agile and forward-looking regulator** a clear mandate for a risk-based and proactive approach to its regulatory activities in line with best practice of other regulators is needed. A new legislative framework will allow for a clearer strategic vision for the regulator and the reduction of barriers to data flows.

o. The Government is committed to maintaining a secure national communications network for smart metering in Great Britain. The body responsible for establishing and operating this does so under the Smart Meter Communication Licence ('the DCC Licence'). The Licence is currently held by Smart DCC Ltd. It was awarded by the government in 2013 for an initial period of 12 years and is due to expire in September 2025. The process for Ofgem to identify a successor licensee is set out in primary legislation and further in regulations. This should lead to the successful selection of a provider, though it does not guarantee it. To mitigate the risk of a successor licensee not being selected, our proposed intervention provides Ofgem with greater flexibility in their process for choosing the next licensee. We do not expect any direct impacts from this measure.

p. The criminal law should adequately protect the public by capturing people who commit harmful acts so that they can be brought to justice.

Rationale and evidence to justify the level of analysis used in the IA (proportionality approach)

47. Indicative analysis of those measures in the Data (Use and Access) Act that formed part of the previous DPDI Bill was previously undertaken at the pre-consultation stage. Since then, the analysis was updated to reflect consultation responses, discussions with cross-government experts and external consultants, assessment of the latest literature, and reflections on the RPC's comments on the methodology. The Data (Use and Access) Act also includes new measures not in the previous DPDI Bill or makes substantial changes to previous measures. This Impact Assessment reflects these changes and additional amendments added during the Bill's passage since its introduction in October. A full list of the amendments highlighted in Table 8 and are listed in full Annex 7.

48. Where evidence is available, we are able to analyse some policies at an individual level, although there are still uncertainties and evidence gaps. We know that some reforms share similar channels of impact and implication, so we have continued to analyse policies within

groups that are consistent with the expected impacts. This ensures that the analysis remains novel, proportionate and robust.

49. In order to explore some of the uncertainties surrounding the data, greater use of sensitivity analysis has been employed across impacts to consider variability in data and assumptions.

50. DSIT has also worked alongside analysts from across Government to establish the rationale, options, costs and benefits, and finer detail of the impact of reforms where analysis has been led by their respective organisations and where relevant tailored towards a specific sector. These organisations are the Department for Business and Trade,[38] the Home Office, Central Digital and Data Office (CDDO), DHSC, DESNZ and the Information Commissioner's Office (ICO).

51. Where evidence exists that has allowed us to attempt to quantify impacts, this has come from a variety of sources referenced throughout. DSIT's UK Business Data Survey continues to be instrumental in this analysis, providing us with an overview of UK businesses' use of data and interaction with data protection. The Annual Survey of International Trade in Services is also used extensively in our trade and data adequacy modelling. Furthermore, we continue to use the European Commission's and Ministry of Justice's 2012 impact assessments (IAs) of the then proposed European data protection regulation and where possible, have integrated these with more recent evidence.

52. Where quantitative evidence is not available, qualitative analysis of impacts has been undertaken and expanded upon since consultation and introduction, including further literature reviews and case studies. On particularly uncertain impacts, such as trade and data adequacy, complementary approaches have been used to provide more evidence of the potential scale of impacts.

53. As part of ongoing monitoring and evaluation, the framework of impacts explored will continue to be refined. Monitoring and evaluation will be important in assessing whether and how the newly proposed reforms will indeed succeed in improving on the deficiencies of previous regulation and what lessons can be learned for any future revisions.

Description of options considered

Background

54. This section discusses the approach taken to identify the various policy options to ensure that this Act of reforms delivers the government's ambition to harness the power of data for economic growth, to support a modern digital government, and improve people's lives. Identifying the correct and most effective set of reforms to achieve this is the key driver behind the decision-making process and this economic analysis.

55. These ambitions have a strong economic rationale and the opportunity for the UK economy is substantial, given its superior starting position in comparison to many of its peers. Data driven companies generated an estimated £343 Billion in annual turnover (6% of total UK turnover) in

[38] Smart Data Impact Assessment, DBT (2024)

2023. While contributing an estimated £84.9 billion (3.8%) in GVA to the UK economy and employing 1.5 million people (5% of total UK employees) in all types of roles in 2023[39].

56. The UK data regime is already among the most comprehensive and open worldwide,[40] which is linked to its superior data governance. The UK needs to ensure that further reforms tackle key issues and introduce net positive impacts on the economy and society. This framework underpins the reforms considered and the process through which these were agreed upon.

Process of shortlisting options

57. This section details the approach of shortlisting the initial reforms included in the Data (Use and Access) Act.

58. Reform measures including Smart Data, Digital identity, NUAR, Online harms and policies from OGDs went through separate options framework detailed in their own impact assessments (IA) or De minimis assessment (DMA). These were assessed independently and the preferred option for those IA/DMAs are the ones in the preferred option here.

59. Reform options were designed to achieve the government's objectives of harnessing the power of data for economic growth, supporting a modern digital government, and improving people's lives. The options continue to underpin a high level of protection for people's personal data and control for individuals over how their personal data is used. The Government also continues to recognise that organisations have and are continuing to invest in understanding, complying and implementing the current regime.

60. A long list of potential reform options was generated in each area, with each option designed to tackle an identified issue. These were then assessed for their likely impact, benefits and costs on stakeholders (the public, organisations in the public and private sector and the wider data economy), and associated risks. The viability of each reform option was then assessed as part of continued engagement internal and external stakeholders, further policy research and analysis looking at their legal, practical feasibility, and effectiveness in delivering the intended policy outcome. Each reform was also re-considered in the context of the wider package of potential reforms in order to assess its fit and interdependencies with other potential measures.

61. The three options alongside the status -quo/do nothing option all fall on the liberalisation side of the data - openness scale when compared to the current regime. Our second option is to make minor changes to the current regime. The intermediate option which looks to combine a suite of data reform policies together which all aim to innovative the ways in which the UK uses data. And the do max option which is the data reform options with additional data protection policies.

List of options initially considered

Table 5: Outline of policy options

Option	Description
0. Do nothing/status quo	No policy change

[39] The UK Data Driven Market (DSIT, 2024)
[40] As confirmed among multiple studies such as the Global Open Data Index from the Open Knowledge Foundation, and the data governance study from Washington University

1. Do minimum	Minor policy changes to the status quo and current data regime
2. Intermediate option	Considerable policy changes to the status quo and current data regime
3. Do maximum	Even bigger policy changes to the status quo, and a complete overhaul of existing legislation, repealing and replacing the existing data regime inc. significant changes to data protection legislation

62. Throughout the development of the Data (Use and Access) Act changes were proposed reflecting stakeholder feedback and ongoing policy development. These developments led to a better understanding of implicit costs and policy risks not previous considered which led to the data protection and ultimately Do maximum option not being suitable for implementation. A list of the reforms within the Do maximum options can be found in the annex.

63. There are reform measures inc. Smart Data, Digital identity, NUAR, Online harms and policies from OGDs went through their own options framework which are in within their own impact assessments (IA) or De minimis assessment (DMA). These were assessed independently and the preferred option for those IA/DMAs are the ones in the preferred option here.

Do nothing option

64. This option is the benchmark counterfactual and describes a scenario in which the current regime is continued without change. This is equivalent to retaining the current framework for data related public service provision. As highlighted in section one, although the current regime is effective in allowing data use and data transfers, and is relatively liberal in comparison with other jurisdictions, there are certain limitations that mean the benefits from this are limited and firms are not maximising their potential gain from data use.

Do minimum option

65. The do minimum option, encapsulates minor policy changes to the current regime in an attempt to resolve aspects of the market failures. This includes key reforms that aim to resolve some of the issues identified as part of the policy process. The majority of reforms have been fairly well received by stakeholders and substantial evidence exists suggesting that they would have a beneficial impact on the economy, LEAs, UK Intelligence Services, and society as a whole.

Table 6: List of all policies in 'do minimum' category[41]

Reform measure	Reform Summary
Research Purposes	● Consolidating research provisions into a single chapter
Research Purposes	● Creating a statutory definition of scientific research
Research Purposes	● Incorporating broad consent for scientific research into legislation
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● National security exemption (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Data subjects' rights to information: legal professional privilege exemption (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Consent to law enforcement processing (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Law enforcement processing and codes of conduct (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Logging of law enforcement processing (DPA 2018 part 3) Automated decision making (DPA 2018 part 3)
Digital Identity	● Enable checks against government-held data but do not create a statutory governance framework (option 3 in Digital Identity DMA)
Digital Identity	● Create a statutory governance framework to oversee the trust framework (Option 2 in Digital Identity DMA)
Smart Data (DBT)	● Pursue non-legislative alternatives (Option 1 in Smart Data IA)
Smart Data (DBT)	● Support sector regulators to independently pursue legislative alternatives (option 2 in Smart Data IA)
Data Architecture (DHSC)	● Enabling legislation to prepare, publish and mandate standards that apply to the products and services provided by IT suppliers
Strategy, Objectives and Duties	● ICO's Objectives and Duties
Strategy, Objectives and Duties	● Statement of Strategic Priorities
Governance Model and Leadership	● Remove the Information Commissioner corporate sole structure. Introduce a Board structure with Chair/CEO.
Governance Model and Leadership	● Remove the requirement for Parliament to agree to a change to the IC salary.

Do intermediate option

66. The intermediate option encapsulates moderate policy changes to the current regime aiming to resolve most aspects of the market failures. This involves modernising and digitalising government services provision. It also incorporates key reforms which aim to address those set out in the King's Speech (see paragraph 6).

Table 7: List of all polices in 'do intermediate' category

Reform measure	Reform Summary
Research Purposes	● Consolidating research provisions into a single chapter
Research Purposes	● Creating a statutory definition of scientific research
Research Purposes	● Incorporating broad consent for scientific research into legislation
Research Purposes	● Extending the "disproportionate effort" exemption on information provision requirements for further processing for research purposes of personal data collected directly from the data subject
Research Purposes	● Extending the exemptions from the regime when conducting scientific research to include when that research is carried out in a commercial setting.
Further Processing	● Clarifying how personal data can be further processed for research purposes
Further Processing	● Clarifying that further processing for an incompatible purpose may be lawful when based on a law that safeguards an important public interest or when the data subject has re-consented
Further Processing	● Exempt archives from further processing rules where personal data was originally obtained in reliance on consent.
Legitimate interests	● Recognised Legitimate Interests. The act will introduce a new lawful ground for non-public bodies when processing personal data for "recognised legitimate interests". This is limited to a small number of public interest objectives, such as the prevention of crime, safeguarding vulnerable individuals and responding to emergencies. Under the current law, data controllers have to do a detailed assessment of whether their interests are outweighed by the rights of data subjects when processing personal data for such purposes
AI and Machine Learning	● Future proofing Article 22
AI and Machine Learning	● Enhancing the approach to explainability and accountability for fair processing in the context of AI
AI and Machine Learning	● Clarifying the circumstances in which safeguards apply to significant decisions that are taken about individuals on the basis of profiling.
Data Adequacy	● Underpinning the UK's future approach to data adequacy regulations with principles of risk-assessment and proportionality
Data Adequacy	● Relaxing the requirement to review data adequacy regulations every 4 years
Alternative Transfer Mechanisms	● Power for SoS to formally recognise new ATMs
Alternative Transfer Mechanisms	● Changes to the standard approach to alternative transfer mechanisms. (Art 46)
Alternative Transfer Mechanisms	● Ensuring businesses are able to continue to use their pre-bill existing transfer mechanisms without a requirement for further checks and avoiding additional costs.
Alternative Transfer Mechanisms	● Clarifying that transfers of personal data under the UK-US Data Access Agreement can be made under the 'public interest tasks' lawful ground

Reform measure	Reform Summary
Public Interest	● Clarifying that private organisations & individuals asked to carry out an activity on behalf of a public body may rely on that body's lawful ground for processing the personal data under Art 6(1)(e)
Digital Economy Act 2017 (CDDO)	● To extend powers under section 35 of the Digital Economy Act 2017 aimed at improving public service delivery to business undertakings, beyond the current scope of solely individuals and households
Public Safety and National Security (Home Office): Subject Access Requests	● Time limits for responding to requests by data subjects (SAR) (DPA 2018 part 3/4)
Public Safety and National Security (Home Office): Part 4	● Amendments to Part 4 of the DPA 2018 - Joint processing by intelligence services and competent authorities
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● National security exemption (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Data subjects' rights to information: legal professional privilege exemption (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Consent to law enforcement processing (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Law enforcement processing and codes of conduct (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Logging of law enforcement processing (DPA 2018 part 3) Automated decision making (DPA 2018 part 3)
Public Safety and National Security (Home Office):	● Transfers based on special circumstances (Schedule 6 DPA, Section 76)Subsequent transfer's (Section 78 DPA)

Reform measure	Reform Summary
International Transfers	
Public Safety and National Security (Home Office): International Transfers	● Clarify conditions on the use of international processors by UK competent authorities (Part 3 DPA)
Public Safety and National Security (Home Office): Biometrics	● Retention of biometric data and recordable offences
Public Safety and National Security (Home Office): Biometrics	● Retention of biometric data from INTERPOL
Public Safety and National Security (Home Office): Biometrics	● Retention of biometric data from other international partners
The National Underground Asset Register	● National Underground Asset Register Legislation to underpin a national register of underground assets (cables etc.)
The National Underground Asset Register	● Create powers to ensure the full participation by all owners of underground assets in NUAR and enable a sustainable charging regime.
Data Preservation Notices	● Establishing a data preservation process which will require OFCOM, following instruction by a coroner, to issue data preservation notices to online service companies to ensure they retain data that may later be requested by a coroner when carrying out an inquest into a child's death.
Smart Meter Data (DESNZ)	● Create new power to give Ofgem more flexibility in the process it needs to follow to identify the successor holder of the Smart Meter Communication Licence.
Smart Meter Data (DESNZ)	● Enable Ofgem to modify conditions of existing licences and industry codes if it considers that it is necessary or expedient to do for the purpose of granting a Smart Meter Communication Licence.
Online safety researchers access to data	● Create powers for the Secretary of State (SoS) to place a duty on platforms to comply with any regulations later passed by SoS allowing researchers access to certain data held by platforms.
Electoral Purposes	● Amend Schedule 1 of the Data Protection Act 2018 so that the 4 day threshold in which outgoing elected representatives have to process special category data on behalf of their constituents without explicit consent, is changed to 30 days, to overcome these operational barriers.
Electoral Purposes	● Amending exemptions in Sch 1 DPA 2018 (special category data) to permit elected representatives to process political opinions data.
Subject Access Requests	● Clarifying that controllers are not required to make disproportionate searches in response to subject access requests - necessary as a result of the loss of the EU principle of proportionality under the REUL Act. (Home Office measure)
Privacy and electronic communications	● To add three low privacy risk exceptions to the prohibition on storing information, or accessing information stored, on a user's connected device. For example, collecting statistical information to improve the service/website requested by the user.
Privacy and electronic communications	● Empowering ICO to take action against organisations for the number of unsolicited direct marketing calls 'sent' as well as calls 'received' and connected.

Reform measure	Reform Summary
Privacy and electronic communications	● Amending the regulations' powers of enforcement so that they are aligned with the enforcement regime under the Data Protection Act 2018, including fine levels, whilst keeping bespoke tools such as third-party information notices.
Privacy and electronic communications	● Extending approved code of conduct provisions under Article 40 UK GDPR to the PEC Regulation
Privacy and electronic communications	● Extending the reporting period for breaches under reg 5A PEC Regulation from 24 to 72 hours
Updating Special Category Data	● Create a new power for the Secretary of State to add new types of data to the list of special categories of data that get extra protection. This will provide the flexibility to add new types in the future including in response to new technological developments, to ensure heightened protections for citizens.
Digital Identity	● eIDAS/trust services
Digital Identity	● Data checking gateway
Digital Identity	● Trust framework accreditation and certification
Digital Identity	● Trust framework governance
Digital Identity	● Validity of digital identity
Digital Identity	● Mutual recognition of digital identities
Digital Identity	● Mutual recognition of trust services
Digital Identity	● Welsh and Scottish safeguards for Digital Verification Services
Digital Identity	● Include a power for DSIT SoS to approve additional rules for particular sectors or use cases which build on the rules in the UK digital identity and attributes trust framework; to make provision for organisations to be certified against those additional rules; and to make provision for the DVS Register to note which sets of additional rules (if any) an organisation has been certified against in addition to the trust framework. In policy terms, we refer to a set of additional rules as a 'scheme', and we expect the equivalent term in the Act to be 'supplementary code'.
Digital Identity	● To amend the Immigration Act 2014 and the Immigration Asylum and Nationality Act 2006 to permit regulations to specify that, where digital checks are undertaken, these are undertaken by a DVS provider on the DVS register.
Smart Data (DBT)	● Smart Data: Introduction of primary legislation, creating new "regulation-making" powers to enable Smart Data schemes to be introduced in any given sector. [1]
Smart Data (DBT)	● Expanding the definition of ''customer data'' to include transactions between the customer and third parties, and clarify the scope of action initiation, or 'write access' services
Smart Data (DBT)	● Provisions to clarify the powers of enforcers to investigate and monitor compliance, and the process for setting fines, penalties and fees and to allow existing data sharing requirements in other legislation to be incorporated into Smart Data regulations.
Smart Data (DBT)	● Clarification of the power to make provision in connection with business data – to expressly facilitate a Smart Data delivery model where data holders provide business data to a specified third party, who then provides (or publishes) the business data to other third parties
Data Architecture (DHSC)	● Enabling legislation to prepare, publish and mandate standards that apply to the products and services provided by IT suppliers
Data Architecture (DHSC)	● Enabling legislation to prepare, publish and mandate standards that apply to the products and services provided by IT suppliers, to ensure that those products and services enable and support data to be accessed, interrogated and processed in real time by anyone with the basis to appropriately access that data, irrespective of the system used by the health or social care provider who collated, produced or otherwise processed that data.

Reform measure	Reform Summary
Home Office: Public Interest	● Processing in reliance on relevant international law (Joint DSIT/HO measure)
Home Office: Sensitive Processing	● Power to add categories of sensitive processing (Mirroring provision from UKGDPR to Part 3 and 4 DPA)
Public Safety and National Security (Home Office): Birth and Deaths	● Remove the requirement for paper birth and death registers moving to an electronic register
Strategy, Objectives and Duties	● ICO's Objectives and Duties
Strategy, Objectives and Duties	● Statement of Strategic Priorities
Governance Model and Leadership	● Remove the Information Commissioner corporate sole structure. Introduce a Board structure with Chair/CEO.
Governance Model and Leadership	● Remove the requirement for Parliament to agree to a change to the IC salary.
Accountability and Transparency	● Accountability and Transparency - require publication of key documents
Accountability and Transparency	● Statutory codes of practice - ICO required to undertake and publish an impact assessment and consult with a panel of experts when developing or updating statutory codes of practice, unless exempt
Complaints	● Complaints - organisations required to have a complaint handling process
Enforcement Powers	● Enforcement - power to commission technical reports
Enforcement Powers	● Enforcement - power to compel witnesses to attend interview
Enforcement Powers	● Enforcement - notice of intent extension
Enforcement Powers	● Enforcement - without attending premises clarification

Do Maximum option

67. Reforms in the “Do maximum” option were deemed to not currently meet the bar set in terms of available evidence or feasibility to progress at this stage. Amassing the evidence and balancing priorities would introduce delays and the Government is prioritising making progress quickly on the issue of data policy.

68. The preferred option was the intermediate package of reforms, outlined above. This set of options were expected to meet objectives of the government has prioritised harnessing the power of data for economic growth, supporting a modern digital government, and improving people’s lives. Changes were later made to consider policy risks and implicit costs. Going forward in this impact assessment we assess the costs and benefits of the preferred option only compared to the baseline ‘do nothing’ scenario.

Policy objective

69. The proposed set of reforms that form part of the preferred package are designed to benefit the UK as a whole. These include policies targeted at resolving market failures for both the private and public sector as well as creating a framework for effective oversight of the UK's data protection regime. These sets of reforms largely reflect and align with the priorities set out in the Kings Speech: harnessing the power of data for growth, improving people's lives, and a modern digital government.

70. The objective of Smart Data legislation is to enable new, and accelerate existing, Smart Data schemes, and create a common framework for consistent regulations. This is intended to improve poor consumer and business outcomes, increase competition, create greater opportunities for innovation, produce time saving for users, reduce costs, increase the quality of services, improve the security of data sharing and increase the trust in data sharing mechanisms.[42]

71. Reforms to enable people to use swift and secure identification to prove things about themselves aim to unlock economic gains associated with a functioning digital identity system, enabling the full realisation of the digital economy. Having a system which is more secure can support protection against fraud for businesses and people and enhance privacy. There is also an aim to promote inclusive solutions and remove barriers to inclusion. More information on how the proposed policy will overcome market failures in the digital identity market can be found in the Digital identity and attributes - De Minimis Assessment.[43]

72. The National Underground Asset Register will provide secure access to privately and publicly owned location data from 700+ organisations about the pipes and cables beneath our feet. The digital map gives planners and excavators standardised access to the data they need, when they need it, to carry out their work effectively and safely. It also includes features to keep data secure and improve its quality over time. The policy objectives include increased efficiency of data sharing; reduced asset strikes; reduced disruptions for citizens and businesses; and expedited delivery of projects like new roads, new houses and broadband roll-out.

73. The objective of removing the requirement for paper birth and death registers moving to an electronic register is to introduce a change to the legislation which will remove the requirement for paper registers to be held in 175 Local Authorities. Local Authorities within England relate to county, district or parish councils, London borough councils, the Common Council of the City of London and the Council of the Isles of Scilly. In Wales, Local Authorities relate to any county, county borough or community council in Wales. This removes the requirement for records of births, still-births and deaths to be held in two mediums (paper and online). There will be no requirement for registrars to store paper registers in the future reducing the risk of loss or theft of those registers for those seeking to commit identity fraud, therefore resulting in public protection and counter fraud benefits. The move to an electronic register will provide savings to central and local governments and remove the duplication of processes.

[42] Smart Data Impact Assessment 2024 - DBT
[43] Digital identity and attributes - De Minimis Assessment, 2024 DSIT

74. The objective for changing data use in the health and social care sector, across providers of care and IT systems, is using information standards to ensure systems are fully interoperable, so data can flow through the system in a usable and standardised form. The measures provided in the DUA act are intended to enable this vision to be delivered further, faster – by extending the scope of information standards to apply to IT suppliers of products and services used in the health and care system. Further, there is value to patients from improved patient safety. In addition, improved standardisation of information will facilitate research and promote innovation, further supporting improved patient outcomes, as well as improved decision-making enabled by access to accurate and complete information and supporting a more dynamic and responsive health and care IT market.

75. The proposed reforms aim to update UK data processing laws, including those related to law enforcement and national security, to maintain high data protection standards and bolster public confidence in how the public sector uses data. The Home Office seeks to simplify legislation, reduce administrative burdens, and ensure consistency across data processing regimes, such as aligning the definition of consent in law enforcement with UK GDPR. The reforms will also support Law Enforcement Agencies in making better use of Automated Decision Making (ADM), and improve international data flows

76. There has been growing global support for legislation providing independent **researchers access to online safety related data** to conduct associated research. This issue was raised during the passage of the OSA. Good quality research will help identify unknown or emerging risks and will provide evidence on the impact of providers' activities, enabling protective actions from Ofcom, government, providers, and civil society. The European Union's Digital Services Act mandates access to data for researchers. This provision aims to provide SoS with the ability to create regulations on researchers' access to data. Should SoS decide to regulate, the regulations will provide a legal basis for researchers to request or access online safety related information to conduct research. The evidence base for the decision to introduce a framework, as well as what any future framework will look like, will be developed by Ofcom's report into the matter and a government consultation.

77. Reforms also seek to ensure your data is well protected. We are modernising and strengthening the ICO. It will be transformed into a more modern regulatory structure, with a CEO, board and chair. And it will have new, stronger powers. This will be accompanied by targeted reforms to some data laws that will maintain high standards of protection but where there is currently a lack of clarity impeding the safe development and deployment of some new technologies.

78. A further reform objective is to establish a Data Preservation Process that coroners (and procurators fiscal in Scotland) can initiate when they decide it is necessary and appropriate to support their investigations into a child's death. This will help coroners get access to online information they need when investigating a child's death.

79. These policies are designed to **boost trade and remove barriers to international data flows.** Consumers and businesses collect, share and process personal data internationally in order to use or trade digital products and services. According to the World Trade Organisation, trade in data-enabled services grew from $1.0 trillion in 2005 to $3.9 trillion in

2022.[44] Data flows have a larger impact in raising world GDP than the trade in goods.[45] In 2024 the UK exported £330 billion in data enabled services (65% of total UK services exports) and imported £154 billion in data-enabled services (49% of total UK services imports).[46]

80. The objective of amending the Smart Meter Communication licensing procedure is to provide Ofgem with flexibility in the way in which it appoints the future licence holder. The process for Ofgem to identify a successor licensee is set out in primary legislation and further in regulations. Ofgem has recently consulted on the specific measure in this Act, proposing that changes to the legislative framework that specifies the process by which a new licensee is appointed, would be in the interests of consumers. This consultation engaged industry stakeholders, including the incumbent licence holder.

81. Separately, since 2021, in anticipation of the current DCC licence term coming to an end, Ofgem have been undertaking a review of the regulatory framework for it. They have consulted with industry at each stage of the development of that framework.[47] A September 2022 consultation set out the key principles that they were seeking to achieve, together with a series of proposed regulatory options, evaluated against those principles. That consultation culminated in a published document in August 2023 setting out Ofgem's decisions on the overarching regulatory framework. A wide variety of industry stakeholders, including the incumbent, were engaged in and responded to that consultation.

82. The proposed measure does not impact on the regulatory framework for the future licence which Ofgem will implement using its existing powers. Rather the measure aims to provide flexibility in how the process to appoint the licensee is carried out.

Amendments made to the preferred package of reforms (October 2024 – June 2025)

83. Since the Bill's introduction in October 2024, a number of amendments were proposed, reflecting stakeholder feedback and further policy development. These are set out in the amendment papers for the Bill. These amendments were made as the Bill progressed through the Lords and Commons. The impact analysis section has assessed these amendments where there are additional economic or wider impacts to UK businesses, the public sector or data subjects. For substantial technical and policy amendments, we have included an outline of their rationale for inclusion. These include the following:

Table 8: List of all amendments since the DUA Bill's introduction (October 2024)

Amendment	Rationale for inclusion
Lawfulness of Processing & Rights of Data Subjects: This amendment adds an express reference to children meriting specific protection with regard to their personal data when the SoS is considering whether to use regulations to add to	During Lords Committee stage, peers raised concerns about what they saw to be a lack of specific protections for children's personal data. They emphasised children's unique vulnerabilities and the need for stringent safeguards across educational, social media, and health platforms. A key issue was the omission of the opening part of Recital 38 of the UK GDPR, which states, 'Children merit specific protection with regard to their personal data,' from Clause

[46] DSIT Internal analysis estimating the UK's data enabled services trade using ONS experimental estimates for proportion of UK services trade delivered remotely.
[47] https://www.ofgem.gov.uk/decision/dcc-review-phase-1-decision

the list of ‘recognised legitimate interests’	91 of the Act, which provides the ICO with a duty to consider that children may be less aware of the risks of consequences of processing and their rights in relation to it in all its data protection activities where relevant. To address these concerns and ensure consistency in areas where similar language was used, the amendment adds the opening wording from recital 38 to the start of the existing duty in Clauses 70 (recognised legitimate interests) and 91 (the ICO’s duties). The amendment was designed to improve the clarity of an existing Act provision in Clauses 70 and 91.
Information Commissioner’s Office - Privacy by design: children’s higher protection matters	This amendment builds on existing duties under Article 25 of the UK GDPR to design their processing activities in a way that complies with the data protection principles. It requires Information Society Services that are likely to be accessed by children (and are already subject to the Age-Appropriate Design Code) to consider how best to protect and support children when designing their services; and to take account of the fact that children merit specific protection because they may be less aware of the risks of the processing, and may have different needs at different ages. During Lords stages of the Bill, peers raised concerns that the ICO duty alone would not sufficiently increase protections for children, unless data controllers were also under a clear legal obligation to consider children’s interest in the design of their processing activities.
Direct Marketing - Regulation 22 of the PEC Regulations prohibits the transmission, by means of electronic mail, of unsolicited communications to individual subscribers. This amendment creates an exception from the prohibition for direct marketing carried out by a charity for charitable purposes.	Regulation 22 of the PEC Regulations applies to the transmission of unsolicited communications by electronic mail to individual subscribers. Electronic mail covers, among others, communication by email or text messages. Under this regulation unsolicited communication by such means is in principle prohibited without the recipient’s consent, unless exceptions apply. Currently regulation 22 of the PEC Regulations provides for one exception. It allows anyone (companies, charities, or other organisations) to send electronic marketing communications to an individual (recipient) without their explicit consent, if their contact details were collected during the sale of a product or service, or negotiations of a sale. The direct marketing materials benefiting from this exception may only concern similar products and services and the individual recipient must be offered a simple means of opting out of receiving marketing communications, both at the time the contact details are collected and in all subsequent communication sent. Both safeguards are aimed at limiting an individual’s exposure to spam and nuisance communications. This exception is commonly known as the ‘soft opt-in'. The current exception does not enable charities to send direct marketing messages to individuals in order to fundraise or promote campaigns, which is a core activity for some charities in helping them to deliver their charitable purpose(s). The government engaged with stakeholders, listening to the concerns raised by the sector over the difficulties it has experienced through covid and cost of living situation and has taken steps to support charities resilience.

Smart Data	During the Act's passage through the House of Commons, the government introduced amendments to Part 1 which are summarised below under four groups. These amendments were accepted and now form part of the Act. **Group 1 –** These amendments expressly allow regulations to require business data to be provided to a third party appointed by a public authority and to require that third party to publish or disclose the business data. **Group 2 –** This group of amendments contains changes to fee charging under section 11. The amendments have the following aims: a. Allowing regulations to provide for charging of fees that exceed expenses where appropriate. Under the initial drafting, regulations could only enable persons listed in section 11(2) (including data holders, decision makers, interface bodies, enforcers and others) to charge fees to cover the costs of performing duties or exercising powers conferred by or under Part 1 regulations. The amendment ensures that Smart Data schemes can operate on a commercial basis if necessary. b. Enabling regulations to clarify whether or not powers to charge arising outside of regulations made under Part 1 can be used to charge fees in connection with performing duties or exercising powers conferred by or under those regulations. The amendment also provides that section 11 does not prevent or limit what third-party recipients can charge (with some exceptions). The policy intention has always been that the basis of charging arrangements between third party recipients and customers is a commercial matter for them to determine. c. The amendments to section 15, mirror the changes above, ensuring that the Treasury's power to confer rule-making powers on the FCA regarding fees is consistent with the general fee charging power under section 11. **Group 3:** This group contains amendments regarding The Treasury's power to confer rule making powers to the FCA. The amendments to section 14, allow the Treasury to delegate powers to the FCA to set rules around interface requirements for persons who are enabled by regulations to take action on behalf of a customer (sometimes referred to as action initiation). This amendment brought the drafting of the Act in line with the policy intention and will ensure that Open Banking-enabled payments continue to work effectively. **Group 4:** The government also introduced further amendments that are either clarifying amendments or have otherwise been assessed to have minimal impact.

New section 251ZC of the Health and Social Care Act 2012 (public censure of relevant IT providers) if that would contravene the data protection legislation.	Government minor and technical amendment – details are captured in the commons amendments[48]
NUAR - Devolved Government Consent	The NUAR measures legislate in a devolved area. Amendments tabled during Bill passage mean that the Secretary of State will be required to gain the consent of devolved governments before regulations can be made, where the regulations relate to apparatus in the street in Wales and Northern Ireland, or otherwise touch on devolved competencies.
NUAR - Requirement to produce guidance	This amendment requires The Secretary of State to produce guidance for persons gaining access to NUAR through regulations made under section 106C and article 45C informing them on how to protect information kept in, or obtained from, NUAR.
Adds references to investigating crime to existing references in the Data Protection Act 2018 to detecting or preventing crime.	Government minor and technical amendment
Copyright works and artificial intelligence systems	This clause commits the government to publishing a report and Impact Assessment within 9 months of Royal Assent: • The Impact Assessment will cover the options laid out in the consultation, as well as any alternative options that are under consideration. • The Report will cover the policy options from the consultation as well as any other options the Secretary of State considers appropriate following the consultation. The report must consider and make proposals with regard to; • Technical measures and standards that may be used to control use of works, or accessing works by webcrawlers • The effect of copyright on access to and use of data by AI developers, including SMEs • The disclosure of information by AI developers about their use of copyright works and how they have accessed them (transparency) • Licensing of copyright works for AI training • Potential approaches to models trained overseas Approaches to enforcement of rules relating to copyright, AI and web crawlers, including potential future regulatory options.

[48] Data (Use and Access) Bill [HL]

Summary of preferred option with description of implementation plan

84. This section and the rest of this Impact Assessment reflects the original preferred package of reforms combined with the changes made throughout the policy development of the DUA Bill. The table below provides a list and summary of all of these reforms.

Table 9: All policy reforms and measures included in the preferred package

Reform measure	Reform Summary
Original measures as introduced October 2024	
Research Purposes	● Consolidating research provisions into a single chapter
Research Purposes	● Creating a statutory definition of scientific research
Research Purposes	● Incorporating broad consent for scientific research into legislation
Research Purposes	● Extending the “disproportionate effort” exemption on information provision requirements for further processing for research purposes of personal data collected directly from the data subject
Research Purposes	● Extending the exemptions from the regime when conducting scientific research to include when that research is carried out in a commercial setting.
Further Processing	● Clarifying how personal data can be further processed for research purposes
Further Processing	● Clarifying that further processing for an incompatible purpose may be lawful when based on a law that safeguards an important public interest or when the data subject has re-consented
Further Processing	● Exempt archives from further processing rules where personal data was originally obtained in reliance on consent.
Legitimate interests	● Recognised Legitimate Interests. The Act will introduce a new lawful ground for non-public bodies when processing personal data for “recognised legitimate interests”. This is limited to a small number of public interest objectives, such as the prevention of crime, safeguarding vulnerable individuals and responding to emergencies. Under the current law, data controllers have to do a detailed assessment of whether their interests are outweighed by the rights of data subjects when processing personal data for such purposes
AI and Machine Learning	● Future proofing Article 22
AI and Machine Learning	● Enhancing the approach to explainability and accountability for fair processing in the context of AI
AI and Machine Learning	● Clarifying the circumstances in which safeguards apply to significant decisions that are taken about individuals on the basis of profiling.
Data Adequacy	● Underpinning the UK’s future approach to data adequacy regulations with principles of risk-assessment and proportionality
Data Adequacy	● Relaxing the requirement to review data adequacy regulations every 4 years
Alternative Transfer Mechanisms	● Power for SoS to formally recognise new ATMs
Alternative Transfer Mechanisms	● Changes to the standard approach to alternative transfer mechanisms. (Art 46)

Alternative Transfer Mechanisms	● Ensuring businesses are able to continue to use their pre-bill existing transfer mechanisms without a requirement for further checks and avoiding additional costs.
Public Interest	● Lawful ground for transferring personal data under the UK-US Data Access Agreement ● Clarifying that private organisations & individuals asked to carry out an activity on behalf of a public body may rely on that body's lawful ground for processing the personal data under Art 6(1)(e)
Digital Economy Act 2017 (CDDO)	● To extend powers under section 35 of the Digital Economy Act 2017 aimed at improving public service delivery to business undertakings, beyond the current scope of solely individuals and households
Public Safety and National Security (Home Office): Part 4	● Amendments to Part 4 of the DPA 2018 - Joint processing by intelligence services and competent authorities
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● National security exemption (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Data subjects' rights to information: legal professional privilege exemption (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Consent to law enforcement processing (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Law enforcement processing and codes of conduct (DPA 2018 part 3)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Logging of law enforcement processing (DPA 2018 part 3) Automated decision making (DPA 2018 part 3)
Public Safety and National Security (Home Office): International Transfers	● Transfers based on special circumstances (Schedule 6 DPA, Section 76) Subsequent transfer's (Section 78 DPA)
Public Safety and National	● Clarify conditions on the use of international processors by UK competent authorities (Part 3 DPA)

Security (Home Office): International Transfers	
Public Safety and National Security (Home Office): Biometrics	● Retention of biometric data and recordable offences
Public Safety and National Security (Home Office): Biometrics	● Retention of biometric data from INTERPOL
Public Safety and National Security (Home Office): Biometrics	● Retention of biometric data from other international partners
The National Underground Asset Register	● National Underground Asset Register Legislation to underpin a national register of underground assets (cables etc.)
The National Underground Asset Register	● Create powers to ensure the full participation by all owners of underground assets in NUAR and enable a sustainable charging regime.
Data Preservation Notices	● Establishing a data preservation process which will require OFCOM, following instruction by a coroner, to issue data preservation notices to online service companies to ensure they retain data that may later be requested by a coroner when carrying out an inquest into a child's death.
Smart Meter Data (DESNZ)	● Create new power to give Ofgem more flexibility in the process it needs to follow to identify the successor holder of the Smart Meter Communication Licence.
	● Enable Ofgem to modify conditions of existing licences and industry codes if it considers that it is necessary or expedient to do for the purpose of granting a Smart Meter Communication Licence.
Online safety researchers access to data	● Create powers for the Secretary of State (SoS) to place a duty on platforms to comply with any regulations later passed by SoS allowing researchers access to certain data held by platforms.
Electoral Purposes	● Amend Schedule 1 of the Data Protection Act 2018 so that the 4-day threshold in which outgoing elected representatives have to process special category data on behalf of their constituents without explicit consent, is changed to 30 days, to overcome these operational barriers.
Electoral Purposes	● Amending exemptions in Sch 1 DPA 2018 (special category data) to permit elected representatives to process political opinions data.
Subject Access Requests (Joint DSIT/HO)	● Clarifying that controllers are not required to make disproportionate searches in response to subject access requests - necessary as a result of the loss of the EU principle of proportionality under the REUL Act
Subject Access Requests (Joint DSIT/HO)	● Time limits for responding to requests by data subjects (SAR) (DPA 2018 Part 3/4)
Privacy and electronic communications	● To add three low privacy risk exceptions to the prohibition on storing information, or accessing information stored, on a user's connected device. For example, collecting statistical information to improve the service/website requested by the user
Privacy and electronic communications	● Empowering ICO to take action against organisations for the number of unsolicited direct marketing calls 'sent' as well as calls 'received' and connected.

Privacy and electronic communications	● Amending the regulations' enforcement tools and sanctions so that they are aligned with the regime under the Data Protection Act 2018, including fine levels, whilst keeping bespoke tools such as third-party information notices.
Privacy and electronic communications	● Extending approved code of conduct provisions under Article 40 UK GDPR to the PEC Regulation
Privacy and electronic communications	● Extending the reporting period for breaches under reg 5A PEC Regulation from 24 to 72 hours
Updating Special Category Data	● Create a new power for the Secretary of State to add new types of data to the list of special categories of data that get extra protection. This will provide the flexibility to add new types in the future including in response to new technological developments, to ensure heightened protections for citizens.
Digital Identity	● eIDAS/trust services
Digital Identity	● Data checking gateway
Digital Identity	● Trust framework accreditation and certification
Digital Identity	● Trust framework governance
Digital Identity	● Validity of digital identity
Digital Identity	● Mutual recognition of digital identities
Digital Identity	● Mutual recognition of trust services
Digital Identity	● Welsh and Scottish safeguards for Digital Verification Services
Digital Identity	● Include a power for DSIT SoS to approve additional rules for particular sectors or use cases which build on the rules in the UK digital identity and attributes trust framework; to make provision for organisations to be certified against those additional rules; and to make provision for the DVS Register to note which sets of additional rules (if any) an organisation has been certified against in addition to the trust framework. In policy terms, we refer to a set of additional rules as a 'scheme', and we expect the equivalent term in the Act to be 'supplementary code'.
Digital Identity	● To amend the Immigration Act 2014 and the Immigration Asylum and Nationality Act 2006 to permit regulations to specify that, where digital checks are undertaken, these are undertaken by a DVS provider on the DVS register.
Smart Data (DBT)	● Smart Data: Introduction of primary legislation, creating new "regulation-making" powers to enable Smart Data schemes to be introduced in any given sector.[
Smart Data (DBT/HMT)	• That the Smart Data primary legislation includes the four groups of Smart Data amendments introduced throughout the Data (Use and Access) Act's passage through parliament, as set out in Table 8.
Data Architecture (DHSC)	● Enabling legislation to prepare, publish and mandate standards that apply to the products and services provided by IT suppliers
Data Architecture (DHSC)	● Enabling legislation to prepare, publish and mandate standards that apply to the products and services provided by IT suppliers, to ensure that those products and services enable and support data to be accessed, interrogated and processed in real time by anyone with the basis to appropriately access that data, irrespective of the system used by the health or social care provider who collated, produced or otherwise processed that data.
Public Safety and National Security (Home Office): Birth and Deaths	● Remove the requirement for paper birth and death registers moving to an electronic register
Strategy, Objectives and Duties	● ICO's Objectives and Duties
Strategy, Objectives and Duties	● Statement of Strategic Priorities

Governance Model and Leadership	● Remove the Information Commissioner corporate sole structure. Introduce a Board structure with Chair/CEO.
Governance Model and Leadership	● Remove the requirement for Parliament to agree to a change to the IC salary.
Accountability and Transparency	● Accountability and Transparency - require publication of key documents
Accountability and Transparency	● Statutory codes of practice - ICO required to undertake and publish an impact assessment and consult with a panel of experts when developing or updating statutory codes of practice, unless exempt
Complaints	● Complaints - organisations required to have a complaint handling process
Enforcement Powers	● Enforcement - power to commission technical reports
Enforcement Powers	● Enforcement - power to compel witnesses to attend interview
Enforcement Powers	● Enforcement - notice of intent extension
Enforcement Powers	● Enforcement - without attending premises clarification
Measures introduced via amendments	
National Underground Asset Register	• Guidance will be required to be provided to end users to about how to protect information kept in or obtained from NUAR
National Underground Asset Register	• Changes made to reflect agreement with devolved government establishing how the devolved governments will be engaged in the delivery of NUAR regulations.
Express reference to children meriting specific protection with regard to their personal data	• Provides ICO with a duty to consider that children may be less aware of the risks of consequences of processing and their rights in relation to it in all its data protection activities where relevant.
Data protection by design: children's higher protection matters	• Provides ICO with a duty to consider that children may be less aware of the risks of consequences of processing and their rights in relation to it in all its data protection activities where relevant.
Creating, or requesting the creation of, purported intimate image of an adult	• Criminalising the creation, or requesting the creation of, a purported intimate image (deepfake) of another person aged 18 or over without the adult's consent or reasonable belief in consent.
Copyright works and artificial intelligence systems	• The Act requires that a set of reports on the use of copyright works in the development of AI systems are published within 9 months, and that a statement of progress is provided within 6 months
Direct Marketing	• Allowing charities to send direct marketing for the purposes of furthering one or more of their charitable purposes.

85. A theory of change sets out how policies have direct and indirect effects that contribute to achieving final intended outcomes and objectives. We have developed a theory of change for our preferred package of policies using economic principles and evidence of the impact of comparable policies.

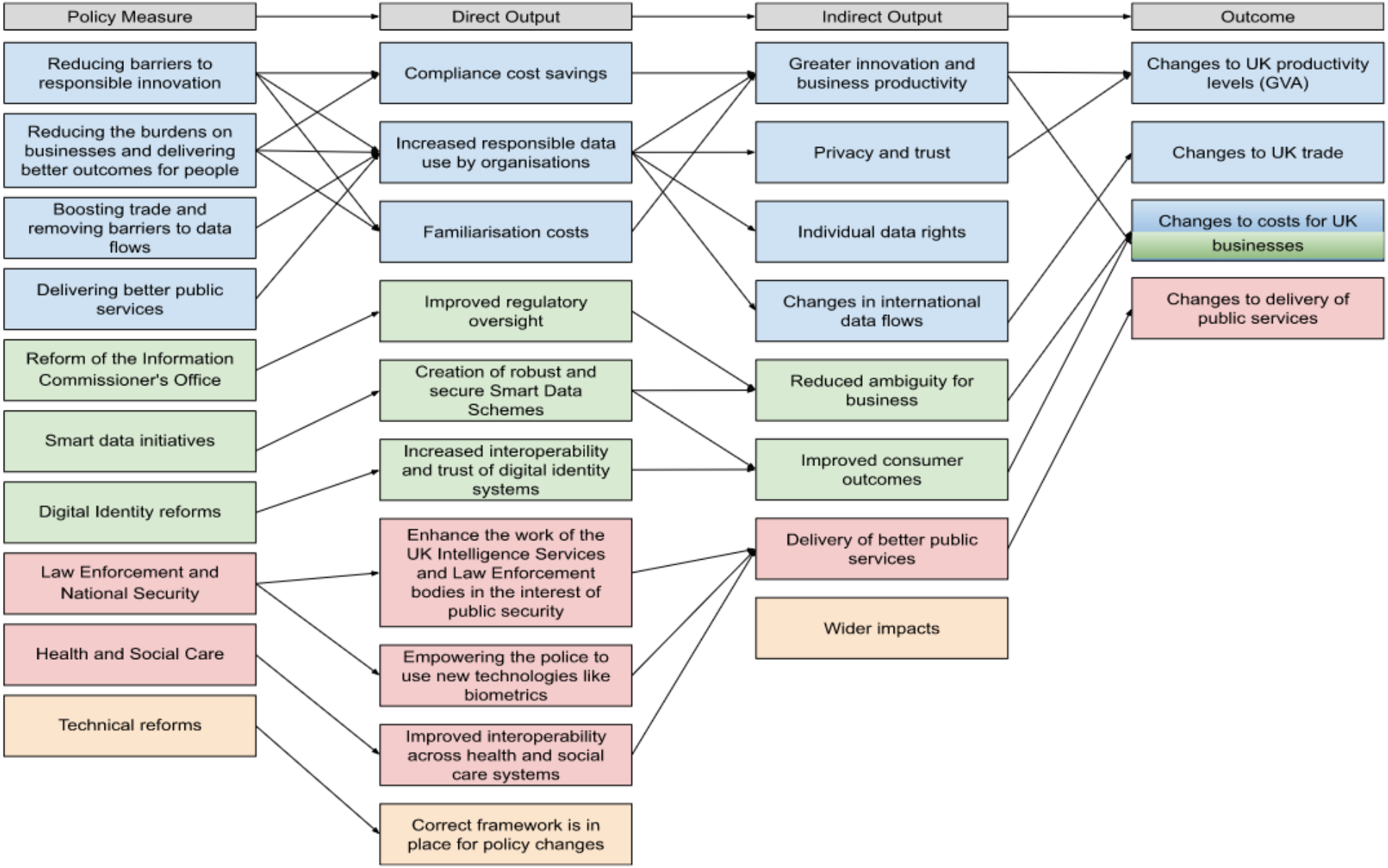
86. The figure below sets out the theory of change for the group of reforms. Where we have sufficient evidence and we have been able to make reasonable assumptions, we have quantified the net impact in terms of changes relative to the baseline. We assume the baseline is where the status quo remains in place with respect to the current data protection regime.

87. The preferred package of policy options is designed to correct for the current market failures by encouraging greater responsible data use, reducing costs for businesses and encouraging more effective use of personal data in public organisations. As a result of this we expect to see an increase in productivity across businesses in the UK and an increase in trade as international data transfers increase.

88. More detailed theory of change for the Smart Data initiatives[49], Digital Identity[50], National Underground Asset Register[51] and Interoperability of Health Care Systems[52] reforms can be found in their respective impact assessments. We have simplified these here to provide an overview of the impacts and outcomes.

[49] Smart Data Impact Assessment 2024 - DBT
[50] Digital identity and attributes - De Minimis Assessment, 2024 DSIT
[51] NUAR Impact Assessment, 2024 DSIT
[52] DHSC Open Data Architecture Information Standards Impact Assessment, 2024

Figure 1: Theory of change for preferred option



89. The policies included in this package will be primary legislation and some will be followed up by further secondary legislation. Analytical evidence for the reforms that are likely to be followed up by secondary legislation tends to be limited in these early stages, though we have included all that is available. More analytical detail will be provided in the secondary legislation Impact Assessments. The table below details the reforms in the Act that will likely be followed by secondary legislation and whether these are likely to include any direct costs or benefits to business – further details can be provided as policy develops.

Table 10: List of all reforms that are being followed up with secondary legislation

Reform Heading	Reform subheading	Will secondary legislation include direct costs and benefits to UK businesses?	Who will be responsible for the secondary legislation IAs?
AI and Machine Learning	Future proofing Article 22 Enhancing the approach to explainability and accountability for fair processing in the context of AI	Yes	DSIT
Delivering better public services	To extend powers under section 35 of the Digital Economy Act 2017 aimed at improving public service delivery to business undertakings, beyond the current scope of solely individuals and households (CDDO)	No	CDDO
Digital Identity	Digital Identity: Create a governance framework and enable checks against government-held data[53]	No	DSIT
Smart Data	Smart Data: Introduction of primary legislation, creating new regulation-making powers to enable Smart Data schemes to be introduced in any given sector[54]	Yes	This will be sector specific
Health and Social Care	Create primary legislation for a new power for the Secretary of State for Health and Social Care to direct suppliers to adopt an open data architecture approach[55]	Yes	DHSC
National Security and Law Enforcement	Joint processing by intelligence services and competent authorities	Yes	Home Office
NUAR	National Underground Asset Register Legislation to underpin a national register of underground assets (cables etc.). Only some of the NUAR policy is subject to secondary legislation.	Yes	DSIT

[53] This is the preferred option in the Digital identity and attributes - De Minimis Assessment 2024 published by DSIT
[54] This is the preferred option in the Smart Data initiatives Impact Assessment 2024 published by DBT
[55] An overview of how this policy will be implemented can be found in the DHSC Open Data Architecture Information Standards Impact Assessment, 2024.

Reform Heading	Reform subheading	Will secondary legislation include direct costs and benefits to UK businesses?	Who will be responsible for the secondary legislation IAs?
Online Safety Researchers' Access to Data	Amend the OSA via the DUA to provide SoS with a regulation making power regarding researchers' access to data.	Yes	DSIT

90. In order to measure the continued success of these reforms, we are building a monitoring and evaluation framework that will ensure that we measure and monitor the changes to the key impact variables including GVA and business costs throughout the life of the policies.

Impact Analysis

Assumptions and methodology

91. The preferred package of reforms has been analysed and estimations of the potential costs and benefits can be found below. These are assessed over a period of 10 years from 2024 to 2033, and are discounted using the Green Book's suggested discount rate of 3.5%.[56]

92. Where analysis has already been published with respect to some of the policies included in the Act, this is referenced accordingly. This is the case for the Digital Identity measures[57], the Smart Data policies[58], the NUAR measures[59], the Interoperability of Health Care systems measures[60] and the Researchers' Access to Data provisions61. In these cases, where appropriate, all costs and benefits have been appraised over 10 years and the same base year has been applied. Where other government departments have fed into this analysis, this is also the case.

93. The expected impact of the policies will fall on private organisations that use data and those that currently face barriers in doing so. Public sector organisations will also be impacted by reforms designed to improve the efficiency of data transfers across government departments and increase the interoperability across health and social care systems. Many of these reforms are also designed to make data use for Law Enforcement Agencies (LEAs) and Intelligence Services more efficient.

94. Where sufficient robust data is available, we have estimated the monetary impact of the various reforms, both direct and indirect. Where this evidence is not yet available, we have provided an in-depth outline of the potential costs and benefits and ensured that any evidence gaps will be referenced in our monitoring and evaluation plan which can be found at the end of this IA.

95. This section begins by looking at the direct monetised benefits of implementing the package of reforms, this includes the saving in compliance costs for UK businesses and a deep dive into the benefits of increased regulatory oversight and data-use in national security and law enforcement. This is followed by qualitative analysis of the direct benefits where monetary evidence is currently limited.

96. Following the analysis of the direct benefits, we look at the indirect benefits. Using analysis, we have estimated the potential impact on UK productivity levels of an increase in data use resulting from these reforms. We have also conducted analysis that looks at the potential impacts to consumer trust and privacy as well as the reduction in ambiguity for businesses and the delivery of better public services.

97. We expect the package of reforms to have a net positive impact overall, however we provide an overview of the direct and indirect costs that could be faced by UK businesses as a result of these policies. These costs are likely to consist mainly of familiarisation costs faced by

[56] HMT: The Green Book, 2022
[57] DSIT: Digital identity and attributes - De Minimis Assessment, 2024
[58] DBT: Smart Data Impact Assessment, 2024
[59] DSIT: NUAR Impact Assessment, 2024
[60] DHSC Open Data Architecture Information Standards, 2024
[61] DSIT: Researchers' Access to Data Impact Assessment, 2024

businesses and public sector organisations having to update any processes and systems to be in line with the new guidance.

98. As well as looking at the costs and benefits to UK businesses we have also estimated the impact on international trade. For this analysis we have used a variety of approaches however as the modelling uses many variables and assumptions that create uncertainty, we are excluding this from the total estimated NPV for the package of reforms.

99. Alongside the potential trade impacts of the reforms, we are also aware that any changes to the UK's current data adequacy regulations are likely to have an impact on these results. We have used consultation responses to build upon the analysis previously conducted, and refined our methodology to present a possible range of the monetary impact to the UK if Adequacy with the EU were to be removed.

100. As there is a wide array of reforms in the package the cost benefit analysis is split out in table 11 and the reforms are classified as being either monetisable or not, having direct or indirect impacts, whether or not they will be followed by secondary legislation or not, and who is likely to be impacted.

101. Some of the measures assessed here are enabling only and given the uncertainty over the contents of the secondary legislation, will be assessed more fully at that stage (scenario two in the RPC's primary legislation guidance). The impacts of these secondary measures are either indirect or unquantifiable at this stage. Usually where this is the case, an impact assessment would present two EANDCBs. However, in this case they are the same and therefore the EANDCB figures presented here cover the set of policies as a whole.

102. Throughout this section references are made to data controllers, data processors and joint controllers. Data controllers are understood to be the individual or organisation who determine the purpose and means of processing personal data, they exercise overall control over the data being processed and are ultimately responsible for the processing. Data processors are understood to be the individual or organisation that processes personal data on behalf of the controller, they act under the authority, and in the interests of, the data controller. Joint controllers are where two or more data controllers jointly determine the purpose and means of processing; they have the same shared purposes. Controllers are not considered joint controllers if they are processing the same data for different purposes[62].

Impact of Criminalising the creation, or requesting the creation of, a purported intimate image (deepfake) of another person aged 18 or over without the adult's consent or reasonable belief in consent.

103. We expect low levels of police recorded crime: as this offence relates solely to the creating or requesting of these images, often without any intention that the person in the image is aware, many instances may not be reported to the police.

104. Conversely, where the new offences are reported, it is likely that this will occur along with the offences of sharing or threatening to share the image which has been created. If an intimate image deepfake were to be shared without consent or threatened to be shared it would be captured under existing legislation in the Sexual Offences Act 2003, carrying a sentence of up to two years in custody. We expect that the police would pursue this more

[62] ICO: What are 'controllers' and 'processors'?

serious charge as well as the “creating” offence, and that the offender would be sentenced for the totality of their offending behaviour.

105. To estimate the costs to the Criminal Justice System (CJS) of this measure, data from South Korea was used, where the creation and sharing of sexually explicit deepfakes was criminalised in 2021, alongside data from the Security Hero ‘State of Deepfakes’[63] report, which covers the ‘reality, state and impact’ of online deepfakes over the period 2019 to 2023.

106. South Korea is used as a comparison as it is one of the few countries where sexually explicit deepfakes have been criminalised for long enough for there to be useful data. However, this data is suggestive only, due to differences in the relevant criminal law and the wider cultural environment.

107. For the “requesting” offence there is even more limited data as it is a novel offence. We assume that, since the law in South Korea is even more comprehensive (possession of sexually explicit deepfakes is criminalised), our methodology using volumes in South Korea as a base covers both offences.

108. To estimate the impacts of Option 1, we have used the following scenarios:

a. The ‘low’ scenario assumes the increase in sexually explicit deepfakes has been linear between 2019-2023 (17,422 and 95,820 respectively - the two given data points in the Security Hero report) and has increased at a rate of roughly 13% per year. It also applies the Security Hero observational data which shows South Koreans to be the victims of 53% of online deepfakes, whilst UK victims form 6% of the total. This gives a ratio of 8.83, which has then been applied to South Korea’s police recorded crime figures.

b. The ‘high’ scenario adjusts the South Korea police recorded crime figures with the ratio of voyeurism offences observed in South Korea to the UK between 2013-2018 (3.17). It applies the compound growth rate of police recorded crime in South Korea between 2021 and 2024 (62%), which could approximate the observed trend in the UK due to the expected trajectory of detection and policing changes after criminalisation, as well as technological and accessibility improvements.

109. The ‘best’ estimate takes the average of the high and low scenarios, which are calculated as above and presented in Section F, and form a wide range reflecting the lack of robust evidence to base estimates off:

110. In both the ‘high’ and ‘low’ scenarios, the prevalence of sexually explicit deepfakes is assumed to increase for 5 years following the last observed data point (2024 for police recorded crime in South Korea) before reaching a steady state. This is to reflect likely technological and accessibility improvements over the appraisal period

111. These assumptions result in baseline 2024 UK police recorded crime figures of around 80 in the low estimate and around 210 in the high estimate. We expect these to serve as an overestimate.

63 2023 State Of Deepfakes: Realities, Threats, And Impact

Impact of reporting on copyright works and artificial intelligence systems

112. The Act requires that an impact assessment is carried out on the four options consulted on in section B.4 of the Copyright and AI Consultation Paper and is published within 9 months, and that a statement of progress is provided within 6 months. As part of the Better Regulation Framework, it is a requirement for government departments to carry out final-stage impact assessments for measures which are brought forward for legislation, including the short-list options considered. Work on producing an impact assessment can therefore be considered business as usual, and would not add significant additional public costs compared to the counterfactual. However it does guarantee than an economic assessment is published in this time period, and it will be of benefit to stakeholders who engage with the results of the assessment. This is not monetised.

113. The Act requires that a set of reports on the use of copyright works in the development of AI systems are published within 9 months, and that a statement of progress is provided within 6 months. These reports would provide the public with more detail several issues regarding the use of copyright works in AI model training. Work on these subjects is expected to be conducted by government officials with consultation from stakeholders. This work will be absorbed into business as usual resource, therefore there will be limited additional public cost to producing the reports. This is not monetised.

Table 11: Breakdown of all costs and benefits by category

Benefits

Benefits	Reform	Monetised?	Direct?	Followed by secondary legislation?	Who is impacted?
Compliance cost savings	Harness the power of data for economic growth	Monetised	Direct	No	UK Businesses
Compliance cost savings	Improve people's lives	Monetised	Direct	No	UK Businesses
Support a modern digital government	Relaxed requirement to review data adequacy decisions	Monetised	Direct	No	Government (ICO)
Support a modern digital government	Enforcement Powers	Monetised	Direct	No	Government (ICO)
Support a modern digital government	Complaints	Monetised	Direct	No	Government (ICO)
Harness the power of data for economic growth	Harness the power of data for economic growth	Monetised	Indirect	No	UK Businesses
Creation of Innovative and Secure Smart Data Schemes (DBT): Increase in use of Smart Data schemes indirect benefits	Introduction of primary legislation, creating new "regulation-making" powers to enable Smart Data schemes to be introduced in any given sector	Non-Monetised	Indirect	Yes - to be followed up with sector specific legislation	Consumers, businesses, data holders and data recipients
Support a modern digital government	Increased Interoperability and Trust of Digital Identity Systems - Create a governance framework and enable checks against government-held	Monetised for four	Indirect	Yes - to be followed up	UK businesses and consumers

Benefits	Reform	Monetised?	Direct?	Followed by secondary legislation?	Who is impacted?
	data	examples use cases		with sector specific legislation	
Support a modern digital government	Increased Interoperability and Trust of Digital Identity Systems - Create a governance framework and enable checks against government-held data	OBJ	Indirect	Yes - to be followed up with sector specific legislation	UK businesses and consumers
Improve peoples' lives: Privacy, trust and individual data rights	Harness the power of data for economic growth	Non-Monetised	Indirect	No	UK consumers
Improve peoples' lives: Privacy, trust and individual data rights	Improve people's lives	Non-Monetised	Indirect	No	UK consumers
Support a modern digital government: Delivery of better public services	Clarifying that private organisations & individuals asked to carry out an activity on behalf of a public body may rely on that body's lawful ground for processing the personal data under Art 6(1)	Non-Monetised	Indirect	No	UK businesses and public sector organisations
Support a modern digital government: Delivery of better public services	Exemption for Archives from further processing rules	Non-Monetised	Indirect	No	Data subjects, Archives and public sector organisations
Support a modern digital government: Delivery of better	To extend powers under section 35 of the Digital Economy Act 2017 aimed at improving public service delivery to business undertakings, beyond the current scope of solely individuals and households (CDDO)	Non-Monetised	Indirect	Yes	UK businesses and Government

Benefits	Reform	Monetised?	Direct?	Followed by secondary legislation?	Who is impacted?
public services					
Improve peoples' lives: Improved Customer Outcomes	All reforms	Non-Monetised	Indirect	No	Consumers
Improve peoples' lives: Improved Interoperability across Health and Social Care Systems	Improved Interoperability across Health and Social Care Systems: Create primary legislation for a new power for the Secretary of State for Health and Social Care to direct suppliers/suppliers to adopt an open data architecture approach through the use of ISNs. [64]	Non-Monetised	Indirect	Yes	Healthcare providers, patients and third-party providers
Improve peoples' lives: Improved Interoperability across Health and Social Care Systems	Improved Interoperability across Health and Social Care Systems: Create primary legislation for a new power for the Secretary of State for Health and Social Care to direct suppliers/suppliers to adopt an open data architecture approach through the use of ISNs.[64]	Non-Monetised	Direct	Yes	Healthcare providers, patients and third-party providers
Improve peoples' lives: Improved Interoperability across Health and Social Care Systems	Improved Interoperability across Health and Social Care Systems: Create primary legislation for a new power for the Secretary of State for Health and Social Care to direct suppliers/suppliers to adopt an open data architecture approach through the use of ISNs. [64]	Monetised	Indirect	Yes	Healthcare providers, patients and third-party providers
Improve peoples' lives: Improved Interoperability across Health and Social Care Systems	Improved Interoperability across Health and Social Care Systems: Create primary legislation for a new power for the Secretary of State for Health and Social Care to direct suppliers/suppliers to adopt an open data architecture approach through the use of ISNs. [64]	Monetised	Direct	Yes	Healthcare providers, patients and third-party providers
Support a modern digital government: Law Enforcement	Logging of law enforcement processing (Part 3 DPA)	Monetised	Direct	No	Government (LEAs) and private sector

[64] This is the preferred option in the DHSC proposed reforms

Benefits	Reform	Monetised?	Direct?	Followed by secondary legislation?	Who is impacted?
Agencies					LEAs
Support a modern digital government: Law Enforcement Agencies	Data subjects' rights to information: legal professional privilege exemption (Part 3 DPA) Data subjects' rights to information: legal professional privilege exemption (Part 3 DPA)	Non-Monetised	Direct	No	Government (LEAs and UK Intelligence Services)
Support a modern digital government: Law Enforcement Agencies	Time limits for responding to requests by data subjects (Part 3 and 4 DPA)	Non-Monetised	Indirect	No	Government (LEAs and UK Intelligence Services)
Support a modern digital government: Law Enforcement Agencies	National security exemption (DPA 2018 part 3)	Non-Monetised	Indirect	No	Government (LEAs and UK Intelligence Services)
Support a modern digital government: Law Enforcement Agencies	Amendments to Part 4 of the DPA 2018 - Joint processing by intelligence services and competent authorities	Non-Monetised	Direct	Yes	Government (LEAs and UK Intelligence Services)
Support a modern digital government: Law Enforcement Agencies	Consent to law enforcement processing (DPA 2018 part 3)	Non-Monetised	Indirect	No	Government (LEAs and UK Intelligence Services)
Support a modern digital government: Law Enforcement Agencies	Transfers based on special circumstances (Schedule 6, Section 76 DPA)	Non-Monetised	Indirect	No	Government (LEAs and UK Intelligence Services)

Benefits	Reform	Monetised?	Direct?	Followed by secondary legislation?	Who is impacted?
Support a modern digital government: Law Enforcement Agencies	Subsequent transfer's (Section 78 DPA)	Non-Monetised	Indirect	No	Government (LEAs and UK Intelligence Services)
Support a modern digital government: Law Enforcement Agencies	Retaining biometrics disseminated by Interpol and other international exchange routes	Monetised	Direct	No	Government (LEAs and UK Intelligence Services)
Support a modern digital government: Law Enforcement Agencies	Remove the requirement for paper birth and death registers moving to an electronic register	Monetised	Indirect	No	Government (LEAs and UK Intelligence Services)
Support a modern digital government: Law Enforcement Agencies	Remove the requirement for paper birth and death registers moving to an electronic register	Non-Monetised	Indirect	No	Government (LEAs and UK Intelligence Services)
Harness the power of data for economic growth	Introduction of provision to operationalise the National Underground Asset Register (NUAR), which is a digital map of underground pipes and cables.	Monetised	Direct	Yes	UK businesses and government
Harness the power of data for economic growth	Introduction of provision to operationalise the National Underground Asset Register (NUAR), which is a digital map of underground pipes and cables.	Monetised	Indirect	Yes	UK businesses and government

Benefits	Reform	Monetised?	Direct?	Followed by secondary legislation?	Who is impacted?
Harness the power of data for economic growth	Introduction of provision to operationalise the National Underground Asset Register (NUAR), which is a digital map of underground pipes and cables.	Non-Monetised	Indirect	Yes	UK businesses and government
Support a modern digital government	Create powers for the Secretary of State (SoS) to place a duty on platforms to comply with any regulations later passed by SoS allowing researchers access to certain data held by platforms.	Non-Monetised	Indirect	Yes	Individuals, businesses and government
Improve peoples' lives: Privacy, trust and individual data rights	Compliance benefits from charities having a clearer legal basis to send direct marketing for the purposes of furthering one or more of their charitable purposes.	Monetised	Direct	No	Businesses
Improve peoples' lives: Privacy, trust and individual data rights	Allowing charities to send direct marketing for the purposes of furthering one or more of their charitable purposes leading to additional donations.	Non-Monetised	Direct	No	Individuals, businesses
Strengthen the criminal law and increase confidence in Criminal Justice System	Introduction of two new offences to protect individuals and educate the public about the unacceptability of the creating and requesting intimate deepfakes, and intimate image abuse more generally.	Non-Monetised	Direct	No	Individuals, Criminal Justice System
Increase public knowledge of the key issues, factors and impacts to be considered ahead of potentially legislating on AI and copyright.	Producing reports and an economic impact assessment on AI and Copyright.	Non-monetised	Indirect	No	Individuals, UK businesses and government.

Costs

Costs	Reform	Monetised ?	Direct?	Followed by secondary legislation?	Who is impacted?
Familiarisation costs	Harness the power of data for economic growth	Monetised	Direct	No	UK businesses
Familiarisation costs	Improve people's lives	Monetised	Direct	No	UK businesses
Familiarisation costs	Enhancing the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO)	Monetised	Direct	No	Government (LEAs and UK Intelligence Services)
Familiarisation costs	New ICO Duty to consult	Monetised	Direct	No	Government (LEAs and UK Intelligence Services)
Familiarisation costs	Mandatory IAs for statutory codes and guidance	Monetised	Direct	No	Government (LEAs and UK Intelligence Services)
Familiarisation costs	Setting up expert panels for statutory codes and guidance	Monetised	Direct	No	Government (LEAs and UK Intelligence Services)
	Governance changes	Monetised	Direct	No	Government

Costs	Reform	Monetised ?	Direct?	Followed by secondary legislation?	Who is impacted?
Familiarisation costs					(LEAs and UK Intelligence Services)
Support a modern digital government (Enhance the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO))	Introduce the ability to actively review automated decisions	Monetised but not included in calcs	Direct	No	Government (LEAs) and UK businesses
Support a modern digital government (Enhance the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO))	Time Limits for responding to requests by data subjects (Part 3 and 4 DPA)	Non-monetised	Direct	No	Government (ICO, LEAs and UK Intelligence Services)
Support a modern digital government (Enhance the work of the UK intelligence services and Law Enforcement Agencies in the interest of public	Law enforcement processing and codes of conduct (Part 3 DPA)	Non-monetised	Direct	No	Government (ICO, LEAs and UK Intelligence Services)

Costs	Reform	Monetised ?	Direct?	Followed by secondary legislation?	Who is impacted?
security (HO))					
Support a modern digital government (Enhance the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO))	Amendments to Part 4 of the DPA 2018 - Joint processing by intelligence services and competent authorities	Non-monetised	Direct	Yes	Government (ICO, LEAs and UK Intelligence Services)
Support a modern digital government (Enhance the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO))	Remove the requirement for paper birth and death registers moving to an electronic register	Monetised	Indirect	No	Government (ICO, LEAs and UK Intelligence Services)
Support a modern digital government (Creation of Robust and Secure Smart Data Schemes (DBT): Increase in use of Smart Data schemes indirect costs)	Introduction of primary legislation, creating new “regulation-making” powers to enable Smart Data schemes to be introduced in any given sector	Non-Monetised	Indirect	Yes - to be followed up with sector specific legislation	UK businesses and consumers

Costs	Reform	Monetised ?	Direct?	Followed by secondary legislation?	Who is impacted?
Improve people's lives (Increased Interoperability and Trust of Digital Identity Systems)	Create a governance framework and enable checks against government-held data	Monetised for 4 examples use cases	Indirect	Yes - to be followed up with sector specific legislation	UK businesses and consumers
Improve people's lives (Increased Interoperability and Trust of Digital Identity Systems)	Create a governance framework and enable checks against government-held data	Non-Monetised	Indirect	Yes - to be followed up with sector specific legislation	UK businesses and consumers
Improve people's lives (Delivery of better public services)	To extend powers under section 35 of the Digital Economy Act 2017 aimed at improving public service delivery to business undertakings, beyond the current scope of solely individuals and households (CDDO)	Non-Monetised	Indirect	Yes	UK businesses and Government
Improved Interoperability across Health and Social Care Systems	Prepare, publish and mandate standards that apply to the products and services provided by IT suppliers, to ensure that those products and services enable and support data to be accessed, interrogated and processed in real time by anyone with the basis to appropriately access that data, irrespective of the system used by the health or social care provider who collated, produced or otherwise processed that data.[65]	Non-Monetised	Indirect	Yes	Healthcare providers, patients and third-party providers
Improved Interoperability across Health and Social Care Systems	Prepare, publish and mandate standards that apply to the products and services provided by IT suppliers, to ensure that those products and services enable and support data to be accessed, interrogated and processed in real time by anyone with the basis to appropriately access that data, irrespective of the system used by the health or social care provider who collated, produced or otherwise processed that data.[65]	Monetised	Direct	Yes	Healthcare providers, patients and third-party providers
Operationalise the National Underground Asset	Introduction of provision to operationalise the National Underground Asset Register (NUAR), which is a digital map of underground pipes and cables.	Monetised	Direct	Yes	UK businesses and government

[65] This is the preferred option in the DHSC proposed reforms

Costs	Reform	Monetised ?	Direct?	Followed by secondary legislation?	Who is impacted?
Register					
Operationalise the National Underground Asset Register	Introduction of provision to operationalise the National Underground Asset Register (NUAR), which is a digital map of underground pipes and cables.	Monetised	Indirect	Yes	UK businesses
Operationalise the National Underground Asset Register	Introduction of provision to operationalise the National Underground Asset Register (NUAR), which is a digital map of underground pipes and cables.	Non-Monetised	Indirect	Yes	UK businesses and government
Facilitate Researchers' Access to Online Safety Data	Create powers for the Secretary of State (SoS) to place a duty on platforms to comply with any regulations later passed by SoS allowing researchers access to certain data held by platforms.	Non-Monetised	Direct	Yes	UK Businesses
Costs to relevant agencies in the Criminal Justice System	New offences will increase volumes flowing through the Criminal Justice System, resulting in additional costs.	Monetised	Direct	No	Agencies relating to the Criminal Justice System
Public costs of researching, drafting and publishing.	Producing reports and an economic impact assessment on AI and Copyright.	Non-Monetised	Direct	No	UK government

Wider impacts

Wider Impacts	Reform	Monetised ?	Direct?	Followed by secondary legislation?	Who is impacted?
Impact on Competition	All reforms	Non-Monetised	Indirect	N/A	N/A
Impact on Equalities	All reforms	Non-Monetised	Indirect	N/A	N/A
Impact on Individuals	ICO Taxonomy of Harms Artificial Intelligence Ethics Increased Interoperability and Trust of Digital Identity Systems Use of data for purposes relating to electoral services	Non-Monetised	Indirect	N/A	N/A
Environmental Impacts	All reforms	Non-Monetised	Indirect	N/A	N/A
National Security Impacts	All reforms	Non-Monetised	Indirect	N/A	N/A

Benefits

Summary

Analysis of the benefits of the proposed package of reforms has been split in the following way, and further details can be found in the continuing sections.

1. Direct Benefits
    a. Monetised
        i. Compliance cost savings
        ii. Improved regulatory oversight
        iii. Enhancement of the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security
        iv. Delivery of the National Underground Asset Register
        v. Improved interoperability across health and social care systems
    b. Non-monetised
        i. Enhancement of the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security
        ii. Improved interoperability across health and social care systems
        iii. Strengthening of the criminal law to protect victims, reduce abusive conduct and prevent emotional distress and adverse physical health impacts associated with being a victim of abuse, thereby also increasing confidence in the Criminal Justice System.
        iv. Direct marketing carried out by a charity for charitable purposes.
2. Indirect Benefits
    a. Monetised
        i. Impact on UK business productivity and innovation
        ii. Increased interoperability and trust of digital identity systems
        iii. Remove the requirement for paper birth and death registers moving to an electronic register
        iv. Improved interoperability across health and social care systems
        v. Delivery of the National Underground Asset Register
    b. Non-monetised
        i. Creation of innovative and secure Smart Data schemes
        ii. Privacy, trust and individual data rights
        iii. Delivery of better public services

iv. Exemption for Archives from further processing rules

v. Improved customer outcomes

vi. Improved interoperability across health and social care systems

vii. Enhancement of the work of the UK Intelligence Services and Law Enforcement Agencies in the Interest of Public Security

viii. Remove the requirement for paper birth and death registers moving to an electronic register.

ix. Powers relating to verification of identity or status (DSIT & Home Office)

x. Power to add categories of sensitive processing (DSIT & Home Office) (DSIT & Home Office)

xi. Processing in reliance on relevant international law (DSIT & Home Office)

xii. Searches in response to data subjects(DSIT & Home Office)

xiii. Clarify conditions on the use of international processors by UK competent authorities (Part 3 DPA)

xiv. Delivery of the National Underground Asset Register

xv. Improved interoperability and trust of digital identity systems

xvi. Facilitating online safety researchers' access to data

114. Benefits arise from a variety of impacts including an estimated increase in responsible data use and a reduction in compliance costs. We estimate the whole package of reforms will generate benefits of between **£3.2 billion and £20.1 billion over ten years, discounted and in 2024 prices**. These benefits arise mostly from the measures relating to reducing barriers to responsible innovation and reducing burdens on business and delivering better outcomes for people. The rest of this section sets out our approach and evidence used to quantify these benefits.

Direct benefits - Monetised

115. The preferred package of reforms is designed to be beneficial to both the private and public sector, where evidence is available, we have calculated monetised estimates of some of the direct benefits of the policies below. These include efficiency benefits from the use of NUAR, the compliance cost savings firms will experience, the efficiency benefits of the reforms to the ICO and the benefits to Law Enforcement Agencies of removing the need to log the 'justification' for consulting / disclosing data disclosure.

Compliance cost savings

116. We have identified the reforms within the package that are likely to impact UK business compliance costs and updated these to reflect any post-consultation stage policy changes. Using data from the UK Business Data Survey,[66] we have estimated the total number of businesses likely to be impacted following implementation.

117. The table below sets out some of the key compliance requirements and activities that we assume result from the current UK GDPR/DPA requirements, and the associated unit-costs or time-cost (costs incurred by organisations to undertake such activities or complete requirements).

118. The full list of legal activities, estimated costs and sources can be found in the table below. We have updated our modelling to use a more up to date exchange rate,[67] and uplifted fees to 2024 prices. These are derived from the best available evidence, however, there remains a large degree of uncertainty. For example, we assume that the baseline cost of some compliance activities varies depending on the size of the organisation (e.g. establishing a lawful ground for data processing) whereas others do not (e.g. cost of seeking legal advice).

119. We have updated the impact assessment with all the relevant material as of Autumn 2024 made further updates to the modelling. These updates include changes to the estimated number of businesses in each sector and size category using 2023 ONS Business Population Estimates and use of the 2024 UK Business Data Survey to estimate the proportion of businesses affected by each measure.

120. Where data was available, we have updated the modelling to the 2024 edition of the UK Business Data Survey (UKBDS). UKBDS 2024 did not suggest many significant changes since 2022, however several smaller changes have had a cumulative impact on some of the model results. For this reason, we scrutinised all instances in which we used updated UKBDS figures. In some cases, we found that 2024 results were not sufficiently comparable to previous iterations of the UKBDS, for example due to different survey routing. In these cases, we tried to find compromise solutions, usually involving trying to draw and combine insights from previous survey iterations. For example, estimates for the number of businesses who handle digitised data and personal data were calculated by finding the average response to these questions across the three editions of the UK Business Data Survey (2021[68], 2022[69] and 2024[70]). While the estimate for the proportion of businesses who analyse data to generate insights or

[66] DSIT: UK Business Data Survey
[67] We assume that 1 EUR = £0.85 which is the 2024 Q2 European Central Bank average
[68] DSIT: UK Business Data Survey, 2021
[69] DSIT: UK Business Data Survey, 2022
[70] DSIT: UK Business Data Survey, 2024

knowledge was calculated using an average between the 2021 and 2024 releases, as the question was not asked in 2022.

121. The modelling assumes full compliance with legislation, both pre-and post We have updated the impact assessment with all the relevant material as of autumn 2024 implementation. Over or under compliance can occur as a result of complexity of legislation. While this is not accounted for in our modelling, we acknowledge that this could, in theory, impact the compliance cost savings to a business. For example, if a business is currently non-compliant either will experience no impact as a result of the changes, or an increase the costs for that business if they become compliance as a result of clarification of the requirements. Similarly, a business that is over compliant, could continue to do so after the changes and not see a reduction in compliance costs.

Table 12: A list of all compliance activities and their estimated cost

Activity	Description	Annual cost per activity per business (£)
Seeking legal advice	Businesses often require external legal advice in order to maintain their compliance with regulation. This includes advice on how and whether data can be used. (Excludes the cost of establishing a legal basis for data processing)	£1,278/year cost of legal advice (equivalent to 4 hours of a legal professional and 2 hours of a clerical worker)[71]
Acquiring consent to store or access information	There is a prohibition on businesses storing information, or accessing information, on a user's connected device unless they obtain the user's consent or they can rely on two further exceptions. They often fulfil this requirement by having 'opt-in' functionality on their website	£80.54 cost per business per year to run opt-in[72]
Preparing Data Protection Impact Assessments (DPIAs)	DPIAs must be completed by businesses where data processing is likely to result in a high risk to individuals. They describe the nature and scope of processing, identify the risks to individuals of processing and ways to mitigate those risks. DSIT confirmed that under each of the measures a DPIA would still be required	£1,278/year cost of legal advice (equivalent to 4 hours of a legal professional and 2 hours of a clerical worker)[73]
Other internal compliance activities	Other internal compliance activities not listed above include, but are not limited to, notifying the authorities of processing of data which might represent specific risks to individuals, and responding to consumer questions about how the business is following data protection principles	Annual wages for DPO (medium and large enterprises): £50,000 for medium and large enterprises; annual labour costs for DPO-type functions: £900 for small and micro enterprises[74]

[71] Proposal for an EU Data Protection Regulation, Ministry of Justice, (2012)
[72]The EC evaluation of Directive 2002/58 conducted by Deloitte estimated that technical implementation of the opt-in / opt-out solution on a businesses website costs 75 EUR, once uplifted to 2024 prices and converted to GBP, this figure is £80.54
[73] Proposal for an EU Data Protection Regulation, Ministry of Justice, (2012)
[74] Data Protection Officer Salaries - Glassdoor (2021)

Activity	Description	Annual cost per activity per business (£)
Direct marking for charities	Charities save in legal costs in understanding regulation when they use data to gain donations	On average £946/year

122. We have updated these activities to reflect the fact that 'establishing a legal basis for data processing' forms part of 'seeking legal advice'. As a result, our estimation for the total **annual** cost of compliance saved by firms can be seen in the table below split by reform.

Table 13: Estimated compliance cost savings by reform, 2024 prices

Reform	Average Annual Compliance Costs (£million) Low Scenario	Average Annual Compliance Costs (£million) Medium scenario	Average Annual Compliance Costs (£million) High scenario
Legitimate Interests	0.4	2.5	6.5
AI and Machine Learning	0.7	7	19.4
Research Purposes	1.1	4.7	10.7
Privacy and electronic communications	8.6	17.1	25.7
Direct marketing for charities	0.1	0.5	1.3
Total	10.9	31.8	62.3

123. These results can be broken down by reform and compliance activity. For example, the table below sets out the estimated annual compliance cost saving from creating a limited non-exhaustive list of legitimate interests for which businesses can use personal data without applying the balancing test. We also estimate the savings for businesses by clarifying that activities, such as direct marketing or ensuring network and information security, fall into the scope of the legitimate interest basis for processing personal data. We estimate these reforms to result in a total cost saving for businesses of between £0.4 and £6.5 million and the central estimate is presented in the table below.

Table 14: Breakdown of compliance cost saving calculations as a result of creating a limited non-exhaustive list of legitimate interests, 2024 prices

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations actually affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
Effect on legal advice costs	1.0 million businesses that use data to generate new insights or knowledge[75]	On average 41% of the organisations that have sought legal advice on GDPR/DPA2018 use data to improve marketing or sales performance[76] and 6% have sought legal advice in the last year to comply with UK data protection[77]	£37.9 million annual costs of legal advice for these organisations	6.3%: assuming that 25% of legal advice costs are related to issues clarified by this measure[78], and that for those issues the cost of legal advice will fall by 25% as a result of the measure[79]	2.4
Reduction in customer complaints about data use relating to non-permissible uses of data	Number of customer complaints: 2,976, according to ICO - data on number of complaints to ICO on how data is being used/collected	Not applicable	Cost of responding to legal complaints: £913[81]	6.3%: assuming that 25% of all data uses are affected and there is a 25% reduction in complaints as a result of the measure[82]	0.2

[75] DSIT: UK Business Data Survey, 2024
[76] UK Business Data Survey, 2024
[77] DSIT: UK Business Data Survey, 2024
[78] This is an assumption made in the model. As there is currently a lack of evidence available of the true number of issues this is something that is tested in the sensitivity analysis section and a proposal of how this will be measured going forward will be included in the Monitoring and Evaluation plan.
[79]In the model we assume that clarification can reduce costs in around 25% of cases where legal advice would have been sought. As this is an assumption we test this in the sensitivity analysis section and propose a way of monitoring this in the M&E plan.
[81] Average cost of each ICO investigation (2016/17), uplifted to 2024 prices
[82]We assume that 25% of data uses will be affected by this measure and that the measure will impact 25% of these. We understand that this measure will not eliminate all of the complaints under the categories listed above. Businesses are less likely to do things that break the law and if the guidance is clearer, but we assume this will be minimal based upon consultation responses. We test this assumption in the sensitivity analysis section.

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations actually affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
	[80]				

Total annual reduction in compliance costs (£million): **2.5**

124. The table below shows the average annual decrease in compliance costs from all of the AI and machine learning reforms in the Act. We estimate these savings to be approximately between £0.7 million and £19.4 million a year.

125. By including the additional reform that clarifies that profiling is only subject to the safeguards associated with solely automated decision-making when significant decisions are taken about an individual on its basis without meaningful human involvement, firms that use data for AI-driven ADM will have more clarity on the use of data for profiling activities within solely automated decision-making processes. This clarification will reassure firms that may currently be unsure about using data for this purpose and that spend money and time seeking legal advice on the matter. This increase in confidence could therefore lead to a decrease in costs of compliance and employing legal assistance. We assume that there will be a 20% further reduction in the legal advice requested because of the additional measure. Evidence is limited to suggest the exact percentage however we have remained conservative in our estimates as we acknowledge this is not the only reason why these firms would seek legal advice. Because of this the assumption is tested using sensitivity analysis.

126. Assuming that approximately 835,000 businesses use personal data with AI and 13% of these do not find regulatory guidance published by the ICO guidance clear[83] applying the assumption above we estimate that this additional reform could lead to an increase in compliance cost savings of £6.9 million a year.

Table 15: Breakdown of compliance cost saving calculations as a result of AI and Machine learning measures, 2024 prices

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
Effect on legal advice costs	834,722 businesses that use personal data and use AI	13%: organisations that don't find ICO regulatory guidance clear and easy to	£139 m annual costs of legal advice	5%: assuming that 20% of legal advice costs for affected organisations are related to processing personal data to	6.9

[80] ICO Complaints and concerns data sets
[83] DSIT: UK Business Data Survey, 2024

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
		understand[84]		improve accuracy of AI systems, and that 25% of legal costs in these cases could be saved as a result of the measure[85]	
Reduction in customer complaints about data use	Number of customer complaints: 2,976, according to ICO - data on number of complaints to ICO on how data is being used/collected [86]	8% of organisations associated with research purposes	Cost of responding to legal complaints: £913[87]	6.3%: assuming that 25% of all data uses are affected and there is a 25% reduction in complaints as a result of the measure[88]	<0.1

Total annual reduction in compliance costs (£million): 7.0

127. The table below shows the average annual decrease in compliance costs resulting from simplifying the use of personal data for research purposes. This includes amending existing legislation to support responsible research activity using personal data as well as extending the exemptions by incorporating 'research in a commercial setting' into the definition of research purposes for data protection legislation.

128. Businesses will benefit from the improved legal certainty of definitions. As a result, we predict a reduction in the need for businesses to seek legal advice and a reduction in the number of customer complaints about the use of personal data for commercial research purposes.

[84] DSIT: UK Business Data Survey, 2024 Businesses that responded "Strongly disagree" and "tend to disagree" to the question "My business finds the regulatory guidance published by the ICO clear and easy to understand?"
[85] We assume that AI is a smaller subset of use cases than with the legitimate interest measure hence 20% is applied. We understand that even with clearer guidance, some legal advice will still be required. The amount of time spent seeking legal advice is an assumption due to the current lack of data. Because of this we test these assumptions in the sensitivity analysis section and make plans for their measurement going forward.
[86] ICO Complaints and concerns data sets
[87] Average cost of each ICO investigation (2016/17), uplifted to 2024 prices
[88] We assume that 25% of data uses will be affected by this measure and that the measure will impact 25% of these. We understand that this measure will not eliminate all of the complaints under the categories listed above. Businesses are less likely to do things that break the law and if the guidance is clearer, but we assume this will be minimal based upon consultation responses. We test this assumption in the sensitivity analysis section.

129. Using the 2024 UK Business Data Survey (UKBDS), we estimate that the number of businesses that use data to generate new insights or knowledge, employ someone who leads on R&D and have sought legal advice because of UK GDPR or the DPA 2018 in a year is approximately 42,000.

130. Assuming a constant cost of legal advice of £1,278 for these businesses we estimate that the total cost is approximately £53.1m a year.

131. Initially we assumed that policies designed to amend existing legislation to support responsible research activity using personal data, constitute 10% of the legal costs faced by these firms. By adding this additional reform that further clarifies the businesses that can rely on 'research purposes' we assume that an extra 25% of legal costs will be impacted.

132. The total savings are estimated to be approximately between £1.1 and £10.7million a year.

Table 16: Breakdown of compliance cost saving calculations as a result of research purposes measures, 2024 prices

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations actually affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
Effect on legal advice costs	41,572 [89] [90]	All businesses	£53m annual cost of legal advice	9%: assuming that 35% of legal advice costs are related to issues clarified by this measure, and that for those issues the cost of legal advice will fall by 25% as a result of the measure[91]	4.7
Reduction in customer complaints about data use	Number of customer complaints: 2,976, according to ICO - data on number of complaints to ICO on how data is being	3.7% of organisations associated with research purposes	Cost of responding to legal complaints: £913[93]	6.3%: assuming that 25% of all data uses are affected and there is a 25% reduction in complaints as a result of the measure[94]	<0.1

[89] DSIT: UK Business Data Survey, 2021 and 2024
[90] DSIT: UK Business Data Survey, 2021 and 2024
[91] We assume that Research purposes are a smaller subset of use cases than with the legitimate interest measure hence only 10% is applied. We understand that even with clearer guidance, some legal advice will still be required. The amount of time spent seeking legal advice is an assumption due to the current lack of data. Because of this we test these assumptions in the sensitivity analysis section and make plans for their measurement going forward.
[93] Average cost of each ICO investigation (2016/17), uplifted to 2024 prices
[94] We assume that 25% of data uses will be affected by this measure and that the measure will impact 25% of these. We understand that this measure will not eliminate all of the complaints under the categories listed above. Businesses are less likely to do things

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations actually affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
	used/collected[92]				

Total annual reduction in compliance costs (£million): **4.7**

133. Allowing organisations to use cookies or similar technologies by introducing the new low-risk processing exceptions could achieve between £8.6 million and £25.7 million cost savings on average each year.

Table 17: Breakdown of compliance cost saving calculations as a result of PEC Regulations measures, 2024 prices

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations actually affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
Obtaining opt-in consent	708,027 organisations that collect personal data through website analytics [95]	All businesses	£57 m	30% of businesses will no longer offer opt-in consent[96]	17.1

Total annual reduction in compliance costs (£million): **17.1**

134. The estimated figures above rely on many modelling assumptions as a result of the level of evidence available being restrictive at this time. We go on to test these assumptions in our sensitivity analysis section later on in this report. By modelling a low and high scenario where we flex these assumptions, we estimate that the total compliance cost saved will fall between £10.7 and £62.3.

135. The DUA Bill compliance cost model estimates the direct marketing measure could lead to some compliance cost saving of circa £0.5million per annum from creating an exception for which charities can use personal data without applying the balancing test. This will save

that break the law and if the guidance is clearer, but we assume this will be minimal based upon consultation responses. We test this assumption in the sensitivity analysis section.

[92] ICO Complaints and concerns data sets

[95] DSIT: UK Business Data Survey, 2024

[96] Businesses that will no longer need to offer opt in/out: 30% of business will no longer need to offer opt-in/out services. The EC evaluation of Directive 2002/58 conducted by Deloitte found that, of the websites that use cookies, 70% use tracking cookies whilst 30% do not use tracking cookies. We have therefore assumed that the portion of businesses that do not use tracking cookies will benefit from this measure.

charities £946 per business per annum as a result of not needing to seek legal advice to clarify regulation.

Improved Regulatory Oversight - ICO analysis

136. We propose measures to reform the Information Commissioner's Office (ICO); this modernising reform agenda is an investment in the ICO's future success and will sustain its world-leading reputation. The policies cover the following areas of ICO activity:

a. Strategy, Objectives and Duties

b. Governance Model and Leadership

c. Accountability and Transparency

d. Codes of Practice and Guidance

e. Complaints

f. Enforcement Powers

137. These reforms aim to move the ICO away from handling a high volume of low-level complaints and towards addressing the most serious threats to public trust and inappropriate barriers to responsible data use. All costs and benefits will be borne by the ICO and will be absorbed into their current funding structure.

138. The proposed legislative changes are set in the wider context of increased complexity and scale of processing, which increases demand for upstream support and the complexity of downstream enforcement and supervision. They are also set against the backdrop of ongoing work to ensure the ICO has the skills and capacity to respond to increased demand for our activities arising from the implementation of UK GDPR. This existing work is planned on the basis of retention of the ICO's current fees model.

139. Working alongside the ICO we have been able to provide monetary estimates of the predicted impact of these reforms on the ICO directly. Evidence for these calculations has been gathered from internal conversations, research and consultation responses. To estimate the impact a time-cost approach has been used. Estimates for the amount of time needed following the introduction of these reforms to implement changes and familiarise staff with new systems has been provided. This is then multiplied by the average wage of ICO staff

140. We are able to estimate the potential cost savings of these reforms to the ICO using a time-cost approach and evidence gained from discussions with the ICO on resourcing, wage costs and activities[97]. For example, where we expect the impact to be small this is equivalent to only a minor change in 1 - 5 employees' work. In this section we focus on the cost savings that would result from the implementation of these policies on the ICO, compared to a status quo scenario with no change.

141. The analysis in this paper remains preliminary, and indicative only of the potential magnitude and balance of costs and savings to the ICO of implementing the proposals in the government's

[97] ICO analysis uses a 40% uplift to account for non-wage costs. In order to align with the rest of the IA, we have updated this to 22%.

consultation. More detailed assessment will be needed before these are used for the ICO's business planning purposes. Finalised proposals with a greater level of granularity will be required to enable this. It should be noted that, in many cases the savings to the ICO are more likely to be realised as increased efficiency and ability to meet that demand than in reduction in total staff numbers.

142. The first policy we expect to have a net positive impact on ICO costs is the reform of the test used to determine whether other countries' data protection standards are adequate. **Relaxed requirements to review data adequacy regulations every four years**, could reduce some of the requirements for ICO to input into these reviews. Although the ICO is still likely to need to provide input into any ongoing review or assessment process which means these savings are potentially small. The estimated cost saving is broken down in the table below:

Table 18: Expected impact on ICO of changes to data adequacy regulations decision making process, 2024 prices

Reform	Impact	FTE Estimate Low	FTE Estimate High	Cost Saving Estimate (£million) Low	Cost Saving Estimate (£million) High
Relaxed requirement to review data adequacy regulations	Small	1	5	<0.1	0.2

143. The second set of policies we expect to have a positive impact on ICO costs are those that focus on reforming **ICO enforcement powers**. These new powers could result in more efficient, effective investigations. However, investigations are also likely to continue to get more complex, particularly now that they have taken on supervisory responsibility for major digital companies. Therefore, these proposals are likely to deliver a high-medium positive impact, relative to the 'do nothing' option. Benefits in this area are most likely to be realised as increased efficiency and productivity in the context of the growing demand. A breakdown of the estimated cost savings can be seen in the table below

Table 19: Expected impact on ICO of changes to Enforcement Powers, 2024 prices

Reform	Impact	FTE Estimate Low	FTE Estimate High	Cost Saving Estimate (£million) Low	Cost Saving Estimate (£million) High
Enforcement Powers	High-Medium	11	15	0.5	0.7

144. Based on the proposals set out in the government response to the consultation and subject to transitional arrangements, the introduction of a criteria by which the ICO can decide not to investigate a given complaint, potentially has a large positive impact in the long term. This is entirely contingent upon the ICO retaining wide discretion to determine whether to investigate a complaint, even after a period of 45 days during which an individual can complain directly to a

controller to try to resolve the matter, has elapsed. Realising this benefit will take some time given the work required in the short-medium term to support organisations to put in place effective complaints resolution processes. As an all-economy regulator the ICO receives a high volume of cases which they handle directly, which is not true of many other regulators. The estimated impact on the ICO of changes to the complaints process is lower that the analysis within the DUA act as there are some changes to the measures compared to this act to account for changes to this measure in the Act.

Table 20: Expected impact on ICO of changes to the complaints process, 2024 prices

Reform	Impact	FTE Estimate Low	FTE Estimate High	Cost Saving Estimate (£million) Low	Cost Saving Estimate (£million) High
Complaints	Low-Medium	6	10	0.3	0.4

145. Total cost savings are likely to start in year 2 after implementation, once processes have been established and are likely to be annual benefits of between £0.9 million and £1.5 million.

Table 21: Expected positive impact on ICO of all policy changes, 2024 prices

Reform	Impact	FTE Estimate Low	FTE Estimate High	Cost Saving Estimate (£million) Low	Cost Saving Estimate (£million) High
Relaxed requirement to review data adequacy regulations	Small	1	5	<0.1	0.2
Enforcement Powers	High-Medium	11	15	0.5	0.7
Complaints	Low-Medium	6	10	0.3	0.4
Total cost savings	Total	18	30	0.8	1.3

Enhance the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO)

146. This section of analysis has been provided by the Home Office, and is broken down by measure. Where evidence is unavailable benefits have been assessed qualitatively and can be found in the ‘non-monetised section’

Logging of law enforcement processing

147. Currently, LEAs are required to keep logs of several processing activities that they carry out, in automated processing systems, including the accessing and disclosure of personal data. The logs must include information on the date and time the systems were consulted, or data

disclosed, and, so far as possible, the identity of the person consulting the system/disclosing and receiving the data. They must also include the justification for consulting the system/disclosing the data.

148. This proposal removes the requirement to record a 'justification'. This is because police forces have indicated that it is technologically challenging for them to automatically log a 'justification' meaning that they often need to record it manually. Moreover, it holds limited value in maintaining accountability, for example in investigations into misconduct, an individual misusing the database is unlikely to record their true motive and instead record a dishonest justification. We are only removing the 'justification' element; the other requirements to monitor compliance will remain in legislation.

149. To give a sense of scale, automated processing systems within policing are used at three levels: national, local and stand-alone or small systems. The number of these systems varies greatly across police forces but is generally high. For example, the Metropolitan Police Service (MPS) has approximately 600 automated processing systems, while the comparably smaller forces of Hampshire Constabulary and Thames Valley Police have approximately 45.

150. The MPS have provided data for four of their systems, describing the number of times each system was accessed in 2021. Each login would require a 'justification' to be recorded and would take two minutes. For this analysis 2 minutes (120 seconds) has been taken as the high estimate, 0.7 minutes (40 seconds) as low and 1.3 (80 seconds) as central.

151. They have also stated that these tools would be used by constables, sergeants and administrative staff. The wage for administrative staff was taken from the Annual Survey of Hours and Earnings (ASHE) 2023 Table 14.5a (SOC code 41), uplifted to 2024 prices using the CPIH Index and uprated to include non-wage costs of 22 percent. This increased the hourly wage from £14.11 to £17.22. Hourly wages for constables and sergeants were taken from internal Home Office data at £27.97 and £46.43 respectively. These were adjusted to 2024 prices using the CPIH index and final values were obtained at £28.65 and £47.56. Wages for admin are taken as the low estimate, constables as the central and sergeants as the high.

152. To calculate the time savings benefit, it is assumed that the number of times the systems are accessed is constant over the 10-year appraisal period. This is a strong assumption, given that the MPS provided only one year of data, and the result should be used as an indication of scale rather than an accurate estimate.

153. This number is multiplied by the hourly wages and time spent by employees in recording justification. It is assumed that these costs continue over the 10-year appraisal period, adjusting using the discount rate.

Table 22: MPS recording justification ongoing benefits for four automated systems, 2024 prices.

Estimate	No. system access per year (million)	Time spent recording justification (hrs)	Hourly wage (£)	Benefit per year (£ million)	Total benefit (£ million PV)
Low	22.42	0.01	17.22	4.3	36.9

Estimate	No. system access per year (million)	Time spent recording justification (hrs)	Hourly wage (£)	Benefit per year (£ million)	Total benefit (£ million PV)
Central	22.42	0.02	28.65	14.3	122.8
High	22.42	0.03	47.56	35.5	305.9

Source: MPS Consultation, ASHE Table 14.5a, Home Office Staff Costs Database.

Notes: Totals may not sum due to rounding.

154. This means that for the four systems in the MPS, the estimated ongoing benefits of this proposal lie in the range of **£36.9 to £305.9 million** (PV), with a central estimate of **£122.8 million** (PV) over 10 years.

155. This can be upscaled to apply for all LEAs by multiplying the number of system accesses by low, central and high values of 2, 3 and 4 respectively. The high value is taken from the consultation with the MPS where they suggested that the MPS represents a quarter of all police officers. There were 135,301 police officers in England and Wales in 2021,[98] compared to 33,326 in the MPS (as of 28 February 2022).[99] Dividing the total number of officers by the MPS numbers, gives a value of 4.06 which provides evidence for the MPS consultation response.

156. The high estimate assumes identical utilisation of automated systems which is unlikely. The low and central estimates assume that utilisation across the country is one-half and two-thirds respectively, relative to the MPS.

Table 23: All police force recording justification ongoing benefits, No. hrs, £, £ million (PV), 2024.

Estimate	No. system access per year (million)	Time spent logging justification (hrs)	Hourly wage (£)	Benefit per year (£ million)	Total benefit (£ million PV)
Low	44.83	0.01	17.22	8.6	73.8
Central	67.25	0.02	28.65	42.8	368.5
High	89.67	0.03	47.56	142.1	1,223.5

Source: MPS Consultation, ASHE Table 14.5a, Home Office Staff Costs Database.

Notes: Totals may not sum due to rounding.

157. Estimated ongoing benefits for all police forces lie in the range **£73.8 to £1,223.5 million** (PV), with a central estimate of **£368.5 million (PV) over 10 years.**

Non-compliance risks

158. There is currently an exemption available to controllers/ processors at Schedule 20(14) DPA 2018 (as amended by the Data Protection Act 2018 (Transitional Provision) Regulations 2023)

[98] Police workforce, England and Wales: 31 March 2021 - GOV.UK (www.gov.uk)
[99] The structure of the Met and its personnel | Metropolitan Police

which allows them not to have to comply with the logging requirement (and, hence, the need to record a justification), for automated processing systems set up before 6 May 2016, where compliance would involve disproportionate effort. This exemption ceases to have effect on 6 May 2026. If controllers/processors fail to comply with this requirement after that date, they may face compliance risks.

159. Since it is only the requirement to record a justification that police forces have indicated is difficult to comply with, this proposal should reduce the non-compliance risks associated with 'justifications' in automated system

Retaining biometrics disseminated by Interpol and other international exchange routes (Home Office)

160. The National Security Determination (NSD) regime is recognised to come with high resource requirements, as it requires the police to develop a detailed national security case for retaining the biometrics. Building the national security case, particularly on biometrics received via INTERPOL where there is limited information and where seeking further background from the originating country is not necessarily possible or desirable, can require a significant resource input from police officers.

161. An application also requires sign-off by a Chief Officer, as well as by the independent Biometrics Commissioner. As the change exempts INTERPOL biometrics from the NSD regime, we expect this to significantly reduce the resource burden on policing related to the NSD regime. We do not assess there to be any economic costs of implementing this exemption.

162. Counter-Terror Police (CTP) receive on average 300 biometrics per month disseminated by Interpol,[100] however volumes of biometrics may fluctuate significantly due to operational factors.

163. CTP estimate that it takes an officer approximately 4 hours to develop an NSD application.

164. If the average volume of biometrics received over the appraisal period remains at 300 biometrics per month, the time savings over a 10 year period are estimated as approximately £3.2 million (2024/25 prices, PV).

165. For non-Interpol sources, these changes are expected to significantly reduce the number of NSDs processed by CTP. As a result, we expect this to reduce the resource burden on CTP associated with NSD applications. There may be some limited initial resource implications for CTP in processing a 'backlog' of cases to ensure they comply with the requirements introduced by this provision, as the provision will also apply retrospectively to material already held by CTP. But the overall resourcing implications will be net positive (i.e., reduce the resource impacts of handling these biometrics for the police).

166. CTP have estimated that inbound biometrics received through wider international cooperation could increase to up to 200 biometrics per month over time.[101] When this will occur is an evidence gap, as this figure is dependent on the necessary international agreements being signed, which as of now do not have a timeline. The decision has therefore been made to

[100] This is taken from the average number of INTERPOL Notices which CTP receives per month (approximately 600), of which approximately 50% have biometrics attached to them.
[101] CTP currently receive biometric data in tranches, at an average of 10 to 15 per month. There can be significant monthly variance, with potential for the volume of biometric data received to spike rapidly if CTP request or receive a large tranche of data from a specific country.

model annual biometrics using a linear expansion, starting from 10-15 a month (120-180 annually) in the first year and reaching 200 a month (2,400 annually) in the final year of appraisal (Year 10).

167. As above, CTP estimate that it takes an officer approximately 4 hours to develop an NSD application. If the volume of biometrics received over the appraisal period follow the above growth rate, the time savings over a 10 year period are estimated as approximately £1.1 million (2024/25 prices, PV).

168. This does not take into consideration that a limited amount of administrative work will still be required in order to process biometrics received by these routes. For example, the process of pseudonymising the data. These costs have not yet been quantified by CTP as it will be a new process implemented on commencement of the legislation, so cannot be included at this stage.

169. Total resource savings from CTP being able to retain biometrics is estimated at between £2.7 million and £5.9 million with a central estimate of £4.3 million.

Table 24: Police Retention of biometric data, 2024 prices

Estimate	Hours per application	Volumes per month - INTERPOL	Volumes per month – Non-INTERPOL	Hourly Labour Cost (£)	Total Benefit – INTERPOL (£ million PV)	Total Benefit – Non-INTERPOL (£ million PV)
Low	4	150	10-200	25.82	1.6	1.1
Central	4	300	12.5-200	25.82	3.2	1.1
High	4	450	15-200	25.82	4.8	1.1

Source: Internal Home Office Calculations
Notes: Totals may not sum due to rounding.

Delivery of the National Underground Asset Register

170. This analysis has been taken from the NUAR Impact Assessment 2024[102] published by DSIT. For a more detailed breakdown of some of the indicative sector specific costs and benefits please refer to the NUAR Impact Assessment directly.

On-site efficiencies from the use of NUAR

171. On-site personnel undertaking excavations will need to accurately identify the location of all underground assets (and their relevant attributes, such as width and depth) in the area of interest. This is often made more challenging by the fact that data comes in multiple formats and scales, making orientation by personnel on-site more time consuming and inefficient.

172. Furthermore, some excavations may find, but not necessarily strike, an asset that may not be present on a map or personnel may struggle to interpret the poor quality data and maps on

[102] DSIT: NUAR Impact Assessment, 2024

hand. These situations have resource and inefficiency implications ranging from either having to abandon the site, or conduct additional due diligence to determine whether the dig site is still viable for the planned works, before resuming activity or changing plans entirely. These often happen when assets are not on record, or when they are not in the place shown by the plans, but can also happen with otherwise accurate plans that are difficult to align with those from other asset owners.

173. A unified platform such as NUAR provides a single, integrated view of all the underground assets, saving on-site teams from having to interpret multiple maps.

174. To estimate these on-site savings, an assessment of the potential costs from abandonment, resumption and field time needed to interpret maps was estimated. This was based on literature and industry information where possible, and where information was missing, was supplemented through interviews and discussions with industry experts and practitioners.

175. The assessment splits out the potential cost of abandoning or resuming excavations associated with small projects and large projects. Small project costs are based on the rework costs of a 2 day delay, covering project manager labour to replan works and equipment rental to re-survey the site. Large project costs are based on interviews and industry expert engagement.

176. The number of incidents per year were assumed to occur in the same proportions as “low-severity strikes” as identified in the Utility Strike Avoidance Group (USAG) (2014) report. Low-severity strikes are likely to do minimal damage to assets - aligning with the process of finding, but not necessarily striking an asset. The number of incidents that could be affected by NUAR was assumed to be the proportion of projects that use searches (2.2m searches on Linesearch Before Udig (LSBUD) platform compared to 4m excavations overall)[18], that is around 61% of these excavations were in scope of being affected by NUAR, of which 2%[19] are likely to be a low severity strike.

177. For field efficiencies, we used the findings from the NUAR regional pilots in Northeast England and London to understand both the time taking to interpret multiple maps currently, and the time savings that were achieved through the NUAR pilot prototype, valued at the trade rate for such site projects.

178. Total benefits due to on-site efficiencies are expected to total £107.1 million over 10 years (2024 prices). A further breakdown is provided in the NUAR Impact Assessment.[103]

Enabling better data sharing/ Back-office efficiencies through the NUAR

179. When preparing for an excavation a planner has to source data on the location and position of underground assets which may be impacted by the excavation. This is collected by (1) manually contacting each subsurface asset owner, (2) using a commercial third party service, and/or (3) paying an external search firm to provide a data compilation service.

180. Responses from multiple sources need to be aggregated and collated by the requester to be in a suitable form for passing on to site teams. Even responses from aggregation services will be in the form of multiple individual responses from asset owners which need collation. This

[103] DSIT: NUAR Impact Assessment, 2024

existing process for accessing, requesting and sharing underground asset information between asset owners, third party intermediaries and project planning teams is fragmented and results in multiple administrative time and cost burdens for all parties involved.

181. NUAR, as a single platform with comprehensive data of all underground assets in England, Wales and Northern Ireland, will lead to efficiencies in this existing process by removing many of the steps currently required.

182. Evidence was gathered from a survey commissioned by the Geospatial Commission across a range of stakeholders involved in excavation activities. This ranged from those undertaking digs (e.g. site teams from Tier 1 contractors[20], highways authorities, utility asset owners) to those who hold underground asset data (e.g. utility asset owners, other infrastructure asset owners). Overall, 84 stakeholders of varying sizes, asset classes and regional spread were surveyed: 24 Highways authorities; 29 Utility asset owners; 2 Other infrastructure asset owners; and 29 Tier 1 contractors .

183. The surveys identified and quantified the key time and cost drivers involved in the requesting data and responding in “business-as-usual” and “NUAR” scenarios. These drivers included (but were not limited to): the number of data requests involved in one excavation, average cost per search (both internal and outsourced to external providers), number of data requests sent and received and average time spent collating and analysing the data and putting it into site-packs for the site team.

184. These results from the sample were then scaled up to national level using national level statistics on no. of excavations per year in the UK of 4,000,000[21], national water and electricity mains kilometres[22] and population density estimates (ONS). These results were sense-checked with input from sector experts.

185. The difference in time and costs between the “business-as-usual” (without a central data sharing platform) and “NUAR” scenarios yields the data exchange and back-office efficiency savings.

186. As a sense-check of our results, we looked at results from Project Iceberg (a collaborative research project into above/below ground planning conducted by the Future Cities Catapult, the British Geological Survey and Ordnance Survey, which reported its findings in 2017) which collected a number of useful statistics and estimates that contextualised our analysis potential scale of the overall economic impact. International exemplars, such as KLIP in Belgium, also provided references for estimates of the data exchange savings

Specific data sharing benefit to local authorities:

187. A significant proportion of assets are owned by public sector bodies, including approximately 368 local government organisations, 32 transport authorities, and 12 other bodies. The data held by these organisations relates to assets which could have serious safety and cost implications if discovered unexpectedly or damaged by mistake. They include assets such as traffic signs, streetlights and CCTV cabling.

188. As with utilities and telecommunication companies, these organisations are also required to make data about underground assets available to others for the purposes of safe digging per

section 79 of the NRSWA 1991. However, these organisations - in particular local authorities - have unique challenges in doing this as data is often held across different departments.

189. A survey of 100 local government organisations commissioned by the Geospatial Commission in 2021 found only 31% of organisations manage these datasets via a 'central GIS Team', with 43% reporting a mix with some data managed centrally and others managed by individual departments / teams within their organisation. This compares with 54% and 11% for utility companies respectively.

190. This means local government organisations often have an added step of liaising across departments/teams for data in order to respond to requests or data requestors having to contact different parts of the same organisation for complete data. NUAR will help address this by enabling public bodies to upload data how they see fit. Organisations with central teams could assign one user to share all updates with NUAR. Alternatively, where data is held separately, different departments could be responsible for sharing different datasets, eliminating the need for this to be coordinated centrally. Furthermore, these organisations will no longer require the use of in-house teams or procured services to respond to requests for data for the purposes of safe digging, they could refer all requests to the NUAR service.

191. A step-by-step of the calculation of these benefits is given in Annex B of the NUAR Impact assessment[104]

Improved interoperability across health and social care systems

192. The DHSC measures deliver benefits by removing burdens from local health and social care providers, reducing reliance on the disclosure and transfer of large datasets containing confidential patient information to third parties, and supporting the use of data for purposes beyond direct care while protecting patient privacy.

193. Adoption of common information standards by health and social care providers is expected to reduce mapping and standardisation costs across relevant integrated care systems (ICSs) (cash-releasing): Currently without common information standards in place, there is a cost to relevant ICSs lacking these information standards to standardise and convert data from individual electronic patient records (EPRs) or IT systems to be mapped to ShCRs. We expect this cost could be eliminated with the implementation of common information standards. This cost is, on average, £1.26 million per ICS and is one-off and cash-releasing. This has been calculated based on survey responses from health and care providers on spend per annum on mapping and standardising data from clinical systems to Shared Care Records (ShCR). Based on this, the ten-year present value cost saving from standardisation and mapping costs, attributable to DUA is £21.6 million. For a more detailed breakdown of the estimated benefits of the DHSC measure, please refer to the DHSC Open Data Architecture Information Standards Impact Assessment.[105]

[104] NUAR Impact Assessment, 2024 - DSIT
105 Open Data Architecture Information Standards, DHSC (2024)

Direct Benefits - Non-Monetised

194. Where evidence is available, we have estimated the monetised direct benefits of the preferred package of reforms. Where this has not been possible, we provide a detailed qualitative assessment of these impacts including the increase in responsible data use by firms and the enhancement of the work of the UK Intelligence Services and Law Enforcement Agencies in the interest of public security.

Enhance the Work of the UK Intelligence Services and Law Enforcement Agencies in the Interest of Public Security

Introduce a 'legal professional privilege' exemption

195. In the UK GDPR there is a 'Legal Professional Privilege' exemption from the right of access and the right to be informed for personal data in respect of which a claim to legal professional privilege could be made in proceedings or where a duty of confidentiality is owed by a legal adviser to their client. By contrast, controllers and processors under Part 3 must currently rely on ad hoc restrictions contained within Sections 44 (Right to be informed) and Section 45 (Right of access). Stakeholders have indicated that they must conduct the balancing exercise that these sections require, even though the restriction will almost certainly always be applied in that context. This change will replicate the UK GDPR exemption reducing the burden on controllers.

196. This proposal may result in efficiency benefits as controllers and processors under Part 3 will no longer have to spend time evaluating and justifying ad hoc restrictions based on individual circumstances and will instead be able to refer to the new specific exemption.

Amendments to Part 4 of the DPA 2018 - Joint processing by intelligence services and competent authorities

197. Policing and the intelligence services are governed by different data protection regimes which adds friction when working in partnership. This proposal will introduce a power that would allow the Secretary of State to issue a notice authorising a law enforcement body to process data under the Intelligence Services regime in Part 4 of the DPA 2018 in specified circumstances.

198. This proposal will mean that there are fewer areas of potential administrative friction and bureaucracy generated by cross-regime working. This should lead to more efficient ways of working for relevant Law Enforcement Agencies (LEA) and UK Intelligence Service employees as well as more effective close working.

Improved interoperability across health and social care systems

199. Several additional benefits are expected to arise following implementation of this measure, these have not been quantified due to lack of sufficient data and evidence to inform a robust assessment. Please refer to the DHSC Open Data Architecture Information Standards Impact Assessment for a full breakdown of expected impacts.[106]

106 Open Data Architecture Information Standards, DHSC (2024)

200. These benefits include earlier diagnosis and reduce downstream costs, care pathway optimisation, time saved on inefficient processes and duplicative efforts across systems, and improved integration of health and social care services in England.

201. In addition, we anticipate the following non-monetary benefits to arise:

a. **Improving competition and market expansion in the IT supplier market:** Improved competition in the IT supplier market is a benefit stemming from the implementation and the enforcement of information standards. Mandating information standards ensures that all IT suppliers must adhere, which creates a level playing field in the market. IT suppliers are incentivised to innovate and differentiate their offerings to stand out in the market - this competition drives continuous improvement and encourages suppliers to develop more advanced, efficient, and user-friendly solutions.

b. **Lower barriers to entry for new entrants into the IT supplier market to meet regulatory requirements**: This is since all suppliers must comply with the same standards. In addition, health and social care providers would benefit from easier procurement and avoid vendor lock-in, this would support innovation by enabling providers to choose from a diverse set of supplier products and systems. This is in the knowledge that they will not lose access to information and that the technology will work with technologies in other parts of the health and social care system. The increased choice creates competition and enables each provider to choose the IT solution that best meets their needs. Furthermore, there are opportunities for market expansion - information standards would be designed to confirm with international norms; therefore, compliance opens up opportunities for IT suppliers to enter new markets, driving further competition and innovation on a global scale.

202. Allowing charities to send direct marketing for the purposes of furthering one or more of their charitable purposes has additional benefits beyond that of compliance. The amendment to direct marketing backs the third sector in reaching out to more potential donors, potentially helping them boost their finances, which in turn could have valuable societal benefits. It will enable charities to engage with supporters in order to fundraise and promote campaigns.

203. The measure will mean that some people will receive direct marketing materials that they would not have previously received. This code increases the number of complains to the ICO, and the burden on individuals leading to a social cost on individuals. Safeguards have purposefully been designed to provide people with a means of controlling the messaging they receive from a charity.

204. ICO guidance would need to be updated to take this amendment into account and there may be more complaints received.

Criminalise the creating, or requesting the creation, of a purported intimate image (deepfake) of another person aged 18 or over without the adult's consent or reasonable belief in consent.

Victims

205. This measure will strengthen the criminal law so that it captures the intrusive and distressing practice of creating and requesting the creation of intimate image deepfakes without consent or reasonable belief in consent. It will offer greater protections to victims.

206. The new offence should see a reduction in abusive conduct; this should result in preventing emotional distress and adverse physical health impacts associated with being a victim of abuse.

The Public

207. This measure may increase confidence in the criminal justice system for the public and ensure individuals who engage in this activity are held criminally accountable for this behaviour.

208. The creation of the new offences may also serve to educate the public about the unacceptability of the creating and requesting intimate deepfakes, and intimate image abuse more generally.

Indirect Benefits - Monetised

209. Due to the nature of the reforms and the extensive list of indirect benefits, many of these are hard to quantify due to a lack of available evidence. Using economic theory, we know that data is a valuable asset for firms and forms a part of the 'technology and knowledge' aspect of a firm's production function. Therefore, we know that by increasing business access to data, this can lead to further innovations and technological developments that ultimately increase and improve production and efficiency at a firm level. We have therefore estimated the potential impact of this in the following section.

Impact on UK Business Productivity and innovation

210. There is evidence that the current UK GDPR raises high compliance burdens, relative to size and turnover of SMEs.[107] This is corroborated with evidence that the average SME in the EU could expect its annual costs to increase by £2,500 to £6,000, representing 16 and 40% of current annual SME IT budgets compared to 2013 under UK GDPR.[108] Research on start-ups in Germany found that while the UK GDPR can stimulate innovation, the cumulative impact of privacy regulation reduces start-ups' access to data making certain products and technologies harder to develop, especially in the field of big data and AI. Also, data protection regulation might lead firms to abandon products or product ideas that are judged, possibly incorrectly, to be incompatible with the regulation.[109] UK firms have also reported that the current regime can be complex to interpret and apply, especially for small and medium businesses.[110] Such complexity is understood to be a barrier to compliance and lead to uncertainty, and potential over- or under-compliance (through strategy or error).[111]

211. Many of the reforms within the Act are designed to encourage firms to better harness the power of the data already available to them and to encourage more firms to use data in decision making and for efficiency gains. Some proposed measures will specifically increase data

[107] European Commission (2020) Two years of application of the General Data Protection Regulation
[108] Christensen et al.(2013) The Impact of the Data Protection Regulation in the E.U.
[109] Martin et al. (2019) How Data Protection Regulation Affects Start-up Innovation
[110] The European Commission's (2020) evaluation of the GDPR identified challenges for organisations, in particular SMEs.
[111] Christensen et al.(2013) The Impact of the Data Protection Regulation in the E.U. To note, this is a forecast of the proposed GDPR rather than an ex-post impact evaluation.

processing for specific activities, such as those in relation to R&D. In our initial analysis note we conducted a literature review that found data is a factor of production and driver of firm-level productivity, with more (or higher quality) data driving higher output through lower costs, better coordination and improved products.

212. Since the consultation stage, we have carried out a further literature review looking at the relationship between data use and productivity. The review found that there is overall agreement in the hypothesis that an increase in data use leads to an increase in businesses productivity and therefore GVA as a result, however, the impact of data at the firm level is complex and varies across sectors and industries. Its value to organisations is widely reported in terms of driving greater firm-level efficiency, enabling new products (often personalised and free), and powering new technologies through big data, AI and data analysis.

213. DSIT have carried out research into the role of data in the UK economy and its impact on productivity growth. The study supports the hypothesis that data capital boosts labour productivity growth, although highlights that increased data intensity of intangible assets is expected to hinder commercial knowledge diffusion and diminish TFP. The study splits data investment into three categories; databases, data stores and data intelligence, each of which make up around 33 percent of data assets. Of these categories, only data intelligence is shown to have a significant impact on labour productivity growth, suggesting that the relationship between data capital and productivity is primarily driven by data intelligence. Total investment in data assets is shown to be driven by five industries, in 2019, manufacturing, wholesale and retail trade, information and communication, financial and insurance activities, and professional, scientific and technical services accounted for 69% of total investment. The potential for data capital to contribute to productivity growth is shown to be substantial yet the extent of its impact is dependent on the nature of the activity, increased sharing and skills are expected to boost productivity but are hindered by the tendency to exclusive data access.

214. There are many mechanisms by which the acquisition of data can improve and increase outputs. In essence, data-intensive analytics can be used to discover new insights which enhance decision-making and optimise processes or coordination. This includes quality improvements in existing products and services, cost reduction in delivering products and services, (e.g. analytics can reduce the costs of delivery, better credit scoring can reduce the cost of delivering, lower wastage and dynamic efficiency from improved data on performance), and greater innovation in development of new products and services.[112]

215. The measures relating to reducing barriers to are likely to generate an increase in responsible data use, for example, creating a limited list of legitimate interests for which businesses can use personal data without applying the balancing test will give organisations more confidence to process personal data without being concerned about liability. Similarly, helping organisations building or deploying AI tools to interpret existing data regulation and simplifying legislation where appropriate will facilitate new entrants to data-driven markets and help to ensure beneficial data processing is not impeded.

216. Using the UKBDS findings, we are able to estimate the total number of businesses that could be impacted, however, in reality we expect that only a proportion of these businesses are

[112] Additional examples include the development of new financial products, smart contracts and supply chain tracking services, new products that rely on applications such as online maps or translation, and new consumer goods based on analysis of purchasing trends. From World Bank (2021) World Development Report 2021: Data for Better Lives

likely to change their activities. We have used evidence from the UKBDS and ONS to help inform the estimates of the true proportion of firms impacted and where evidence is less readily available, we have gone on to conduct sensitivity analysis which can be found in the risks and assumptions section of this IA.

Table 25: Estimated number of businesses expected to increase their data use as a result of these reforms.

Reform	Upper bound number of organisations potentially affected[113]	Proportion of these organisations actually affected (assumed medium scenario)[114]	Total estimated number of businesses affected
Creating non-exhaustive list of ways businesses can use data	4,881 businesses that analyse data, don't find GDPR clear, and have been prevented from implementing a new or improved product as a result, 39% of which use data to improve marketing or sales performance[115]	25%	379
Simplifying rules for data processing for R&D	428 businesses that analyse data, adopt R&D, don't find GDPR clear, and have been prevented from implementing a new or improved product as a result	35%	150
Enhancing the approach to explainability and accountability for fair processing in the context of profiling in AI systems	5,678 businesses that adopt AI, don't find GDPR clear, and have been prevented from implementing a new or improved product as a result	10%	568

217. The underlying methodology of the productivity modelling has not changed since the previous analysis, however due to slight differences in the structure of some UKBDS questions, and the compounded impact of decreases to relevant metrics, the business volume figures have reduced. As can be seen in the table, we estimate approximately 1,000 businesses may change their use of data as a result of these policies.

218. In order to estimate the impact of our specific reforms on the we rely on the significant relationships identified in three academic papers; Bahkshi et al. 2014,[116] Brynjolfsson et al. 2011[117] and Bassetti et al. 2020.[118] Bahkshi et al. find that a one-standard deviation increase in the use of online data is associated with an 8% higher level of productivity (TFP). Looking at

[113] UK Business Data Survey, 2024
[114] Not all firms would increase their data sharing as a result of these measures. Where evidence is not available, we have applied informed assumptions that are tested in the sensitivity analysis section further into the document.
[115] UK Business Data Survey, DSIT, 2024
[116] The analytical firm: Estimating the effect of data and online analytics on firm performance, Nesta, 2014
[117] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486
[118] Bassetti, T., Borbon Galvez, Y., Del Sorbo, M. and Pavesi, F., Artificial Intelligence – impact on total factor productivity, e-commerce and fintech, EUR 30428 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-24694-7, doi:10.2760/448034, JRC122268.

decision making based on data and business analytics ('data driven decision making' or DDD), Brynjolfsson finds firms adopting DDD have output and productivity 5-6% higher than what would be expected, all else being equal. Bassetti et al. look at the relationship between TFP, wages and AI patents; the headline finding is that every AI patent graded contributes to a higher TFP by 3.2%.

219. There are various ways of understanding the role of data in the creation of value by organisations: as a factor of production, as a productivity enhancer, as a by-product, or as an output itself. We do not attempt to directly quantify data as a primary output or a by-product itself. Instead, we consider data as an input to businesses, as a factor of production driving output and productivity.

220. Data may also be conceptualised as a driver of total factor productivity (TFP) by providing additional information or insight. Increases in TFP reflect a more efficient use of factors of production, often thought to be driven by technological advances. Businesses use data along with various technologies to become more productive by improving their business processes, learning more about their clients and customers, developing new products, or making better data driven decisions. In this context, the addition of data to the production process makes the main factors of production more efficient, leading to better performance.

221. Quantifying, and particularly monetising, the value of this data poses a difficult challenge. For example, defining the volume of data in terms of bytes does not reflect the quality of that data in terms of its many characteristics (such as accuracy, timeliness, and the degree to which it is processed). The value of data will vary greatly according to context and there is limited information on prices. Nonetheless, rather than omitting a monetised impact from our analysis, we use GVA as one potential way to capture the value added to the economy on a top-down basis. Through the mechanisms described above, we expect that data use will improve TFP, improving allocation of resources and coordination to increase firm-level output with all other inputs unchanged.

222. In order to estimate the impact of the package of reforms on UK Gross Value-Added (GVA), we also use data from the UKBDS findings in the table above. We use the estimated number of organisations currently using data where legislation might have held them back. We assume only a subset of these firms will actually benefit from rules revision, this is both with an aim to remain conservative in our analysis but also as we don’t expect legislation to be the only, or main, hindrance to all the firms that answered positively to this question. As well as the number of organisations not currently using data at all, that could potentially benefit from doing so. As well as UKBDS data we also use the McKinsey Digital Survey to estimate how many businesses are applying AI to data.

223. We use these academic findings to estimate the economic impact of the reforms, based on the general consensus observed across studies regarding the scale of impacts. We also ensure that we are capturing all uncertainties by:

- Carrying out sensitivity analysis on all assumptions used in the modelling.
- Making this a focus area for future analysis by building capacity to monitor and evaluate the impact of data reforms on productivity. This requires observing the impact on the market over a period of time, and for this reason the department aims

at conducting longitudinal studies looking at the relationship between productivity and data use (more details of this are in the monitoring and evaluation section).

224. We make the following assumptions when looking at each reform:

- A proportion of potentially affected organisations would increase data use, which in total constitute a fraction of the estimated number of firms using data
- The impact of additional data use on productivity is linear: in other words, the effect of increasing data use by 10% is the same regardless of whether the organisation starts from a low or a high initial level of data use. This is a simplifying assumption to:
    - Reflect the lack of evidence in the literature indicating increasing or diminishing marginal returns.
    - Ensure we remain conservative in our analysis. For example, if we were to assume diminishing marginal returns, this would greatly increase total estimated benefits as the majority of firms in the UK are classified as micro and start from a lower level of data use than large firms.[119]

225. In order to calculate the total impact on GVA of each reform, we take the total number of firms that analyse data to gain insight and knowledge, and the proportion of these that find current guidelines hard to follow and have therefore been stopped from implementing a change or a new product into business practices. We then assume on the likely increase in data use as a result of these measures. All assumptions in the model are tested in the risks and assumptions section of the IA.

226. By applying the assumptions and the findings from Bahkshi et al. and Bassetti et al. we can estimate the expected increase in productivity as a result of the increase in data use from each measure. The results of this analysis can be seen broken down by measure below:

Table 26: Estimated impact on UK productivity of each proposed reform, 2024 prices

Reform	Average annual benefit to UK productivity (GVA) £million
Legitimate Interests	11.9
Research Purposes	9.1
AI and Machine Learning	14.8
Total	35.8

227. We consider a GVA approach to be a clear and empirically sound method to appraise the value of data. Studies that attempt to estimate the value of personal data are typically based on income, market or contingent valuation. However, these are typically context-specific and may therefore be unreliable or inaccurate in a more general context of analysis.

[119] As observed in DSIT:UK Business Data Survey, 2021

228. In order to model this impact, we have had to make assumptions for policies where existing evidence is weak. More on these assumptions can be found in the sensitivity analysis section. Testing these assumptions by using a low, medium and high scenario tells us that the total GVA impact is between £15.0 million and £73.6million.

Table 27: Estimated impact on UK productivity of each proposed reform split by scenario, 2024 prices

Reform	Impact on UK productivity (GVA) (£million) Low scenario	Impact on UK productivity (GVA) (£million) Medium scenario	Impact on UK productivity (GVA) (£million) High scenario
Legitimate Interests	2.4	11.9	35.8
Research Purposes	5.2	9.1	15.6
AI and Machine Learning	7.4	14.8	22.2
Total	**15.0**	**35.8**	**73.6**

Increased Interoperability and Trust of Digital Identity Systems

229. More detail on the calculation of the monetised value of potential benefits of the proposed Digital Identity reforms can be found in the published Digital identity and attributes - De Minimis Assessment.[120] In this Data (Use and Access) Act Impact Assessment we provide an outline of the main monetised benefits of the proposal. This analysis looks at four potential use cases and compares the benefits across 3 different scenarios.

230. These benefits are classified as indirect as impacts are subject to the private sector organisations adopting digital identities and some are further contingent on customers/individuals using digital identity methods for ID verification. Whether the private sector will adopt digital identities is difficult to predict as it will depend on various unknowns, and so it is not possible to accurately predict the behaviour change that far into the future. The private sector organisations that do adopt digital identity verification methods will incur organisational change costs, but indirect benefits that have been modelled will only start to accrue, if and once, customers/individuals start using digital identities methods of ID verification.

231. DSIT analysts have estimated these indirect benefits from the perspective of the private sector market of digital identity services. These estimates were produced on the basis that different government data sets are required depending on the use case. Higher value transactions (like purchasing a home) were selected as they require higher levels of identity assurance, and DSIT analysts expect that these will generate larger economic benefits. As the number of use cases increases, additional economic benefits may accrue. Additionally, the utilisation of reusable digital identities may increase economic benefits further. They have not been considered in this impact assessment at this stage.

232. DSIT analysts note that the benefits calculations in this impact assessment relate specifically to the implementation of these measures. The economic benefits estimated in this

[120] Digital identity and attributes - De Minimis Assessment DSIT, 2024

analysis focus entirely on the private sector digital identity market. Since this analysis was carried out, Government has announced a Government-issued digital identity product. This analysis does not cover the potential costs or benefits of this Government-issued digital ID. Government will continue to assess the market as policy work develops. Additional analysis will be produced in to assess the impacts of a government-issued Digital ID on the economy.

233. All scenarios are compared to the steady state base case. The total number of digital identity checks we expect to take place under the steady state is detailed in the table below, it is assumed that all of these checks will become digital and that the proxies used to estimate the number of checks in the research project capture the majority of checks within these use cases. For the steady state to occur, this requires different government data sets to be opened depending on the use case. We understand that the majority of use cases rely on passport data. These use cases cover Disclosure and Barring Service (DBS) checks, Return To Work (RTW) checks, travel and ticketing, home buying and trusted financial transactions. The only use case that requires a different dataset is for the qualification checking use case. Qualification checking either needs access to professional bodies datasets or requires something simpler like a portal for uploading qualification certificates

Table 28: Total number of annual DI checks at steady state by use case

Category of checks	Total number of checks
DBS checks	7,174,588 - 9,694,574[121]
RTW checks	8,225,000
Qualification checks	1,727,250
Travel authorisation and ticketing	259,595,875
Home buying	8,882,775
Trusted financial transactions	860,772
Total	287,726,253

234. A central, best- and worst-case scenario is modelled in which the number of years it takes for both the first Digital Identity checks to take place and the amount of years it takes to reach a 100% uptake level varies. In this impact assessment we will look solely at the central case and the total range of estimations, however more detail can be found on the best- and worst-case scenarios in the Digital identity and attributes - De Minimis Assessment.[122]

235. The indirect benefits for the 4 use case scenarios are split down into the following categories:

[121] Unlike for other DI checks, for DBS we have a forecast of the number of checks each year over the 10-year appraisal period. DBS has forecasted 7,174,588 checks in Year 1. The number of checks is expected to increase over time, and in Year 10 we expect the number of checks to be 9,694,574. See Appendix 2 in the Digital identity and attributes - De Minimis Assessment for forecasted checks for each year

[122] Digital identity and attributes - De Minimis Assessment DSIT, 2024

a. Employee Mobility

i. According to Deloitte analysis,[123] a fully functioning digital identity market may positively impact employee mobility by:

1. **Digitising the right to work checks process:** This process requires all employers to check the identity of the individual being hired and their right to work in the UK.

2. **Allowing digital qualifications checks:** Refers to the process used by employees to verify the qualifications of professionals being hired.

3. **Allowing digital employment status checks:** This is the EU Settlement scheme process run by the Home Office to allow EU citizens to remotely verify their identity through an app.

ii. Deloitte examined the benefits of using digital identity to reduce friction in employee mobility and predicted that digital identity checks may bring monetised benefits by:

1. I**mproving delivery:** New hires can reduce onboarding time by proving their identity digitally for right to work (RTW checks), to carry background checks and to provide proof of qualifications in a significantly faster, self-service way and receiving a real-time response and confirmation.

2. **Reducing costs:** Reduce administrative effort by minimising face-to-face and document verification for RTW, DBS and qualification checks.

iii. Deloitte also expects digital identity to bring the following second order indirect benefits to employee mobility:

1. **Increased efficiency in sectors with short notice periods:** Employees in industry with short notice periods or that are expected to start work immediately (e.g. hospitality) may be less likely to miss their start date due to lengthy and inefficient RTW checks.

2. **Productivity improvements:** Less trips may be required to issue the necessary documentation. This may particularly benefit shift workers with unpredictable shift patterns who may struggle to get their documents verified during the typical office hours.

3. **Reduce fraud:** Hiring workers with false credentials can lead to significant losses for businesses and consumers, especially in key sectors such as medical professions and aviation. Digital identity checks are more likely to detect fraudulent applications, and thus reduce the number of fraudulent workers hired, relative to traditional right to work checks.

[123] Economic analysis, Measuring the economic benefits of adopting digital identity, Deloitte, 2020, is available upon request.

b. Travel authorisation and ticketing

i. According to the Deloitte analysis, a fully functioning digital identity market can streamline the travel authorisation and ticketing process by:

1. **Allowing digital passport data verification when booking a flight:** Refers to the process of digital passport details collection by airlines. The airline may integrate a remote identity verification passenger may use to submit their details for real-time verification.

2. **Reducing in-journey ID verification:** Refers to the process of setting up digital identity checks to potentially reduce the numerous ID verification steps an individual need to carry throughout a journey (e.g. at check-in or when renting a car). Digital identification may be used at any step of the journey, starting from when the ticket is booked to when the luggage is collected. Stakeholders which may be affected by digital in-journey ID checks include travel booking agents, airports, railway stations, port authorities, airlines, car hire service.

ii. Therefore, using digital identity in the context of this specific use case may bring benefits through:

1. **Improved delivery:** Costs for businesses and individuals may be reduced as digital identity may allow faster and more frictionless travel. For instance, passport information could be instantaneously validated allowing real-time response and confirmation reducing wait times.

2. **Reduced costs:** Fines arising for individuals from incorrect data input may be reduced and the interactions required throughout a journey could be minimised (e.g. by providing an alternative to in-person passport controls)

c. Home buying

i. The full use of digital ID throughout the home buying process is expected to reduce friction. The considered steps of the home buying process are:

1. Setting up a savings account
2. Searching the property
3. Bidding for the chosen property
4. Requesting and receiving the funding (e.g. mortgage application)
5. Closing the contracts (e.g. mortgage contract)
6. Moving in (e.g. having to change doctors or schools)
7. Registering transfer of title at HM Land Registry

ii. Specifically, Deloitte estimates that applying digital identity in the context of home buying is expected to bring monetised benefits by:

1. **Improving delivery:** Digital identity checks may streamline the home buying process and offer real-time response and confirmation of the

various steps required for home ownership (e.g. when applying for a mortgage)

2. **Reducing costs:** Using digital identity may reduce administrative effort from face-to-face and document verification.

d. Trusted financial transactions

i. According to Deloitte, a fully functioning digital identity market is expected to help ensure that financial transactions are secure by:

1. **Improve customer on-boarding to financial services products** (e.g. bank accounts): Refers to the process used by financial services to check the identity of their customers during the onboarding process or when accessing a service.

2. **Authenticate transactions to reduce fraud:** The use of digital identity products may allow customers to verify their identity when needed, for instance when transacting with an institution online. It may also allow organisations to prove to their customers that they offer a legitimate service, for instance by being a member of the trust framework.

ii. Therefore, according to the Deloitte analysis, using digital identity within this use case is expected to bring monetised benefits by:

1. **Improving delivery:** Digital identity may provide a more cost-efficient alternative to in-person interaction during on-boarding identity checks (KYC checks) for businesses and individuals when opening a bank account. Digital identity gives users a self-service option for identity verification and secure transactions, which saves time by offering a real-time response.

2. **Reducing costs:** Using digital identity may reduce administrative effort from face-to-face and document verification and lowers the risk of fraud through upfront ID check.

236. The central estimation of the ten-year undiscounted value of the benefits unlocked by a fully realised digital identity market for the four use cases together is £7012.1m. Whereas, we estimate that the total value of the benefits worst- and best-case scenario may be £4,926m and £8,502m respectively.

Table 29: Indirect benefits of Digital Identity schemes: total, £, millions, 2024 price year

Benefits	Annual value of the benefits[124]	Benefits over the 10-year appraisal period (undiscounted) (£million) Central case estimate	Benefits over the 10-year appraisal period (undiscounted) (£million) Best case estimate	Benefits over the 10-year appraisal period (undiscounted) (£million) Worst case estimate
Employee mobility (including second order)	334.9	2,092.8	2,880.1	1,271.9
Travel authorisation and ticketing	339.5	2,376.6	2,716.1	1,765.5
Home buying	152.0	1,064.2	1,216.2	790.5
Trusted financial transactions	211.2	1,478.4	1,689.6	1,098.2
Total	**1,037.7**	**7,012.1**	**8,502.0**	**4,926.1**

Remove the requirement for paper birth and death registers moving to an electronic register

237. The data on the volume of births and deaths shows that 613,936 births and 607,922 deaths were registered in the UK in 2020. The number of deaths registered was 14% higher compared to 530,841 in 2019 and significantly higher than any year back to 2010, [125] and birth figures for 2019 were 640,370. The Home Office makes no official forecast of future volume or birth and death registration. For the purpose of this IA, ONS figures for births and deaths for each year between 2010 to 2019 were used to form a low, central and high assumption. Over the 10 years, the low assumption was calculated using the minimum of these values, the high scenario was calculated using the maximum and the central scenario was calculated using the average. Births and deaths were summed and rounded to give total registrations to be used in estimates. See the table below

Table 30: Volume of births, deaths, total registrations and scenario volumes, 2010 - 2019

Estimate	Births	Deaths	Total Registrations
2019	640,370	530,841	1,171,211
Low	640,370	484,367	1,124,737
Central	694,117	514,554	1,208,671
High	729,674	541,589	1,271,263

[124] The annual values of the benefits assume that the digital identity market has reached its steady state.

[125] https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/impactofbirthsanddeathsonukpopulationchange/2020#:~:text=In%20the%20calendar%20year%20of%202020%20there%20were%2090%2C173%20deaths,fall%20of%2029%2C489%20from%202019.

238. The data used to calculate the costs of tasks relating to the time taken by a superintendent registrar, registrar and administrative worker are taken from the figures used in the Registration of Births, Deaths, Marriages and Civil Partnership (Fees) Regulations 2016.

239. Costs of issuing registers and blank stock and the associated resource and postage costs have been obtained from the General Register Office (GRO) which is responsible for providing stock to the registration service. Approximately 5,000 new registers are dispatched every year.

240. Wherever employee time has been costed, a low, central and high wage per minute for both registrar and superintendent registrars have been used. The gross wage per hour was calculated using Local Registration Service (LRS) data for 2024 salaries. The net annual salary was taken, and the national insurance and pension were added on to get the gross salary. This was then divided by 210 days,[126] then divided by 7 hours. Table 2 presents these below. Within the IA, these figures are divided by 60 minutes, to give the per minute value for calculations

241. **Table 31:** Gross wage per hour (£/hr) for superintendent registrars and registrars, 2024 prices.

Estimate	Superintendent Registrar	Registrar
Low	28.30	23.71
Central	44.12	31.28
High	72.36	46.45

Registration service

Administration of paper registers

242. Resource savings for local authorities: there is a reduction in registrar time in printing off the register page, putting it into the register folder and securely putting away the register in the safe. Currently, the registrar enters the details of the birth or death into RON which generates the register page for checking and signing by the informant(s) and the registrar. The registration is complete when the register entry has been signed by the registrar and informant(s). That signed, paper, copy of the registration is retained in register folders which then is replaced back in the safe.

243. The action to print the register page, put it into the register and lock the register away takes approximately two minutes,[127] within a range of 1.75 to 2.25 minutes. The cost per hour for a registrar is given in the table above. The cost of time taken is multiplied by the number of births and deaths per year (low, central and high scenario) from the ONS. The estimated savings in

[126] The average number of days worked by registrars by year across all 174 local authorities. This figure has been agreed by a sub-committee of the National Panel for Registrars.
[127] Average time was identified as part of the process for developing fees by the Home Office. Time and motion studies are conducted by the National Panel for Registrars.

salaries lie in a range of £7.2 to £20.6 million, with a central estimate of £11.7 million (PV) over 10 years in 2024 prices.

Retrieval of paper registers

244. Resource savings for local authorities: registrars will not have to retrieve the paper register from the safe and lock it away again each time they issue a birth or death certificate after the original registration. The RON system is used to produce birth and death certificates electronically at the time of registration and subsequently. On each occasion, the registrar has to retrieve the legal, paper register from the safe and return it there again after the certificate has been issued. For the purposes of the IA, it is assumed that the number of certificates issued by the registration service (excluding those issued at the time of the initial registration) is the same as the amount issued by GRO. The resource saving has been made based on one minute of registrar time for 31,250 (increased/decreased by 10% for high/low scenarios) birth and death applications received each year (taken from information provided by the registration service for requests for certificates once the register has been closed and filed away). The time taken is varied to give a low estimate of 0.75 minutes and a high estimate of 1.25 minutes, as per standard practice of estimating ranges in Impact Assessments. The estimated cost is calculated as:

registrar time saving (hrs) x registrar wage (£/hr) x volume of birth and death applications in a year

245. This amounts to a savings in salaries in the range of £0.1 to £0.3 million with a central estimate of £0.2 million (PV) over 10 years in 2024 prices.

Certification process

246. Resource savings for local authorities: superintendent registrars will not have to complete the certification process. Currently, each registration is certified (the process is detailed above) individually by a superintendent registrar. The new process will not require a formal certification to take place which will save two minutes of superintendent registrar time. A high value of 2.25 is assumed and a low value of 1.75 minutes. The cost for a superintendent registrar, per hour, is given in Table 32. The total saving is calculated as:

time saving x cost of superintendent registrar x total number of births and deaths per year.

247. This amounts to savings in salaries in a range of £8.6 to £32.1 million, with a central estimate of £16.6 million (PV) over 10 years in 2024 prices.

Home Office

Supply of manual register folders

248. Reduction of cost to Home Office regarding supply of manual register folders. The cost to GRO (who supply the register folders to the registration service) is £22.38 for each birth or death register and a total of 4,113 registers were issued to the registration service in 2023/24. The reduction in cost is estimated as:

Total number of registers x cost to GRO of each register.

249. This represents an annual saving of £92,049. This is a saving of £0.9 million (PV) over 10 years in all scenarios.

Supply of registration paper

250. Reduction of cost to Home Office regarding supply of loose leaf and water marked registration paper. Loose leaf, water marked register paper is supplied to the registration service by GRO. During 2023/24 a total of 4,113 registers were issued by the local registration service when registering births and deaths in England and Wales. A set of paper is needed for each register per year at a cost of £1.89 per pack of 300 sheets, this will save £7,774 each year, with estimated savings of £0.1 million (PV) over 10 years, for all scenarios.

Distribution of registers, paper registers and registration paper

251. Reduction in secure delivery costs for distributing register covers and registration paper. The register folders and loose leaf, registration paper needs to be sent by a secure delivery service at a cost of £4.50 per parcel. The registration service order register folders and paper as required throughout the year. The number needed is dependent on the number of birth and death registrations in each district and this figure varies considerably across the country. With 4,113 registers sent and assumed to continue at this rate across the appraisal period, this equates to annual savings of £18,508.50. The total savings is therefore estimated at (PV) over 10 years, for all scenarios.

Table 32: Total monetised benefits of the reform, £million, 2024 prices

Total Monetised Benefits	Low scenario	Medium scenario	High scenario
Supply of manual register folders (GRO)	0.9	0.9	0.9
Supply of registration paper (GRO)	0.1	0.1	0.1
Distribution of registers and paper registers and registration paper (GRO)	0.2	0.2	0.2
Administration of paper registers (LRS)	7.2	11.7	20.6
Retrieval of paper registers (LRS)	0.1	0.2	0.3
Certification process (LRS)	8.6	16.6	32.1
Total Benefits	17.1	27.3	54.2

Improved interoperability across health and social care systems

252. **Interoperability benefits:** Broader interoperability benefits are expected to be achieved through the adoption of common information standards, which facilitates interoperability alongside the required interoperable architecture and infrastructure. These have been split into cash-releasing and non-cash releasing below:

Cash-releasing benefits:

i. **Cost savings from reduction in duplicate tests (diagnostic and lab tests):** Improved access to comprehensive patient data, and more up-to date and accurate patient records is expected to minimise unnecessary duplicate tests, procedures and medication prescriptions, leading to a reduction in health and social care costs.

Research has shown that up to 30%[128] of medical tests, and 20-30% of blood tests[129] are duplicated. Interoperable systems with integrated decision support could assist in minimising unnecessary tests due to lack of, or poor patient data. Data suggests an average reduction in duplicate laboratory tests of 8.8%[130] from the implementation of decision support within the electronic health record, whilst ensuring interoperability at national level could contribute to reduced duplicated medical imaging of 10%.[131]

The ten-year present value cost saving from the reduction in laboratory and diagnostic imaging tests, attributable to information standards adoption and DUA is £65.4 million.

ii. Non-cash releasing benefits: **Reduction in cost of excess bed days, from reduction in transition and non-transition medication errors:** Improved patient safety is expected from a reduction in errors resulting from re-entering information across systems and care settings, and by ensuring clinicians and carers have the data they need on patients during transfers, discharges and referrals.[132] Also, enhancing patient safety can mitigate adverse drug reactions by minimising the risk of medication errors and overprescribing. This would reduce the resources that the NHS dedicates to medication errors, and thus lead to a reduction in the number of excess bed days.

A University of Manchester study showed that implementing the DAPB4013 standard for Medicine and Allergy/Intolerance Data Transfer could lead to a 40% reduction in the number of transition medication errors and episodes. This could lead to 14,275 fewer days of inpatient care, saving around £6.59 million per year and preventing 20 people dying per year from these errors nationally.[133]

The estimated ten-year present value cost saving from reduction in excess bed days from reductions in transition medication errors, attributable to DUA is £16.1 million.

E-prescribing, enabled by interoperability, was shown to result in up to a 6% reduction in medication errors in Estonia and a 15% reduction in prescription errors in Sweden.[134]

[128] A new EPR can help stop unnecessary medical tests – EPR (airedale-trust.nhs.uk)
[129] Electronic Patient Record (EPR) benefits realisation case study (ouh.nhs.uk)
[130] A preliminary look at duplicate testing associated with lack of electronic health record interoperability for transferred patients - PMC (nih.gov)
[131] EUR-Lex - 52022SC0131 - EN - EUR-Lex (europa.eu)
[132] Information standards for health and adult social care in England - GOV.UK (www.gov.uk)
[133] Meds_Interoperability_full_report_Elliott_et_al_2023.pdf (manchester.ac.uk)
[134] EUR-Lex - 52022SC0131 - EN - EUR-Lex (europa.eu)

The benefits of interoperability go beyond just transition errors. Health and social care providers and patients could also benefit from the reduction in other prescription, administration and monitoring errors. The cost saving from prevented excess bed days from non-transition medication errors is estimated to be £5.1 million each year, with an assumed reduction in 80 deaths – this is based on a reduction in number of severe and avoidable non-transition medication errors.[135]

The estimated ten-year present value cost saving from reduction in excess bed days from reductions in non-transition medication errors, attributable to DUA is £5.8 million.

iii. **Value of time saving (patient record access):** Working with standardised data and interoperable systems would save staff time due to quicker and more efficient access to patient data. This would remove the need for manually retrieving physical notes or accessing multiple records as well as reduce the time spent on information gathering or reviewing data. It would result in time saving for health and social care workers, which could be refocused on more value-add activities to the benefit of patients. It was estimated that the joining up of direct care within the OneLondon programme had a time saving per system access of at least 0.5 minutes, with potential for up to a 20 minute time saving on more complex cases.[136] Scaling this time saving estimate up for the estimated number of patient accesses across England[137], it is estimated that the ten-year present value of staff time saved attributable to regional interoperability and information standards under DUA is £31.8 million.[138]

iv. **QALY value of prevented fatalities from medication errors, value of time saved reporting errors, and reduction in reporting costs for patient safety incidents (PSIs):** As described above, information standards and interoperability are expected to reduce the prevalence of avoidable medication errors. In addition, access to real-time patient data can support providers making better informed decisions. Standards can reduce the risk of miscommunication or misunderstandings which can compromise patient safety and hence prevent patient safety incidents. This reduction in medication errors and patient safety incidents can reduce the time spent reporting and investigating such errors for staff, as well as the consequences for patient health and fatalities.

Studies show that the average time spent reporting a medication error is 4 minutes per error.[139] This creates the opportunity for significant time savings from the reduction of medication errors. Based on the value of staff time per minute and a 6.8 million reduction in the number of medication errors[140], the estimated value of time

[135] Calculated based on number of patient errors by category and proportion of severe and avoidable errors across prescription, monitoring and administration errors. Source: https://qualitysafety.bmj.com/content/30/2/96.long#DC1
[136] Economic Analysis of Digital Health Infrastructure: The Case of OneLondon's Impact on Time Efficiency and Safety in Healthcare Services
[137] Based on number of outpatient and A&E attendances in a year
[138] Based on the average NHS staff salary per minute of £0.37, based on https://digital.nhs.uk/data-and-information/publications/statistical/nhs-staff-earnings-estimates/september-2023-provisional-statistics
[139] Prescribing error reporting in primary care: a narrative synthesis systematic review - PMC (nih.gov)
[140] Calculated based on a 6% reduction in non-transition medication errors per annum in line with evidence from Estonia (EUR-Lex - 52022SC0131 - EN - EUR-Lex (europa.eu)). This is applied to the total number of non-transition errors per year (100.7 million, as

saving is £10.1 million nationally each year. The ten-year present value benefit attributable to DUA is £11.4 million.

In the year to June 2022, there were 2.5 million patient safety incidents in England.[141] It was reported in a study by Adam et al that 7.9% of patient safety incidents were related to problems with Electronic Health Record interoperability.[142] In addition, the average cost per incident form is £337.16 – hence there is a potential cost saving of up to £6.76 million per year from the reduction in patient safety incidents from improved regional interoperability facilitated by DUA. The ten-year present value benefit attributable to regional interoperability and information standards under DUA is £158.0 million.

The value of prevented fatalities from transition and non-transition medication errors has also been quantified in terms of the additional Quality-Adjusted-Life-Years (QALYs) gained. This is calculated based on the number of estimated deaths prevented from a reduction in medication errors, DHSC data on fatalities by age due to adverse drug reactions (ADRs), average life expectancy[143], and using the Green Book 2022 estimates of a QALY (£70,000) which is adjusted for each age group.[144] The benefit is further apportioned based on assumptions outlined below to attribute to information standards and DUA. The ten-year present value of QALYs gained due to the reduction in transition and non-transition medication errors attributable to regional interoperability and information standards under DUA is £30.3 million, this benefit is discounted at a 1.5% discount rate in-line with Green Book guidance for QALY health effects.[145]

For a full breakdown of the expected impacts of the DHSC measure, please refer to the Open Data Architecture Information Standards Impact Assessment.[146]

Delivery of the National Underground Asset Register

253. This analysis has been taken from the NUAR Impact Assessment 2024[147] published by DSIT. For a more detailed breakdown of some of the indicative sector specific costs and benefits please refer to the NUAR Impact Assessment directly.

a. Underground asset strikes have an associated cost, both direct and indirect, which can range from administrative costs and the cost of repair, to wider business disruption, traffic delays and programme overrun costs. NUAR will support the reduction in asset strikes by reducing the likelihood of potential interpretation errors that stem from these various data-related issues.

---

per https://qualitysafety.bmj.com/content/30/2/96.long#DC1). In addition, a 0.7 million reduction in transition errors is included (based on a University of Manchester study -(PDF) Estimating the impact of enabling NHS information systems to share patients' medicines information digitally (researchgate.net))

[141] https://www.england.nhs.uk/publication/national-patient-safety-incident-reports-up-to-june-2022/

[142] The Impact of Electronic Health Record Interoperability on Safety and Quality of Care in High-Income Countries: Systematic Review - PMC (nih.gov)

[143] National life tables – life expectancy in the UK - Office for National Statistics (ons.gov.uk)

[144] The Green Book (publishing.service.gov.uk) - QALY value of £70,000 is adjusted for age group using EQ-5D scores - DSU Age based utility - Final for website.pdf (sheffield.ac.uk); nice.org.uk/guidance/ng90/documents/economic-report-3

[145] The Green Book (publishing.service.gov.uk)

[146] Open Data Architecture Information Standards, DHSC (2024)

[147] NUAR Impact Assessment, DSIT, 2024

b. As part of the benefits appraisal, a comprehensive academic and industry literature review was undertaken to understand the scale and potential costs of strikes. The average cost of a utility strike also varies across different utility categories - for example, strikes to high voltage cables and high pressure gas pipelines have a far higher cost than strikes to fibre optic cables.
c. The average direct cost per strike is estimated to be £3,371 (in 2021 prices), this is used directly in our analysis. The cost per strike ranges depending on the type of asset struck, from c£680 for the mean Telecoms strike, to £5,375 for the mean water infrastructure strike. Indirect benefits methodology is set out in the next section. This methodology accounts for the range in costs per strike, and for the relative frequency of each strike type.
d. A widely reported industry statistic of 60,000 strikes per year[148] on buried service pipes and cables per year was used as the basis of the strike reduction benefits. The total economic costs of utility strikes are therefore estimated at £2.4bn a year
e. A significant challenge has been identifying what proportion of strikes could be avoided with better data. Those same industry reports[149] categorise strikes based on the cause of the incident. Those linked to inadequate plans and on-site procedures for using data made up around 30% of total incidents. This analysis conservatively assumes that a 15% reduction in asset strikes could be achieved if (a) all asset owners are onboarded to NUAR and (b) all excavations use NUAR on digs. These effects are factored into the benefits analysis, see section “Apportioning benefits across the appraisal period”.
f. However, once NUAR is fully operational, this percentage could increase as the user feedback mechanism in NUAR could encourage asset owners to improve their data quality in response to user feedback, enabling the full 30% of causes to be mitigated.

Other indirect benefits

254. For the other indirect benefits of reducing strikes, the reviewed literature[150] estimated the indirect costs of strikes based on a series of industry case studies. Indirect costs include (but are not limited to) programme overruns and costs to local highways from closing/redirecting traffic.

255. The study found that these indirect strike costs are, on average, 29 times larger[151] than direct costs, so this scale factor is applied to estimate the full scale of utility strike costs. This gives us the full direct and indirect strike costs of £2.4bn (2021 prices) - made up of £0.2bn direct, and £2.2bn indirect. A full breakdown of these benefits can be found in the NUAR Impact Assessment[152].

256. For the purposes of this impact assessment, all of these benefits due to strike avoidance are treated as indirect. A breakdown of how these indirect benefits are distributed amongst beneficiaries is set out further in the NUAR Impact Assessment151 - particularly to the public sector (Central Government and Local Authorities), business and wider society. For example, reducing traffic delays are considered a wider societal impact. The general reductions in costs to commercial enterprises (for example, by not needing to close business for the day if there are burst water mains or damaged gas supply) are considered a business impact.

[148] USAG, Strike Damages Reports, (2014 - 2019)
[149] USAG, Strike Damages Reports, (2014 - 2019)
[150] Makana, L., Metje, N., Jefferson, I., Sackey, M. and Rogers, C. 2019. Cost Estimation of Utility Strikes: Towards Proactive Management of Street Works, Infrastructure Asset Management
[151] Makana, L., Metje, N., Jefferson, I., Sackey, M. and Rogers, C. 2019.
[152] NUAR Impact Assessment, 2024 - DSIT

Indirect Benefits - Non-monetised

257. Whilst there is plenty of literature surrounding some of the wider indirect benefits, at this point we are unable to quantify these impacts robustly. We have instead provided an in-depth qualitative description of these benefits and the evidence supporting them.

Creation of Innovative and Secure Smart Data Schemes (DBT)

258. This analysis has been taken from the Smart Data Impact Assessment 2024 published by DBT. For a more detailed breakdown of some of the indicative sector specific costs and benefits please refer to the Smart Data Impact Assessment directly.

259. We do not expect any direct impacts to businesses from the primary legislation alone. While the primary legislation mandates the participation of data holders it is the secondary legislation that makes use of the mandating. There will be no immediate implications to the data holders until the secondary legislation utilises the powers.

260. By accelerating the implementation of Smart Data schemes consumers would realise the benefits sooner. Customers, Approved Third Parties (ATPs) and wider society are the main groups who could see benefits from Smart Data schemes. Indicative analysis within the DBT Impact Assessment has provided estimated benefits associated with speeding up the implementation of a Smart Data scheme in the telecommunications sector and a Road Fuel Open Data Scheme.

261. The extension of Smart Data will, in time, deliver new innovative services, stronger competition in the affected markets, and better prices and choice for consumers and small businesses, including through reduced bureaucracy. Competitive data-driven markets can reduce friction for established market players, and drive start-ups, investment, and job creation.[153]

262. Greater productivity and competition benefits enabled by personal data mobility have been estimated to increase UK GDP by £35 billion, which is 1.3% of GDP.[154,155,156] This figure, as reported by 'Ctrl-Shift',[157] has been quantified by aggregating the estimated value of data mobility for a wide range of sectors. For this analysis we have assumed that the benefits are spread evenly across the economy and therefore we have used this estimated annual GDP uplift as a basis for these benefit calculations.

263. We expect that the impacts of the primary legislation will indirectly bring forward the implementation of Smart Data schemes in secondary legislation. Due to this, DBT have

[153]BEIS: Next steps for Smart Data, 2020
[154] Ctrl-Shift (2018): "Data mobility: The personal data portability growth opportunity for the UK economy", £27.8bn based on 2017 GDP estimates. The GDP estimates have been uprated to 2024 prices. The economic estimates were developed using a GDP wide modelling approach, as such the accuracy of the impact on specific sectors is prone to significant discrepancies due to the differing use of commercial and economic impact of personal data within each sector.
[155] This estimate was also sense checked against a McKinsey data mobility benefit figure. This highlighted that open financial data has the opportunity to impact GDP by 1-1.5% by 2030.
[156] This figure, as reported by Ctrl-Shift, has been quantified by estimating the value of data mobility for a wide range of sectors as a proportion of GDP, adjusting this for the impact of that sector and applying the adjusted impact rate to economy-wide GDP. This quantification for data mobility is anchored in the financial services sector.
[157] This figure is based on assumptions about impacts in: energy, water, retail, transport, accommodation, publishing, telecommunications, financial services, insurance, pensions, education, health, arts, services and household services.

estimated the potential additional benefits of bringing forward the implementation of different Smart Data schemes, therefore running of the schemes for additional time.

264. To provide an indicative estimate of the potential benefits, DBT has focussed on the potential benefits associated with introducing Smart Data schemes in the telecommunications and road fuel sectors. In 2019, the telecommunications sector accounted for around 1.8% of the total general value added in the UK.[158]From this we can assume an annual benefit of £618m per annum with the full rollout of smart data schemes, facilitating greater personal data mobility. While the Road Fuel Open Data scheme is estimated to create net consumer fuel savings of between £3.1 and £18.4 billion over a 10-year appraisal period.[159]

265. The additional impacts of the primary legislation compared to the 'do nothing' scenario is expected to be:

a. ***Speeding up the delivery of smart data schemes***: bringing forward the benefits and the costs highlighted in the following sections.
b. ***Increasing legislative consistency***: increasing the overall benefit through more consistent schemes, with increased opportunity for interoperability and cross-sector innovation.
c. ***Enabling new schemes***: creating new benefits for customers, new opportunities for businesses to innovate but also new costs for industry to operationalise the schemes.

266. The following section looks at the wider cross-sector impact of Smart Data at the secondary legislation stage. Instead of focusing on quantitative scheme level impacts, the costs and benefits of Smart Data to customers, data holders, data recipients and regulators are considered in more detail qualitatively.

267. This analysis builds on the experience of Open Banking (as the only live Smart Data scheme), and considers wider evidence from the finance, telecommunications, energy, and pension sectors.

268. The benefits and costs from Smart Data schemes will vary in magnitude and accrue across varying timescales, therefore it has not been possible to make an overall estimated annual net direct cost or benefit. The indicative evidence included in the following sections does however support the view that Smart Data benefits will outweigh the costs.

269. This analysis is not fully quantified given that:

a. More detailed analysis will be required in future impact assessments alongside sector-specific secondary legislation.

b. Impacts will vary significantly across sectors, so until sector specific evidence has been collated and secondary impact assessments completed an overall assessment of the impact is not possible.

270. As well as more detailed analysis at the secondary legislation stage, DBT would expect additional research and further consultation for specific Smart Data schemes. This should

[158] ONS (May 2021): "Regional gross value added (balanced) by industry: all ITL regions". 61 was used for this purpose.
159 DESNZ (January 2024): Road fuel retail market consultation: impact assessment (publishing.service.gov.uk)

include research into and further engagement with relevant stakeholders, including data holders, ATPs, consumer and business groups, social enterprises, and charities.

271. Multiple groups could see benefits from the introduction of Smart Data. These include customers (consumers and businesses), data holders, data recipients (ATPs), and wider society. In some cases, benefits are transfers from one economic agent to another. This is to be expected of Smart Data schemes as they aim to reallocate benefits from incumbent data holders to customers and smaller, new entrants to markets.

272. An overview of the potential benefits to be gained at the secondary legislation stage can be found in the table below. For more information on how these might be measured please refer directly to the DBT Smart Data Impact assessment.

Table 33: Indirect benefits of the creation of Smart Data Schemes by recipient

Customers – consumers and businesses	Data holders	Data recipients – third party providers
• Access to new and innovative services, within and across sectors • Save time and effort – e.g. quicker and easier to access data and understand what it means • Save money – e.g. help finding and switching to better suited deals • Lower prices and higher quality due to increased competition • Opportunities for targeted support for vulnerable consumers • Improved security and fraud reduction through the use of secure APIs • Better and wider range of services, allowing customers to use their data more effectively to navigate the market.	• Opportunity to create new innovative services and improve existing services • More effective growth and competition for smaller providers • Reduced time and resources spent on dealing with fraudulent activity and responding to data access requests. • Opportunity to access wider product and performance data across the market e.g. can improve customer offer and market reach • Build customer trust and confidence through transparency • Improve technical infrastructure for data sharing and for wider business use, helping create more revenue. For example, supply chain optimization • Opportunity to work collaboratively with	• Access to new data creating valuable new markets and reducing the cost of market access • Opportunity to create new innovative services and improve existing services • Opportunities to compete with existing data holders and other third-party providers • Opportunities for government as the data recipient – e.g. HMRC using Open Banking payment services for PAYE • Potential for increased productivity for ATPs, and growth in the number of ATPs in the market • Regulations allow for ATPs to receive data in a consistent, easier to understand format allowing them to offer more effective services; and lower the

Customers – consumers and businesses	Data holders	Data recipients – third party providers
• Smart Data amendments may lead to a higher quality of services	regulators to shape future regulation • Clarifies that fines, financial penalties and charges must be set out in regulations, making it clearer to data holders and ATPs what they need to do/cannot do. • Amendments allow for schemes to be designed where regulations allow for data holders to charge for the data at a rate that exceeds expenses.	barriers to entry for ATPs. • ATPs receive a wider range of data, allowing them to offer a wider range of innovative services. • Clarifies that fines, financial penalties and charges must be set out in regulations, making it clearer to data holders and ATPs on what they need to do/cannot do. • The increase in effectiveness of enforcement is also likely to lead to a reduction in costs for authorised persons and consumers who use Smart Data schemes as they will likely receive more consistent coverage from data holders. • Amendments confirm that section 11 does not limit or restrict ATPs from charging for their services. This could increase the quality of the services they are offering and allow more effective long-term business models.

Primary Legislation Benefits of the Smart Data Amendments:

273. Group 2 of the Smart Data amendments enable a greater range of options for fee charging within a Smart Data Scheme.

274. This allows each Smart Data scheme to be designed effectively to meet the needs and objectives of the sector or market.

275. The added flexibility in fee charging provision and potential for commercial models, may allow for greater long-term sustainability for the services offered within Smart Data schemes. Due to competition, ATPs may also use the profits made from their services to re-invest them within the solution, allowing for higher quality services for consumers.

276. If a Smart Data scheme is designed to allow data holders to charge commercially for access to the data, then the data holders may be more incentivised to share this data and to improve the quality of their services and datasets.

277. If customers are required to pay fees to a data holder (and regulations allow for this) Introducing fees, this may limit the uptake of Smart Data schemes (the service was free for customers) and therefore reduce the benefits of scheme, particularly. if the regulations allow for fees to exceed expenses. Customers may also only be willing to pay for a service if it is with a trusted company due it being perceived as lower risk of fraud etc., meaning that they may be more likely to pay for the service with a large company than a small challenger business, limiting the competition benefits of a scheme.

278. For a more detailed breakdown of these benefits please refer directly to the DBT Smart Data Impact Assessment.

Privacy, trust and individual data rights

279. Typically, greater data protection may benefit data subjects to the detriment of other potential data users and vice versa, however, many avenues exist to encourage data use without compromising privacy.

280. By nature, any regulations around data protection affect both data controllers and data subjects. Any reforms should therefore carefully assess whether there will be significant impacts in terms of privacy, the rights and powers of data subjects, and potential impacts on trust in data use.

281. We have begun to consider the consumer side impact of measures on privacy and levels of trust in the data regime. We have assessed the evidence on the hypothetical value of privacy rights currently enshrined in the UK GDPR, and on the impact of trust on data sharing. Individual data sharing behaviours and the valuation of an individual's data can be impacted by a range of factors and contexts, making overall quantitative estimates challenging to obtain. As such, we have not monetised the impact of consumer trust within this impact assessment. Based on the existing evidence summarised below, we hypothesise that perceptions of trustworthiness of organisations and how they handle their data may influence some consumers' willingness to share data with that organisation, but we also recognise that this may be one of many factors influencing consumer behaviour.

282. Recent evidence suggests that UK consumer views of data use and data privacy is nuanced, context dependent, and gradually changing. Research conducted by the Responsible Technology Adoption (RTA) Unit[160] (formally the Centre for Data Ethics and Innovation) found 57% of adults agreed that data is useful for creating products and services that benefit them as individuals, an increase from 51% in 2021. A smaller proportion (44%) agreed that data

160 Public attitudes to data and AI: Tracker survey (Wave 3) (2023)

collection and analysis is good for society, however, this still represented an increase since 2021.

283. There are variations in views of the benefits of data, with people with higher digital familiarity being more likely to see benefits in data use compared to those with lower familiarity. Viewing data collection as good for society is also associated with being around three times more likely to reporting comfort with providing data to the government for policy development or delivering public services[161]. Similarly, a DMA survey[162] found that in 2021 45% of UK adults agreed that they would be happy for a business to share their personal data with other businesses if it gave them more tailored services or products, an increase from 31% in 2017. There is however variation by age group, with the increase in support most notable in those aged 18-45, and support among those aged 55 and over remaining largely unchanged since 2017. This suggests that while there may be a positive shift in attitudes towards data use, this may not be the case among all demographic groups.

284. Evidence suggests that support for data use is context dependent. The 2023 DCMS Participation survey[163] found that people were more likely to report being comfortable with data use for altruistic purposes than for financial purposes. For example, 67% of adults (16+) said they were comfortable with UK Governments using data to make public policies which help keep people safe, compared to 40% who were comfortable with data being used by private companies to improve their products or services.

285. A 2021 ICO survey[164] found that among those with a high level of trust and confidence in organisations storing and using personal information, the most commonly given main reason for this high trust was legislation. This was given as a 'main reason' by 17% of those with high trust, suggesting that for some individuals, legislation may have an impact on consumer trust in sharing, however the literature also suggests other factors, such as broader trust in the company, impacts stated trust in that business handling data. In 2020[165], a DCMS commissioned survey run by the ONS found 65% of adults (16+) said that 'knowing the company was compliant with data protection laws' would help improve trust in organisations when managing data about them.

286. There are still public concerns with data use, with factors beyond legislation affecting self-reported trust in data use. TheRTA 2022 survey[166] found that when controlling for demographic factors, people who said they trusted the government were more than three times more likely to say they were comfortable with providing the government with data for policy development, suggesting the level of trust in an organisation more broadly is associated with comfort in sharing data with that organisation. The RTA Unit found that public confidence that individuals have control over their data is divided, with 35% agreeing they have control and 40% disagreeing[167]. The same study provided participants with a list of potential risks of the use of data in society, and found that '*data will not be held securely and could be hacked or stolen'* and '*data will be sold onto other organisations or companies to profit from*' were the two most selected risks (57% and 55% of adults saying they felt these were risks). The ICO 2021 survey

161 Public attitudes to data and AI: Tracker survey (wave 2) (2022)
162 UK Data Privacy: What the Consumer Really Thinks?, DMA (2022)
163 Participation Survey, 2022-23, DCMS
164 Information Rights Strategic Plan: Trust and Confidence (Annual Track), ICO (2021)
165 DCMS commissioned ONS Opinions and Lifestyle Survey, 2020.
166 Public attitudes to data and AI: Tracker survey (wave 2) (2022)
167 Public attitudes to data and AI: Tracker survey (wave 3) (2023)

found that among those with low trust and confidence in companies storing data, 20% said this was because '*they sell your personal information to third parties'*. This was the most common main reason for low trust and confidence[168]. Maintaining high data protection standards will be important to maintaining consumer comfort and support for data use.

287. Evidence as to the extent that data protection concerns influence engagement with businesses is largely focused on stated rather than revealed behaviour. The ICO annual track survey[169] found that 73% of adults said that personal information being collected or used without their knowledge would stop them from using a company or organisation. A subsequent ICO survey found that 24% of people aged 16+ say they have switched companies because of data privacy concerns and 32% said they have requested removal of their personal data from a company's system. The DMA found that 40% of people rated trusting an organisation being in their top three factors making them happier to share data.

288. Some studies suggest that there can be a mismatch between stated preferences and revealed behaviours[170] with regards to providing data to businesses. This mismatch between stated and revealed preferences, which has sometimes been referred to as the 'Privacy Paradox', has been attributed to many factors, such as the benefit of service and perceived risks of sharing data[171], the framing of privacy choices, consumer knowledge and the level of friction in managing privacy setting[172].

289. Some studies have attempted to measure the value consumers place on data privacy through willingness to pay studies. For example, Which?[173] conducted a willingness to pay study in relation to the choice requirement remedy, requiring platforms to give consumers the choice not to share their data for personalised advertising. They found consumers' willingness to pay to not share their data ranged from 50p to £1.09, and the willingness to accept payment to share their data ranged from £1.06 to £4.03. This value was dependent on whether they were making an informed or non-informed choice but also varied in relation to the respondents' overall comfort with data sharing personal data, their age and gender.

Public views of data use for AI and machine learning.

290. Changes within this legislation aims to support the use of data for AI and machine learning. There is some evidence relating to consumer views of data being used this way. Currently, awareness of the use of AI in decision making is relatively low and support for its use varies by context. The Ada Lovelace Institute[174] found that in 2023, 19% of adults had heard of AI technologies being used to assess welfare eligibility, 34% had heard of it being used to assess risk of cancer and 35% had heard of it being used for assessing loan repayment risk or assessing job eligibility. A majority of respondents (88%) felt that the use of AI to assess risk of cancer will be beneficial, but support for other uses was lower, with only 43% viewing it as beneficial for assessing welfare eligibility and 37% viewing this as beneficial for assessing job

168 Information Rights Strategic Plan: Trust and Confidence (Annual Track), ICO (2021)
169 Information Rights Strategic Plan: Trust and Confidence (Annual Track), ICO (2021)
170 For example: Barth et al (2019) 'Putting the privacy paradox to the test: Online privacy and security behaviours among users with technical knowledge, privacy awareness, and financial resources or Reynolds et al (2011) Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours, 'Unwillingness to pay privacy: a field experiment', University of Cambridge 2010
171 Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics and informatics, 34(7), pp. 1038-1058
172 The Myth of the Privacy Paradox, Solove,D, The George Washington Law review (2021)
173 Which? The Value of the Choice Requirement Remedy (2020)
174 'How do people feel about AI?' Ada Lovelace Institute (2023)

eligibility.

There are some concerns with the use of AI for decision making. The study found that even where there was broad support for the technology, such as to assess risk of cancer, many people were still concerned about technology being less able than a human to account for individual circumstances, overreliance on technologies over professional judgement, and a lack of transparency about how decisions are made. In the case of assessing job eligibility, 64% were concerned that professionals will 'rely too heavily on their technology rather than their professional judgements' and 52% said that it would be more difficult to understand how decisions about job applications and assessments are made.

291. The ICO 2021 'Annual track' survey[175] found that 'The right not to be the subject of automated decision making and profiling' was the most important right under GDPR for 8% of respondents, and in the top three most important for 29% of respondents. The survey suggests it was less frequently flagged as important than some of the main GDPR rights. It is however possible that awareness of automated decision making is lower, as 37% said they didn't know anything about that right. This suggests that consumers may not be fully informed about how data is used for decision making or what their data protection rights are relating to this.

292. The proposed measures are designed to maintain key safeguards and high standards of data protection, while shifting to more outcomes-based requirements and therefore we do not expect the proposals to lead to worse outcomes for individuals. For example, we propose making accountability more flexible and risk-based while still maintaining the accountability framework itself. Data subjects would maintain their rights to a SAR and those that wish to access their data would still be able to.

a) Legitimate Interests

293. In terms of the reform to clarify activities that fall into the legitimate interests basis of processing. It is also important to consider that the scale of these impacts is dependent on the number and willingness of firms to change their approach from relying on an alternative basis to that of 'Legitimate Interests'.

294. According to the ICO, legitimate interests 'promotes a risk-based approach to compliance as you need to think about the impact of your processing on individuals, which can help you identify risks and take appropriate safeguards. This can also support your obligation to ensure 'data protection by design', and help you identify when you might need to do a data protection impact assessment (DPIA). Using this basis for processing that is expected and has a low privacy impact may help you avoid bombarding people with unnecessary consent requests and can help avoid 'consent fatigue'. It can also, if done properly, be an effective way of protecting the individual's interests.

295. The RTA unit highlights the importance that data subjects place on openness when it comes to firms processing their personal data. In addition, the DCMS Participation Survey[176] found A majority of adults (46% agree and 16% strongly agree) were comfortable with data being used when it is easy for them to understand how and why it is being used. If this openness were to

[175] ICO Annual Track 2021
176 Participation Survey, 2022-23, DCMS

change then consumers may be less inclined to engage with a business, resulting in a decrease in available data for firms to use and a decrease in firm level productivity as a result.

b) Extending approved code of conduct provisions under Article 40 UK GDPR to the PEC Regulation

296. The PEC Regulations place specific requirements on organisations in relation to use of personal data in electronic communications. They include rules on the use of emails, texts and phone calls for direct marketing purposes and the use of cookies and similar technologies.

297. Feedback from stakeholders has indicated that there is sometimes a need for guidance on complying with the legislation that is more bespoke than ICO's general regulatory guidance. Provisions were tabled to allow representative bodies to design codes of conduct on complying with the PEC Regulations that reflect their specific processing operations to overcome these barriers. This will be particularly beneficial to representative bodies who are developing codes for processing activities that are subject to the requirements of both the UK GDPR and the PEC Regulations.

298. The impact of this provision will depend on which industry codes of conducts will be created and when. However, it is expected to reduce costs for businesses in these industries as they will have easier access to more detailed guidance, meaning they are more likely to be compliant and not have to pay third parties for advice or services.

299. More generally, a main benefit for businesses of adhering to an approved code is it will assist them in demonstrating to customers and the regulator how they comply with relevant legislation. This increase in trust between data subjects and businesses could lead to an increase in data sharing and access for firms.

c) Changes to breach reporting requirements under PEC Regulations

300. The ICO defines a personal data breach in PEC Regulation as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise protected in connection with the provision of a public electronic communications service".

301. Under regulation 5A of PEC Regulation, 'service providers' have a specific obligation to notify the Information Commissioner's Office (ICO) – and in some cases their own customers – about a 'personal data breach'. Regulation 611/2013 sets out additional requirements regarding the information that must be submitted for data breach reporting under regulation PEC Regulation 5A. Regulation 611/2013 requires breaches to be reported to the ICO within 24 hours. Although where the organisation is unable to provide all of the required information, the regulation does allow further information to be submitted within a further 72 hours. Failure to meet the data breach reporting requirements could incur a fixed monetary penalty notice (MPN) under PEC Regulation 5C.

302. Amending Regulation 611/2013 and regulation 5A of the PEC Regulation will extend the data breach reporting time under PEC Regulation 5A from 24 to 72 hours and aligns reporting

periods to those in the UK GDPR. This will allow more time to gather the information required and reduce the burden of reporting breaches for UK businesses.

303. We assume that notifying a breach to the ICO includes three activities on which equal time is spent on each of these: investigating the breach itself, reporting this to the ICO and responding to subsequent ICO queries following the breach. ICO data from 2022 on reported personal data breaches[177] shows that approximately 24,000 data breaches were reported to the ICO in 2022. We estimate the percentage of low-impact personal data breaches was 22.5%, or about 5,000 breaches.[178] Of these 5,000 breaches, approximately 800 were reported to the ICO within 24 hours. According to DSIT's Cyber Security Breaches survey, the combined average staff time cost[179] and short-term direct cost[180] for the most disruptive breach or attack for all businesses is £630.

304. As a result of this provision, we expect that UK businesses who experience personal data breaches will find it easier and more achievable to report breaches within the given timescales. By making it easier for firms to report breaches within the given time period, there may be a fall in costs of them doing so. For example, additional time may increase the accuracy of their report reducing the time cost needed to respond to follow up requests.

305. It is expected that the provision will also lead to a reduction in the incidence of late reporting as businesses have a more reasonable timeframe in which to report, which in turn will lower costs as businesses won't have to pay MPNs, and the ICO can deploy less resources on issuing nominal fines to providers.

306. Whilst this provision may make the process of reporting breaches more achievable for businesses there may be some providers who may not wish to take the regulatory risk to report beyond the current statutory timescales, limiting the potential impact of the reform.

Delivery of better public services

307. Expected benefits from the package of reforms include increased sharing, coordination and collaboration between the public and private sectors, which would allow the delivery of better public services, ultimately leading to better outcomes for citizens. Whilst the link between data use and public services is apparent, numerical evidence supporting this is still lacking. Therefore, we have carried out an extensive qualitative literature review to provide a sufficient evidence base.

308. In the context of Covid-19, responsible data use has been crucial to the public response. Globally, around 75,000 scientific publications on Covid-19 were published between January and November 2020, of which more than three quarters were open access.[181] Research databases and scientific publishers removed paywalls so that the scientific community could quickly share COVID-19-related data and publications.

---

[177] ICO (2022). Data security incident trends.

[178] We assume that reported personal data breaches where the ICO has taken 'no further action' are 'low-impact'.

[179] Staff time costs include paid time to staff to investigate or fix the problem the breach has caused.

[180] Short term direct costs include payments made to external IT consultants to investigate or fix the problem, as well as any payments made to attackers.

[181] OECD (2021) notes that "the pandemic has triggered an unprecedented mobilisation of the scientific community"

309. Data flows allowed labs at the forefront of the outbreak to share information and rapidly develop tests for the virus.[182] Spirometers, a device used to measure lung capacity, were issued by the NHS to patients at extreme risk from Covid-19. The device allowed patients to measure their lung capacity and share this information remotely with their doctors via an app.

310. More widely, the OECD[183] highlight that there are three ways in which the public sector can use data to generate public value;

a. The first way is using data for **"anticipation and planning"** and focuses on how data can be used in designing policy and anticipating change.

b. The second is **"delivery**" and explores how data can inform and improve the implementation of policies.

c. The third way is **"evaluation and monitoring"** which focuses on how data can be involved in measuring impact and monitoring performance.

311. The OECD suggests that by applying data in these three ways the public sector can generate public value and deliver more efficient public services, highlighting its importance.

312. This is in line with Maciejewski 2016, who found that using big data provides significant benefits to the delivery of public services that match customer's needs. This is a result of an increase in the accuracy of decision-making, leading to a more efficient delivery of public services. According to Maciejewski, the successful application of big data methods in the public sector has three potential results:

a. Significant increase in the accuracy of decision making, created by:

i. The expansion of the information database for analysing and drawing conclusions

ii. Feasibility to complete extensive work involving analysis

iii. The application of new methods of data presentation

iv. The creation of algorithms to suggest appropriate solutions.

b. Significant acceleration of the performance of internal 'information tasks' through automating data analysis.

c. Significant reduction in the costs related to the decision-making process.

313. This once again highlights the importance of removing any barriers to data use in the public sector to unlock these outcomes.

314. There is evidence that there remain important barriers to data use in the provision of public services, including time taken to access data and constraints in data access for commercial companies, not just data protection rules. When surveyed, members of the health data user

[182] Deep mind (2020) Computational predictions of protein structures associated with COVID-19
[183] OECD (2019) The Path to Becoming a Data-Driven Public Sector

community reported that only 25% of recent requests for data had been completely successful, and only 45% of requests for clinical trial data were successful.[184]

315. Providing clear processing conditions would help to provide data controllers with more certainty. Our proposals aim to address the barriers to data use by clarifying the conditions under which data can be processed and encourage greater data use, whilst empowering public bodies to process data where it is in the public interest.

Exemption for Archives from further processing rules

316. The legislation which consolidates and clarifies the existing rules around when a controller is permitted to re-use personal data, or, more specifically creates a clearer guide for how to comply with the existing purpose limitation principle.

317. The purpose limitation principle is one of the key principles of the GDPR. This requirement aims to ensure that a controller is clear and open about their reasons for obtaining personal data, and how a controller uses that data is within the reasonable expectations of the individuals concerned. This principle is viewed as fundamental to building public trust in how personal data is used and has clear links with other principles such as fairness, lawfulness and transparency.

318. The purpose limitation principle as outlined in Article 5(1)(b) has two limbs: It requires that processing be for:

a. 'Specified, explicit, legitimate purposes'. This limb is to prohibit indiscriminate and aimless data collection.

b. 'Not further processed in a manner incompatible to those purposes. This limb is to ensure that the re-use of data is what a reasonable data subject would expect.

319. The UK GDPR builds on the second limb of the purpose limitation principle in Article 6(4) which states that if a controller wants to further process or re-use data for a different purpose, they must assess whether it is compatible. To demonstrate 'compatibility' as outlined in Article 6(4) of the UK GDPR, a controller must determine among other things:

a. any link between the original purpose and the new purpose;

b. the context in which the personal data was collected, including the relationship between the data subject and the controller;

c. the nature of the personal data, including whether it is a special category of personal data (see Article 9), or personal data related to criminal convictions and offences (see Article 10);

d. the possible consequences of the intended processing for data subjects;

e. the existence of appropriate safeguards (for example, encryption or pseudonymisation).

320. Although the UK GDPR sets out clearly how to assess whether a controller's processing is compatible, it is currently unclear about when purposes are "incompatible", e.g. a company collects customer data (commercial purpose) but must inform the police of a crime they suspect

[184] MDC (2019) Use of health data by the life sciences industry. Sample: online survey of UK health data user community, including academic and charitable as well as commercial users of health data.

the customer has committed (crime prevention purposes). The UK GDPR is also unhelpful about situations where a controller got the data subject's consent for one purpose but wants to re-use that data for a different purpose.

321. The Act aims to clarify the interplay between the rules on compatibility and the rules for consent's validity. It firstly sets out an explicit general prohibition against changing the purpose of processing without fresh consent. Secondly, it outlines a list of exemptions to this prohibition in Annex 2, such as for crime investigation purposes and responding to emergencies. The Act contains a power for the Secretary of State to add to this list.

322. The provisions in the Act are largely intended to reflect existing law (Article 6(4) UK GDPR) and recital 50. The provisions aim to set out more clearly what the permitted routes are for further processing broadly.

323. In the UK GDPR, archiving is already exempt from the purpose limitation principle (Article 5(1)(b) and recital 50). In effect, this means that a controller that collected data for one purpose can always re-use that data for an archiving in the public interest purpose provided they have satisfied a 6(1) lawful ground. However, we do not believe this exemption necessarily or clearly overrides other parts of the UK GDPR, in particular the conditions of consent.

324. As a result of this provision, archives who previously sought consent more than once in order to re-use data, will no longer need to spend time and resources attaining this consent again. This will result in operational cost savings, and the freeing up resources that can be spent on alternative tasks. We also anticipate any legal costs that were previously incurred by archives to establish a lawful basis will no longer be necessary.

325. This provision might also increase the quantity of data that is reused. For example, the increased clarity provided by this reform may decrease the perceived risks in reuse by Archives. This increase in data use may result in benefits to data subjects. For example, a researcher who wanted to re-use data originally collected on consent for a commercial purpose would then not need to obtain fresh consent for the RAS purpose (research, archiving and statistical purposes) for further processing. This additional research, archiving or use of data for statistical purposes could bring wider benefits to data users in the form of efficiencies or benefits to society as a whole.

326. By exempting archives from the further processing rules laid out in the Act, we would also expect to see an increase in compliance for these organisations carrying out compliant data handling. This would therefore result in a decrease in the resources needed to identify and penalise non-compliance.

Impacts of changes to the Digital Economy Act

327. Analysis in this section has been provided by the Central, Digital and Data Office.

328. The Digital Economy Act (2017) currently provides departments with the data sharing powers to improve services for individuals and households, but this legal gateway is not available for services that support businesses. Furthermore, there are no powers within the Digital Economy Act 2017 to amend section 35 by secondary legislation, and therefore primary legislation must be used.

329. As there are few examples of where this data has been shared between departments previously, this means that the evidence base for the analysis of potential benefits is currently limited. As a result, we are only able to provide a qualitative assessment of the likely scale of the impacts of this primary legislation reform. A more thorough quantitative assessment of benefits will be provided at the secondary legislation stage as per RPC guidance.

330. There will be little or no direct benefits of the extension of data sharing powers. The impacts will be experienced when public authorities utilise these powers to share data in order to support government services for businesses. We therefore expect not only the public sector but private organisations working with government data to benefit from this proposal.

331. The table below provides high level quantitative analysis of the potential benefits of the reform for both sectors. More analysis will be provided at a secondary legislation stage when data sharing powers are enacted.

Table 34: Indirect benefits of the changes to the Digital Economy Act by recipient

Impacted party	Benefits
Businesses	**Reduced duplication of data entry:** Businesses will save time and therefore costs by only being required to provide information to the government once. Furthermore, this benefit will occur each time that a business applies for a new service/grant/subsidy etc as they will no longer be required to submit their information on each unique occasion. The Estonian government has set up the eesti.ee portal, where all information and requirements regarding opening up and running a company are gathered in one place. It aims to help established and continuing businesses to fulfil their information obligations and to reduce their administrative burden.[185] **Ease of access to government support:** Having a single portal for applying for business support services will allow businesses to more easily engage with the government. This could save time for businesses when attempting to apply for the services that they require. Businesses may also be able to use this route to receive financial assistance in ways that they did not know were possible. For example, the proportion of firms claiming R&D tax credits is very low, despite HMRC setting aside Actions in funding.[186] Many firms don't understand if their operations qualify as innovative or are unable to complete the application due to lack of expertise.[187] **Induced investment by the private sector, driving growth and productivity** The BEIS/HMT Business Productivity Review evidence shows that many of the productivity constraints on businesses are caused by internal factors, including; weak management skills, shortcomings in business

[185] Digital Government Factsheet 2019 - Estonia
[186] AI Sector Deal
[187] Poor knowledge of government incentives is holding back the innovation economy, Business Money, 2021

Impacted party	Benefits
	planning and reluctance to take external advice.[188] Many managers are unclear about what support is available that would benefit their business, and where to find it. It is therefore possible that with better data HMG could target marketing at these businesses to reduce the information asymmetry and induce them to invest or co-invest in improving their business processes or management skills.
Government	**Reduced duplication of data processing:** As data about businesses becomes increasingly connected across government, data will no longer have to be collected and processed in multiple departments. This would result in efficiency benefits for HMG as civil servants who were initially involved in processing this data are able to provide support elsewhere. **Improved policy-making, allocation of resources and impact:** Better access to data and ability to turn data into useful insights helps create economic value, as these insights can be used by decision-makers to optimise the allocation of resources.[189] Research shows that firms adopting data-driven decision-making can have 5-6% higher output and productivity.[190] **Reduction of programme costs:** If BEIS has the ability to segment the business population and market services directly, this could reduce the need to fund a direct marketing company to recruit businesses to a programme. While the admin costs may rise slightly to undertake the targeting, it is likely that the total cost to taxpayers would be lower. **Reduced fraud and error:** A centralised source of information about businesses may enable increased cross-checking of details about businesses. This will result in more accurate assignment of funding and reduce the ability of businesses to submit fraudulent applications of funding. Members of the fraud prevention service, Cifas, share data with other members outside of their own organisation in order to improve fraud prevention. Cifas members prevented fraud totalling over £1.4 billion in 2018.[191] **Corporate transparency and regulation:** Better use of data held by the government, in accordance with the Data Standards Authority framework, promotes a culture of transparency, safeguarding and assurance, which builds and maintains public trust. As

[188] Business Productivity Review, 2019, BEIS
[189] Connected Open Government Statistics, ONS
[190] Strength in Numbers: How Does Data-Driven Decision-making Affect Firm Performance, Erik Brynjolfsson SSRN Electronic Journal
[191] Tackling fraud in Government with data analytics Starting the conversation CO/DSIT, 2019

Impacted party	Benefits
	a result, businesses will be more willing to provide data and the government will have a more comprehensive view on business information and activity, aiding the regulation of markets.

Improved customer outcomes

332. It is expected that when consumers are better informed, through sharing their data, they will make different consumption choices. These different choices will result in benefits not captured by loyalty penalty estimates. For example, analysis of the Pensions Dashboard highlights the potential recovery of up to £19.4m of "lost" pension pots.[192] Consumers will have more information available to them to make better informed choices and engage more effectively with the market.

333. Consumers being informed does not necessarily mean they will choose the cheapest deal, but consumers may choose the deal that is best suited to them. For example, Ofcom found that 71% of people who changed their mobile phone provider in the last 12 months did not consider mobile phone signal strength as a factor when making this decision. Of these respondents, 20% stated this was because it did not occur to them, 9% said they did not know where to find the information, and 7% said it was too much hassle.[193] Similar non-price factors are also important to SMEs, and this type of comparable information may not be available for them without Smart Data.[194]

334. Further benefits may manifest as a result of consumers being better informed. For example, previous analysis of the energy and retail markets[195] have highlighted the effects of better-informed decisions in increasing energy efficiency and healthier choices, leading to carbon savings and improved health outcomes. Again, these benefits are expected to be sector specific, so they will likely be captured by sector schemes through ongoing evidence gathering or in future sectoral analysis.

Improved Interoperability across Health and Social Care Systems

335. Analysis in this section is based on analytical findings from the DHSC Open Data Architecture Information Standards Impact assessment, where a full breakdown of the expected impacts of the reforms is provided.[196]

336. Currently only 42% of sampled health and social care providers comply with non-mandatory core information standards.[197] As evidenced in Estonia[198] and Northern Ireland[199], government regulation is the most effective means to address the issue of achieving compliance with

[192] DWP (October 2019): "Pension Schemes Act 2019 Impact Assessment"
[193] Ofcom (August 2020) "Open Communications: Enabling people to share data with innovative services"
[194] Ofcom (August 2020) "Open Communications: Enabling people to share data with innovative services"
[195] DECC (2014): "Legislation to require energy suppliers to provide key, personal information on consumers acts in a machine-readable format" & BIS (2012): "Order making power for midata"
196 Open Data Architecture Information Standards, DHSC (2024)
197 Information Standards and Interoperability Survey, NHS, Feb 2024
198 WP8_willis.indd (ox.ac.uk)
199 eHealth and Care Strategy | Department of Health (health-ni.gov.uk)

common information standards in health and social care, and government regulation can unlock further compliance and benefits in several ways:

337. First, it allows for the establishment of standardised guidelines and clear rules that ensure a consistent approach to data exchange among health and social care providers and technology vendors. This standardisation is crucial for seamless communication among different systems.

338. Secondly, government regulation prioritises public interest, particularly the protection of patient data. It enforces stringent data security, privacy, and ethical usage standards, thereby guaranteeing the responsible handling of sensitive medical information.

339. Thirdly, government intervention provides accountability and enforcement mechanisms. Regulatory bodies can investigate and penalise entities that do not comply with interoperability standards, fostering adherence and ensuring that stakeholders take these standards seriously.

340. This approach facilitates multi-stakeholder engagement, resulting in regulations that reflect the diverse interests of health and social care providers, technology vendors, and patient advocates. Overall, government regulation offers the necessary oversight, consistency, and protection essential for addressing the complex challenges of IT system interoperability in the health and social care sector.

341. Implementing interoperability via the legislation on IT suppliers could significantly enhance the quality of care, improve patient outcomes, and enable seamless access to information[200]. This could not only pave the way for comprehensive research, effective strategic planning, and innovation at a population-wide level, but could also optimise clinical outcomes.[201]

342. It has the potential to enhance procurement and commissioning strategies within health and social care providers, fostering a dynamic and adaptive health and social care IT market[202]. Applying new legislation-based information standards to IT suppliers enables providers to choose from a diverse set of supplier products and systems, fostering competition and encouraging suppliers to innovate and improve their offerings to meet the standards. This not only enhances the quality and variety of products available to health and social care providers but also drives advancements in technology and service delivery within the health and social care sector.[203]

Enhance the Work of the UK Intelligence Services and Law Enforcement Agencies in the Interest of Public Security

343. This section of analysis has been provided by the Home Office, and is broken down by measure. Where evidence is available costs have been monetised. Where this has not been possible a qualitative assessment of the potential costs for each measure has been provided.

Time limits for responding to request by data subjects (Part 3 and 4 DPA)

200 01.06.22 Clean DHSC Primary Impact Assessment - Cleared- DSIT edit (1) (2).pdf
201 TO PUBLISH: Updated Final DPDI (2) Act Impact Assessment March 2023.docx (parliament.uk)
202 TO PUBLISH: Updated Final DPDI (2) Act Impact Assessment March 2023.docx (parliament.uk)
203 Information standards for health and adult social care in England - GOV.UK (www.gov.uk)

344. A data subject can exercise their right to request what information is held about them through a SAR. under Part 3 (Law Enforcement) and 4 (Intelligence Services) need to be actioned within one month. Unlike the UK GDPR, Parts 3 and 4 of the DPA 2018 do not recognise and allow for a proportionate time period for dealing with particularly complex requests. The proposal is to mirror an existing UK GDPR provision within Part 3 and 4 of the DPA 2018 that permits a two-month extension to a SAR time period when a request is particularly complex. This will introduce greater consistency across the legislation.

345. Increasing the deadline for responding to SARS should reduce the probability that compliance issues arise and may result in cost savings through reduced fines in the future.

346. The Northern Ireland Courts & Tribunal Service (NICTS) received 48 SARs during 2018 and 60 in 2019. Given that NICTS have a staff in the range of 1,000, this is a significant burden. It took an average of two to six weeks over the one-month period of time for NICTS to respond to complex SARs. Court documents range from 300 to 3,000 pages and data controllers must give due regard to public safety which adds to the problem of meeting this one-month deadline.

347. The Crown Prosecution Service (CPS) faces a similar problem. In 2018 an SAR file had over 100,000 pages, relating to a complex fraud case which resulted in non-compliance with the one-month period.

National security exemption (Part 3 DPA)

348. Currently, the national security restrictions in Part 3 are not as extensive as in Parts 2 or 4. Mirroring the national security exemption into Part 3 will better enable LEAs to protect national security, as well as assist close working between LEAs and UK intelligence services.

349. There may be greater efficiencies when LEAs and the UK Intelligence Services work together. This benefit is specifically related to counter terrorism (CT) policing and the UK Intelligence Services.

Consent to law enforcement processing (Part 3 DPA)

350. Although rarely used, the ‘consent’ of a data subject is an available lawful basis for processing under Part 3 of the DPA 2018. However, unlike UKGDPR, there is currently no definition of the term in Part 3. Since ‘consent’ can have different meanings within the policing context, there is a very slight risk that it may be interpreted incorrectly in the absence of a clear definition. As such, the inclusion would provide data controllers under Part 3 with a clear and uniform definition of ‘consent’ they can refer to. Therefore, to ensure that the term is interpreted consistently across both regimes, this proposal seeks to replicate the UK GDPR definition into Part 3.

Transfers based on special circumstances (Section 76 DPA)

351. Introducing some minor amendments to Section 76 DPA 2018: which concerns the international transfer of personal data where ‘special circumstances’ are present, to make clearer that as long as the transfer is not excessive transfers are not limited to individual pieces of data. The reform ensures law enforcement to have the confidence to use this section to transfer multiple records where it is necessary for the detection and prevention of crime.

352. Adding flexibility should give greater legal clarity to competent authorities when transferring multiple records, therefore potentially reducing the chance that they will face legal costs associated with related legal challenges.

Subsequent transfer's (Section 78 DPA)

353. Under the current legislation, UK competent authorities must make it a condition of any transfer for a law enforcement purpose that data is not to be further transferred to a third country or international organisation without the authorisation of the UK competent authority transferring controller (or another competent authority). This reform introduces a narrow exception to this requirement in the case of an immediate and serious threat to public or national security and where authorisation cannot be obtained in good time. In such cases, the third country would be required to notify the relevant UK competent authority of the transfer as soon as practicable.

Remove the requirement for paper birth and death registers moving to an electronic register

354. Reduction in secure delivery costs for distributing register covers and registration paper. The register folders and loose-leaf registration paper needs to be sent by a secure delivery service at a cost of £2.27 for each parcel. The registration service order register folders and paper as required throughout the year. The number needed is dependent on the number of birth and death registrations in each district and this figure varies considerably across the country.

Non-quantified benefits

355. The registration service will save money by not needing to purchase future storage space for paper registers which, currently, must remain in the custody of the registrar. The value of this saving is difficult to quantify as each registration district and sub-district undertake different amounts of registrations which means they have differing storage needs. Also, the cost of storage differs across England and Wales.

356. Entries made directly on to RON away from the ‘home’ register office will remove any vulnerability to theft or loss of registers while in transit.

357. Whilst the proposed changes would modernise delivery of registration services, it will also ‘future proof’ records as, long term, the quality of the paper registers deteriorates, and older records are now starting to fade.

358. The abolition of paper registers and the removal of secure delivery costs also makes an environmental contribution: reducing paper use (saving raw materials and less emissions), less secure transport usage (less consumption of fuel and less emissions). While at the margin, these contributions are still positive.

Increase in data use for research purposes

359. As well as the quantified benefits above, we also acknowledge that there are likely to be other indirect impacts of reforms designed to encourage research, including

a. There will be benefits to the public associated with the increase in the use of data in commercial settings for R&D. For example, Artificial Intelligence related R&D, a data

intensive activity, can add the equivalent of an additional £232bn to the UK economy, therefore highlighting the potential benefits of R&D to living standards and the economy.

b. In 2022, almost half (46%) of UK consumers were classified as Data Pragmatists; people who are happy to exchange data with businesses so long as there is a clear benefit for doing so. Including categories such as 'commercial R&D' or 'product development and data science' are terms that are still undefined and could have different interpretations by businesses. This could lead to a discrepancy in the threshold by which scientific research is considered. Therefore, there is a risk that data subjects may feel as though their data is being used for R&D that is not in their benefit or for purposes that are not made clear to them. As a result, this damage to public trust may render them less likely to share their data with these businesses. If data sharing falls, or if firms choose to continue to pay for legal resources to demonstrate that their purposes fit within this definition, then there is a risk that compliance costs will not fall, and data use will decrease instead of increase.

Powers relating to verification of identity or status (DSIT & Home Office)

360. Requiring employers and landlords who choose to carry out certain digital right to work and right to rent checks to use only DVS-registered organisations will increase the security of the checking regime, in turn supporting a possible further expansion to other documents such as expired British passports (a common request from the business community) and supplement proposals to increase penalties for non-compliance.

Power to add categories of sensitive processing (DSIT & Home Office)

361. This proposal will provide a regulation making power, and so there is no impact upon Part 3 or Part 4 controllers until the power is exercised. When the power is exercised, depending on the additions and variations made, there may be some cost to organisations processing under Part 3 or 4 DPA to ensure compliance. A breakdown of these costs will be provided at the time such regulations are made

Processing in reliance on international law (DSIT & Home Office)

362. This will ensure efficient functioning of the DAA enabling both US and UK law enforcement to prevent, detect, investigate and prosecute serious crime. It will also mean a reduction in time to receive data used for evidential purposes usually acquired through Mutual Legal Assistance Treaties (MLAT) requests, which usually take 12 months on average, made between the UK and US. We will look further into the specifics of this reduction, with additional information provided at enactment.

Searches in response to data subjects' requests (DSIT & Home Office)

363. It is expected that there will be minimal, if any, impact upon controllers and data subjects given that this is a codification of the current status quo. It will however provide confidence and assurance that this is the standard expected of controllers when responding to subject access requests. It will also provide similar assurance to data subjects that controllers are explicitly required, by legislation, to conduct a consistent level of search when in receipt of an access request from the data subject.

Clarifying conditions on the use of international processors by UK competent authorities (Part 3 DPA).

364. The intention is for this new mechanism to be fulfilled through the contracts that need to be put in place between controllers and processors in accordance with section 59 of the DPA. Therefore, it would not require an additional document to be put in place. On the basis that UK competent authority controller, to international processor transfers, are currently permissible under Part 3 of the DPA , controller to processor contracts relied upon for such transfers will continue to stand and not be invalidated by the introduction of this amendment. This proposal is therefore cost neutral.

Delivery of the National Underground Asset Register

365. This analysis has been taken from the NUAR Impact Assessment 2024 published by DSIT. For a more detailed breakdown of some of the indicative sector specific costs and benefits please refer to the NUAR Impact Assessment directly.

366. There are also a number of indirect benefits that have not been quantified due to the dependencies involved in realising these benefits beyond the provision of NUAR, or because of a lack of data. Underground asset location data are one of multiple inputs required for better subsurface management to be realised, such as technical solutions and expertise and local planning policy.

367. Instead, these indirect benefits are qualitatively assessed. One such indirect benefit is better subsurface planning, coordination and management that comes from having a more complete understanding of the underground spaces that are most and least occupied/densely located. This use case extends beyond excavation planning and safe digging, and supports users to better optimise the use of underground spaces, improve above ground planning, and infrastructure resilience planning. Key users might be local transport authorities and local housing and development planning who can assess the relative density of underground assets by requesting and compiling data more efficiently and having a more complete picture of the subsurface environment.

368. Additionally, the NUAR service can also contribute to further improving data quality in the future. For example, as data will need to be provided in a prescribed form based on the NUAR data model (which aligns with an internationally recognised standard), details of the requirement will give asset owners objective information which could be used to define focus areas for data quality improvements. Furthermore, the NUAR service also allows excavators to report inaccuracies back to data owners to correct at source, which will also improve the quality of data over time. These data quality improvements can help reduce some of the other the known data issues to realise additional strike reductions, which might be because the data itself isn’t accurate.

369. There are also likely to be environmental benefits by reducing the amount of carbon and other pollutants (such as particulate matter levels, PM10, and oxides of Nitrogen, NOx) that result from excess roadworks - for example thrown up during excavations, or from skip loader trucks ferrying materials and machinery between dig sites, coming from reducing the number of speculative or abandoned digs. However, given that the volume of material and travel varies based on location, size and scale of the dig, and with limited data available, it is not currently feasible to robustly quantify these impacts.

370. Finally, if prescribed as part of the details of the secondary legislation, access to the NUAR database might be expanded for use by a broader set of stakeholders (such as non-statutory users and third parties). These users could include developers and local planners when assessing the suitability of a parcel of land, which can ensure the right developments are built

on the most viable land, supporting local level house building. Other value add services might also be enabled in the commercial sector. However, it should be noted that this is theoretical at this stage, as it relies on NUAR being operationalised in the first instance before feasibility can be confirmed to a sufficient level of confidence.

371. This analysis has been taken from the NUAR Impact Assessment 2024 published by DSIT. For a more detailed breakdown of some of the indicative or specific costs he NUAR Impact Assessment directly.

Increased Interoperability and Trust of Digital Identity Systems

Reduced familiarisation costs for relying parties

372. As the number of use cases that use schemes increases, there may be a potential further cost saving from the establishment of DVS schemes. This is because relying parties (businesses that need to verify identity or eligibility) will not have to rely solely on their own procurement processes to assess whether a digital identity service meets their requirements. This can make procurement of digital verification services easier for relying parties and will result in more consistency in the services provided across a sector or use case.

Reduced transition costs for relying parties

373. As the number of use cases that use schemes increase, there may be a potential further cost saving from the establishment of schemes. This is because enabling the establishment of schemes will support the uptake of digital identity across a wider variety of use cases, through the reduction of barriers to entry for relying parties who may lack the technical expertise and the resource to develop and assess against their own unique requirements. This can enable cost and efficiency savings beyond the estimated quantifiable benefits outlined in the DMA

Facilitating online safety researchers' access to data

374. The benefits flowing from regulation enabled by this primary legislation are the increased knowledge provided to individuals, businesses, and government about online harms. Though we do not have an estimate for the effect of the policy on the rate of online harms, we can estimate the magnitude of social benefits/avoided harms required for the policy to "break even" with the illustrative costs to business of complying with regulations enabled by this legislation. For a full breakdown of illustrative impacts please refer to the Researchers Access to Data Impact Assessment.[204]

375. Our estimated cost of compliance for an illustrative application-based data access model, over the ten-year appraisal period, is £3.3 million to £7.5 million, therefore an estimated monetised benefit of £3.3 million to £7.5 million in avoided harms would be required to offset it. This is equivalent to a 0.001%-0.002% decrease in the around £361 billion estimated value of online harms faced in the UK, according to the Online Safety Act Impact Assessment. [205]

204 DSIT: Researchers' Access to Data Impact Assessment, 2024
205 The harm figure presented here is in 2024 prices, 2024 base year, 10-year PV with 2025 commencement

Costs

Summary

Analysis of the costs of the proposed package of reforms has been split in the following way, and further details can be found in the continuing sections.

1. Direct Costs
    a. Monetised
        i. One off familiarisation cost
        ii. Improved Regulatory Oversight
        iii. Enhancement of the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security
        iv. Powers relating to verification of identity or status
        v. Delivery of the National Underground Asset Register
        vi. Improved interoperability across health and social care systems
        vii. Costs to the Criminal Justice System
    b. Non- monetised
        i. Enhancement of the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security
        ii. Improved interoperability across health and social care systems
        iii. Facilitating online safety researchers' access to data
2. Indirect Costs
    a. Monetised
        i. Increased interoperability and trust of digital identity systems
        ii. Remove the requirement for paper birth and death registers moving to an electronic register
        iii. Delivery of the National Underground Asset Register
    b. Non-monetised
        i. Creation of innovative and secure Smart Data schemes
        ii. Increased interoperability and trust of digital identity systems
        iii. Delivery of better public services
        iv. Improved interoperability across health and social care systems

v. Costs to businesses of increased data use

vi. Delivery of the National Underground Asset Register

Direct Costs - Monetised

376. Where evidence is available, we have provided monetised estimates of the direct costs associated with the preferred package of reforms. These include estimates of the initial familiarisation costs faced by UK businesses and public sector organisations of the reforms.

Familiarisation Costs

Familiarisation Costs for UK Businesses

377. Other quantifiable impacts include familiarisation costs associated with the new measures.

378. We continue to use a time-cost approach to estimate the administrative costs of reading the new legislation. This approach to familiarisation costs had been adapted from the ICO's methodology used in their Impact Assessment for the Data Sharing Code.[206] While the ICO modelled familiarisation costs for a single piece of guidance (the Code), the main difference in approach is that the familiarisation costs have been broken down by policy measure, as different measures apply to different populations of businesses. Familiarisation costs for each measure have therefore been calculated individually, and then subsequently summed together.

379. In line with previous analysis, we identify the relevant 'number of affected businesses' per measure, by looking at an organisation's data use to determine if they are in scope of the model. We assume that familiarisation costs are borne in year one as all organisations read the new guidance, taking this direct measure of impact. We draw from an analysis commissioned by Frontier Economics which identifies the relevant population of businesses per measure.

380. Since the previous analysis we have updated our estimates for the number of businesses in each sector and size category using 2023 ONS Business Population Estimates[207]. We have also updated, where possible, our estimates for the proportion of businesses impacted by each measure using the UK Business Data Survey 2024. Due to noticeable variation between UKBDS releases, our estimates for the proportion of businesses that handle data or personal data were calculated by finding a mean across the 2021, 2022 and 2024 UKBDS releases.[208] Similar variation was seen in the proportion of businesses who stated that they use data to generate new insights or knowledge, in this case an average was calculated across the 2021 and 2024 releases due to lack of data in 2022.

381. The ICO assumes that one data protection officer per organisation would be required to read guidance. The hourly wage cost for a data protection officer was estimated by the ICO to be equivalent to the median hourly earnings of the ''Managers, Directors and Senior Officials' occupational group in the ONS Annual Survey of Hours and Earnings (ASHE), uplifted by 22% to account for non-wage costs.

[206] Data Sharing Code of Practice Impact Assessment, ICO, (2019)
207 ONS Business population estimates (2023)
208 DSIT: UK Business Data Survey (2021, 2022, 2024)

382. Following the ICO's methodology and using 2023 ASHE[209] data uplifted to 2024 prices, the estimated hourly unit costs of this work for small, medium and large businesses is £30.68. For micro-sized firms (zero employee firms) we have updated our wage assumptions by applying median annual earnings estimates of the self-employed from DWP's Family Resources Survey and estimating the hourly unit cost of this work at £11.97.[210] The self-employed wage assumption is used as a simplification to reflect the average wage of firms with zero employees.

383. We continue to assume that the guidance would be at a similar level of reading difficulty to the ICO's data sharing code, and therefore have used a similar Fleisch reading ease score of 40, which corresponds to a reading speed of 75 words per minute. Assuming an average number of words per page of 500, this gives a reading speed of 9 pages per hour. Based on these assumptions, we estimate one off familiarisation costs to be the following:

Table 35: Total one-off familiarisation cost by scenario and reform for UK businesses, 2024 prices

Reform	Total Familiarisation Cost (£million) Low scenario	Total Familiarisation Cost (£million) Medium scenario	Total Familiarisation Cost (£million) High scenario
Research Purposes	5.3	6.2	7.2
Legitimate Interests	5.2	6.2	7.1
AI and machine learning	4.2	4.9	5.6
Privacy and Electronic Communications	3.7	4.3	5.0
Total	18.4	21.6	24.9

384. As well as these changes to the existing model, we have also broken down these costs by size of business and sector.

385. We have also looked into the inclusion of any long-term training costs that would have to be undertaken following the implementation of the Act. To estimate these costs, we conducted an extensive literature review into the reported costs of training UK businesses for changes to data policy. The UKBDS found that only 23% of respondents that handle personal data had run training in the last 12 months to comply with UK data protection rules[211]. Christensen et al. (2013)[212] also report that "the training of staff at most Small and Medium Enterprises (SME's)

209 ONS Annual Survey of Hours and Earnings (2023)
210 DWP Family Resources Survey (2023)
211 UK Business Data Survey (2024)
212 The Impact of the Data Protection Regulation in the E.U. by L. Christensen, A. Colciago, F. Etro and G. Rafert, 1 February 13, 2013

will take up to one week a year for a DPO (for both new starters and refreshers for existing staff and preparing training materials) “.

386. After further investigation of the surrounding literature and the smaller magnitude of the proposed changes when compared to UK GDPR, we are assuming no additional training costs. DPOs would likely cover the changes as part of standard refresher training that would occur in both the do-minimum and do-something; on-going training is evidenced by the average UK employee undertaking 3.6 days of training per year (UK Employer Skills Survey, 2019). Any training to disseminate to colleagues within firms is already part of a DPO’s responsibilities. For new DPOs, given the changes replace aspects of DPA rather than create additional responsibilities, we can assume that the time taken to become certified would remain the same. For those who train DPOs, we assume any small familiarisation costs would likely be recouped quickly through the market via the cost charged to students. The assumption also ensures reduced risk of double counting as it is likely that the cost of SSCs implicitly capture other marginal costs from the changes.

Familiarisation Costs of enhancing the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO)

387. This section of analysis has been provided by the Home Office, and is broken down by measure. Where evidence is unavailable costs have been assessed qualitatively and can be found in the relevant ‘non-monetised section’.

388. Stakeholders were unable to provide comprehensive responses to data requests. This was mainly due two factors:

389. Time constraints, where there was a possibility that data could be obtained but there was not enough time to put it together.

390. The specificity of the data required, meaning that stakeholders did not record the data required for monetisation.

391. Therefore, many costs and benefits have not been monetised. In these cases, a qualitative analysis of costs and benefits was undertaken.

392. The number of competent authorities was taken from Law Enforcement Directive (LED) impact assessment for the DPA 2018. The UK Intelligence Services was then added to this. The number of organisations in scope is estimated to be between 407 and 507, with a central estimate of 457. This includes a number of private businesses between 34 and 134, with a central estimate of 84.

393. The length of guidance (2,400 words) was also taken from the LED IA as well as the average wage bracket of those affected by guidance (Higher Executive Officer) and the average number of employees expected to require training (50).

394. The appraisal period is 10 years, and the discount rate used is 3.5 per cent. All monetised costs and benefits are given in 2024 prices and are assumed to be direct unless stated otherwise.

395. Implementation costs are temporary costs which are assumed to factor in only in the first year of the proposals being implemented. These will include any familiarisation costs, as well as any additional temporary burdens such as the cost of additional infrastructure.

396. Familiarisation costs are expected to apply with any change in regulation and apply to all proposals. They represent the cost of time to an organisation of employees having to read new guidance. Below, an overall familiarisation cost will be calculated which will encompass the effects of all proposals.

397. It is assumed that the familiarisation cost applies to all competent authorities (including UK Intelligence Services) as a result of the relevant proposals being implemented, with low, central and high values representing the range of uncertainty.

398. It is estimated that there are between 407 and 507 competent authorities (including UK Intelligence Services) with a central estimate of 457. Of these, there are between 34 and 134 which are private entities, with 84 as a central estimate.

399. It is assumed that between 25 and 100 employees will have to read new guidance, with a central estimate of 50. The average wage of an employee required to read guidance is assumed to be that of a Higher Executive Officer (HEO) which is between £22.60 and £31.44, with a central estimate of £27.07 taken from internal HO data with a price base year (PBY) of 2023. This was then adjusted for inflation using the CPIH index. In 2024 prices, the wages are assumed to lie between £23.15and £32.20, with a central estimate of £27.67.

400. The high estimate of the guidance is taken from the LED IA, at 2,400 words. Low and central estimates are calculated as a proportion of the high estimate; 1,200 (50 per cent) and 1,800 (75 per cent) respectively. These proportions are used as default as the Government has not been able to obtain an estimate from stakeholders, but since these proposals are an update, it is assumed that the guidance will be shorter than for the whole LED.

401. The time spent reading guidance is calculated using a reading soft calculator, using reading speeds of 700 words per minute (wpm) for low, 400 wpm for central and 200 wpm for high. This includes extra re-read time which is based on the estimated levels of comprehension and number of words. Estimated total time spent reading guidance is in the range 0.03 to 0.3 hours, with a central estimate of 0.1 hours.

402. To calculate familiarisation costs, the total number of employees expected to read guidance was obtained by multiplying the number of competent authorities (including UK Intelligence Services) and employees per authority assumed to read guidance. This total number of employees was then multiplied by the average wage and time spent reading guidance.

403. This familiarisation cost can be split into private and public costs, by multiplying the cost by the proportion of private firms in the total cohort.

Table 36: Familiarisation Costs 2024 PBY[213]

Costs	Total Employees L[214]	Total Employees C	Total Employees H	Average Wage of Employees (£ hours) L	Average Wage of Employees (£ hours) C	Average Wage of Employees (£ hours) H	Time Spent Reading Guidance (hours) L	Time Spent Reading Guidance (hours) C	Time Spent Reading Guidance (hours) H	Familiarisation Cost (£) L	Familiarisation Cost (£) C	Familiarisation Cost (£) H
Private	850	4,200	13,400	23.15	27.67	32.20	0.03	0.1	0.3	600	11,600	125,000
Public	9,325	18,650	37,300	23.15	27.67	32.20	0.03	0.1	0.3	6,500	51,600	360,300
Total	10,175	22,850	50,700	23.15	27.67	32.20	0.03	0.1	0.3	7,100	63,200	489,800

404. Total familiarisation costs are estimated to lie in the range of £0.01 million to £0.49 million, with a central estimate of £0.06 million (2024 PBY) in year 1 only.

405. The Home Office estimates their familiarisation cost using a different methodology compared to DSIT because the organisations affected by their policies are authorities that process personal data for law enforcement and the relevant guidance has different requirements.

Improved Regulatory Oversight - ICO analysis

406. We propose measures to reform the Information Commissioner's Office (ICO); this modernising reform agenda is an investment in the ICO's future success and will sustain its world-leading reputation, while preserving its regulatory independence. The policies cover the following areas of ICO activity:

a. Strategy, Objectives and Duties

b. Governance Model and Leadership

c. Accountability and Transparency

d. Codes of Practice and Guidance

[213] Source: LED IA, HO Staff Costs Database, readingsoft.com
[214] Notes: Low (L), Central (C), High (H). Rounding may lead to slightly different results if calculated using values in the table.

e. Complaints

f. Enforcement Powers

407. These reforms aim to move the ICO away from handling a high volume of low-level complaints and towards addressing the most serious threats to public trust and inappropriate barriers to responsible data use.

408. The proposed legislative changes are set in the wider context of increased complexity and scale of processing, which increases demand for upstream engagement and advice and the complexity of downstream enforcement and supervision. They are also set against the backdrop of ongoing work to ensure the ICO has the skills and capacity to respond to increased demand for our activities arising from the implementation of UK GDPR. This existing work is planned on the basis of retention of our current fees model and will be further supported by the proposed approach to fine retention currently being discussed with the government.

409. Working alongside the ICO we have been able to provide monetary estimates of the predicted impact of these reforms on the ICO directly. Evidence for these calculations has been gathered from internal conversations, research and consultation responses.

410. We estimate that the package of reforms will help reduce barriers to data use, however we also acknowledge that these policy changes are likely to have short run and ongoing costs to the ICO as they adapt to the new changes and legislation. In this section we have looked at the initial costs, medium term costs and the long run recurring costs compared to a status quo scenario where these changes do not occur.

411. The analysis in this paper remains preliminary, and indicative only of the potential magnitude and balance of costs and savings to the ICO of implementing the proposals in the government's consultation. More detailed assessment will be needed before these are used for business planning purposes. Finalised proposals with a greater level of granularity will be required to enable this. It should be noted that, in many cases the savings to the ICO are more likely to be realised as increased efficiency and ability to meet that demand than in reduction in total staff numbers.

412. In the short run we expect there to be a period of adjustment in which systems and guidance will change. Activities expected in the short term have been split into two stages. Stage 0 accounts for the immediate impact of standing up resource to manage the Act process, expected in years 0 and 1. While stage 1 accounts for transition costs expected in years 1 and 2. When including pre-implementation costs in the overall value of the Act, we have applied a negative discount prior to including in the BIT calculator. Stage 0 includes the following activities:

Stage 0:

a. Co-ordinating Act process internally in the ICO and with DSIT

b. Internal ICO expertise required to input on Act proposals and implementation plans

413. We are able to estimate the potential costs of these reforms to the ICO using a time-cost approach and evidence gained from discussions with the ICO on resourcing, wage costs and

activities[215]. A breakdown of the costs estimated to occur in stage 0 can be found in the table below, these are annual costs and are expected to be incurred in the year before and the first year after implementation.

Table 37: Estimated Stage 0 (0-1 year) costs to ICO of policies, 2024 prices

Reform	Impact	Familiarisation Cost (£million) Low	Familiarisation Cost (£million) High	Annual Cost Estimate (£million) Low	Annual Cost Estimate (£million) High
Legislative reform team	Low-Medium	6	10	0.3	0.4
Data Act working groups	Small	1	5	<0.1	0.2
Stage 0 total	-	7	15	0.3	0.7

414. The activities expected to fall under stage 1 are outlined below. The previous analysis had split transition costs into stage 1 and 2. Following ongoing policy development and analysis, these have been condensed into one stage.

Stage 1:

a. Governance, administrative and legal changes to prepare for the change in the ICO's legal status represented by the move away from a Corporation Sole Model. This includes changes to all contracts, leases, agreements etc to reflect our change in legal status.

b. Systems and IT changes will need to be prepared for and put in place for 'day 1', when legislative changes come into effect. Examples include complaints, where proposals could result in different procedures for organisations to follow that will require different back-end systems and reporting processes.

c. Identifying updates to all existing ICO guidance and information to ensure it reflects the updated legislation, including where it will be necessary to resolve areas of complexity or ambiguity.

d. Training and information for staff, particularly those providing externally facing advice services to ensure all staff are able to provide up to date support and engagement from day 1.

e. Development of key new guidance products likely to be required on day 1, to maximise regulatory certainty for businesses.

f. Developing clear policies and approaches to the management of supervisory activity likely to fall across the transition to the new legislative framework, including legal

215 ICO analysis uses a 40% uplift to account for non-wage costs. In order to align with the rest of the IA, we have updated this to 22%.

advice and updated staff training and advice.

g. Updating internal processes and procedures including changes to existing processes such as engaging with and approving risk assessments, codes of conduct and certifications, and setting up new processes for expert panels etc.

h. Incorporating the implication of the reforms in any ongoing work with the ICO's sandbox participants and representative bodies or organisations developing codes of conducts or certification schemes, including assessing the impact on agreed project delivery dates and overall feasibility. Developing and agreeing an approach to assessing the impact on existing certification schemes.

i. The ICO regulatory action policy (RAP) will need to be updated following changes to legislation across the board and the new strategic direction given by the new objectives, powers and duties. This will include development of clear policies and approaches to using new and enhanced powers, setting up any required appeals processes or safeguards etc.

j. Changes to the approach to auditing based on the new accountability framework. The current approach is based on a toolkit, and this will need to be changed based on the new Privacy Management Programme approach

k. Initial increase in reactive advice and support required, as organisations seek ICO input on new legislative requirements

415. Planned proactive work to support key sectors or organisations where there is likely to be the greatest change/highest risk. This would build on existing approaches but would require additional focus during the transition period.

416. There are now additional changes to the eIDAS scheme which were not consulted on initially and included in our estimate. There will be legal and policy costs to us updating our approach to regulation.

417. The table below provides a breakdown of the costs estimated to occur in stage 1, these are annual costs expected to be incurred in the first and second year after implementation.

Table 38: Estimated Stage 1 (1-2-year) costs to ICO of policies, 2024 prices

Reform	Impact	FTE Estimate Low	FTE Estimate High	Annual Cost Estimate (£million) Low	Annual Cost Estimate (£million) High
Governance, admin and legal costs of move from Corporation Sole	High-Medium	11	15	0.5	0.7
Systems & IT	High-Medium	11	15	0.5	0.7
Updating processes and procedures	Small	1	5	<0.1	0.2
Updates to existing	High-Medium	11	15	0.5	0.7

Reform	Impact	FTE Estimate Low	FTE Estimate High	Annual Cost Estimate (£million) Low	Annual Cost Estimate (£million) High
guidance					
Staff Training & Info	Small	1	5	<0.1	0.2
Key new guidance products	High-Medium	11	15	0.5	0.7
Supervisory policies and approaches	Small	1	5	<0.1	0.2
Ongoing work with stakeholders	Small	1	5	<0.1	0.2
eIDas	Small	1	5	<0.1	0.2
RAP	Low-Medium	6	10	0.3	0.5
Auditing Changes	Small	1	5	<0.1	0.2
Reactive advice and support	High-Medium	11	15	0.6	0.9
Proactive external support	Small	1	5	<0.1	0.2
Stage 1 Total	-	68	120	3.0	5.3

418. After the initial costs outlined above, we expect there to be an increase in annual costs compared to the status quo as the ICO responsibilities and structure changes. These are costs are outlined below

a. New ICO duty to consult with other regulators. This introduces a new set of checks and balances which will require more staff coordination. This overall will have a small impact.

b. Mandatory impact assessments when developing statutory codes and statutory guidance, will require an expansion of resources to ensure robust impact assessments which are supported with appropriate evidence.

c. Setting up expert panels for statutory codes of practice and statutory guidance: giving the Secretary of State for DSIT the power to require the ICO to set up a panel of persons with expertise when developing statutory codes of practice and statutory guidance. This builds on existing ICO work but will require some additional work to identify, recruit and provide support to relevant panels. This may be a small impact, though this will be dependent on the number of statutory codes and guidance the ICO are asked to produce.

d. Governance changes: salary for the new board. There are likely to be small ongoing net costs for additional NEDs.

e. Codes of conduct: the provision to allow codes of conduct under PEC Regulations will require us to respond to demand in the market for codes under PEC Regulations. This is a

new area where Competent authorities may send us codes of conduct to comment on as and when developed which will take 8-12 weeks. We do not know how many of these may come forward therefore demand is unpredictable. Taken together this is a likely small impact.

f. Joint processing by Intelligence Services and Competent Authorities: there will be a process to consult the ICO when a designation notice of joint processing is issued by the SoS. This is unlikely to be a significant demand and is analogous to the current process of consultation on national security certificates.

g. Reporting costs as a result of ongoing updated reporting requirements on the ICO to report on new duties and objectives etc.

h. Systems and IT costs ongoing to account for operation and maintenance of any new systems.

Table 39: Estimated annual costs to ICO of policies, 2024 prices

Reform	Impact	FTE Estimate Low	FTE Estimate High	Annual Cost Estimate (£million) Low	Annual Cost Estimate (£million) High
Reporting requirements	Small	1	5	<0.1	0.2
Systems and IT	Low-Medium	6	10	0.3	0.4
New ICO duty to consult	Small	1	5	<0.1	0.2
Mandatory IAs for statutory codes and guidance	Small	1	5	<0.1	0.2
Setting up expert panels for statutory codes and guidance	Small	1	5	<0.1	0.2
Governance changes	High-Medium	11	15	0.5	0.7
Codes of conduct (under PEC Regulations)	Small	1	5	<0.1	0.2
Intelligence services and competent authorities	Small	1	5	<0.1	0.2
Costs Total	-	23	55	1.0	2.4

Enhance the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO)

419. This section of analysis has been provided by the Home Office, and is broken down by measure. Where evidence is unavailable costs have been assessed qualitatively and can be found in the ‘non-monetised section’

Introduce the ability to actively review automated decisions

420. Currently, LEAs are required to inform a data subject as soon as reasonably practicable when a decision which produces an adverse legal effect, is made which is based solely on automated decision making (ADM). The purpose of this is to allow the data subject to then request that a human either reconsiders that decision or takes a fresh decision not based solely on ADM.

421. The police have stated that this can cause them difficulties. For example, in a scenario where automated decision making is used to match an individual to a record on a watchlist of potential suspects, the police must then either inform the data subject that they are under investigation (thereby tipping them off that they are of interest) or, alternatively, ensure that there is human intervention in the decision (thereby removing the need to inform the data subject but running the risk that by the time the human review had been completed, it is too late to act).

422. This proposal will provide an alternative option for LEAs to provide for a human to review the decision after it has been taken ('active human review') as soon as is reasonably practicable thereby removing the need to notify the data subject at the time. It effectively builds in the remedy that the data subject should have had were they notified that a decision had been made based solely on automated processing. However, in order to ensure that the new power is only used when necessary, LEAs will only be able to use it if informing the data subject would engage one of the grounds set out under section 44(4) of the DPA (e.g. to avoid obstructing an official or legal inquiry, investigation or procedure, to safeguard national security etc.). This change ensures that the rights of data subjects who are subject to ADM continue to be protected whilst improving the ability of the police to tackle crime, ensure public safety and bring offenders to justice. It contributes to the HO priority outcomes of reducing crime and the risk of terrorism to the UK and UK interests overseas.

423. This is permissive legislation as it is assumed that LEAs will only use it if they expect the benefits to equal or exceed the costs. This proposal should result in a 'no worse than zero net cost'.

424. There will be increased efficiency costs for LEAs if they decide to 'actively human review' an automated decision instead of notifying the data subject. This is because of the increased workload on policing arising from the increased number of automated decisions.

425. Also, since the police sometimes decide not to deploy systems which use ADM because of the current notification requirement this change would better enable the use of such systems which will allow data to be processed more swiftly, thereby providing efficiency savings for LEAs.

426. Where there is a risk of compromising investigations and/or police capabilities, the MPS stated that they expect to use active human review in around 90 per cent of cases; this was taken as a central value, with 80 and 100 percent used as low and high values respectively to represent uncertainty around the central estimate. This is likely to lead to an increase in workload and a corresponding increase in costs for LEAs. This is a strong assumption given the likelihood that some form of human review would have been conducted anyway; however, it is likely that the volume of human reviews will increase as a result of this proposal.

427. The MPS also estimate that their current caseload is in the low hundreds annually. This implies a range of between 100 and 500 with an average central estimate of 300. This number of cases was then multiplied by 2, 3 and 4 respectively to give values for the whole of the UK. These values come from the fact that the MPS employs one quarter of all UK police officers so the highest

figure assumes that there will be identical utilisation of active human review throughout the UK with the low and central estimates representing lower utilisation.

428. The time taken to complete an active human review was given as between 0.5 and 1 minutes (where comparing two records to determine if they relate to the same person) and between 15 and 30 minutes (for more complex matters where, for example, there may be a number of data points to be analysed). The low estimate is taken as 1 minute, central as 15 minutes and high as 30 minutes.

429. For cases involving investigations, the review would be conducted by a police officer or police staff depending on the type of review conducted. For cases involving a series of linked pieces of intelligence, it would be performed by an intelligence analyst. Pay grades for these professions were not provided, however, an hourly pay rate was taken from the ASHE Table 14.5a[216] (ASHE SOC code 3). The wage of £16.53 (2023 prices) was then adjusted to £20.66 to reflect non-wage costs and 2024 prices.[217]

430. The number of cases, percentage of cases for which active human review would be pursued, time taken per review and wage of employees are multiplied to give the ongoing cost.

Table 40: Active human review ongoing costs, 2024

Estimate	No of cases	Percentage reviewed (%)	Review time (hrs)	Reviewer wage (£/hr)	Cost per year (£)	Total Cost (£ PV)
Low	160	80	0.02	20.66	60	500
Central	810	90	0.25	20.66	4,200	36,000
High	2,000	100	0.50	20.66	20,700	177,800

Source: MPS Consultation, ASHE Table 14.5a
Notes: Totals may not add due to rounding.

431. Ongoing costs lie in the range £0.00 to £0.18 million (PV), with a central estimate of £0.04 million (PV) over 10 years in 2024 prices.

Powers relating to verification of identity or status (Home Office & DSIT)

432. The proposal will not impose any additional costs on providers who are already certified. For providers who are not currently certified but who subsequently wish to become certified a cost estimated by DSIT to be between £10,000 and £15,000 will be incurred (2024 prices).

433. Research is currently being conducted by DSIT to determine how many providers are not certified and what the expected cost of becoming certified is. Through feedback from the certified IDSP working group, it is predicted these 43 verified firms represent the majority of providers in the UK.

434. Using a low/medium/high scenario to represent this as 95%/75%/50% of the total number of firms respectively, the cost from current unverified firms getting certified is estimated to be between £20,000 and £570,000, with a central estimate of £160,000 in 2024 prices.

435. The total number of firms that would need certification over the appraisal period is an evidence gap, so it is assumed that there will be no additional firms needing verification during the appraisal period. This makes this cost a transition cost only.

[216] Annual Survey of Hours and Earnings (ASHE) - Guide to tables - Office for National Statistics (ons.gov.uk)
[217] Statistics | Eurostat (europa.eu)

436. The proposal may also impose a cost on employers and landlords if they have contracts with non-certified providers and they are required to change providers. There is uncertainty regarding the extent of this cost.

Table 41: Restricting IDVT RtW/RtR scheme checks, 2024 prices.

Estimate	Total number of firms	Percent of market affected (%)	Number of firms that will need to sign up	Cost of certification (£)	Total setup Cost (£)
Low	40	5	2	10,000	20,000
Central	51	25	13	12,500	160,000
High	76	50	43	15,000	570,000

Notes: Totals may not add due to rounding.

Delivery of the National Underground Asset Register

437. This analysis has been taken from the NUAR Impact Assessment 2024 published by DSIT. For a more detailed breakdown of some of the indicative sector specific costs and benefits please refer to the NUAR Impact Assessment directly.

438. Total direct costs of the introduction of legislation will be £225m over 10 years, discounted and in 2024 prices. This includes data transformation costs and familiarisation costs faced by businesses and charges levied on asset owners.

439. The full list of compliance activities, estimated costs and sources are summarised below:

a. **Vectorisation of data** - Some asset owners hold data in a non-vector format (such as PDF, JPEG and PNG). These organisations may be required to convert data into a vector format prior to sharing it with NUAR in the future (specifically, image files that detail the location of features such as pipes and cables).

To date, the NUAR team has held ‘data workshops’ with 311 organisations, representing 44% of total known asset owners as of July 2023. Of these organisations, 18 reported owning location data related to features in a non-vector format (12 energy, 2 local government, 2 water, 1 pipeline, 1 transport). Using this finding, we project there to be approximately 50 organisations across all organisations who may be impacted should this requirement be enacted, the majority being within the energy sector, particularly Independent Distribution Network Operators (IDNOs).

During the NUAR Pilot and Preparation Phase (2019-21), work was commissioned to test the feasibility and costs of ‘vectorising’ raster datasets. This work involved a local authority and two energy companies. Findings from this work demonstrated that there are a variety of options available to asset owners who may need to convert their data. Options range from using in-house or specialist staff to convert the data manually using off the shelf software, to procuring commercial data services on the open market. The findings also found the resource, capabilities and technology used depended heavily on the size and condition of the data requiring conversion.

The pilot's findings demonstrate a range in costs. For example, one of the participating energy companies introduced new internal systems for vectorising data and deployed these systems to convert all their data for the London region at a cost of £84k (2021 prices). Likewise, the participating local authority vectorised 8 disparate datasets at a cost of £55k (2021 prices). As the actions taken by these organisations (and thus the cost occurred) mirror the action any non-compliant organisations will need to take should this requirement be enacted, and as their data is likely to be similar, we estimate costs to be between £55k (low) and £84k (high). However, as costs depend largely on the size and condition of the data held, we have also applied sensitivity analysis to account for uncertainty.

b. **Initial data transformation costs** - This cost involves a one-off activity to map source AO data with the NUAR data model and to setup tools to automate data transformation processes (e.g. FME workbench creation, etc). Asset owners completing onboarding activities by 30 September 2024 will have had this work completed on their behalf as part of the Build Phase of delivery, funded by the Geospatial Commission. As such they will not incur additional costs. We have therefore assumed that this will fall to 25% of asset owners, as approximately 75% asset owners will have had their data transformed through the initial roll out.

c. **Data refresh** - Asset owners will be required to keep the data they share with NUAR up-to-date by providing regular refreshes or change only updates.

In addition, from time-to-time the tools used to carry out transformation activities may need to be reconfigured where changes are made to their own / NUAR data schema. Though the costs of these activities will fall to asset owners, the quantity and frequency of work will vary by organisation. Costs will also vary by the tools and systems individual asset owners deploy and the quality of their data.

d. **Familiarisation costs** - As with any new regulation, some resource in the form of staff time is required for each organisation to understand the new obligations and how they apply to their organisations. These costs apply to all asset owners as a result of the relevant proposals being implemented, with low, central and high values representing the range of uncertainty.

e. **Administration costs** - Resource in the form of staff time will also be required to oversee and support successful completion of new obligations.

Table 42: Summary of transition and ongoing costs to businesses of NUAR

10 year average annual, 2024 prices, discounted) The input figures in this section are in 2021 prices. They are converted to 2024 prices for the final output.

Activity	Description	Estimated annual cost per activity across all businesses,	Number of organisations potentially impacted	Estimated effect £/year per business on average
Vectorisation	Organisations who hold data in a non-vector format (PDF, JPEG, PNG) may need to convert their data prior to sharing it with NUAR. This is a one-off cost.	£3.5m	50	£70k (these costs will fall during the transition period)
Initial data Transformation	Activities involved in mapping source AO data with the NUAR data model and setup of tools to automate data transformation processes (e.g. FME workbench creation, etc)	£2.1m	176	£11.9k (these costs will fall during the transition period)
Ongoing data refresh	Executing data transformation activities to provide updates to NUAR where data or the data model has changed.	£13.7m	705	£19.4k
Familiarisation costs	Resource in the form of staff time required to understand the new regulatory requirements.	£169k	705	£240 (these costs will fall during the transition period)

Activity	Description	Estimated annual cost per activity across all businesses,	Number of organisations potentially impacted	Estimated effect £/year per business on average
Administration costs	Resource in the form of staff time required to oversee and support successful completion of new obligations.	£48k	705	£68

Improved interoperability across health and social care systems

The following analysis is taken from the DHSC Open Data Architecture Information Standards Impact Assessment, please refer here for the full breakdown of expected impacts.[218]

Familiarisation costs

440. As a result of enacting the legislation, IT suppliers will incur up front familiarisation costs to read and understand the new legislation and any guidance provided to support it. Health and care providers will not incur familiarisation costs under DUA, as they would have already familiarised themselves with the legislation/guidance under the HCA.

441. To estimate the familiarisation costs faced by IT suppliers, we have used evidence from a Post Implementation Review for an analogous measure, the Network and Information System (NIS) regulations[219] to estimate the time required for IT suppliers to familiarise themselves with the legislation and multiplied this by an hourly cost rate to obtain the total cost. There will be 36 hours required in total per IT supplier. The cost per hour of this time will on average be £21.56, calculated using median hourly earnings for the Information and Communication sector from the ONS Annual Survey of Hours and Earnings 2023[220], uplifted by 22% to account for non-wage costs. The Information and Communication sector is used as it is assumed, this is the sector IT suppliers operate in, and that familiarisation will be required by staff to help understand what changes are required. The familiarisation costs will be incurred with each batch of standards released ahead of implementation, so IT suppliers can familiarise themselves with guidance.

442. The 10-year present value of familiarisation costs across stakeholders considered is estimated to be £0.02 million.

Training costs

218 Open Data Architecture Information Standards, DHSC (2024)
219 Post-Implementation Review of the Network and Information Systems Regulations 2018 (publishing.service.gov.uk)
220 ONS: Annual Survey of Hours and Earnings, 2023

443. We expect there to be changes to how data needs to be processed by health providers to conform with the new mandatory standards for IT suppliers, alongside upskilling staff to use new systems or new functionalities in upgraded existing systems. This will incur training costs.

444. Training costs will be incurred once clinical systems are updated with the standards. Based on this, the cost attributed to each legislation will be dependent on our assumption of compliance take-up (details of compliance assumptions are outlined in the DHSC Open Data Architecture Information Standards Impact Assessment). As such 76% of health and care providers will incur training costs because of DUA.

445. To estimate these training costs, we have used published workforce data on the number of staff that will need to be trained in each stakeholder group and primary research on the training time required per individual. As part of the primary research, the NHSE information standards and interoperability survey, health providers indicated that 2.2 hours of training will be required per individual on the mandated information standards. This provides us with the total time required for training across each stakeholder group, which we have then multiplied by average annual hourly costs to obtain the full training cost. The cost rate per hour of training is based on average hourly salary costs in related sectors for each organisation. The average hourly cost assumptions have been converted to the full cost of employment, based on the Regulatory Policy Committee guidance. The individual assumptions and cost rates used are detailed in the DHSC Open Data Architecture Information Standards Impact Assessment.[221] It is acknowledged that training time may be repurposed from existing earmarked time; however, it is prudent to reflect the value of that time in this assessment.

446. The 10-year present value for training costs across stakeholders considered is estimated to be £50.1 million.

Information standards related systems update

447. We expect there to be costs directly related to ensuring clinical systems adopt the mandatory standards as set out by the Secretary of State – where the systems do not already comply.

448. We expect there to be reconfiguration costs for IT suppliers who seek to modify their products and services to meet the required standards to supply products and services to health and social care providers. These costs will be incurred for those suppliers that currently do not provide products or services that comply with the standards. Based on data from the NHSE information standards and interoperability survey, it is estimated these costs will be incurred by 44% of IT suppliers[222].

449. We expect there will be additional costs associated with transitioning providers existing systems and processes to make them compliant with the standards. It is assumed that transition costs will occur because of this. These costs are likely to be passed on to health and social care providers. No costs for cleansing or renormalisation of historic data are considered. Also, as health and social care providers will need to procure compliant IT products and services, we anticipate that there may be administrative costs associated with revisiting existing

221 Open Data Architecture Information Standards Impact Assessment, DHSC (2024)
222 Information Standards and Interoperability Survey, NHS, Feb 2024

contract arrangements and/or switching suppliers should any of their procured products or services be non-compliant. These impacts are likely to vary between provider sizes and types.

450. To estimate the cost of the relevant updates to systems in relation to the information standards, we obtained data from IT suppliers through the NHSE information standards and interoperability survey. The survey indicated that uplifts in cost were likely to be 15% of the existing contract value. Baseline contractual values were identified for the majority of the public health and social care providers using publicly available contract information. Where information was not available, we developed cost assumptions using secondary research, interview data, and accounting for the relative size of the organisation – with separate assumptions used per the size of the organisation considered.

451. The 10-year present value for information standards related systems update costs across stakeholders considered is estimated to be £148.6 million.

Conformance testing and accreditation costs

452. Establishing an accreditation scheme requires additional regulations. The full impacts cannot be accurately appraised at this stage because of significant uncertainty regarding the timing of any use of the powers and the content of any regulations. We will improve our assessment of the impact on both providers and suppliers and how we can mitigate this as part of the development of such regulations. Regulations will also be designed to minimise these costs to small and micro business as far as possible.

453. Below we provide our current assumptions regarding the accreditation scheme and associated costs.

454. To implement the information standards for IT systems in the health and social care sector, IT suppliers' products will need to be tested to prove their conformance with required standards. Different standards will require different assessment approaches, and this flexibility will be built into our process design. There will be three options for conformance testing and accreditation:

i. **Self-assessment** – as part of the standards publication, a clear set of tests and supporting tools to assess conformance will be provided to suppliers who will then be able to self-assess conformance. Suppliers may be required to provide the detailed results of their tests to buyers as part of procurement, compliance checks, or as part of accreditation.
ii. **Central assurance** – as part of the process for onboarding and remaining on procurement frameworks, NHSE may conduct testing either using its own staff or a subcontractor. This model is already used to some extent with Primary Care and Social Care record systems which are tightly and actively managed via enduring contractual arrangements that sit alongside procurement framework. This may also be performed as part of compliance process (e.g., if care providers report non-conformance).
iii. **Certificates of Conformance** – a formal scheme for assessing conformance will be developed in conjunction with the United Kingdom Assessment Services (UKAS) that oversees conformance testing of industry standards in the UK. Third party Conformance Assessment Bodies (CAB) would register with and be assessed by UKAS as fit for conformance testing and providing certificates of conformance to

suppliers. Suppliers would be required to show a valid certificate of conformance issued by a CAB

455. It is estimated that accreditation costs will be required for each IT supplier. To estimate these costs, we have used the cost for other national standard certifications as a reasonable benchmark to estimate the likely costs associated with accreditation. This cost has been based on average costs associated with ISO 27001 certification. In addition to these costs, we have also included an estimate for internal costs incurred by IT suppliers to demonstrate compliance and gain accreditation. This estimate is based on the time required each year, which is assumed to be two months of one FTE per IT supplier. Refer to the Open Data Architecture Information Standards Impact Assessment for further detail on assumptions and calculations.[223] The 10-year present value for accreditation costs is £2.6 million.

Compliance, monitoring and enforcement costs

456. The potential costs that NHSE or an equivalent organisation may face in relation to overseeing and enforcing compliance with DUA legislation in England extend beyond the initial accreditation process. The accreditation process is typically a point-in-time evaluation, which ensures that IT suppliers meet the required standards at the time of assessment. However, continuous monitoring is necessary to ensure that these suppliers and health and care providers maintain compliance with standards across both HCA and DUA legislation.

457. NHSE or a similar body would incur costs relating to monitoring and enforcing compliance with DUA legislation in England. These costs would include the development and implementation of monitoring mechanisms, staff training on data protection laws, and the establishment of audit processes to ensure adherence to DUA regulations. The compliance monitoring body would also need to allocate resources for regular assessments and audits to evaluate IT suppliers' compliance with the legislation. Legal and regulatory experts may be required to provide guidance and oversight. This cost also includes the costs required to run the public censure process. Overall, these costs would be essential for maintaining the integrity and security of patient data, safeguarding privacy, and upholding legal compliance within the evolving landscape of digital health and social care innovation.

458. For this RIA, we assume that a small regulatory body will suffice to enforce compliance with DUA regulations. We anticipate that an intelligence-led approach to monitoring will enable a compact yet efficient team. To estimate the necessary full-time equivalent (FTE) staff, we have used the FTE count from the Postal Service Commission (Postcomm), a small regulatory body, now integrated into Ofcom, as a reference for the regulator's potential size. In selecting this benchmark, we assessed the size of all UK regulators to find one similar to our proposed regime. Among the smallest regulators, such as the Gambling Commission (350+ FTE), Pensions Regulator (900 FTE), and Information Commissioner's Office (1,000 FTE), we deemed Postcomm as the most fitting comparison. Postcomm's shift towards compliance monitoring and upholding the universal service obligation, with minimal direct intervention, mirrors our expected regulatory approach, which is less extensive than other economic regulators. Additionally, its small size corresponds with our projected requirements. However, it should be noted that the specific operating model for this new regulator remains to be developed.

223 Open Data Architecture Information Standards Impact Assessment, DHSC (2024)

459. The 10-year present value for compliance monitoring and enforcement costs for IT suppliers is estimated to be £1.6 million.

Criminalise the creating, or requesting the creation of, a purported intimate image (deepfake) of another person aged 18 or over without the adult's consent or reasonable belief in consent.

Police

460. We have estimated the police costs of enforcing the new offences by applying both the unit police investigation cost (£1,011 in 25/26 prices) and a multiplier (1.5) of violence without injury offences (deemed to be the most similar offence group) from the Economic and Social Cost of Crime (2015).[224]

461. On this basis, the average annual cost of the new offences to the police is expected to be £0.2m in the low estimate, £1.0m in the central estimate and £1.8m in the high estimate.

HMCTS

462. To calculate the expected number of prosecutions, observed data for Voyeurism, a proxy offence was used. In the low scenario, we assume that 6% of police recorded crimes lead to prosecutions, and in the high scenario 7% do. The following table shows the estimated number of prosecutions in the low and high scenario, with the central being the midpoint:

Prosecutions	**Year 1**	**Year 2**	**Year 3**	**Year 4-10**
low	5	5	6	7
Central	14	22	35	55
high	24	39	63	102

463. These cases are then multiplied by Magistrate Court sitting day unit costs, to give an average annual cost of less than £0.05m in the low estimate, and £0.1m in both the central and high estimates.

Legal Aid Agency

464. The additional prosecutions will also result in an increased caseload for the LAA.

465. It is assumed that 50% of defendants in the magistrates' courts will be eligible for Legal Aid. The average annual cost to the LAA is estimated to be less than £0.05m in the low, central and high estimates.

HMPPS

466. HMPPS will be impacted by the creation of these offences as some convictions will result in custodial sentences and probation.

467. The analysis assumes 30% of convictions lead to custodial sentences, where the low scenario uses a sentence length of 2 months, and the high scenario uses a sentence length of 6 months (the maximum for this offence). The following table shows the estimated number of

[224] https://assets.publishing.service.gov.uk/media/5b684f22e5274a14f45342c9/the-economic-and-social-costs-of-crime-horr99.pdf

additional prison places needed in the high and low scenario over the 10-year appraisal period, with the central estimate being the midpoint (all these estimates have been rounded up so serve as potential overestimates):

Prison Places	**Year 1**	**Year 2**	**Year 3**	**Year 4-10**
low	1	1	1	1
high	2	3	5	8

468. Due to on-going prison capacity issues, it is assumed that additional custodial sentences will require the construction of additional prison places. According to MoJ published data, the construction of a prison place costs £600,000 and the cost of a prison place per year is £56,000 in 2025/26 prices.

469. Therefore, the central estimate is that the construction of the required additional prison places will result in a one-off cost of £0.7m in the low estimate, £3.2m in the central estimate and £5.8m in the high estimate.

- The annual running costs of these prison places is expected to result in an average annual cost of £0.1m in the low estimate, £0.3m in the central estimate and £0.4m in the high estimate.
-
- The Net Present Value (NPV) of this measure across 10 years, is estimated to be –£2.8m in the low estimate**, -£14.3m in the central estimate** and -£25.6m in the high estimate. The NPV is negative as there are no monetised benefits.

Direct Costs - Non – Monetised

470. This section of analysis provides a breakdown of all non-monetised costs that UK businesses and public organisations could face as a result of this package of reforms.

Enhance the Work of the UK Intelligence Services and Law Enforcement Agencies in the Interest of Public Security

471. This section of analysis has been provided by the Home Office, and is broken down by measure. Where evidence is available costs have been monetised. Where this has not been possible a qualitative assessment of the potential costs for each measure has been provided.

T**ime limits for responding to requests by data subjects' (Part 3 and 4 DPA**)

472. A data subject can exercise their right to request what information is held about them through a SAR. Currently all SARs under Part 3 (Law Enforcement) and 4 (Intelligence Services) need to be actioned within one month. Unlike the UK GDPR, Parts 3 and 4 of the DPA 18 do not recognise and allow for a proportionate time period for dealing with particularly complex requests. The proposal is to mirror an existing UK GDPR provision within Part 3 and 4 of the DPA 18 that permits a two-month extension to a SAR time period when a request is particularly complex.

473. The UK Intelligence Services and National Crime Agency (NCA) expect that there will be little actual change regarding costs associated with processing SARS. This is because SARs will still be processed, regardless of how long it takes, so a two-month extension for complex SARs will not result in an increase in ongoing costs.

474. It is assumed that this response from the UK Intelligence Services and NCA is representative of all competent authorities

Law enforcement processing and codes of conduct

475. In the UK GDPR codes of conduct can be produced by representative bodies (for example, trade associations) to clarify the application of data protection laws in particular sectors, which are then approved by the ICO. There is no equivalent power under Part 3 DPA 2018, and stakeholders have indicated that this could be a useful tool to future-proof their data use. This proposal therefore replicates the power for similarly representative bodies to create codes of conduct under Part 3.

476. This is permissive legislation, as it does not mandate representative bodies to create a code of conduct. Such bodies should only engage in this activity if they deem the costs greater than or equal to the benefits. It is therefore assumed that this proposal will result in a 'no worse than zero net cost' to representative bodies.

477. There will be an additional cost to LEAs of representative bodies introducing codes of conduct as this will require their employees to familiarise themselves with the codes.

478. There will be increased efficiency costs associated with the drafting of codes of conduct for the representative bodies who decide to undertake this.

479. There is, however, nothing to stop an organisation from voluntarily adopting a code issued by another body which may reduce the overall set-up costs of this proposal.

480. This may, however, lead to a 'free-rider' problem where organisations have reduced incentives to expend resources to create their own code of conduct if they believe other bodies will do so for them. This may provide a disincentive to be a 'first mover' in creating a code of conduct.

481. The ICO will also have to consider and approve new codes of conduct which will create an additional efficiency cost as ICO employees will have to dedicate their time to approval processes. This cost will depend on the number of representative bodies who decide to introduce codes of conduct.

482. Representative bodies who decide to introduce codes of conduct will be expected to put in place monitoring processes on an ongoing basis to ensure that the code is followed. The time spent by employees on doing this will be an additional cost.

Amendments to Part 4 of the DPA 2018 - Joint processing by intelligence services and competent authorities

483. Currently, policing and the intelligence services are governed by different data protection regimes which present challenges to joint operational working.

484. UK Intelligence Services believe that this proposal will lead to more dynamic working practices with police, such as the option to share databases. It should also lead to improved confidence in sharing data.

485. There will be additional administration requirements on controllers which will increase costs. This will be limited by the fact that this proposal will only take effect in very limited circumstances.

Improved Interoperability across Health and Social Care Systems

Penalty costs to businesses

486. This penal regime represents a potential cost to IT suppliers. Given each fine would be determined by the severity of the breach and the individual circumstances of the businesses, it would not be proportionate to accurately quantify this cost. Furthermore, Better Regulation guidance states that when calculating the NPV, business NPV and EANDCB, we should not include any costs (for example fines or penalties) incurred by companies for non-compliance.

Training costs: care workers

487. Training will only be required across clinical staff in public and private hospitals and consultants at GPs. A small number of care workers may require training for public and private social care providers i.e., those involved in the development of service user care plans in association with healthcare providers and social workers, but the number is expected to be negligible as carers are focused on delivering pre-defined tasks assigned in service users care plans, hence it is not proportionate to quantify this cost as part of this assessment.

Facilitating online safety researchers' access to data

488. All costs involved in our modelling are illustrative direct costs to business only, as any regulation enabled by this primary legislation will place requirements on platforms directly to allow researchers access to certain requested data. Therefore, there will be no cost to households resulting from this legislation. The cost inputs are in 2022 prices – in this IA they have been inflated to 2024 prices using ONS data.[225]

489. These illustrative costs fall into three main categories:

Familiarisation costs – the potential cost to platforms of familiarising themselves with the guidance and understand what is expected of them.

490. Summing the wage costs of each staff member, multiplied by the RPC non-wage uplift guidance of 1.22, over the time required, provides a cost of familiarisation per firm of around £705. Multiplied by 30-40 platforms, we estimate the range of total cost of familiarisation for all firms in Table 1 below.

Table 43 – Illustrative familiarisation costs

Estimates	Low	Central	High
Familiarisation costs	£21,200	£24,700	£28,200

225 ONS Quarterly National Accounts, March 2024 release. 8.8% uplift used. https://www.gov.uk/government/collections/gdp-deflators-at-market-prices-and-money-gdp

Adaptation costs – the up-front costs firms could face when adapting to any potential regulation enabled by this primary legislation.

491. Summing the wage costs, multiplied by the non-wage uplift, for the adaption focused tasks shown in the Researchers' Access to Data Impact Assessment[226], as well as the cost of adopting a secure online environment, the total cost of adapting to potential regulation is estimated to be around £10,200-£16,600 per platform. Multiplied by the range of 30-40 platforms, we arrive at the total cost of adaptation for all firms in Table 43 below.

Table 44 – Illustrative adaptation costs

Estimates	Low	Central	High
Adaptation costs	£0.3m	£0.5m	£0.7m

Ongoing costs – the extra ongoing costs platforms could face following implementation of regulation enabled by this legislation. Under the illustrative application-based data access model, platforms would incur the cost per data request of processing a request. These costs are broken down into *processing and approving requests*, *collating and reformatting data and legal review*.

Table 45 – Cost of data requests

Request	Low scenario	High scenario
Processing and approving a request	£200	£430
Collating and reformatting data	£1,400	£2,200
Legal review	£160	£160
Cost per single data request – sum of above rows	£1,800	£2,800

492. The final ongoing cost is the annual cost of upkeep for the secure online environment to host the data for researchers. As outlined earlier, this is between £11,700[18] and £19,600[19] per year, per organisation, which equates to around between £0.4 million and £0.6 million per year for all organisations combined.

493. The ongoing costs i.e. the cost of upkeeping the secure online environment and the costs of fulfilling research requests together total an illustrative estimated cost to business of around £0.4 million to £0.8 million per year.

494. Please refer to the Researchers' Access to Data Impact Assessment for a full breakdown of illustrative costs.[227]

Criminalise the creating, or requesting the creation of, a purported intimate image (deepfake) of another person aged 18 or over without the adult's consent or reasonable belief in consent.

Police

495. There may be familiarisation costs to the police from the new offence. These are expected to be minimal as the purposes and structures of the new offences should be familiar, therefore these costs should fall under business-as-usual.

226 DSIT: Researchers' Access to Data Impact Assessment, 2024
227 Researchers' Access to Data Impact Assessment, DSIT, 2024

CPS

496. The CPS may face additional costs associated with the additional cases being prosecuted under these offences, however we expect these to fall under business-as-usual costs.

HMPPS

497. It is assumed that offenders receiving custodial sentences will spend half of these in prison, and HMPPS will incur additional costs associated with offenders on probation and on licence. Likewise, 70% of offenders will not receive a custodial sentence of whom the majority are assumed to receive community sentences.

498. It has, however, not been possible to monetise these costs due to a lack of information on unit costs for non-custodial sentences.

Indirect Costs - Monetised

499. This section of analysis provides a breakdown of all indirect monetised costs that UK businesses and public organisations could face as a result of this package of reforms, specifically the creation of innovative and secure Smart Data schemes and the Increased Interoperability and Trust of Digital Identity Systems.

Increased Interoperability and Trust of Digital Identity Systems

500. More detail on the calculation of the monetised costs of the proposed Digital Identity reforms can be found in the published Digital identity and attributes - De Minimis Assessment.[228] In this assessment we provide an outline of costs of the proposal. This analysis looks at the same four potential use cases measured in the benefits section.

501. All costs to business are indirect because the legislation only allows public sector organisations the option to open their data for private sector use. It does not mandate anything for private sectors companies to do, not even when it comes to familiarisation. As a result of the legislation being permissive, these estimated costs are not included in the NPSV or EANDCB of the Act.

502. More detail on the calculation of the monetised value of potential costs of the proposed Digital Identity reforms can be found in the published Digital identity and attributes - De Minimis Assessment.[229] In this Data (Use and Access) Act Impact Assessment we provide an outline of the main monetised costs of the proposal. This analysis looks at the same four potential use cases measured in the benefits section;

a. Employee mobility
b. Travel authorisation and ticketing
c. Home buying
d. Trusted financial transactions

and compares the benefits across the 3 different scenarios (central, best and worst case) and both the costs to both private and public sector organisations.

[228] Digital identity and attributes - De Minimis Assessment DSIT, 2024
[229] Digital identity and attributes - De Minimis Assessment DSIT, 2024

503. DSIT carried out a stakeholder engagement exercise to attempt to define the indirect costs[230] businesses may face to comply with the legislation, both for digital identity as a whole and in relation to the four specific use cases. We engaged with a variety of sectors. Multiple responses came from organisations that currently operate within the digital identity sector, such as identity service providers, or relying parties that would use the digital identification system. Other responses came from various different sectors. The organisations that took part ranged from micro to large businesses. The engagement enabled us to make some qualitative and quantitative assumptions of what costs businesses may face to familiarise and adapt to the digital identity legislation.

504. The quantitative estimations were then used to model the costs under the three scenarios. Due to the early stage of the legislative planning, it was difficult to precisely estimate what costs businesses are expected to incur. Nevertheless, we expect these costs to be rather small especially for digital identity providers already established in the market as they believe they are expected to undertake limited development work to adapt to the legislation.

505. We assume that only UK medium and large businesses face the costs to adapt to digital identity because their incentive from the potential cost savings allowed by digital identity are expected to outweigh the costs to adapt to the new technology 30. Therefore, the estimated costs per business were multiplied by the number of medium-large UK businesses to estimate what the costs may be for all businesses as a whole.

506. We assume that the size of the total per check fees costs follows the estimated trend of the digital identity market towards the steady state. This is because we expect the number of digital identity checks carried out in the UK to be proportional to the size of the market.

507. Focusing solely on one-off costs to private sector businesses of the proposed changes to digital identity schemes across all use cases, include:

a. **One-off familiarisation costs for businesses:** the costs businesses expect to face to familiarise with the potential digital identity legislation based on the estimations provided by the stakeholder engagement exercise

b. **One-off organisational change costs for businesses:** Organisational change costs consider the costs businesses face to adapt the structure of the organisation, both in terms of how it functions and the staff employed. Examples include the cost to implement a digital identity solution, the cost to hire new staff, or the costs to purchase or change technology platforms.

c. **One-off connection fee for service providers:** We assume that organisations wishing to perform checks against government-controlled data may have to pay a one-off fee upfront

d. **Certification fee for service providers:** We expect service providers to pay a certification fee to be certified against some given standards.

e. **Annual membership fee for service providers:** We expect certified service providers to pay the governance function an annual membership fee.

[230] All costs to business are indirect because the legislation only allows public sector organisations the option to open their data for private sector use. It does not mandate anything for private sectors companies to do, not even when it comes to familiarisation.

508. As well as one off familiarisation costs, we assume that UK businesses wishing to make digital identity checks against government-held databases may have to pay an annual fee in order to carry out each check Therefore the annual cost of per check fees for businesses have been estimated for each use case. We calculate this annual cost as the annual total expected number of checks times the expected price per check which varies depending on the type of identity check.

509. The estimated cost of these checks will vary depending on the type of check, the scenario (time taken for adoption for each use case) and the estimate of the total number of checks for each type of request. More information on these assumptions can be found in table 19 of the Digital identity and attributes - De Minimis Assessment.[231] The total estimated costs for each use case are in the table below alongside the total one-off costs.

510. The estimated total costs include the estimated total cost of the per check fee for all four use cases, one-off familiarisation costs, one-off organisational change costs for the relying parties and one-off total connection fees and membership fees for service providers. The central estimate of the undiscounted costs to UK private sector organisations is £1,597.3m over the 10-year appraisal period. We estimate that the lower and upper bound of the total undiscounted costs all medium and large businesses together may face over the appraisal period are £897.1m and £2,924.8m respectively.

Table 46: Estimated total private sector costs to private sector of Digital Identity reforms by scenario and cost, 2024 prices

Costs	Central estimate Annual estimated costs, £, millions	Central estimate Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)	Best estimate Annual estimated costs, £, millions	Best estimate Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)	Worst estimate Annual estimated costs, £, millions	Worst estimate Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)
Employee mobility: per check fee costs	4.9	31.5	3.0	21.9	9.8	46.2
Travel authorisation and ticketing: per-check fee costs	64.9	454.3	38.9	311.5	129.8	675.0
Home buying: per-check fee costs	2.2	15.5	1.3	10.7	4.4	23.1
Trusted financial transactions: per-check fee costs	0.2	1.5	0.1	1.0	0.4	2.2

[231] Digital identity and attributes - De Minimis Assessment DSIT, 2024

Costs	Central estimate Annual estimated costs, £, millions	Central estimate Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)	Best estimate Annual estimated costs, £, millions	Best estimate Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)	Worst estimate Annual estimated costs, £, millions	Worst estimate Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)
One-off familiarisation costs	-	263.3	-	131.6	-	526.6
One-off organisational change costs	-	821.1	-	410.6	-	1,642.3
One-off connection fees cost for service providers	-	0.7	-	0.5	-	0.9
Certification fees cost for service providers	-	3.6	-	4.1	-	2.8
Annual membership fee for service providers	0.6	5.7	0.5	5.3	0.7	5.9
Total, £, millions	-	1,597.26	-	897.13	-	2,924.84

511. A breakdown of the monetised costs for public sector organisations can be found in the Digital identity and attributes - De Minimis Assessment. DSIT engaged with three public bodies to try and estimate the costs[232] public organisations may pay to adapt to the potential digital identity legislation and thus allow the digital identity market to fully develop. For instance, we gathered some information on the potential costs public sector bodies may face to understand the legislation or make the organisational changes required to allow the private sector to check the databases they hold. We expect public sector organisations to face some rather significant costs to adapt to the legislation, especially to allow the private sector to make checks against the Government-held datasets.

512. We define the worst case estimate as the scenario based on the assumptions that lead to the highest expected costs. We predict high costs for all public sector bodies in a high digital identity uptake scenario where more Departments invest resources to familiarise and adapt to the digital identity system. In order for digital identity to fully develop a high uptake across public

[232] All cost7 to Government bodies are indirect because the legislation only allows public sector organisations the option to open their data for private sector use. It does not mandate anything for public sector organisations to do.

sector bodies is required. Therefore, the worst-case cost estimate is not necessarily unwelcomed.

513. For the worst-case scenario, we have assumed that all departments that may hold significant identity or eligibility data, 9 in total,[233] will face these costs. For the central and best-case scenario, we have assumed that only Home Office, DVLA, DWP, HMRC, and DfE[234] in line with the four digital identity use cases analysed.

514. Based on our assumptions we estimate that, on average, public sector bodies may face a one-off cost of £49,896.0 to ensure that members of the policy teams familiarise with the legislation. However, these are rough estimates based on a small sample size so should be considered indicative only.

515. Total one-off estimated familiarisation costs for public sector organisations can be seen in the table below:

Table 47: One-off public sector familiarisation costs, 2024 prices

Estimates	Estimated one-off familiarisation costs per Department, £	Number of Government Departments	Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)
Central case estimate	49,896.0	5	0.25
Best case estimate	49,896.0	5	0.25
Worst case estimate	49,896.0	9	0.45

516. Additional indirect costs estimated for public sector firms also include:

a. **The cost to allow private sector access to Government-held datasets for public sector organisations:** we expect Government Departments to face costs both to allow the private sector to make checks against their data and to maintain the system in place. The costs estimated in the analysis are baseline and in practice will be subject to iteration. Further examples of these costs can be found on page 54 of the Digital identity and attributes - De Minimis Assessment DSIT, 2024. [235]

b. **Cost to set up and run a governance function:** The digital identity market may function in a trusted and interoperable way conditional on the fact that there is an effective governance function overseeing the market. For instance, we expect the governance function to ensure trust in the market by checking that the members of the Trust

[233] The 9 Departments are: Home Office, DWP, HMRC, DVLA, DfE, HM Land Registry, DHSC, Companies' house, and MoJ.
[234] These are the Departments that are required to open their databases in order for digital identity checks to be carried out in the four use cases.
[235] More information on how this is calculated can be found in the Digital identity and attributes - De Minimis Assessment DSIT, 2024

Framework meet the required standards. Therefore, we assume that without functioning governance the benefits of a fully functioning digital identity market may not be realised.

517. DSIT analysts note that the cost calculations set out in this impact assessments relate specifically to the implementation of these measures. The costs considered here do not cover any costs to the public sector or businesses as a result of the development of the GOV.UK wallet and app. The GOV.UK wallet was announced by DSIT Secretary of State on the 21st January 2025[236].

518. We estimate that, based on our assumptions, the costs public sector bodies may face over the appraisal period to fully realise the digital identity market may range from £199.4m to £577.8m. The central case estimate for the estimated public sector costs is £171.4m.

Table 48: Estimated costs over the 10-year appraisal period, £, millions, (undiscounted), 2024 prices

Costs	Central case estimate	Best case estimate	Worst case estimate
One-off familiarisation costs	0.25	0.25	0.45
Organisational change costs	158.39	158.39	570.22
Governance function funding costs	12.73	40.71	7.08
Total, £, millions	171.37	199.35	577.75

519. The central estimate of the undiscounted costs to UK private and public sector organisations is £1,604.6m over the 10-year appraisal period. We estimate that the lower and upper bounds of the total undiscounted costs all organisations together may face over the appraisal period are £932.8m and £2,926.5m respectively.[237]

Digital Identity monetised costs

520. We expect some public sector organisations to have direct familiarisation costs as a result of this legislation. We expect Government Departments to face indirect costs to open their databases for private sector checks if they wish to as a result of this legislation. There are also costs associated with the setting up and running the digital identity governance function until it becomes self-sustainable. We also expect some UK businesses to face indirect costs. For these businesses there are one-off costs to familiarise with their legislation and adapt to the digital verification system. We also expect UK businesses to face indirect annual costs in the form of fees levied by public sector organisations to connect to government-held datasets and to check data. These fees are intended to offset public sector costs and maintain value for money for the taxpayer.

[236] Digital driving license coming this year, GOV.UK, 21st January 2025
[237] More information on how this is calculated can be found in the Digital identity and attributes - De Minimis Assessment DSIT, 2024

Remove the requirement for paper birth and death registers moving to an electronic register

521. This section of analysis has been provided by the Home Office. Data on the volume of births and deaths and the scenarios used in the modelling can be found in table 31. Gross wages of superintendent registrars and registrars can also be found in table 32.

Set up Costs

IT set up costs

522. The Home Office will update RON functionality to accommodate a move to the electronic register for births, still births and deaths. This cost is estimated at £500,000 (2024 prices) based on the requirements identified which are similar to recent changes to the IT system for other services. Based on the uncertainty surrounding this figure and the fact it is an IT cost, optimism bias has been applied (0%, 25%, 50% for the low, central and high scenarios). The low estimate is about £0.5 million, the central estimate is about £0.6 million and the high estimate is £0.8 million.

Set up cost to registration service (Closure of open registers)

523. There will be a cost to the registration service of closing the current birth and death registers in year 1 only. Each of the 782 registrars of births and deaths for England and Wales holds an open birth and an open death register. This means that a total of 1,564 registers (taken from secure stock records held by GRO) will need to be closed. A low, central and high length of time taken is estimated at 4, 5 and 6 minutes. The gross wage per hour is outlined in baseline volumes. The estimated cost is in the range of £2,500 to £7,300, with a central value of £4,100 in year 1 only (PV, 2024 prices).

Home Office set up cost

524. Changes to processes are minimal therefore face-to-face training for the registration service will not be required. The Home Office will issue new guidance for registration officers together with instructions for the closing of current birth and death registers. The cost of providing written guidance is minimal and is included within business as usual costs so has not been included for the purpose of this IA.

Ongoing Costs

525. The current process in which the superintendent registrar checks and certifies all birth and death entries will be replaced by a quality assurance check of the records. For the purpose of this IA, it has been assumed superintendent registrars will complete a quality check of 20 percent of all births and deaths registered by registrars. This check is likely to take less time than the old certification process which involved the superintendent registrar retrieving the register from a locked safe and then cross-referencing all parts of the register entry to be sure that the information from the register has been correctly keyed into the electronic RON system. This new quality check will take approximately one minute of a superintendent registrar's time for each birth, still birth or death registration. 0.75 minutes are taken as a low scenario, and 1.25 as a high scenario. This is calculated as: time (hours) taken to check entries x cost per hour of superintendent registrar time (see baseline volumes) x number of births and deaths per year. This gives costs in the range of £0.7 to £3.6 million, with a central estimate of £1.7 million (PV) in 2024 prices over 10 years.

Table 49: Summary of impacts, (£ million, 10-year present value), 2024 prices.

Costs (£ million, PV)	Low	Central	High
IT (one off costs) (GRO)	0.5	0.6	0.8
Closure of open registers (LRS)	0.0	0.0	0.0
Superintendent checks (LRS)	0.8	1.7	3.6
Total	**1.2**	**2.3**	**4.3**

Delivery of the National Underground Asset Register

526. This analysis has been taken from the NUAR Impact Assessment 2024 published by DSIT. For a more detailed breakdown of some of the indicative sector specific costs and benefits please refer to the NUAR Impact Assessment directly.

Charges levied on businesses

527. Primary legislation will include a power to enable asset owners to be charged for use of the NUAR platform. The details of the charging scheme will be set out in secondary legislation.

528. Broad, initial principles are that charges would be split across asset owners in the following way:

a. Primary legislation will include a power to enable asset owners to be charged for use of the NUAR platform. The details of the charging scheme will be set out in secondary legislation.
b. Broad, initial principles are that charges would be split across asset owners in the following way:
    i. Asset owners, in their capacity as data providers, would be charged a membership fee based on the anticipated level of benefit they receive from sharing data through NUAR.
    ii. Asset owners would be assigned a charging tier based upon their predicted level of estimated benefit. This could be based on proxy metrics (such as an organisation's network size and total number of connections) used to predict the frequency their data will appear in search requests. Asset owners, whose data is likely to appear most frequently to NUAR end users, would be placed in the changing tier with the highest charge, reflecting the high number of requests they will no longer need to reply to directly (or via a commercial service) as a result of sharing it with NUAR. Those whose data is likely to appear less, would be assigned a charging tier subject to a lower fee.
    iii. The level of charges in different tiers is likely to be a significant reduction in the current costs for asset owners to manage the requirements of the existing legislation. This is supported by findings from the programme's discovery and pilot phases, consultation responses, and feedback received on the emerging MVP service. Additionally, we have used learnings from comparable services internationally and domestically in Scotland.
    iv. Some organisations, such as public sector bodies and SMBs may be assigned a tier with a nominal charge or no charge at all. In all cases, the basis of the fees will be cost recovery, meaning the fees in aggregate are to cover the cost of the service only and thus capped on that basis.

529. Note that as per the Better Regulation Framework, Section 22 of the Small Business, Enterprise and Employment Act (2015), charges are excluded from the definition of regulatory provision, and so do not feature in the EANDCB.

Table 50: Summary of charges levied on businesses following implementation of NUAR

(10 year average annual, 2024 prices, discounted) The input figures in this section are in 2021 prices. They are converted to 2024 prices for the final output.

Estimated annual cost per activity across all businesses	Number of organisations potentially impacted	Estimated effect £/year per business on average
£5.0m[238]	305	£16.4k

Indirect Costs - Non-Monetised

530. Where indirect costs to businesses and the public sector cannot be monetised due to a lack of historical evidence we have provided an in-depth qualitative analysis alongside other government departments.

Creation of innovative and secure Smart Data schemes

531. This analysis was led by DBT as part of the published Smart Data Impact Assessment. For a more detailed breakdown of these costs and benefits please refer directly to the Smart Data Impact Assessment. We expect that the impacts of the primary legislation will make the implementation of Smart Data schemes in secondary legislation happen sooner. Due to this, DBT have estimated the possible, additional (as a result of bringing forward the implementation and running of the schemes for additional time) costs of implementing different schemes in the Smart Data Impact Assessment. In the ‘secondary legislation costs’ section we provide a further, qualitative assessment of the categories of costs for different affected groups that may occur when secondary legislation is in place.

532. When Smart Data schemes are introduced via secondary regulations, there will be costs incurred to operationalise the schemes successfully, and to ensure adequate regulatory oversight. These costs will initially fall on the sector regulator, or any other administrator, who will be named in the secondary regulations as responsible for specific roles. Resources to cover the costs incurred by regulators and scheme administrators will not come from central government, and instead they will be recouped from industry via charges or using the sector regulators existing levy raising mechanisms.

533. The costs incurred from Smart Data can therefore be separated into two categories:

[238] This is the average annual operational costs of running NUAR across the ten year appraisal period. See Annex B of the NUAR impact assessment for details on how this has been profiled. These average annual running costs have included a 10% Optimism Bias adjustment.

a. Costs incurred by regulators and scheme administrators which are then recouped from industry via charges and levies (referred to in this IA as 'implementation costs');

b. Costs incurred directly by data holders and ATPs to participate in the Smart Data scheme

534. As discussed throughout the Smart Data IA, due to several uncertainties, it is not possible to isolate or predict the costs of potential future Smart Data schemes. The full impacts of future Smart Data schemes would be detailed and analysed when these specific schemes are introduced in secondary legislation.

535. The telecommunication sector and Open Banking estimates in the Smart Data Impact Assessment use the Open Banking scheme as a basis. The Road Fuel scheme analysis uses the bottom-up approach used in the Road Fuel Open Data scheme IA. We would expect the 'implementation costs' for future schemes to be lower than those incurred by Open Banking as a result of technical differences between schemes, and lessons from Open Banking.[239]

536. The Smart Data IA analysis of the costs of Open Banking, Telecommunications and Road Fuel showcases how costs will vary depending on the needs of the sector and the design of the schemes. This is why analysis has been completed to present estimates of individual schemes separately, as the total costs will depend on the sectors involved and scheme design at secondary legislation level.

537. For a more detailed breakdown of these indicative costs please refer directly to the DBT Smart Data Impact Assessment.

538. As stated above, we do not expect any direct costs from the delivery of primary legislation alone. The following table sets out some of the potential costs that could emerge at the secondary stage, following the introduction of a sector scheme. This analysis builds on the experience of Open Banking (as the only live Smart Data scheme), and considers wider evidence from the finance, telecommunications, energy, fuel, and pension sectors.

539. Various groups could see costs from the introduction of Smart Data. These include regulators/other scheme administrators, data holders and data recipients (ATPs).

540. Further discussion and evidence on the costs of Smart Data can be found in the Impact Assessment.

Table 51: Summary of non-monetised costs of Smart Data regimes

[239] Ofcom (July 2021): "Statement: Update on Open Communications: Enabling people to share data with innovative services"

Regulators/Other scheme administrators	Data holders	Data recipients – third party providers
• Regulation and enforcement of Smart Data schemes. • Regulations allow for SoS or the Treasury to regulate the interface body and Treasury can sub-delegate to the FCA to issue direction in respect of the interface body for financial services Smart Data schemes. • Expands the monitoring and compliance powers that regulation makers can give to the 'enforcer' of the Smart Data scheme. • It is likely that there are administrative costs to enforcers, as there will be some costs associated with requesting documents and attendance at meetings by participants and interpreting this information. • Provides powers for the Secretary of State and the Treasury to mandate via regulations that data holders must provide standardised business data to a public authority specified in regulations. It is also includes further powers that regulation makers can mandate that this specified entity must publish or make available this business data upon request. • The Secretary of State and the Treasury can provide financial assistance to the specified entity for the purposes of meeting expenses incurred by the regulations. • Amendment expands the rule making powers of the FCA to ensure drafting is in line with the policy intention.	• Initial implementation of Smart Data scheme. • Familiarising employees with regulations. • Upgrading or improving technical and system infrastructure • Ongoing costs to comply with regulations. • Resources to cover specified costs will be recouped from industry in accordance with regulations, possibly through levies, charges or another funding model.	• Familiarising employees with regulations. • ATPs face the cost of accreditation, to be authorised to handle and use customer data. • Setting up and running technical infrastructure e.g. APIs and customer interface. • Amendments regarding fees enable regulations to allow for data holders to charge ATPs for the data at a rate that exceeds expenses. This could result in a cost to ATPs and there is the possibility that this is passed through to consumers.

Regulators/Other scheme administrators	Data holders	Data recipients – third party providers
• Amendment expands the rule-making powers of the FCA to cover regulations related to fees and action initiation.		

NOTE: Smart Data schemes are intended to be self-financing and should not require funding from existing government funds. ATPs will not be mandated to participate in a Smart Data scheme, therefore any costs that they incur will be at their own discretion.

Primary Legislation Costs of Smart Data Amendments

541. Smart Data amendments give more options to the government when making decisions around fee charging within a Smart Data scheme.

542. We anticipate that there will be a shift in impacts, compared to the illustrative estimates above, as the amendments allow for scheme designers to choose from more options when developing the regulations linked to fees. For example, where regulations are designed to allow data holders to charge a fee, ATPs may face a cost to access data, compared to no cost in a scheme where regulations explicitly do not allow data holders to charge a fee.

543. The amendments also provide the option to design Smart Data schemes where data holders can charge at a rate exceeding expenses for access to the data. This would mean that regulations may provide for data holders to charge ATPs (or others) commercial rates. This may have competition impacts, as the fees could be set at a rate where larger firms would be able to afford them, but smaller firms may have more difficulty paying them. This could also mean that there is a transfer of these costs to consumers (for example, if the data holder charges the ATP, then the ATP may react by increasing the price to consumers).

Increased Interoperability and Trust of Digital Identity Systems

544. More detail on the calculation of the non-monetised costs of the proposed Digital Identity reforms can be found in the published Digital identity and attributes - De Minimis Assessment.[240] In this assessment we provide an outline of costs of the proposal. This analysis looks at the same four potential use cases measured in the benefits section.

a. Employee mobility

   i. We expect businesses to face some costs to adapt their organisation in order to carry out real-time digital verification for DBS, RTW and employability checks. For instance,

[240] Digital identity and attributes - De Minimis Assessment DSIT, 2024

businesses may be required to set in place a platform which determines the requirements based on nationality and work location. Consequently, new hires may be invited to complete a self-service right to work check and may be able to provide the necessary attributes through a digital identity service to complete the checks. We expect businesses wishing to use digital ID checks to carry out these checks to have to pay for the required platform. The payment will most likely be on a subscription basis but were unable to estimate these ongoing costs at this early stage.

b. Travel authorisation and ticketing

    i. Verifying passport data when booking a flight and reducing in-journey ID verification

        1. We expect businesses to shoulder costs to use digital identity to reduce in-journey ID verification. For instance, businesses may need to integrate a remote identity verification solution through a platform that passengers may use to submit their passport details for real-time verification. We expect businesses to outsource the required platform and pay it on a subscription basis, therefore creating an ongoing cost for the business. However, we are unable to estimate what these costs may add up to at this early stage.

    ii. Costs to align with industry initiatives on passenger identification (e.g. ICAO's OneID)

        1. We also expect businesses to take actions to align with industry initiatives on passenger identification to streamline the journey of passengers by creating an interoperable system between airports, airlines and governments. We are currently unable to estimate what these costs may add up to.

c. Home buying

    i. Cost to extended ID verification to witnesses

        1. We assume businesses may have to take actions to extend remote ID verification to witnesses to facilitate identity proof throughout the home buying process, where necessary. Currently, the real estate market relies significantly on witness proofing, which in turn may require the identity verification of the involved witnesses. Unless the steps taken to digitise the identity verification system of the home buyers is extended to witnesses, the market will be unable to fully function digitally and the benefits of using digital identity will not be maximised. We are unable to predict such costs at this early stage.

        2. It is also possible that the requirements for witnessing certain deeds may change in future. In particular the use of Qualified Electronic Signatures, in conjunction with the digital identity trust framework, is something which can be explored further as a means of replacing existing requirements for witnessing.

    ii. Reducing friction in the home value chain

        1. We assume that businesses may have to adapt the ID checking process required throughout the entire house buying process to the digital identity verification system. We believe that these steps are essential in order to use digital identity across the multiple identity verification process required throughout the home

buying process. Unless all identification steps are digitised, the real estate market will not be able to fully function using digital identity.

2. Businesses are expected to face costs to create and maintain the system for any potential platform required to remove the friction in the home value chain. Businesses may incur costs to adapt to closing contracts digitally. However, due to the level of uncertainty we are unable to estimate these costs.

d. Trusted financial transactions

i. Businesses may pay to adapt their organisation in order to digitally prove the identity of customers throughout financial transactions. Businesses may either outsource or build and maintain the platform in-house. However, we are currently unable to estimate what these costs may add up to.

545. A breakdown of the non-monetised impact on the **public sector** can be found in more detail in the Digital identity and attributes - De Minimis Assessment.[241]

Delivery of better public services

Impacts of changes to the Digital Economy Act - CDDO

546. The below section is based on analysis by the Central, Digital and Data Office.

547. The Digital Economy Act (2017) currently provides departments with the data sharing powers to improve services for individuals and households, but this legal gateway is not available for services that support businesses. Furthermore, there are no powers within the Digital Economy Act 2017 to amend section 35 by secondary legislation, and therefore primary legislation must be used.

548. As there are few examples of where this data has been shared between departments previously, this means that the evidence base for the analysis of costs is currently limited. As a result, we are only able to provide a qualitative assessment of the impacts of this primary legislation reform.

549. There will be little or no direct costs of the extension of data sharing powers. The impacts will be experienced when public authorities utilise these powers to share data in order to support government services for businesses.

550. The table below provides high level quantitative analysis of the potential costs of the reform for both private businesses and the public sector. More analysis will be provided at a secondary legislation stage when data sharing powers are enacted.

Table 52: Summary table of costs of changes to the DEA 2017 by recipient

Recipient	Costs
Businesses	**One-off administration costs:** There may be a one-time sign up process for businesses, implying a small administrative cost in order to complete this process.

[241] Digital identity and attributes - De Minimis Assessment DSIT, 2024

Recipient	Costs
Government	**Policy-related costs of data sharing:** There will be a cost associated with creating the legal framework that is required in order for data sharing to occur between departments. This process requires the support of policy advisors and analysts, an element of which may be ongoing. **Technical costs enabling data sharing:** Once the legal framework for data sharing is in place, there will be a cost associated with the overhauling of legacy systems. Data technicians would be required to create the cross-government data sharing mechanism. An element of this cost will be ongoing in order to maintain and improve data sharing infrastructure.

Improved Interoperability across Health and Social Care Systems

551. Following implementation of the measure, it is likely that there will be costs incurred by internal IT teams of Health and Care Providers to update other related internal systems, processes and databases in line with the standards. For a further breakdown of the estimated impacts of this measure please refer to the DHSC Open Data Architecture Information Standards impact assessment.[242]

Indirect costs to businesses of increased data use

552. Many of the reforms within the Act are designed to encourage firms to better harness the power of the data already available to them and to encourage more firms to use data in decision making and for efficiency gains. Some proposed measures will specifically increase data processing for specific activities, such as those in relation to R&D, record keeping and processing bases.

553. Using the sources and methodology listed in the 'Indirect benefits - Monetised' section of this report we highlight that greater data use will lead to greater firm level productivity. It is important to consider that for the reforms we anticipate this to be the case for, that there may also be indirect costs associated with directing more resources towards data use.

We predict that the reduction in the burden for firms no longer having to keep records for low risk processing activities will encourage further data use. This will take the form of firms that currently lack incentive to now use data due to the current burden, deciding to now use it, and also firms that now have extra resource spend expanding their data use capabilities. Though these firms will face costs in setting up data processing systems, we expect these quantitative costs to fall in scope of our familiarisation cost estimates. There may also be indirect costs and benefits to businesses of increasing their data use, for example, extra time spent by staff exploring the data costs to businesses of establishing and extending legal frameworks, and the potential additional employment of data specialists. These costs are difficult to quantify as they depend on the initial level of data use within the firm and also whether the infrastructure is already in place.

Delivery of the National Underground Asset Register

Enforcement activity

242 DHSC: Open Data Architecture Information Standards Impact Assessment, 2024

554. Costs of running the enforcement regime will only fall on non-compliant organisations and are not included in the EANDCB. Organisations who fail to share their data as prescribed will be subject to a fine which will be enforced by Crown Prosecution Service (CPS). Late payment of the membership fee will be subject to a late payment charge, enforced by the organisation responsible for charging. Given the benefits to asset owners of using NUAR we do not expect non-compliance to be high, though it is not possible to estimate likelihood at this stage given the innovative nature of the programme.

555. Income from fines will be used to cover costs associated with running the enforcement regime.

Wider impacts

Summary

556. This section of analysis provides an outline of the wider impacts of the proposed package of reforms that do not fall into the cost or benefit categories. These include analysis carried out by DSIT and other government departments and focus on factors such as the impact on competition, equalities, national security and law enforcement and any environmental impacts.

Impact on Competition

557. There are reforms within this proposed package that are considered as pro-competitive as defined by the CMA.[243] For example some proposals are designed to remove the barriers of data use for UK businesses and public sector organisations and as a result increase its use more widely. As a result of this increase, we expect the number of private businesses using data as an asset to increase, helping to render them more competitive. Whilst this is the case for the majority of reforms there are some included in the Act where it is difficult to determine whether the same applies.

558. In digital markets there is increasing concern that access to data is a huge barrier to entry and this leads to concentrated benefits for the small number of businesses with data access, highlighted in CMA's Online platforms and digital advertising interim report. It is believed that relying on pure market mechanisms for increased data sharing/access is unlikely to lead to sufficient solutions for these problems. Similarly, ineffective competition was the motivation for the CMA's Retail Banking Market Investigation Order and the Government's price cap in retail energy.[244] Government intervention is necessary to address this market failure, as discussed in the Furman Review.[245] The measures included in this Act are designed to promote competition and data sharing to overcome this market failure.

559. There are trade-offs with boosting competition in data markets. Data-driven platforms do not face diminishing returns to scale, as data driven algorithmic procedures have high fixed costs but near zero marginal costs, making the platforms indefinitely scalable. This has the impact of both increasing productivity and efficiency gains but also resulting in increased market power for the platforms that are able to scale. [246] Improving competition in the data market therefore has potential to limit efficiency, as businesses cannot fully enjoy the benefits of economies of scope and scale. However, while the use of data on a large scale has been shown to enable efficiency gains, it also has potential to damage market structure through increasing barriers to entry or leading to scenarios where the 'winner takes all'.[247] As stated in a joint statement from the CMA and ICO on competition in digital markets, lack of competition due to poor access to data is likely to result in reduced consumer choice and ultimately lower quality, higher prices and less innovation.[248]

[243] Competition impact assessment, CMA, 2015
[244] CMA (February 2017): "Retail Banking Market Investigation Order 2017" & BEIS (July 2019): "Victory for consumers as cap on energy tariffs to become law"
[245] Jason Furman & Digital Competition Expert Panel (March 2019): "Unlocking digital competition"
246 European commission: An economic perspective on data and platform market power (2021)
247 European Parliament: The emergence of non-personal data markets (2023)
248 CMA & ICO joint statement: Competition and data protection in digital markets (2021)

560. Digital platform markets are considered to operate in 'winner takes all' or 'tippy' markets due to direct and indirect network effects, and economies of scale. Users are attracted towards platforms with a greater number of users, while the efficiency gains from having this greater number of users strengthens the market power of the incumbent. This structure leads the market to 'tip' towards a single dominant platform that acts as a gatekeeper, setting market conditions that reinforce its monopolistic position.[249] It is expected that measures that increase access to data reduce barriers to entry, placing entrants in a better position to overcome network effects and potentially reducing market susceptibility to tipping.

561. Looking more closely at the example of Smart Data. Strong competition drives innovation, high quality, and low prices. Innovative services can help consumers and businesses make better informed decisions in increasingly complex markets. We have seen this emerge in Open Banking[250] since the introduction of Smart Data. However, if the innovative third parties cannot access data, this limits innovation, and customers will miss out on new and improved products and services. This may also mean customers are not able to meaningfully participate in the market as a rational actor.

562. Similarly, in the health sector, there are a number of markets that are dominated by a small number of large suppliers, with high switching costs alongside high barriers to market entry, which are currently not competitive. The Electronic Patient Record (EPR) vendor markets for primary, community and mental health are highly segmented with similar levels of market concentration in each of the relevant segments, and the General Practice EPR market is a duopoly. Therefore, a mixture of interventions to set stronger regulations and promote competition for the market are required to incentivise suppliers to follow standards, improve service, reduce costs and innovate. Although this legislation is currently enabling, we expect the secondary legislation to deliver these market outcomes. However, we also acknowledge that there may be a period after implementation where market competition falls as firms adjust to the new legislation. Please refer to the DHSC Open Data Architecture Information Standards Impact Assessment for a more detailed breakdown of expected impacts on competition.[251]

563. No businesses currently provide a service that is the same or similar to the service that NUAR would provide. There are a small number of businesses which provide services to asset owners to fulfil existing legislative obligations. Services include relaying a request for information on behalf of a data requestor to the relevant asset owner(s), providing data requestors with a list of asset owners who may operate in a given area and providing details on how to contact them, and making some data available directly to data requestors, typically in the form of PDFs. As NUAR will ensure data is available from all asset owners, streamline the way data is shared and accessed for the purposes of excavation planning and safe digging, and may support additional use cases or user bases in the future, such organisations could be impacted by the service.

564. There are also a small number of commercial enterprises who request and consolidate data on behalf of organisations who are planning to carry out works. Though it may be possible for these organisations to access NUAR in the future, the nature of their work may be impacted

[249] European commission: An economic perspective on data and platform market power (2021)
[250] See 'Open Banking use cases' box in the Smart Data Impact Assessment
[251] DHSC: Open Data Architecture Information Standards Impact Assessment, 2024

through delivery of the new digital service where data from all asset owners can be accessed immediately through a single web map interface, rather than maps being received separately.

565. To maximise the value of NUAR while leveraging the wider commercial market in delivering additional value, the legislative reforms being sought will make it possible to widen licensed access to NUAR data where propositions are tested, feasibility and value is confirmed, and the proposal is supported by the wider asset owner community. This could include granting access for commercial entities acting as third party intermediaries to NUAR data which would allow these organisations to adapt their service offerings should they choose to do so. Offerings could include making NUAR data securely available to other use groups or to support other use cases.

566. However, as these opportunities are theoretical at this stage, this impact assessment only considers the potential for immediate impact on these businesses.

567. As asset owners will be required to share data in a form that will be prescribed, NUAR could also create market opportunities as it is likely organisations lacking either the skills or capacity to carry out data transformation activities in-house or share data using in-house staff, will procure services to complete these activities on their behalf.

Impact on Equalities

568. Ministers are required, owing to section 149 of the Equality Act 2010, to have due regard to the public sector equality duty (PSED) when exercising their functions. The PSED requires the Minister to pay due regard to the need to:

a. eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act;
b. advance equality of opportunity between people who share a protected characteristic and those who do not; and
c. foster good relations between people who share a protected characteristic and those who do not.

569. Analysis of these considerations has been undertaken and the Government's does not consider that any potential negative impacts of its proposals for individuals with protected characteristics are disproportionate. The Government has also appropriately considered the need to advance equality of opportunity and foster good relations.

570. There are a limited number of areas, where the Government has identified a potential risk of an indirect negative impact. These are set out below. In each of these cases, the Government has identified mitigations to be put in place to reduce this impact; and/or believes that any impact is proportionate to legitimate policy aims, and is therefore justified. Consequently, the indirect impacts do not amount to indirect discrimination.

571. **Smart Data** aims to improve equality, but there is a risk that vulnerable groups, such as the elderly and digitally excluded, may not fully benefit. Vulnerable consumers, who face challenges in engaging with markets, may be particularly at risk of being left behind. To address this, various measures are proposed, including demographic analysis, targeted interventions, and further research. These initiatives build on research commissioned by DBT[252] to help ensure that Smart

[252] DBT: Design principles for inclusive Smart Data schemes research, July 2023

Data schemes are inclusive, with a focus on trust, consent, control, and support, to prevent worsening inequalities and help all consumers benefit from innovative services.

572. **ICO enforcement.** Modernising ICO enforcement powers under the DPA 2018 and PECR will help to ensure that breaches of those pieces of legislation are investigated and enforced against more effectively. This may be beneficial to society generally by improving compliance with the relevant legislation.

573. However, being called to interview by the regulator could potentially be intimidating and/or difficult at a practical level for individuals, particularly for individuals in protected groups. The government has considered how best to ensure the powers are used appropriately and not in such a way as would impact those with protected characteristics disproportionately, and safeguards have been included so these powers are used fairly and proportionately.

574. **National Security Exemption & Joint Processing by Intelligence Service and Competent Authorities.** Statistically, certain groups (such as males or people from certain ethnic backgrounds) are more likely to be arrested and therefore these groups are more likely to have their data processed by law enforcement bodies. Similarly, other groups – for example Asian or British Asian and Muslim individuals – are disproportionately affected by terrorism legislation. This makes it more likely that such individuals will have their data processed by law enforcement or the intelligence services. There is therefore a risk of indirect impact on based on the protected characteristics of sex, race and religion.

575. However, the Government considers that any indirect discrimination impact caused is proportionate to the legitimate policy aims of keeping the public safe, bringing criminals to justice and maintaining national security. Consequently, any potential indirect impact does not amount to indirect discrimination.

576. Recognised Legitimate Interests. The measure should encourage swift data-sharing in areas such as safeguarding or when responding to emergencies. This could benefit society generally and may be particularly beneficial to children and other vulnerable people in certain circumstances. The Government acknowledges that removing the balancing test could indirectly impact on individuals with protected characteristics such as age or disability as there will be a less specific balancing of rights.

577. However, data controllers will still be required to undertake a proportionality assessment through the requirement that the processing is ‘necessary'. The list is also limited to areas of public interest where the balancing test is more likely to be met, and does not extend to commercial or third sector activities. The Government therefore believes any potential impact is justified and proportionate to the legitimate public interest policy aims set out in the legislation.

578. Solely Automated Decision-making (general processing). These proposals are not aimed at a specific group; therefore we do not believe they will have a direct impact on individuals with protected characteristics. The Government acknowledges that those with protected characteristics such as race, gender, and age are more likely to face discrimination from ADM due to historical

biases in datasets. To mitigate this potential impact, the act maintains the existing limits on the lawful bases when special category data can be processed for solely ADM.

579. Solely Automated Decision-making (law enforcement processing). A study of arrest data shows that men are several times more likely to be arrested as women. Likewise, black people are more than twice as likely to be arrested as white people. Since their data is more like to be processed under Part 3 of the DPA, it follows that they may be more likely to be subject to ADM and the changes proposed to part 3 in this respect. There is, therefore, the potential for these groups to be subject to an indirect impact.

580. To mitigate this potential impact, the Government has included safeguards and limitations on the use of ADM in relation to sensitive processing (special category data under UK GDPR). In addition, the Government considers that any indirect impact caused is proportionate to the legitimate policy aims of keeping the public safe, bringing criminals to justice and maintaining national security. Consequently, the indirect impact does not amount to indirect discrimination.

581. Subject Access Requests – Reasonable and Proportionate Searches. In ensuring the principle established in domestic case law that data controllers only need make “reasonable and proportionate” searches in response to a request continues to apply, the Government acknowledges a low risk this could have a greater impact on data subjects with a disability. Controllers are more likely to hold a higher-than-average amount of information on an individual with a disability (e.g. local councils and GP surgeries) and may view this provision as a reason not to have to search through large amounts of information regardless of the importance of the information to the data subject.

582. This applies equally to law enforcement bodies and the intelligence services who, as controllers under Part 3 and Part 4 of the DPA 2018 respectively, are more likely to process personal data belonging to males, individuals of certain races and ethnicities, and those from particular religious backgrounds relative to the population as a whole.

583. However, the Government considers it likely that the current approach. reflected in both existing case law and ICO guidance on subject access requests, where the importance of the information is taken into account when assessing what constitutes a reasonable and proportionate search, will continue. The Government therefore does not view this proposal as having a negative impact on individuals with protected characteristics.

584. **Data subjects’ rights to information: Legal Professional Privilege exemption.** As noted above, the statistical rate of arrest can differ significantly based on characteristics of sex, race and ethnicity. Since individuals who share these characteristics are more likely to be subject to the legal professional privilege exemption under Part 3 there is the potential for these groups to be subject to an indirect impact.

585. However, since this reform does not expand the scope of the exemptions currently utilised to protect privileged communications between lawyers and their clients, we do not believe that it will lead to an increase in the indirect impact on data subjects. The Government also believes any potential impact is justified and proportionate to the legitimate public interest policy aims set

out in the legislation. Consequently, any indirect impact does not amount to indirect discrimination.

Impact on Individuals

a) ICO Taxonomy of Harms

586. The reforms within the Act are designed to minimise the harms related to imperfect data protection. Harms can result when individuals or groups are prevented or impeded from asserting their information rights (e.g. a lack of transparency around how data is processed or inability to hold a public body accountable). Quantifying data protection and information rights harm is difficult therefore the ICO produced a non-exhaustive and non-hierarchical taxonomy with illustrative examples of harms.[253]

587. The ICO's taxonomy of harms uses the risk management distinctions between causes, events and consequences to focus on harmful consequences. The cause is a factor that alone or in combination gives rise to risk, for example poor data security. The event is an occurrence with some probability of occurring such as a data breach. The consequence is the outcome of the event that leads to a negative impact, for example financial loss which is also the harm. The harm to an individual can vary in degree and type, and harms can include:

a. Physical harm: physical injury or other harms to physical health

b. Material harm: harms that are more easily monetised such as financial harms; or

c. Non-material harm: fewer tangible harms such as distress.

588. The harms may fall into more than one category and can arise from actual damage or intangible harm.[254]

589. There may also be wider societal harms. For example, damage to the economy is described as a harm that has a negative impact on the economy that is significant at local, regional or national level, or for a specific sector and may involve a misuse of personal data leading to an unfair competitive advantage.[255] The reforms aim to mitigate data protection harms by ensuring key safeguards and high standards of data protection are maintained. Approaches to quantifying the value of data protection harms are still being investigated.

b) Artificial Intelligence Ethics

590. The ethical implications of using AI technologies have been considered within the proposed reforms. AI ethics is a set of values, principles and techniques that employ widely accepted standards of right and wrong to guide moral conduct in the development and use of AI technologies.[256]

591. AI ethics are a response to the harms an individual or society may face due to the misuse, poor design or unintended negative consequences caused by AI. The ethics are intended to

[253] Regulatory Policy Methodology Framework, ICO, 2021
[254] Draft journalism code impact assessment, ICO, 2021
[255] Regulatory Policy Methodology Framework, ICO, 2021
[256] Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute

support the production of ethical, fair and safe AI applications. The potential harms caused by AI systems include.[257]

a. Bias and Discrimination: AI systems can reproduce, reinforce and amplify patterns of inequality that exist in society.

b. Denial of Individual Autonomy, Recourse and Rights: When AI systems produce decisions or predictions, there is no directly accountable party responsible for the outcome.

c. Non-transparent, Unexplainable or Unjustifiable Outcomes: AI systems operate using models that are difficult to explain and this lack of explainability may be problematic when the results are considered discriminatory or unfair.

d. Invasions of Privacy: Threats to privacy are posed by AI systems both as a result of their design and development processes, and as a result of their deployment.

e. Isolation and Disintegration of Social Connection: In the future, excessive automation may reduce the need for human-to-human interaction.

f. Unreliable, Unsafe or Poor-Quality Outcomes: Unreliable, unsafe or poor-quality outcomes can do direct damage to the wellbeing of individuals and the public's welfare.

592. The reforms targeted at AI and Machine Learning in this Act include the future proofing of Article 22 and the enhancement of the approach to explainability and accountability for fair processing in the context of profiling. Article 22 is drafted to give a data subject a right not to be subject to a decision made by solely automated processes which has a legal or similarly significant effect, however there is a lack of clarity in practice over how this right is invoked, what constitutes a significant effect, as well as which decisions can truly be said to be made by 'solely' automated processes. This ambiguity means that Article 22 is rarely applied or considered in the way it was intended to be.

593. Automated decision-making (ADM) and profiling are being used more and more frequently by organisations to streamline their processes. These automated processes often rely on AI technologies and as such are a key part of the government's wider approach to the development and deployment of AI systems. These proposals are pivotal in addressing the risks of harm in AI-powered automated decision-making and in deciding the data protection controls required to build and maintain trust in their application.

c) Increased Interoperability and Trust of Digital Identity Systems

594. More detail on the wider impacts of this proposed reform can be found in the Digital identity and attributes - De Minimis Assessment.[258] Here provides a summary of the wider impacts of the preferred reform.

595. Although a digital identity market already exists, it is not developed to its full potential and it presents some key flaws which may exclude minorities or those with protected characteristics. For example:

[257] Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute

[258] Digital identity and attributes - De Minimis Assessment DSIT, 2024

d. When setting up a digital identity, individuals have highlighted that the process usually requires a sequencing of tasks which are considered difficult for people that are, for instance, digitally excluded or neuro-diverse.[259]

e. The digital identity system can be rather rigid, therefore excluding people whose circumstances differ from the expected social structure, such as those wishing to manage two bank accounts at the same bank from one mobile phone.[260]

596. The digital identity legislation, by promoting the growth of the digital identity market in an inclusive way, provides the opportunity to use a digital alternative, giving to excluded individuals an easier option for proving their identity or eligibility. For example, those who cannot afford a passport may instead opt for a digital identity product based on their data or a 'vouch'.[261]

597. Inclusion is explicitly mentioned in the UK digital identity and attributes trust framework. Although signing up to the Trust Framework is not compulsory, organisations will need to be certified against it to prove that their products or services meet the UK Government requirements for checking government-held records of identity-related data. The Framework aims at improving inclusivity by:

a. Stating that all identity service providers should ensure no one is excluded due to their 'protected characteristics'". There are exemptions to this, for instance restricting the availability of a product or service to an individual due to their age (e.g. businesses cannot sell alcohol to underage individuals).

b. Giving examples of ways organisations can increase inclusivity. For instance, when choosing a system for facial recognition, digital identity and attribute providers should ensure that the chosen system is built in an inclusive way. A system which was tested with a small sample of white men risks excluding users of other genders and ethnicities, therefore excluding minorities or those with protected characteristics from being able to use the service.

c. Requesting both public and private sector organisations to meet appropriate accessibility standards. For instance, those that operate in Wales offer products and services available in Welsh.

d. Requiring organisations that sign up to the framework to submit an annual inclusion report.

d) Use of data for purposes relating to electoral services

598. Paragraph 23 of Schedule 1 of the Data Protection Act 2018 allows elected representatives to process special category data of constituents without explicit consent where this is necessary to take action on their behalf. This allows them to take forward and deal with constituency casework (e.g. raising matters with relevant government departments or other public bodies) without seeking explicit consent of data subjects at every step of the process. Paragraph 23(4)

[259] Digital Identity: Ground-up Perspectives Report Summary
[260] Digital Identity: Ground-up Perspectives Report Summary
[261] A vouch is a declaration from someone that knows the user which can be used as evidence for identity proof.

provides that outgoing MPs (or their equivalent in the devolved Parliament/Assembly) are only to be treated as elected representatives for four days following a general election.

599. This means that outgoing representatives have four days to finish their constituency casework. They then cease to be a data controller and can no longer rely on this exemption to conclude outstanding constituency matters. Provisions were tabled to amend Schedule 1 of the Data Protection Act 2018 so that the 4 day threshold in which outgoing elected representatives have to process special category data on behalf of their constituents without explicit consent, is changed to 30 days, to overcome operational barriers.

600. Whilst we estimate no direct economic impact on businesses of changing the time frame from 4 days to 30 days, there could potentially be wider indirect impacts to elected representatives and constituents. Constituents may benefit from the additional time given for their casework to be completed, resolving their concerns or issues, instead of the case being delayed when transferred to a new elected representative. Constituents will also spend less time answering consent requests from the outgoing MP during these 30 days. Benefits for elected representatives also include a clearer and less burdensome handover process and less time spent waiting for explicit consent when handing over casework. This streamlining of the process could lead to efficiency gains within the office of the elected representative and allow for time to be spent elsewhere.

601. Provisions have been made to reduce the regulatory constraints of data protection rules applying to political parties, MPs, and candidates. This consists of two separate provisions. The first provision seeks to permit that the use of personal data gathered by an elected representative for constituency casework purposes be considered always compatible with political campaigning purposes. This is to give elected representatives clarity and legal certainty to continue to be able to report back and correspond with constituents even in a capacity outside of their elected office as a political candidate or campaigner, for example during election time or when parliament is dissolved.

602. The second provision seeks to expand the scope of Paragraph 2 of Schedule 1 of the Data Protection Act 2018. In order to rely on the substantial public interest exemption in Article 9(2)(g) of the UK GDPR, data controllers must identify one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018. It provides a list of situations where processing on grounds of substantial public interest would be lawful if certain conditions and safeguards are met. Paragraph 22 of Schedule 1 provides an exemption for registered political parties to process political opinions data where necessary for their political activities (including campaigning, fund-raising, political surveys and case-work.) Currently the condition does not permit elected representatives, candidates, recall petitioners and permitted participants in referendums to do the same. As it is narrowly defined, it means that individuals (as opposed to those who are acting as a representative of a political party) wishing to put themselves forward during an election campaign are not able to benefit from this condition.

603. We do not expect these reforms to have direct impacts to UK businesses in the form of costs or benefits. There are wider impacts of these reforms that are important to highlight. For example, the first provision may risk giving incumbent elected representatives an unfair advantage over other campaigners, as they are able to use some personal data collected in

their role as an MP, for political communications when they are acting as a candidate or political campaigner. This same data may not always be available to their electoral competitors.

604. The first provision may also impact trust and result in data subjects reducing the amount of data they share as public attitudes to processing data in this manner are likely to be mixed. High trust and confidence in local and national government storing and using personal data is shown to be currently moderate at 51% and 55%, respectively.[262]

605. Finally, the section provision would ensure that elected representatives, candidates, recall petitioners and permitted participants in referendums as well as individuals can benefit from the processing on grounds of substantial public interest in the same ways as political parties. Widening the field of bodies and individuals that can process political opinions data without consent, could increase the amount of information available to individuals and therefore could increase engagement in the democratic engagement process. However, increasing the number of people that can process data for these purposes also increases the risk of data processing errors, breaches and a fall in data subject trust as a result.

Improved Interoperability across Health and Social Care Systems

606. Research and innovation benefits: Adopting common standards for health and social care data is a fundamental requirement to enable and enhance research.

607. Improved patient satisfaction and empowerment: Interoperability provides opportunities to empower citizens and patients with information and tools to support their health, care and wellbeing.

608. Wider productivity gains and taxpayer benefits: Better patient outcomes and more efficient care – because of information standards and interoperability - can lead to less reliance on sickness benefits, fewer absences from work, and a more productive and resilient workforce, ultimately benefiting the economy.

609. Broader environmental benefits: Interoperability can support a greener health and social care system as Data would be held in a cloud-based environment thereby reducing the data centre footprint and reliance on buildings and paper storage.[263]

Environmental Impacts

Primary legislation to extend the Digital Economy Act to benefit businesses

610. There may be less printed documentation required as a result of business data being accessible across the government, providing an environmental benefit

Increased Interoperability and Trust of Digital Identity Systems

611. We expect that the legislation, by fostering the uptake of digital identity checks, will have a positive effect on the environment. This is because less trips will be required during the identity verification process and to allow the individuals to obtain the required physical identities.

[262] , ICO, 2022, ICO, 2022

Furthermore, a greater uptake of digital IDs may lead to less people choosing traditional IDs over digital alternatives which in turn may lead to a lower quantity of IDs produced and disposed every year. This could be beneficial to the environment. However, despite the fact that digital identity should benefit the environment, these benefits are expected to be very small and possibly insignificant. For instance, the total number of trips related to identity verifications carried out every year, although substantial, is not large enough to significantly impact the environment.

Improved Interoperability across Health and Social Care Systems

612. Interoperability can support a greener health and social care system as Data would be held in a cloud-based environment thereby reducing the data centre footprint and reliance on buildings and paper storage.[264]

National Security Impacts

Enhance the Work of the UK Intelligence Services and Law Enforcement Agencies in the Interest of Public Security

613. These wider impacts have been provided by the Home Office.

614. The following proposals are expected to contribute to the Home Office priority outcomes of reducing crime and risk of terrorism to the UK and interests overseas:

a. National Security Exemption (Part 3 DPA) is expected to increase cooperation between LEAs and the UK Intelligence Services, particularly relating to CT.

b. Automated Decision-making (Part 3 DPA)is expected to lead to more effective use of automated systems to identify persons of interest, particularly in border settings, and reduce the risk of tipping them off, therefore increasing the chance that they will be stopped and apprehended.

c. Joint processing by intelligence services and competent authorities is expected to facilitate UK Intelligence Services and LEAs to conduct more effective investigations, increasing the probability that they are successful and contributing to a reduction in crime.

615. The following proposal is expected to help future proof the data protection regime:

d. Law enforcement processing and codes of conduct.

616. The following proposals are expected to increase clarity around data protection rules:

e. Consent to law enforcement processing.

National Security Exemption (Part 3 DPA)

617. Currently, the national security restriction in Part 3 is not as extensive as in Part 2. The current restriction-based approach is more limited than the protections provided by the Part 4 national security exemption. This creates risks when for example, a data subject exercises their rights.

Mirroring the national security exemption into Part 3 would assist close working between law enforcement and intelligence services and provide greater legal certainty for international transfers concerning national security.

618. When collaborating under joint investigations, each data controller is subject to different standards. Part 3 contains fewer national security protections which may lead to disclosures by LEAs which may undermine the intelligence services and expose operational risks. This is a barrier to co-operation.

619. By providing a national security exemption to Part 3 of the DPA 2018, this proposal may lead to more effective CT investigations thus contributing to the Home Office priority outcomes of reducing crime and risk of terrorism to the UK and UK interests overseas

Law enforcement processing and codes of conduct

620. In the UK GDPR codes of conduct can be produced by representative bodies (for example, trade associations) to clarify the application of data preapproved by the ICO. There is no equivalent power under Part 3 DPA 2018 and stakeholders have indicated that this could be a useful tool to future-proof their data use. This proposal aims to expand it to the law enforcement sector enabling similarly representative bodies to create codes of conduct for Part 3 under the purview of the ICO.

The LEAs will be able to adapt data protection standards to suit their needs which will help future-proof data use.

Automated Decision-making (Part 3 DPA)

621. Currently, LEAs are required to inform data subjects as soon as reasonably practicable when a decision which produces an adverse legal effect is made which is based solely on automated decision making. The purpose of this is to allow the data subject to then request that a human either reconsiders that decision or takes a fresh decision not based solely on automated decision making.

622. ADM is the process whereby a decision, which affects a data subject, is made wholly by automated means without any meaningful human involvement.

623. The police have stated that this can cause them difficulties. For example, where ADM is used to match an individual to a watchlist, the police must then either inform the data subject that they are under investigation (thereby tipping them off that they are of interest) or, alternatively, ensure that the decision is reviewed by a human (thereby removing the need to inform the data subject but running the risk the individual may have moved beyond their reach before any action can be taken).

624. This proposal will provide an alternative option for LEAs to provide for a human to actively review the decision after it has been taken as soon as is reasonably practicable thereby removing the need to notify the data subject at the time. However, in order to ensure that the new power is only used where necessary, LEAs will only be able to use it if informing the data subject is necessary for one of the restrictions set out under section 44(4) of the DPA (e.g. to avoid obstructing an official or legal inquiry, investigation or procedure to safeguard national security etc.) This change will ensure that the rights of data subjects who are subject to ADM

continue to be protected whilst improving the ability of the police to tackle crime, ensure public safety and bring offenders to justice. It contributes to the Home Office priority outcomes of reducing crime and the risk of terrorism to the UK and UK interests overseas.

Transfers based on special circumstances (Section 76 DPA)

625. If this proposal leads to more frequent large-scale transfers on the basis of national security or serious and organised crime, it may lead to more effective investigations, thus contributing to the Home Office priority outcomes of reducing crime and risk of terrorism to the UK and UK interests overseas.

Amendments to Part 4 of the DPA 2018 - Joint processing by intelligence services and competent authorities

626. Currently, policing and the intelligence services are governed by different data protection regimes which adds friction when working in partnership and presents challenges to joint operational working. This proposal will introduce a power that would allow the Secretary of State to issue a notice authorising qualified competent authorities to process data under the Intelligence Services regime in Part 4 of the DPA 2018 when it is required for the purpose of safeguarding national security.

627. UK Intelligence Services believe that this proposal will lead to more dynamic working practices with police colleague data.

628. This may result in more effective investigations and a higher probability that they are successful, thus contributing to the Home Office priority outcomes of reducing crime and risk of terrorism to the UK and UK interests overseas.

Transfers based on special circumstances (Section 76 DPA)

629. If this proposal leads to more frequent large-scale transfers on the basis of national security or serious and organised crime, it may lead to more effective investigations, thus contributing to the Home Office priority outcomes of reducing crime and risk of terrorism to the UK and UK interests overseas.

Amendments to Part 4 of the DPA 2018 - Joint processing by intelligence services and competent authorities

564. Currently, policing and the intelligence services are governed by different data protection regimes which adds friction when working in partnership and presents challenges to joint operational working. This proposal will introduce a power that would allow the Secretary of State to issue a notice authorising qualified competent authorities to process data under the Intelligence Services regime in Part 4 of the DPA 2018 when it is required for the purpose of safeguarding national security

565. UK Intelligence Services believe that this proposal will lead to more dynamic working practices with police colleagues, such as the option to share databases. It should also lead to improved confidence in sharing data.

566. This may result in more effective investigations and a higher probability that they are successful, thus contributing to the Home Office priority outcomes of reducing crime and risk of terrorism to the UK and UK interests overseas.

Impact on small and micro businesses

567. The proposed set of reforms are expected to have an impact on small and micro businesses. In 2024, the percentage of small and micro businesses that handle personal data (other than employee data) is 79% and 62%, respectively.[282] Larger businesses tend to have greater levels of data use than micro businesses. On average larger firms are more productive than smaller firms, particularly in manufacturing. This typically reflects the increasing returns to scale through capital-intensive production.[283] Small and micro businesses that process data are less likely to analyse data to generate insight and knowledge when compared to large businesses.[284] This suggests that there are potentially more productivity gains available to small and micro businesses through increased data use than their larger counterparts. There is evidence that larger businesses that handle digitised data are more likely to transfer data internationally than smaller businesses.[285] [286]

568. The reforms aim to provide small and micro businesses with the opportunity to increase their data use to boost innovation and facilitate international trade. Participation in international trade activities is one of the key characteristics of high productivity in firms and enabling more firms to trade might assist in boosting their productivity.[287] The proposed reforms are designed to encourage small and micro businesses to use data more effectively in their decision making and therefore boost productivity. Small and micro businesses are expected to see proportionally higher reductions in compliance costs than larger businesses as a result of the reforms. The reforms are expected to reduce the barriers to sharing data internationally that small and micro businesses face and therefore increase their international trade.

569. The proposed set of reforms are not expected to place a disproportionate burden on small and micro businesses. We expect small and micro businesses to benefit proportionally more from the reforms than larger firms because they are more likely to have lower levels of data use prior to the reforms.

570. There appears to be support for data use by small businesses by some consumers. The DMA 2022 survey found that 52% of adults agreed with the statement '"I don't mind sharing personal information with smaller companies if it helps give them a competitive advantage over larger companies". This rose to around 7 in 10 people aged 18-44 agreeing, but fewer than half of people aged 45 and over agreed.

571. In this section we have analysed the estimated impacts of the reforms on small and micro businesses. Where evidence is available, we have done this for all monetised costs and benefits. Many of the reforms in the preferred package are aimed at improving data use in the public sector so do not fall into the scope for this section. We have focused on providing a breakdown of the compliance cost savings, productivity benefits, familiarisation costs, digital identity schemes and smart data initiatives.

572. Where sector data is available, we have also included sectoral breakdowns of the monetised impacts of the proposed package. We also explore any impacts that may vary due to geographical factors.

Small and Micro Business Impacts

Compliance Cost Savings

630. We predict that the reforms will have a direct benefit on small and micro businesses. As discussed in the direct benefits section, the reforms are expected to change compliance requirements and lower the compliance burden on businesses. Small and micro businesses are expected to achieve greater overall compliance cost savings than larger businesses. There are assumed to be a higher number of micro and small businesses in scope of the reforms and therefore more are expected to benefit from compliance cost savings.

631. The table below shows the compliance cost savings by organisation size. For micro businesses the compliance cost savings are estimated to be £27.3 million, while for small businesses the compliance cost savings are estimated to be £2.9 million. Together this is greater than the total benefit for large firms (£1.4 million).

Table 53: Annual Compliance Cost Savings by organisation size, 2024 prices, (£million), medium scenario

Reform	Micro (0 to 9)	Small (10 to 49)	Medium-sized (50 to 249)	Large (250+)	Total
Legitimate Interests	1.7	0.5	0.2	0.2	2.6
AI and Machine Learning	6.4	0.4	0.1	<0.1	7.0
Research Purposes	3.3	0.9	0.3	0.2	4.7
Privacy and electronic communications	15.6	1.2	0.3	0.1	17.1
Direct marketing for charities	**0.4**	**0.0**	**0.1**	**0.0**	**0.5**
Total	27.3	2.9	1.0	0.5	31.8

Productivity Benefits

632. The preferred package of reforms is designed to encourage businesses to better harness the power of data already available to them and to encourage more businesses to use data in decision making and for efficiency gains. As mentioned above, the impact of additional data use on productivity is assumed to be linear for all businesses that analyse data, therefore we expect that small and micro businesses will achieve the same increase in productivity as larger businesses. As there is a greater share of large businesses the total impact for large businesses will be greater than that of small and micro, however this is down to the distribution of the total number of businesses.

Table 54: Estimated change to UK GVA split by business size, 2024 prices (£million)

Reform	Micro (0 to 9)	Small (10 to 49)*	Medium-sized (50 to 249)	Large (250+)	Total
Legitimate Interests	0.3	0.0	3.2	8.4	11.9
AI and Machine Learning	1.6	0.0	4.8	8.5	14.8
Research	0.1	0.0	1.8	7.2	9.1

Reform	Micro (0 to 9)	Small (10 to 49)*	Medium-sized (50 to 249)	Large (250+)	Total
Purposes					
Total	2.0	0.0	9.8	24.0	35.8

*Likely due to a small sample size, the number of small businesses who stated they had been prevented from implementing a new product or process due to UK data protection law was 0. This has impacted the expected productivity benefit for small businesses however still represents the best evidence available.

Familiarisation Costs

633. We adapted the assumptions of our methodology to reflect the cost of familiarisation on small and micro businesses. This analysis assumes that a micro-sized business has zero employees, and a small business has between 1 and 49 employees. Small and micro businesses are estimated to face greater familiarisation costs than medium-sized and large businesses because we assume that a higher number of small and micro businesses are in scope of the reforms. In line with the methodology used by the ICO, we have estimated the hourly unit cost of this work at £30.68 using occupational estimates from the Annual Survey of Hours and Earnings (ASHE).[265] For micro-sized firms we have adapted our wage assumptions by applying median annual earnings estimates of the self-employed from DWP's Family Resources Survey and estimating the hourly unit cost of this work at £11.97.[266] We do not expect the reforms to disproportionately impact small and micro businesses.

634. The table below shows the familiarisation cost estimates split by business size. For micro businesses this is estimated to be between £11.7 million and £15.8 million, while for small businesses this is estimated to be between £5.6 and £7.6 million. At a business level, the familiarisation costs are expected to cost around £6.65 per micro business and £17.04 per small business.

Table 55: Familiarisation costs split by business size, 2024 prices, (£million), medium scenario

Subheading	Micro (0)	Small (1 to 49)	Medium-sized (50 to 249)	Large (250+)	Total (£million)
Research Purposes	2.5	3.5	0.2	0.1	6.2
Legitimate Interests	4.4	1.3	0.3	0.1	6.2
AI and Machine Learning	3.6	0.9	0.2	0.1	4.9
Privacy and Electronic Communication	3.2	0.8	0.2	0.1	4.3
Total	13.7	6.6	0.9	0.3	21.6

Powers for Digital Identity and Attributes Initiatives

635. Analysis in this section is based on Digital Identity and Attributes Initiatives De Minimis Assessment.[267] Here we provide a summary of the impact on small and micro businesses of the proposed reforms.

[265] ONS Annual Survey of Hours and Earnings 2023)
[266] DWP Family Resources Survey (2023)
[267] Digital Identity and Attributes De Minimis Assessment (2024)

636. Small and micro businesses are not exempt from this legislation. However, we do not expect the legislation to significantly impact small-micro relying parties as we have assumed they will be less likely to adopt digital identity. Regarding service providers, we do not expect a significant disproportionate impact as these businesses are already established in the market so we expect their cost to understand and adapt to the legislation to be minimal.

a. Relying parties.[268]

i. The legislation is expected to not significantly impact small and micro businesses as we assume that small-micro relying parties will be significantly less likely than bigger ones to adopt digital identity because their expected benefits are less likely to outweigh the costs. For instance, businesses are considered small-micro if they employ less than 50 staff members. Therefore, we assume they are less likely to be interested in digital RTW checks as their gains from digital checks will not be significant compared to the cost of familiarising and adapting to digital identity.

ii. According to DBT data, the average turnover of small micro businesses by start of 2023 was £289,001[269] We estimated that the one-off familiarisation costs plus the one-off organisational change costs for a business wishing to adopt digital identity may add up to £20,190.8 . Therefore, these estimated costs add up to roughly 7.0% of the average revenue of a small-micro business by start of 2023. Whereas the equivalent calculation for medium-large businesses adds up to 0.03%. This suggests that the estimated costs of adapting to the legislation may create a greater burden for small-micro businesses relative to larger ones. However, this legislation is not designed to substitute traditional identification checking. Therefore, we expect small and micro relying parties that may experience a significant burden to adopt digital identity to continue to only use traditional identification systems. Therefore, overall, we do not believe that small-micro businesses will be disproportionately affected by the legislation in a significant way.

b. Service providers:[270]

i. Small-micro identity and attribute service providers have a greater risk of being disproportionately impacted by the legislation. We expect these businesses to face familiarisation costs and organisational. These costs may generate a greater burden for small micro firms relative to medium-large businesses. However, we do not believe this disproportionate impact will be significant as small and micro identity and attribute service providers are already established in the market so we expect that their costs to understand and adapt to the legislation to be minimal.

637. The legislation aims at providing the right legislative environment to promote the adoption of digital identity. Therefore, we expect the small-micro providers to experience a growth in

[268] We define relying parties as organisations that get (or 'consume') digital identity products or services.
[269] Business population estimates for the UK and regions 2023: statistical release: DBT, 2023
[270] This assessment defines service providers as organisations that prove and verify users' identities and/or attributes. They might not need to do all parts of the identity checking process. They can specialise in designing and building components that can be used during a specific part of the process.

demand on the back of the legislation. We believe that the resulting increase in revenue will cover some, if not all, the costs businesses may experience due to the legislation.

Regulatory Powers for Smart Data

638. Analysis in the section is based on the Regulatory Powers for Smart Data Impact Assessment produced by DBT.[271] Here we provide a summary of the potential impact on small and micro businesses.

639. Small and Micro Firms (SMFs) are in scope of the legislation to be mandated to participate in a Smart Data scheme. SMFs have not been carved out of the powers to enable Smart Data Schemes at secondary stage, to allow for wider range of options and scheme design. This is so that schemes can be tailored to the specific sector or market in question. For example, there may be schemes where for the use case to be beneficial there needs to be participation from every business within the sector or sectors where a collection of small, but successful, businesses have many customers.

640. The specific thresholds for mandatory participation will be decided for individual schemes to reflect differing market structures and will be set out in secondary regulations. We expect Smart Data to be mandatory for medium/large, incumbent data holders in scope of the regulations, with smaller data holders and Authorised Third-party Providers (ATPs) choosing to participate on a voluntary basis. We would therefore expect SMFs to participate where they see the benefits to exceed the costs for their business.

641. In terms of **cost savings**, Frontier Economics conducted analysis into the benefits of Smart Data to small and micro businesses and ATPs.[272] A full methodology explanation and set of assumptions can be found in their research note.[273] This work indicates the potential benefits over 5 years across banking, finance, energy and communications. For ATPs, the estimates focus on potential productivity gains and growth in the number of ATPs. For SMF users of Smart Data, the estimates focus on potential cost savings. These are a direct benefit of the Smart Data initiatives.

642. Alternatively looking at **costs**, DBT conducted a survey to collect evidence on the costs of Open Banking. Focusing on the costs currently faced by organisations with less than 49 employees can provide an illustration of the costs faced by Small and Micro firms (SMFs) to participate in a mandated data sharing scheme. We found that the majority of small and micro firms faced implementation costs below £200,000. This ranged from £5,000 to £200,000. No SMFs estimated their total one-off implementation costs to be above £2m. The majority of SMFs estimated their annual ongoing costs to be below £75,000 per annum. From those who provided firm estimates, this ranged from £50,000 down to £10,000 per annum. No SMFs estimated ongoing costs to be above £200,000. More detail on this survey can be found in 'Primary Legislation Costs'.

Impact of Amendments on SMFs

[271] Regulatory Powers for Smart Data Impact Assessment, DBT (2024)
[272] BEIS commissioned research (July 2022): Estimating benefits of Smart Data to small and micro firms and third party providers
[273] BEIS commissioned research (July 2022): Estimating benefits of Smart Data to small and micro firms and third party providers

643. Group 2 of the Smart Data amendments enable regulations to provide for Data Holders to charge for access to the data at a rate that exceeds expenses. If regulations were to provide for this, it may mean that there is an unfair advantage to larger businesses acting as ATPs, as SMFs may be less able to pay the fees, acting as a barrier to entry to the market for new smaller firms. If the SMFs do not have the capital to pay these fees whilst starting their business, it may mean that SMFs have to transfer this cost into the price they charge customers. Larger firms who may already have the capital to pay these fees are therefore likely to be able to offer a more competitive price than SMFs.

644. The possible markets that Smart Data may be introduced in will all have their own nuances and market set up that mean Smart Data schemes will need to be designed differently in order to be efficient. If there are potential negative impacts to SMFs, they will be assessed at the secondary legislation stage and decisions on fee charging will be made based on what is appropriate for the particular sector. Section 11(5) of the Act requires that (except where section 15 provides otherwise) regulations must provide for a fee to be either: a specified amount, an amount determined in accordance with the regulations, or an amount not exceeding those amounts. Section 21(3) and (4), provide additional safeguards on the setting of fee amounts.

645. The Act requires that the Secretary of State or The Treasury have regard to the likely effect on small businesses and micro businesses before making data regulations under section 2 or 4.

Improved Interoperability across Health and Social Care Systems

646. DSIT has worked alongside the Department for Health and Social Care to ensure that all policy risks and impacts of the proposed reform to increase interoperability across health and social care systems are included in this impact assessment.

647. Small businesses are defined in the better regulation framework guidance as those that employ between 10 and 49 full-time equivalent (FTE) employees. Micro businesses are businesses that employ between one and nine employees.

648. DHSC used publicly accessible headcount data to determine the number of impacted businesses within each size category. Their analysis has identified 1,317 micro businesses, comprising 362 private GP practices and 955 private social care providers. Additionally, they have identified 3,901 small businesses, which include 3,886 private social care providers, 12 private GP practices, and 3 IT suppliers.

649. DHSC acknowledge that compliance costs for SMBs represent a higher proportion of their total capacity and resources than larger businesses. In this section we have analysed the estimated impact of the legislation on SMBs.

650. Table 56 and Table 57 show the cost to SMBs by type of organisation and cost type.

Table 56: Cost to micro businesses (undiscounted)

Organisation	Cost type	Aggregate cost	Implementation cost per organisation[274]	Annual cost per organisation[275]
GPs	Training costs	£220,246	£800	£0
Private social care providers	Information standards related systems update	£279,433	£660	£0

651. Clinicians in micro-GP practices will be required to undergo training to use the new systems as updated. This cost, at £800 per organisation, represents an allocation of clinicians' time. It is not unusual for clinicians to periodically undergo training. Training time per GP is estimated at 2.2 hours,[276] with the total number of hours varying by headcount at the GP. Only 6%[277] of GPs are considered as operating completely outside of the NHS and therefore considered as private businesses, it is only these GPs included in this analysis.

652. Micro private social care providers will incur a monetary cost of £660 per organisation (average) to update systems to make them information standards compliant as new standards are mandated over a ten-year period. Whilst we have taken the conservative approach to include these costs; it should be noted that NHSE is providing funding of £8.2 million to support a pilot on the digitisation of social care[278] The programme will then support ICSs to scale up the solutions that have the biggest impact. It is unclear what the scale of this support will be, but this should alleviate or significantly mitigate the burden on social care providers.

Table 57: Total cost to small businesses over ten-years(undiscounted)

Organisation	Cost type	Aggregate Cost	Implementation cost per organisation[279]	Annual cost per organisation[280]
IT suppliers	Familiarisation costs	£1,562	£521	£0
IT suppliers	Information standards related systems update	£108,900	£82,500	£0
IT suppliers	Accreditation costs	£453,194	£11,000	£14,006
GPs	Training costs	£25,987	£2,807	£0
Private social care providers	Information standards related systems update	£1,568,266	£910	£0

653. We estimate that all small IT suppliers will incur familiarisation costs of £521 per organisation and accreditation costs made up of £11,000 upfront implementation costs and £14,006 annual costs over 10 years. We expect information standards related systems update

[274] Including 10% optimism bias
[275] Including 10% optimism bias

[276] Based on Information Standards and Interoperability Survey, NHS, Feb 2024. 10% optimism bias is also included on top of the cost of these hours
[277] 2013/14 Healthcare Market Review, LaingBuisson
[278] Digitising social care fund - Digitising Social Care - NHS Transformation Directorate (england.nhs.uk)
[279] Including 10% optimism bias
[280] Including 10% optimism bias

costs will be incurred only by suppliers that are currently not compliant, as new standards are implemented. We estimate the information standards related systems update cost per organisation to be £82,500 over 10 years. It should be noted that only 15% of IT suppliers in this market are considered small businesses.

654. As with GPs classed as micro businesses, we expect training costs for GPs classed as small businesses. This cost represents an allocation of clinicians' time to undertake the training. Training time per GP is estimated at 2.2 hours.[281] GPs that fit within the small business classification have a larger headcount than those in the micro definition, hence why the cost per organisation, at £2,807, is higher. As with small businesses, only 6% of GPs are considered as private businesses.

655. Small private care providers will incur an estimated monetised implementation cost of £910 per organisation to update their systems to make them information standards compliant as standards are mandated over a ten-year period. As pointed out previously, NHSE digitisation support will mitigate the burden on care providers.

Enhance the work of the UK intelligence services and Law Enforcement Agencies in the interest of public security (HO)

656. The proposals are not expected to have a significant economic impact on small and micro-businesses. The vast majority of the proposals and impacts are targeted at LEAs and the UK Intelligence Services. There are some private businesses who are also competent authorities, however, they are unlikely to face the more resource intensive costs and benefits of the proposals such as the recording of 'justification' and ADM proposals as these concern LEAs. Of these private businesses there may be a small number of small and micro-businesses, but they are expected to face significantly smaller impacts compared to LEAs and the UK Intelligence Services.

Online safety researchers' access to data

657. Though any final researcher access to data policy has not been decided, the current policy expectation is that these regulations would not apply to small or micro businesses. Data suitable for research will be held by large platforms with large numbers of users. Small platforms' data is likely to be less valuable to researchers for methodological reasons. Therefore, though details are to be confirmed, there is no burden anticipated for small and micro businesses.

National Underground Asset Register

658. Due to the policy objective of National Underground Asset Register of achieving a fully complete and comprehensive underground assets map, small and micro businesses (SMBs) will be expected to comply with the new requirements, just as they are for existing legislation to share data. Inclusion of data from all organisations, regardless of their size, is important as it only takes late discovery of a single asset - or accidental damage to one - for a project to incur significant delays / costs, abandonment or for worker safety to be put at risk. It will also directly benefit SMBs

[281] Based on Information Standards and Interoperability Survey, NHS, Feb 2024. 10% optimism bias is also included on top of the cost of these hours

who may be less able to maintain teams to respond to requests for their data or pay a service provider to do it on their behalf.

659.

660. Therefore, the legislation being sought is assumed to have an impact on some SMBs, specifically asset owners. We have estimated there to be 47 SMBs within the 705 AOs (7%). Whilst no data exists on their market share or the size of their networks, larger asset owners tend to have greater levels of data use than micro businesses and so the legislation will not place a disproportionate burden on small and micro businesses. More detail is available in the NUAR Impact assessment[282]

Impact on Medium businesses

661. As well as small and micro businesses the package of reforms will also have direct and indirect impacts on medium sized businesses. [283] 99% of medium sized businesses handle some form of digitised data according to the UK Business Data Survey[284] and it was found in 2021 that 80% handle personal data (other than just from their employees), which is more than both small and micro businesses.[285]

662. Similarly to small and micro businesses, the package of reforms is not designed to put a disproportionate burden on medium businesses. We expect medium sized businesses to benefit proportionally more from the reforms than larger firms because they are more likely to have lower levels of data use prior to the reforms.

663. In this section we have analysed the estimated impacts of the reforms on medium sized businesses. Where evidence is available, we have done this for all monetised costs and benefits. Many of the reforms in the preferred package are aimed at improving data use in the public sector so do not fall into the scope for this section. We have focused on providing a breakdown of the compliance cost savings, productivity benefits and familiarisation costs.

Compliance Cost Savings

664. We predict that the reforms will have a direct benefit for medium sized businesses. The reforms are expected to change compliance requirements and lower the compliance burden on businesses. Medium-sized businesses are expected to achieve a smaller overall benefit than small and micro businesses of £0.9 million annually, as seen in table 53. This is because there is a smaller proportion of medium sized businesses in scope of these reforms compared to small and micro businesses.

Productivity Benefits

665. The preferred package of reforms is designed to encourage more firms to use data in decision making that result in efficiency gains and increased productivity. As with small and micro businesses, the impact of additional data use on productivity for medium sized businesses is assumed to be linear. We estimate that medium sized firms will benefit from an annual increase in productivity of £9.8m, this is in line with the proportion of medium sized businesses estimated to increase their data use because of the reforms.

[282] National Underground Asset Register Impact Assessment, DSIT, 2024
[283] Businesses with 50 to 249 employees, as per previous BEIS definitions
[284] UK Business Data Survey 2024
[285]UK Business Data Survey 2021 – (Older release used as this question was not asked in 2024)

Familiarisation Costs

666. We adapted the assumptions of our methodology to reflect the cost of familiarisation on medium sized business. This analysis assumes that a medium sized business has 50 to 249 employees. As seen in Table 57 small and micro businesses are estimated to face greater familiarisation costs than medium-sized and large businesses because we assume that a higher number of small and micro businesses are in scope of the reforms.

- We updated the wage assumptions of our time-cost approach, in line with the ICO methodology, by assuming that the median wages of senior officials in small, medium and large sized enterprises are a suitable estimate of the wages of individuals likely to read the guidance, and estimated the hourly unit cost of this work at £30.68 using occupational estimates from the Annual Survey of Hours and Earnings (ASHE).[286] Using this assumption we estimate that the total familiarisation costs for medium-sized businesses will be between £0.8 and £1.1 million.

Interoperability of health and social care systems

Table 58: Total cost to medium businesses over ten-years (undiscounted)

Organisation	Cost type	Aggregate cost	Implementation cost per organisation	Annual cost per organisation
IT suppliers	Familiarisation costs	£2,604	£521	£0
IT suppliers	Information standards related systems update	£726,000	£330,000	£0
IT suppliers	Accreditation costs	£755,323	£11,000	£14,006
Private social care providers	Information standards related systems update	£1,397,738	£2,825	£0

- We estimate that all medium-sized IT suppliers will incur familiarisation costs of £521 per organisation and accreditation costs made up of £11,000 upfront implementation costs and £14,006 annual costs over 10 years. We expect information standards related systems update costs will be incurred only by suppliers that are currently not compliant, as new standards are implemented. We estimate the information standards related system update cost per organisation to be £330,000 over 10 years. Medium sized private care providers will incur an estimated implementation cost of £2,825 to update their systems to make them information standards compliant, based on existing standards. As pointed out previously NHSE digitisation support will mitigate the burden on care providers.

Sectoral Impacts

667. The data protection reforms aim to increase responsible data use across all sectors of the economy. Better use of data can help organisations of every kind succeed. As of 2024, the two

[286] ONS Annual Survey of Hours and Earnings (2023)

sectors most likely to say they share personal data with other organisations were Finance and Insurance (46%) and Professional, Scientific and Technical (27%).[287]

668. We expect the reforms to have distributional impacts on different sectors as a result of differing levels of data use between sectors. The compliance cost savings estimates are broken down by sector and different assumptions are made on the number of businesses per sector that are in scope of the reforms based on results from the UK Business Data Survey.

Compliance Cost Savings

669. The table below shows the total compliance cost savings estimates by sector. The sectors estimated to benefit the most from compliance cost savings are the Construction sector and the Professional/Scientific/Technical sector with savings of £4.6 million and £4.2 respectively, this can be explained by the fact that these are two of the sectors with the largest number of businesses, while in the case of the Professional/Scientific/Technical sector a relatively large proportion of businesses handle digitised data.. The Mining, Energy and Water sector is estimated to save the least at £0.2million as we predict this sector to be one of the least impacted by the AI and research measures.

Table 59: Compliance cost savings by sector, 2024 prices, (£million)

Sector	Legitimate Interests	AI and Machine Learning	Research Purposes	Privacy and electronic communications	Total
Agriculture, Forestry and Fishing	0.1	0.2	0.1	0.5	0.8
Manufacturing	0.2	0.3	0.3	0.8	1.6
Mining, Energy, Water	<0.1	<0.1	<0.1	0.1	0.2
Construction	0.3	1.1	0.6	2.6	4.6
Wholesale and Retail, Repair of Vehicles	0.3	0.8	0.6	1.8	3.6
Transport and Storage	0.1	0.4	0.2	0.9	1.6
Hotel/Catering	0.2	0.3	0.4	0.8	1.6
Information and Communication	0.2	0.4	0.3	1.0	1.9
Finance and Insurance	0.1	0.1	0.1	0.3	0.5
Real Estate	0.1	0.2	0.1	0.4	0.8
Professional/Scientific/Technical	0.4	0.9	0.6	2.3	4.2
Administrative and Support Service	0.2	0.6	0.4	1.5	2.8
Education	0.1	0.3	0.2	0.9	1.5
Human, Health and Social Work	0.2	0.4	0.3	1.1	2.0
Arts, Entertainment and Recreation	0.1	0.3	0.2	0.8	1.4

[287] UK Business Data Survey (2024)

Sector	Legitimate Interests	AI and Machine Learning	Research Purposes	Privacy and electronic communications	Total
Other Service Activities	0.2	0.4	0.2	1.1	1.9
Total	2.5	6.9	4.7	17.1	31.2

Familiarisation Costs

670. We expect to see distributional familiarisation costs across different sectors of the economy as a result of the reforms. The estimated familiarisation costs differ between sectors based on the business data use results from the UK Business Data Survey. This defines the number of businesses per sector that are impacted by the reforms.

671. The table below shows the familiarisation cost estimates broken down by sector. Similarly to compliance cost savings the sectors with highest estimated familiarisation costs are the Construction and Professional/Scientific/Technical sectors. This is driven by a large proportion of overall businesses operating in these sectors, and in the case of Professional/Scientific/Technical a high level of data use. The sector with the lowest estimated familiarisation cost is Mining, Energy and Water which in comparison has a lower level of data-use so is to be expected.

672. Findings from the UK Business Data Survey, 2024[288] state that businesses in the Finance and Insurance sector were more likely to share personal data than other sectors, however, we do not expect the Finance and Insurance sector to be disproportionately impacted as data suggests that 90% of businesses in this sector already have privacy frameworks in place[289]. Businesses in this sector are also more likely to employ someone leading on data protection compliance when compared to the Construction or Wholesale and Retail sector. Businesses in the Finance and Insurance sector are more likely to be aware of the ICO and state they find their guidance clear to understand. As a result, we expect that this sector will face lower costs when familiarising themselves with these policy changes than other sectors which may not already have frameworks in place.

Table 60: Familiarisation costs by sector, 2024 prices

Sector	Legitimate Interests	AI and Machine Learning	Research Purposes	Privacy and Electronic Communications	Total
Agriculture, Forestry and Fishing	0.1	0.1	0.2	0.1	0.5

[288] DSIT: UK Business Data Survey, 2024
[289] DSIT: UK Business Data Survey, 2021

Sector	Legitimate Interests	AI and Machine Learning	Research Purposes	Privacy and Electronic Communications	Total
Mining, Energy, Water	<0.1	<0.1	<0.1	<0.1	0.1
Manufacturing	0.4	0.3	0.4	0.2	1.2
Construction	0.9	0.7	0.9	0.6	3.1
Wholesale and Retail, Repair of Vehicles	0.6	0.5	0.8	0.4	2.4
Transport and Storage	0.3	0.3	0.3	0.2	1.2
Hotel/Catering	0.3	0.2	0.4	0.2	1.2
Information and Communication	0.4	0.3	0.4	0.3	1.3
Finance and Insurance	0.1	0.1	0.1	0.1	0.4
Real Estate	0.1	0.1	0.2	0.1	0.5
Professional/Scientific/Technical	0.8	0.6	0.8	0.6	2.8
Administrative and Support Service	0.6	0.4	0.6	0.4	2.0
Education	0.3	0.3	0.2	0.2	1.1
Human, Health and Social Work	0.5	0.4	0.4	0.3	1.6
Arts, Entertainment and Recreation	0.3	0.3	0.2	0.2	1.0
Other Service Activities	0.4	0.3	0.3	0.3	1.3
Total Cost	6.2	4.9	6.2	4.3	21.6

Geographical Impact

673. Based on our research and evidence we do not expect the reforms aimed at UK private sector organisations to have disproportionate geographical impacts. We expect the reforms to impact all parts of the UK and have distributional impacts. Results from the UK Business Data Survey show no evidence of disproportionate impacts on Northern Ireland compared to the rest of the UK.

674. Police officers in the Metropolitan Police Service (MPS) make up one quarter of all total police officers in England and Wages and so the impacts of proposals concerning LEAs will be larger in London compared to the rest of the UK.

A summary of the potential trade implications of measures

Summary

675. Cross-border data transfers are a key facilitator of international trade, particularly for digitised services. Transfers underpin business transactions and financial flows. They also help streamline supply chain management and allow business to scale and trade globally. [290]

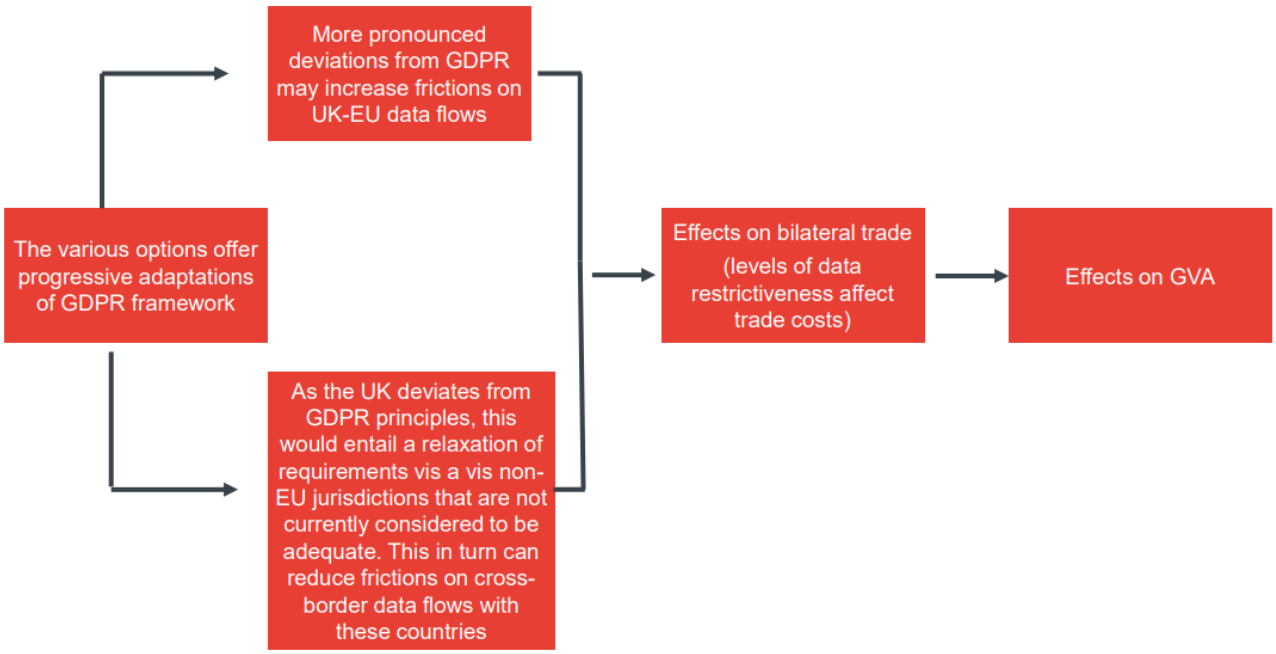
676. DSIT analysis of ONS data shows that the UK exported £330 billion in data-enabled services (65% of total UK services exports) and imported £154 billion services via remote trade (49% of UK services imports) in 2024.[291] This section aims to provide a novel look at the potential of data reform to enable more trade between countries. The analysis however includes several important caveats, outlined below, which means that the results should be treated as merely indicative of the range and scale, rather than a granular and detailed account of the impacts. **For this reason, none of these results are included in the summary EANDCB and NPV**. Instead, this section provides a transparent exposition of all of the research the department has undertaken and gathered as part of this analysis, with an aim to assist in further developing our understanding of this topic and help drive research - while also contributing into defining our monitoring and evaluation framework that will hopefully help us refine our estimations in the future.

677. Cross-country analysis indicates that both data policies on domestic use and the cross-border movement of data are likely to have an effect on productivity. Ferracane et al. 2018 found that countries with stricter data policies have a negative and significant impact on the performance of downstream firms in sectors reliant on electronic data. This adverse effect is stronger for countries with strong technology networks, for service firms, and holds for several robustness checks.[292] Cross-border digital trade has grown rapidly in recent years, as new digital products and business models have been delivered globally by improvements in technology and communication. This changes the nature and compositions of trade, as well as its overall value. In total, the value of UK data-enabled exports grew from £185.8 billion in 2008 to £307 billion in 2022 (76% of total exports), representing 65% growth.[293]

678. Policies that make substantial changes to the UK GDPR framework may lead to EU-UK frictions, and a decrease in requirements with non-EU jurisdictions. As a result, both the data flows and trade between these three groups of countries are likely to change. This will cause a change to production patterns and ultimately productivity, measured by GVA. This theoretical framework is presented in the diagram below.

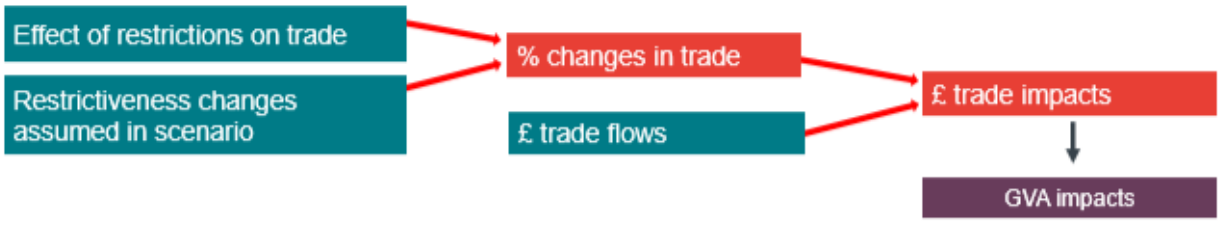
[290] DSIT (2021), International data transfers: building trust, delivering growth and firing up innovation
[291] DSIT internal analysis on the world total of UK services exports, based on 2024 ONS published statistics, using ONS experimental estimates of UK trade in services delivered remotely.
[292] European Centre for International Political Economy (2020) Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?
[293]DSIT calculations: The primary approach used by DSIT is to estimate the UK's data-enabled service exports and imports. DSIT uses ONS trade data and UN classification of 'digitally deliverable services', to aggregate services trade in certain digitally deliverable industries. This provides an estimate of potentially data-enabled services trade.

Figure 2: Theory of change following a change to UK GDPR legislation



679. The proposed measures in the Data (Use and Access) Act designed to boost data use and reduce barriers to data flows. This in turn is expected to increase data-dependent trade, along with higher data sharing and flows with international trading partners.[294] At a high-level, the theory of change for the proposed measures (seen in Figure 3) is that general improvements in flexibility for data transfers and reduced services trade restrictiveness are associated with an increase in trade. Moving to a system which allows personal data to be transferred more flexibly via data adequacy or Alternative Transfer Mechanisms (ATM's) is expected to lower transaction costs and increase cross-border data flows.

Figure 3: Theory of change following a change to GDPR legislation



680. Estimating changes in trade and onward productivity benefits is fundamentally challenging. Data economics is a nascent field and assessing the impact of policy reform is still under development both in academia and the industry. This is even more so the case when looking at the impacts of data policy on trade. To illustrate this point, the EC's impact assessment for implementing GDPR did not evaluate impacts on trade, making the quantification of some of the impacts of reforming data policy novel in their approach.

681. The analysis uses a 'bottom-up' approach developed by DSIT using business-level data. Limited direct impacts of data adequacy can be straightforward to model, businesses no longer

[294] Ferracane, M., van der Marel, E., Do Data Policy Restrictions Inhibit Trade in Services? (2018)

face the need for alternative transfer mechanisms to transfer personal data saving time and legal costs. At the same time, the reduction in non-tariff barriers likely represents an opportunity for additional indirect impacts for increased trade beyond the value of reduced compliance costs and direct loss of export revenue when costs are imposed. This method likely underestimates the impact as a result.

682. The **results of this analysis are therefore indicative** and for the purposes of transparency and **do not** form part of our overall estimates for the total cost and benefits of the package of reforms. Scenario analysis and sensitivity testing is also employed to capture uncertainty with the approach in the following sections of the Impact Assessment.

Rest-of-world data adequacy modelling approach

683. UK data reform will support the UK's ambition to encourage greater flows of data internationally. This is consistent with international commitments in areas such as trade and the Free Flow of Data with Trust framework. These commitments involve supporting the free flow of data and moving away from more protectionist approaches.

684. We have developed an approach that assesses the number of businesses that rely on data to trade, and estimates the potential impact of the following reforms on business costs and trade:

a. Underpinning the UK's future approach to regulations establishing data adequacy with principles of risk-assessment and proportionality

b. Relaxing the requirement to review data adequacy regulations every 4 years

c. A new power for the Secretary of State to formally recognise new ATMs

d. Changes to the standard and approach to alternative transfer mechanisms. (Art 46)

685. Businesses currently face costs to trade with countries we do not have a bridge with when that trade involves sending personal data. As a result, when businesses choose to trade or not, they face compliance costs in the form of implementing International Data Transfer Agreements (IDTAs) or Standard Contractual Clauses (SCCs)[295]; if these costs outweigh potential profits from trade, businesses may choose not to trade. It should be noted that this approach takes a focused look at direct changes in compliance costs for businesses once the UK has data adequacy with those countries. The potential of the reforms would remove the cost of implementing IDTAs in contracts with business partners in those countries. The estimates provided are the **annual, maximum, theoretically realisable benefit once the UK has established data adequacy with all non-red-rated, non-adequate, RoW countries.** It is not necessarily the case that the UK will establish data adequacy with all possible countries, instead the UK is undertaking a prioritisation exercise to identify countries that are most likely to receive one. Since the previous Act Impact Assessment, the UK government has concluded data adequacy assessments with the United States of America and the Republic of Korea.

[295] From 21 March 2022, the ICO's IDTA took effect as a replacement for the EU SCCs. For the purposes of this analysis, the old SCCs and the IDTAs are treated as equivalent in terms of how they function and how much they cost to implement. DSIThas undertaken an evaluation. To maintain the language of the previously published DPDI Bill IA and the published RoW Adequacy Umbrella IA, SCCs are used below throughout.

686. The approach to calculating SCC costs has been improved as the previous estimate made a number of assumptions. This approach is similar to the one taken in the 'Data Protection (Adequacy) (United States of America) Regulations 2023 - UK Extension to the EU-US Data Privacy Framework' Impact Assessment.[296] Individual businesses' SCC costs have now been estimated using UKBDS 2022 results in which businesses estimated the time required to put SCCs in place and the number of SCCs being used per year. It was assumed that these estimates equate to one full time regulatory professional working for the length of time given by the respondent. This combined both internal and external wages as we assume businesses will procure legal advice on completing SCCs correctly. ONS Annual Survey of Hours and Earnings[297] published statistics on median salary by profession were used to calculate the resultant cost per employee.

687. The external wages were collected for legal professionals from the ASHE 2022 data set. The figure is adjusted for companies sending data to the EU using the adequacy decision and removed from the ROW estimate. Per RPC guidance, a non-wage uplift of 22% is applied.[298] These costs are shown below:

Table 61: Average cost of SCC's according to business size, 2024 prices

Number of employees	Average annual SCC cost to businesses
Micro (0 - 9)	£6,666
Small (10 - 49)	£13,052
Medium (50 - 249)	£11,540
Large (250+)	£25,721

688. Previously we assumed a five-year contract cycle to forecast future compliance costs, while the new approach directly estimates the number of SCCs put in place in a single year using UKBDS 2022 results.

689. These cost calculations reflect the average annual cost over all UK businesses in each size category. To establish the total amount being spent by each business size on SCCs per annum in the UK. The large category includes a relatively small number of very large businesses that will incur considerably higher costs.

690. The first direct benefit of data adequacy is the removal of the cost of implementing SCCs, along with derogations under Article 49, in contracts with business partners in that country. Businesses currently trading with those countries no longer face the compliance costs of setting up SCCs. The top-down estimate of the total, global cost (excluding the EU) of this comprises the following steps:

[296] Data Protection (Adequacy) (United States of America) Regulations 2023 Impact Assessment, 2023
[297] Employee earnings in the UK Statistical bulletins, ONS
[298] RPC guidance on implementation costs, 2019

691. Take the total number of UK businesses by size category from ONS Business Population Estimates 2023.[299] The size categories used are commonly-used:

Micro and Sole trader (0 to 9)
Small (10 to 49)
Medium-sized (50 to 249)
Large (250+)

692. The UK Business Data Survey 2022, conducted in September 2021, provided the percentage of UK businesses that send personal data to the ROW and use SCCs, by the same size categories. 'Micro' and 'sole trader' businesses have been combined in this analysis.

693. The product of categories 1 and 2 gives us the number of UK businesses that send data to the RoW and use SCCs.

694. The *UK Business Impacts Model* (described below in the EU Adequacy loss section) was previously used to estimate the cost to individual businesses from implementing SCCs. This was originally used to estimate the cost to businesses of the UK leaving the EU without an Adequacy decision The updated approach uses the cost estimates shown in table 55 to estimate the cost to individual businesses by business size of implementing SCCs with respect to transfers of personal data to non-EU countries.

695. The Business Impacts Model assumed that all relevant businesses would be required to incur this cost upon the UK leaving the EU. Previously, since the contractual relationships that include SCCs with the RoW already existed, the average five-year contract refresh cycle assumption was used here in order to spread the benefit. Therefore, the SCC cost estimates were divided by five to obtain a per-year value. In the updated approach, the SCC cost estimates are now based on the number of SCCs put in place in a single year.

696. Multiplying category 3 and 4 together gives us the total cost by size category to businesses of implementing SCCs with respect to transfers of personal data to non-EU countries.

697. Taking the total over the size categories gives us the final estimate of **around £471m for the current**, **annual SCC cost** representing a direct benefit to businesses.

Table 62: Total annual SCC cost, 2024 prices

Business size	Micro (0 to 9)	Small (10 to 49)	Medium (50 to 249)	Large (250+)	Total
Population	5,287,480	222,785	36,905	7,960	5,555,130
% Send personal data to RoW and use SCCs	1%	3%	6%	14%	2%
Num. send personal data to RoW and use SCCs	72,213	6,207	2,027	1,077	81,543
SCC assumption per year (incl. non-wage cost uplift)	£6,666	£13,052	£11,540	£25,721	£6,934
SCC cost per year / £m	£370m	£62m	£18m	£21m	£471m

[299] https://www.gov.uk/government/statistics/business-population-estimates-2023 2022 Business population estimates (2023), DBT

698. For **small and micro-businesses**, although a relatively small proportion send data to the RoW, because they make up by far the majority of UK businesses the majority of the estimated SCC cost applies to them, at **£432m**.

Top-down - Suppressed Exports

699. Additional export activity will be enabled if other countries' data protection standards are determined as adequate. SCC costs will be removed and no longer act as a non-tariff barrier. The EU Exit modelling work mentioned below, in addition to the SCC cost, also estimates the value of exports that would be lost as a result of the cost of SCCs becoming necessary to receive personal data from the EU in order to export services there. The value of these exports as a proportion of the current total can be used as a 'suppression factor', i.e. the proportion by which exports to the EU would be suppressed by the cost of SCCs acting as a barrier to trade.

700. To estimate the additional export activity, the inverse of this suppression factor is applied to the value of current data-dependent RoW exports, on the assumption that trade is already suppressed in the same manner. Therefore, the following formula is applied to the export value. This formula 'inflates' the current export value back up to 100% from its presumably suppressed value, and takes the difference between that and the suppressed value.

$$d\frac{1}{1-s} - d$$

where:

- Data-dependent RoW exports,[300] £138bn * 14% = £19bn
- The data-dependency value of 14% is taken from the *UK Business Data Survey 2021*[301]
- Suppression factor, *s* = 0.0030 (high=0.005; low=0.0026)

701. Here, data-dependent RoW exports excludes countries that already have data adequacy and those given a red rating during the gate-keeping process mentioned earlier in this document. Two of the most common reasons for exclusion is that a country has little or no data protection legislation and/or there are security or privacy concerns.

702. This gives a value of around **£58 million (with a sensitivity range of £51 - £100 million based on low and high suppression factor estimates) per year in suppressed export revenue** that is assumed would be enabled if all non-red-rated, non-EU and those that do not currently have data adequacy were given data adequacy by the UK.

703. This estimate makes two important assumptions:

a. That the effect of SCC costs on exports to the RoW is currently the same as that on exports to the EU would have been had we not received an Adequacy decision from the EU.

b. That the effect is symmetrical. The EU Exit analysis modelled the need to receive data from the EU in order to export to the EU. The suppressed trade calculation here applies the same

[300] UK Total Trade Statistics (2025), ONS
[301] UK Business Data Survey (2021) Ad-hoc release – data-dependency percentages, i.e. the proportion of rest-of-world traders who use SCCs is based on robust statistical analysis

methodology to exports to the RoW that depend on sending data to the RoW. This assumption is necessary because we currently lack the analysis to differentiate between the two directions.

704. It is not possible to produce a suppressed export revenue figure specifically for small and micro-businesses. Whilst we know from ONS data that between 2016 and 2018 around £15.6bn of exports to the RoW is attributable to these businesses,[302] it is not possible to remove those with adequacy and red-rated countries from this value and so any figure produced would be a considerable overestimate.

Impact on firms on changes to Article 27 representatives

705. This reform provides for additional transitional arrangements in the Act for a wider set of current alternative transfer mechanisms (ATMs). Similar to the approach taken for pre-commencement adequacy regulations and pre-commencement standard data protection clauses, this reform introduces transitional provisions for pre-bill appropriate safeguards in Article 46 UK GDPR, Schedule 21 (paragraph 9) DPA 2018, and Section 75, Part 3, 2018 Data Protection Act currently in operation which meet the required level of protection under the existing framework.

706. Th-used alternative transfer mechanisms incurring familiarisation costs. Businesses would have to check whether the new data protection test is met and potentially seek reapproval by the ICO for some ATMs, even when they meet the required level of protection under the UK's current framework. This would mean a UK data exporter would incur familiarisation costs before they can continue to transfer personal data using the mechanism. The TRA Tool has recently been published in November 2022 and the ICO published an IDTA and TRA (IDTA Toolkit) impact assessment in December 2022 which sets out some of the relevant familiarisation costs. In summary, these additional transitional provisions capturing a wider set of alternative transfer mechanisms mean the familiarisation costs that would have been incurred as a result of the original Act text can be mitigated against.

707. The reform introducing additional transitional provisions acts to mitigate an issue that has been identified since the submission of the Act IA. As a result, compared to the do-nothing scenario, no major additional costs or savings are incurred to those businesses using the transfer mechanisms in scope of this reform. Costs capturing potential familiarisation and compliance costs for those mechanisms not captured in the previous transitional provisions should have been calculated at that time but were not. Qualitatively we acknowledge there may be very small costs for checks required by those responsible for data protection to check in with any guidance to make people aware of which pre-bill Mechanisms will remain valid.

EU Data Adequacy Decisions

708. EU Adequacy decisions are adopted through a unilateral EU process managed by the European Commission. It is for the EU to decide how it monitors and reviews its adequacy decisions.

[302] UK services trade by business characteristics: 2016 to 2018 (2020), ONS, figure 2.

709. A third country is not required to have exactly the same rules as the EU in order to be considered adequate. However, jurisdictions must be considered to provide an ‘essentially equivalent’ level of protection for data subjects.

710. The UK Governments' position is that the proposals within the Act are ‘essentially equivalent’ and have the ability to preserve EU adequate status. That said, it is the Government’s responsibility to model a range of scenarios, including those we consider unlikely, as part of our sensitivity analysis. Therefore, we have included analysis that estimates the impact in the event of a loss of the UK’s adequacy decisions from the EU. This is a scenario the Government considers highly unlikely, and this analysis does not attempt to assign probabilities to the scenario.

711. As there is uncertainty in both the likelihood and timing of any potential decision, the impact is not included in the net present value or other measures in the summary for the IA as a whole. The analysis also only considers the commercial impact of a full and immediate revocation of the GDPR adequacy decision. It does not consider scenarios relating to an amendment or partial suspension of GDPR adequacy and does not consider wider impacts on the provision of public services. The analysis does not include the Law Enforcement Directive adequacy decision. The impacts have been uprated and discounted as if the decision was made presently. The impacts are presented for the purposes of transparency.

712. The model assumes that in the absence of EU adequacy decisions, UK businesses that receive personal data would have to comply with EU Standard Contractual Clauses obligations as an alternative transfer mechanism (because in the absence of adequacy EU organisations would only transfer personal data to the UK if an alternative legal basis such as EU SCCs under EU GDPR were available). These legal requirements and associated adjustment costs would act as non-tariff barriers to trade. The assumption is that businesses whose export revenue from trade with the EU exceeds the cost of implementing EU SCCs would accept the cost impact and continue to operate, while for the rest they will cease to trade with the EU. EU organisations would also incur costs, but these have not been included in the analysis. The overall cost would be captured by total lost export revenue and the total cost of implementing EU SCCs. In the Gravity Modelling Annex, we have included analysis on the trade impacts EU organisations may face if the UK’s EU adequacy was discontinued.

713. As a result, there is a trade-off between the two impacts, as more businesses incur SCC adjustment costs, less export revenue is lost. The model analyses across all goods and services sectors. However, it should be noted that the goods proportion of the result is constant across the scenarios (£200m in lost revenue and £40m in SCC costs) and has not been updated since the previous consultation analysis due to data availability. The analysis was previously carried out by HMRC in a commission from DSIT; we were not given continued access to the underlying HMRC customs data required to update this estimate.

714. Our assumptions over compliance rates, following RPC best practice to assume 100% compliance from year 1, means the analysis is conservative when calculating lost export revenue over a 10-year period as costs are incurred annually. It is instead likely there would be a lead-in period for business compliance meaning lost export revenue would be smaller in nearer years, an approach reflected in our previous methodology.

715. We have maintained the previous assumptions such as:

- Assuming a 100% compliance rate to reflect that all UK businesses comply with all personal data compliance requirements. It is likely an unrealistic, but analytically conservative assumption as some businesses will fail to comply with the regulations in practice (and therefore will continue to trade without additional costs). We have sensitivity tested this parameter with compliance between 80-100%.

- A share of UK businesses that trade with the EU already have SCCs in place, we estimate it to be 14%, based on results from the UKBDS 2021[303]. The figures vary drastically by business size (from 9% for sole traders to 47% for large businesses). 14% is potentially an overestimate due to the two questions in the UKBDS that ask about SCCs being independent from one another.[304] Not all businesses that have SCCs in place necessarily use them with respect to EU trade, if they also share personal data overseas. Findings from the UKBDS 2024 suggest that when transferring personal data with the EU a greater proportion of UK Businesses use alternative transfer mechanisms compared to the proportion of businesses using adequacy.[305] This is based on the lack of clarity regarding how many UK businesses actively use adequacy instead of alternative transfer mechanisms to transfer personal data with the EU, therefore we have continued to apply the estimate from the UKBDS 2021.

- Not all costs are borne by UK businesses and that a percentage of the costs will fall on EU businesses,[306] especially where firms hold market power. Again, the figures vary by business size (from 25% for sole traders to 50% for large businesses). This represents the fact that legal expertise from the EU side is also needed when putting EU SCCs in place meaning some of the cost is passed onto EU businesses in the event the UK no longer had adequacy status. The amount of this legal, which is passed on increases with business size, representing the power of larger businesses to pass on costs to EU partners and implicitly reflects their market power.

- We assume a five-year investment horizon that the business considers when making its decision whether to continue trading or not. If the cost of implementing EU SCCs is greater than five years' worth of export profit, then firms will cease trading. The previous assumption did not reflect the evidence since collected through stakeholder engagement, and while the exact time horizon will depend on the business planning of each firm, a five-year horizon is a more realistic representation. We have also updated the assumed profit margin on exports.[307]

- The profitability of UK company's data shows a 14.6% average profit margin between 2016 and 2020 for service sector businesses. A 5-percentage point downwards adjustment for risk aversion is made resulting in an assumption of 9.4%.

[303] UK Business Data Survey (2021), Annex 2
[304] These 2 questions include 'do you trade with the EU?' and 'do you have SCCs in place?'
[305] UK Business Data Survey (2024) – Of UK businesses that send personal data overseas and only transfer data with the EU/EEA 20% said they use adequacy to transfer data and 41% said they use SCCs to transfer data.
[306] The Cost of Data in Adequacy (2020), New Economics Foundation
[307] Profitability of UK companies – rates of return and revisions the data used is focused on non-financial corporations. Whilst not lining up directly to the business types of focus in our analysis, we take a downwards adjustment for risk aversion. Similarly, the exclusion of financial sector corporations likely has a downwards impact on the average as it is likely the financial sector has high profit margins. The parameter is also adjusted as part of sensitivity analysis below.

- Sensitivity analysis has been conducted around all of the parameters to account for the uncertainty and confidence associated with each. A Monte Carlo simulation has also been undertaken (see Annex 2) to explore how the uncertainty of parameters interact with each other. Discussion of how parameters differ by scenario is in the Risks and Sensitivities section below.

716. The results of the updated modelling estimate an economic impact of £410m (range of £190-£460m) in one-off SCC costs and an annual cost of £240m (range of £210m and £420m) in lost export revenue. Once appraised over a 10-year period, the estimated NPV (2019 prices, 2024 present value) of EU Adequacy is £2 Billion (range of £1.7 and £3.4 billion).

717. Trade impacts may be higher when considering supply chain impacts as this analysis focuses on direct UK-EU exports only. However, unfortunately at this time supply chain data is limited.

718. Including these costs in the calculation of the total NPV for the Act is not appropriate due to uncertainty in both likelihood of the loss of EU adequacy occurring and the timing of which it is lost. It is also important to note that all trade effects would likely take place over the medium/long term and trying to include them in a clear 10-year horizon (NPV calculation) is fundamentally not robust.

719. The table below presents a scenario in which EU adequacy is lost. This is the NPV of the Data (Use and Access) Act if adequacy were to be lost in the first year after the implementation of the Act. This has only been presented for indicative 'worst case scenario' purposes and should not be interpreted as the final NPV of the package of the reforms, or as even a potential scenario based on the Government's engagement with its international partners.

Table 63: Net Benefit (Present Value (PV)) of the Act when EU adequacy is revoked, £million

Estimate	**Net Benefit (Present Value (PV)), £million**
Low	-787.7
High	16938.6
Best Estimate	8406.0

720. Additionally, the table below adds the potential benefit of data adequacy regulations to all possible rest-of-world countries. This is again not a potential scenario, but it is also provided for illustrative reasons and to provide a more comprehensive picture of all the potential effects that the government has considered. As above, an annual benefit of up to £471m in SCC benefits with a range of export revenue benefits (£159m, £181m and £316m) was calculated. Similar to the impacts of the loss of EU adequacy, the timings of individual data adequacy regulations are uncertain and the benefits identified are if all countries are awarded data adequacy regulations. The below should not be interpreted as the final NPV of the package of reforms.

Table 64: NPV of the Act when EU adequacy is revoked but adequacy to all other countries is considered

Estimate	Net Benefit (Present Value (PV)), £million
Low	4635.1
High	23712.9
Best Estimate	13765.4

Interoperability of the Health Care System:

721. **Boosting trade and market expansion**

722. Clinical systems vendor markets for primary, community and mental health are highly fragmented with similar levels of market concentration in each of the relevant segments, with the General Practice EPR market being a duopoly. A mixture of interventions to set regulations and promote competition for the market are required to incentivise suppliers to follow standards, improve service, reduce costs, and innovate.

723. Legislation on information standards can enable products and services to be built on principles of a unified system architecture, open data standards and interoperability – with reference to international best practice. This can support information access and aid system providers and suppliers, whilst giving clarity to new market entrants on information standards requirements in the industry.

724. Furthermore, there is also opportunities for market expansion - information standards would be designed to confirm with international best practice, therefore compliance with information standards opens opportunities for IT suppliers to also expand to new markets, driving competition and innovation on a global scale.

International trade

725. The UK has always protected its right to choose how we deliver NHS health and social care services in trade agreements, and we will continue to do so. The procurement of the UK's public services, including NHS health and social care services, are protected in the trade agreements to which the UK is a party. The protections are based on a set of agreed principles including maintenance of the UK's right to regulate public services. The UK will continue to ensure that the same rigorous protections are included in future trade agreements.

726. The provider selection regime (PSR) is being developed to provide the NHS and local authorities with the tools to deliver better value for patients, taxpayers, and the population. As such, this may cause some divergence between UK rules set out under the PSR and rules under the EU system. Depending on the structure of the new regime, this has the potential to impact international trade and investment, but it is currently not possible to estimate how much given the use of the power is not finalised. In line with Better Regulation Guidance, DHSC are engaging

with partners across Government including the Department for International Trade to fully assess any implications for international trade.

Risks and assumptions

Introduction

727. We have ensured that the analysis carried out in this Impact Assessment is detailed and robust. Where numerical evidence is not yet available, we have provided a qualitative assessment of the costs and benefits of the preferred option. This analysis is detailed and thorough however some of it relied on assumptions that are open to debate. We have therefore ensured that we have carried our sufficient sensitivity analysis and testing to make sure that we accounted for these potential risks. In this section we provide a breakdown of the key risks identified and the sensitivity analysis carried out. We also provide an overview of the policy risks related to the set of reforms.

Policy Risks and Assumptions

Improved Interoperability across Health and Social Care Systems

728. DSIT has worked alongside the Department for Health and Social Care to ensure that all policy risks of the proposed reform to increase interoperability across health and social care systems are included in this impact assessment.

729. Through clinical and non-clinical use case analysis, it is anticipated that the introduction of information standards compliance will be staggered and aligned to resolving interoperability challenges in line with the highest priority patient and citizen pathways. This limit (and signposts) the impact of changes required to be made by suppliers.

730. The risk of IT suppliers leaving the market: Digitisation of healthcare is a global trend, and many suppliers are facing very high demand for their services, leading to significant backlogs for new installations. Many of the biggest suppliers are global (Cerner, Epic) however there are no global standards around interoperability. This means that suppliers can prioritise investing in standard configurations for other, larger markets, such as the US and not in bespoke products to meet the proposed health and care IT standards. Our proposals therefore risk IT suppliers leaving the market due to an increased burden to deliver a product or service that is compliant in England, the rest of the UK and/or other nations. To mitigate this, we intend to consider international best practice concerning interoperability and engage with the health and care IT supplier market to ensure both of these inform the contents of our IT standards.

731. The risk of increased cost of IT products/services: There is a risk that despite an increase in competition, prices increase because the increased cost of compliance outweighs the downward pressure on prices resulting from the increased competition. To mitigate this, we intend to develop the standards themselves and implementation of the measures in consultation with varying supplier types. There may be a small risk to LAs when commissioning care, if IT suppliers pass on any potential increased costs incurred in meeting mandated information standards back to providers of care, who in turn pass them on to local authorities (Las) who have commissioned care. We will consider these carefully when implementing the provisions in the act. We do not anticipate such a risk to social workers developing care plans.

The risk of provider non-compliance due to the inherent differences in the health and social care provider market: Whilst the health care provider market is largely composed of NHS organisations, the providers in the adult social care market (although commissioned by local authorities) are largely independent, autonomous enterprises. **Exemption for Archives from further processing rules**

732. The measure seeks to ensure that a controller is able to re-use personal data for the purpose of archiving in the public interest, regardless of the lawful ground the personal data was originally collected on, including consent. The provision has a particular focus on maintaining 'private archives' which lack a basis in law and therefore are unable to use a public task (Article 6(1)(e)) lawful ground for their processing.

733. There is a risk that data subjects' trust may be impacted as their data can be processed and used for purposes beyond those stated when consent was given. This is particularly pressing as clarity around how data is used has been shown as important to data subjects, the DCMS Participation Study 2021-22 found 64% of respondents agreed or strongly agreed with 'I am comfortable with data being used when it is easy for me to understand how and why it is being used', while only 44% of respondents were comfortable with Private companies using data to grow the economy and create jobs.[308] If trust were to decline as a result of this measure, this could potentially impact a data subject's willingness to share their private data and therefore reduce the potential benefits of the provision.

Analytical risks and Assumptions

734. The analysis presented in this impact assessment is proportionate and detailed. Where costs and benefits have been able to be monetised, this has been carried out using certified and robust data sources. Where assumptions have had to be made due to a lack of available evidence, we have highlighted these and carried out sensitivity analysis to test them where possible.

735. When carrying out the sensitivity analysis we have taken a proportionate approach, in occasions where the assumptions are minor we have flexed these by an arbitrary 15% as suggested in HMT's Green Book, in the case of modelling various scenarios surrounding EU Adequacy we have conducted Monte Carlo simulations to test multiple assumptions. We have also tested the total benefits, costs and NPV using Monte Carlo simulations. These assumptions and results are highlighted below.

Direct Benefits - Compliance Costs

736. Compliance cost savings have been calculated using both assumptions and evidence. The table below outlines the assumptions that are relevant to all measures that are expected to impact compliance costs for UK businesses. The rest of this section goes through the assumptions specific to each proposed reform.

737. Since the last IA we have updated the modelling using the 2024 release of the UKBDS. This release asked businesses whether they had sought legal advice in the last 12 months, meaning

[308] DCMS, 2022 DCMS, 2022

we no longer require sensitivity analysis on the proportion of businesses who seek legal advice in a year.

Table 65: Assumptions used in modelling and RAG rating of confidence in assumptions

Assumption	Description	Source	RAG Rating
Number of businesses affected	Assumed the number of businesses affected by each measure	UK Business Data Survey	Green
Key compliance requirements and activities	Assumed the activities that would incur a compliance cost e.g. seeking legal advice, consumer complaints handling etc.	Frontier Economics and Data Protection and Data: A New Direction consultation	Green

738. As outlined in the direct benefit section of this Impact Assessment, the package of reforms is expected to impact UK firms costs of compliance. As well as modelling our core scenario highlighted in the analysis, we have applied sensitivity analysis to our assumptions to build both a low and high scenario. Firstly, looking at the estimated annual compliance cost saving from creating a limited non-exhaustive list of legitimate interests for which businesses can use personal data. The assumptions feeding into this estimation are below along with the low and high scenario values tested for each.

Table 66: Breakdown of assumptions for the legitimate interest's reform

Measure: Legitimate Interests[309] *Effect: Need to seek legal advice to clarify regulation*	Low scenario	Medium Scenario	High scenario
How much data use is affected by clarification under this measure	10%	25%	40%
% reduction in legal advice required to clarify the legislation in these cases	10%	25%	40%

Measure: Legitimate Interests[309] *Effect: Reduction in customer complaints about data use*	Low scenario	Medium Scenario	High scenario
% data use affected	10%	25%	40%
% reduction in complaints	10%	25%	40%

739. We estimate that businesses that analyse data and firms that use data for activities included on the list of 'recognised legitimate interests' (i.e. improving marketing or sales performance) will see a reduction in their compliance costs.

740. Applying these assumptions in our modelling provides us with an estimated cost saving of between £0.4 million and £6.5 million with the central estimate being £2.5 million.

741. It is also important to acknowledge the risks of the impacts to privacy and trust of these reforms. The scale of these impacts is dependent on the number and willingness of businesses

[309] More information and detail on this reform can be found in the direct benefits - monetised section of this Impact Assessment

to change their approach from relying on an alternative basis to that of 'Legitimate Interests'. Although the legitimate interest basis is flexible and applicable across a wide array of situations, there may be unmeasured costs and risks for businesses changing from a consent only approach to a different basis that requires use of a balancing test.

742. The RTA unit highlights the importance that data subjects place on openness when it comes to businesses processing their personal data.[310] If this openness were to change then consumers may be less inclined to engage with a business, resulting in a decrease in available data for businesses to use and a decrease in firm level productivity as a result (see privacy, trust and individual rights section for further details).

743. Looking at the estimated compliance cost savings for UK businesses that use data for research and development purposes, assumptions have been made where data is lacking or research suggests a varied level of impact. By testing the assumptions feeding into the model we are able to provide a range of potential monetary impact. The assumptions and their ranges are in the table below.

Table 67 : Breakdown of assumptions for the research purposes reform

Measure: Research Purposes *Effect: Need to seek legal advice to clarify regulation*	Low scenario	Medium Scenario	High scenario
How much of data usage is affected by clarification under this measure	20%	35%	50%
% reduction in legal advice required in these cases	10%	25%	40%

Measure: Research Purposes *25%: Reduction in customer complaints about data use*	Low scenario	Medium Scenario	High scenario
% data s affected	10%	25%	40%
% reduction in complaints	10%	25%	40%

744. We estimate the cost saved for these businesses to fall between £1.1 million and £10.7 million depending on the % of legal advice required, number of complaints that relate to research and development and the % reduction estimated in these complaints as well as the other factors listed above. Our best estimate predicts a total cost saving of £4.7 million for businesses using data for research purposes.

745. Reforms aimed at the use of data in AI and Machine Learning are designed to save businesses compliance costs. Our estimations of the monetary value of these savings rely on the following assumptions that we test below using a low medium and high scenario.

Table 68: Breakdown of assumptions for the AI and Machine Learning reform

Measure: AI and Machine Learning *Effect: Need to seek legal advice to clarify regulation on data for AI*	Low scenario	Medium Scenario	High scenario
How much of data usage	5%	20%	35%

[310] Public attitudes to data and AI: Tracker survey, RTA unit 2022

Measure: AI and Machine Learning *Effect: Need to seek legal advice to clarify regulation on data for AI*	Low scenario	Medium Scenario	High scenario
is affected by clarification under this measure			
% reduction in legal advice required in these cases	10%	25%	40%

Measure: AI and Machine Learning *Effect: Reduction in customer complaints about data use*	Low scenario	Medium Scenario	High scenario
% of complaints in firms that use data on AI - related to AI	5%	10%	25%
% data uses affected	10%	25%	40%
% reduction in complaints	10%	25%	40%

746. Changing these assumptions provides an estimate of compliance cost savings for UK businesses of between £0.7-million and £19.4 million with a central estimate of £7.0 million.

747. There will also be wider impacts to both businesses and data subjects because of this reform. Current evidence suggests awareness of the use of AI in decision making is relatively low, as is awareness of individual data protection rights in this area. Support for AI use in decision making varies by context, and there are concerns even in use cases with broad support.(see Privacy, Trust and Individual Rights section). This highlights that this policy has a potential impact data subject levels of trust or comfort with data use in ADMs. By clarifying to businesses, the circumstances in which safeguards apply to significant decisions about individuals on the basis of profiling, there maybe an increase in the use of ADM. This increase use could also increase in data subjects' awareness of the personal data being used in ADM. This increased use has the potential to result in an increase in benefits such as quicker, and more consistent decisions for individuals, particularly in cases where a very large volume of data needs to be analysed and decisions made very quickly which could increase comfort in providing data to be used for these purposes. This in turn could increase support for the technology.

748. The safeguard provisions within the Act aim to ensure that data subjects have the right to be provided with information and express their point of view, to contest them and to seek human intervention to review. If there is an increase in awareness of personal safeguards, this could lead to an increase in trust and comfort in the use of ADM.

749. Conversely, there may be a risk that this increased awareness of use of ADM could also increase the number of people that disagree with the principle, particularly if it is used in circumstances where evidence suggests concerns are currently greater, or if the public view a

lack of fairness or transparency. Support could be further reduced if an individual receives an outcome that is perceived as either negative or unfair as a result of ADM. In this scenario, it is possible some individuals could try to restrict the sharing of data or use of services known to rely on this technology.

750. The safeguard provisions within the Act aim to ensure that data subjects have the right to be provided with information and express their point of view, to contest them and to seek human intervention to review. If there is an increase in awareness of personal safeguards, this could lead to an increase in trust and comfort in the use of ADM.

751. Conversely, there may be a risk that this increased awareness of use of ADM could also increase the number of people that disagree with the principle, particularly if it is used in circumstances where evidence suggests concerns are currently greater, or if the public view a lack of fairness or transparency. Support could be further reduced if an individual receives an outcome that is perceived as either negative or unfair as a result of ADM. In this scenario, it is possible some individuals could try to restrict the sharing of data or use of services known to rely on this technology.

752. The estimated compliance cost savings with regards to the privacy and electronic communications policies depend on an assumption made on the proportion of businesses that will no longer need to offer opt-in services. This assumption is tested using the values in the table below.

Table 69: Breakdown of assumptions for the PECR reform

Measure: Privacy and Electronic Communication *Effect: Activities required to obtain consent*	Low scenario	Medium Scenario	High scenario
Proportion of businesses that will no longer need to offer opt-in	15%	30%	45%

753. These assumptions provide an estimated cost saving of between £8.6 million and £25.7 million with a central estimate of £17.1 million. The total estimated compliance cost savings for UK businesses for each measure are in the table below. We estimate compliance cost savings to fall between £10.7 and £62.3 million annually.

Table 70: Breakdown of total compliance costs saved by reform and scenario, 2024 prices

Reform	Cost by firm size (£million) Low Scenario	Cost by firm size (£million) Medium Scenario	Cost by firm size (£million) High Scenario
Legitimate Interests	0.4	2.5	6.5
AI and Machine Learning	0.7	7.0	19.4
Research Purposes	1.1	4.7	10.7
Privacy and electronic communications	8.6	17.1	25.7
Total	10.7	31.3	62.3

Indirect Benefits - Productivity Impacts

754. Productivity impacts have been calculated using both robust sources of evidence as well as modelling assumptions; the table below outlines the assumptions that are relevant to all measures that are expected to impact UK business productivity. The rest of this section goes through the assumptions specific to each proposed reform.

Table 71: Assumptions used in modelling and RAG rating of confidence in assumptions

Assumption	Description	Source	RAG Rating
Number of businesses affected	Assumed the number of businesses affected by each measure	UK Business Data Survey	Green
Proportion of organisations affected	The number of organisations that will be more productive	Estimate	Amber

755. In this modelling we make informed assumptions on the proportion of firms that would increase their data use because of these reforms. We have tested these assumptions by carrying out sensitivity analysis around these percentages and creating a low scenario where the actual number of businesses increasing data use is less than assumed (10%) and a high scenario where the opposite is the case (50%). We also tested the assumption of the proportion of firms that would increase AI use due to the reforms in the Act, presenting a low scenario (5%) and a high scenario (15%). A list of all assumption per measure for each scenario can be found in the table below:

Table 72: Breakdown of assumptions when modelling the impacts on UK GVA and productivity

Legitimate Interests	Low scenario	Medium scenario	High scenario
Scaling factor to account for the fact that not all firms would increase data use based on this measure	10.0%	25.0%	50.0%
Scaling factor on the productivity impact as measures will only affect data use	5.0%	10.0%	15.0%

Research Purposes	Low scenario	Medium scenario	High scenario
Scaling factor to account for the fact that not all firms would increase data use based on this measure	20.0%	35.0%	60.0%
Scaled proportion of total business that could increase their data use with clearer guidance	0.04%	0.10%	0.2%

AI and Machine Learning	Low scenario	Medium scenario	High scenario
Scaling factor to account for the fact that not all firms would increase AI use based on this measure	5.0%	10.0%	15.0%

756. The results suggest a range in the scale of benefits of between £15.0m and £73.6m. A breakdown of this impact by reform can be found below:

Table 73: Breakdown of total impacts on UK GVA by measure and scenario, in 2024 prices, £million

Measure	Low scenario	Medium scenario	High scenario
Legitimate Interests	2.4	11.9	35.8
Research Purposes	5.2	9.1	15.6
AI and Machine Learning	7.4	14.8	22.2
Total	**15.0**	**35.8**	**73.6**

Direct Costs - Familiarisation costs to UK businesses (private sector)

757. Familiarisation costs have been calculated using a variety of assumptions and evidence sources; the table below outlines the assumptions that are relevant to all measures that are expected to inflict familiarisation costs on UK businesses. The rest of this section goes through the assumptions specific to each proposed reform.

Table 74: Assumptions used in modelling and RAG rating of confidence in assumptions

Assumption	Description	Source	RAG Rating
Number of pages of guidance	Assumed 5 pages of guidance per measure	DSIT policy teams	Amber
Wage Estimates	Assumed the wage of the employee reading the guidance per measure	Annual Survey of Hours and Earnings and ICO/DSIT (2020) Impact Assessment for the Age Appropriate Design Code	Amber
Number of businesses affected per measure	Assumed the number of businesses affected by each measure	UK Business Data Survey	Green
Hours Required	Assumed the reading speed of the employee reading the guidance	ICO/DSIT (2020) Impact Assessment for the Age Appropriate Design Code	Green

758. When calculating the expected familiarisation costs for UK businesses of the proposed package of reforms we test the assumptions that feed into the modelling.

759. We continue to use a time-cost approach to estimate the administrative costs of reading the new legislation. Although this methodology has not changed, we have updated some of our assumptions feeding into the model using new evidence. In order to identify the relevant 'number of affected businesses' per measure, we look at an organisation's data use to determine if they are in scope of the model.

760. We have updated our wage assumptions in line with the methodology used in the ICO Age Appropriate Design Code Impact Assessment by assuming that at small, medium and large-sized enterprises the wages of senior officials are representative of those who would read the guidance, and estimated the hourly unit cost of this work at £30.68 using occupational estimates from the Annual Survey of Hours and Earnings (ASHE) uplifted to 2024 prices.[311] This analysis assumes that a micro-sized firm has zero employees. For micro-sized firms we have updated our wage assumptions by applying median annual earnings estimates of the self-employed from DWP's Family Resources Survey and estimating the hourly unit cost of this work at £11.97.[312]

761. We continue to assume that the guidance would be at a similar level of reading difficulty to the ICO's data sharing code, and therefore have used a similar Fleisch reading ease score of 40, which corresponds to a reading speed of 75 words per minute.

Table 75: Breakdown of total impacts on Familiarisation costs for UK businesses by measure and scenario, in 2024 prices, £million

Reform	Low scenario	Medium scenario	High scenario
Research Purposes	5.3	6.2	7.2
Legitimate Interests	5.2	6.2	7.1
AI and machine learning	4.2	4.9	5.6
Privacy and Electronic Communication	3.7	4.3	5.0
Total	18.4	21.6	24.9

Digital Identity

762. This section of analysis highlights the assumptions and sensitivity analysis undertaken in the Powers for Digital identity and Attributes Initiatives De Minimis Assessment produced by DSIT.[313] The following table outlines how this analysis has been classified into a low, medium and high scenario. More detail on this can be found in the full Impact Assessment.

[311] ONS Annual Survey of Hours and Earnings (2023
[312] DWP Family Resources Survey (2020)
[313] Powers for Digital Identity and Attributes Initiatives De Minimis Assessment, DSIT (2024)

Table 76: Breakdown of all risks and assumptions included when modelling the impact of the Digital Identity measures

Wage estimation

SCENARIO	RISK ASSESSMENT
All scenarios: In the 2024 estimates, our public sector estimates have been inflated to 2024 prices, including overhead adjustments.	No sensitivity analysis has been undertaken.

Estimated cost values

SCENARIO	RISK ASSESSMENT
All scenarios: The values used to calculate the estimated costs have been gathered from an engagement exercise with stakeholders. The cost estimations provided by the engagement exercise in 2021 have been adjusted to 2024 value.	There is a risk that the data collected may not be very representative. We have set different scenarios to attempt to mitigate this risk.
All scenarios: Averages of the inputs gathered throughout the engagement exercise were used to estimate the potential average cost of each task for a business.	N/A
All scenarios: The cost estimations provided by the engagement exercise are in 2021 value.	N/A
All scenarios: Wage per hour has been calculated by dividing the gross annual wage by the number of weeks in a year (52) by the ONS' 2019 average number of working hours in a week. We took the 2019 value as the 2020 value has been significantly affected by Covid 19 and would not have been representative of the usual working patterns.	The change in average over time is minimal
All scenarios: Costs over the 10-year appraisal period are undiscounted.	N/A

Number of businesses

SCENARIO	RISK ASSESSMENT
All scenarios: We assume that only medium and large UK businesses will take up digital identity as their benefits will significantly outweigh the transition costs. Data regarding the Number of UK medium and large businesses was collected from the ONS data release: UK "BUSINESS: ACTIVITY, SIZE AND LOCATION - 2020", table 3.	We updated these figures from the 2020 publication and no sensitivity analysis has been undertaken.

Familiarisation costs

SCENARIO	RISK ASSESSMENT
Central estimate scenario: The values from the engagement exercise have been used to calculate the central estimate of the potential average familiarisation costs per business. **Low estimate scenario:** We reduced the central estimate by 50%. This is a standard assumption. **High estimate scenario:** We inflated the central estimate by 100%. This is a standard assumption.	There is a risk that the data collected may not be very representative. We have set different scenarios to attempt to mitigate this risk.
All scenarios: For each task the estimated costs have been calculated as: average resources required (employees and time) * average wage per hour (including 22% overhead costs)	N/A
All scenarios: We estimated the familiarisation costs per businesses and multiplied the value by the 2020 number of UK medium and large businesses.	N/A
All scenarios: The familiarisation costs are one-off costs.	N/A
All scenarios: We assume all businesses face familiarisation costs in year one independently of the use case.	N/A

Organisational change costs

SCENARIO	RISK ASSESSMENT
Central estimate scenario: The values from the engagement exercise have been used to calculate the central estimate of the potential average organisational costs per business. **Low estimate scenario:** We reduced the central estimate by 50%. This is a standard **assumption.** **High estimate scenario:** We inflated the central estimate by 100%. This is a standard assumption.	There is a risk that the data collected may not be very representative. We have set different scenarios to attempt to mitigate this risk.
We estimated the organisational costs per business and multiplied the value by the 2020 number of UK medium and large businesses.	N/A
Due to the limited number of responses and the presence of outliers we have used the median number of hours gathered from the engagement exercise to calculate the expected costs per business.	N/A
The organisational change costs are one-off costs.	N/A
For each task the estimated costs have been calculated as: average resources required (employees and time) * average wage per hour (including 22% overhead costs)	N/A
We estimated the familiarisation costs per businesses and multiplied the value by the 2020 number of UK medium and large businesses.	N/A
Businesses in the sector related to each of the use cases face the organisational	N/A

SCENARIO	RISK ASSESSMENT
change costs the year that the digital ID checks take place for the first time. (E.g. real estate businesses face the organisational change costs when the checks related to the home buying process begin). If businesses are affected by multiple use cases they face the organisational change costs only once.	
All medium and large UK businesses face organisational change costs to adapt to carrying employee mobility checks digitally.	N/A
Cost estimates from the 2021 DMA have been adjusted to 2024 values. This includes the overhead costs.	N/A

One-off connection fee

SCENARIO	RISK ASSESSMENT
Central estimate scenario: We assume that the one-off connection fee may be £5650. This value has been estimated by a research project carried out by the private sector on behalf of DSIT. **Low estimate scenario:** We assume that the one-off connection fee may be £3900. This value has been estimated by a research project carried out by the private sector on behalf of DSIT. **High estimate scenario:** We assume that the one-off connection fee may be £7400. This value has been estimated by a research project carried out by the private sector on behalf of DSIT.	We set different connection fee costs in each scenario to attempt to mitigate the risk of under or overestimating the connection fee costs.
The number of identity providers that may pay the connection fee has been estimated by the private sector on behalf of DSIT. This number (100) does not vary across scenarios.	No sensitivity analysis has been undertaken.

Linear trend over time of the digital identity market towards the steady state

SCENARIO	RISK ASSESSMENT
Central estimate scenario: We assume that the digital identity uptake grows over time following a linear trend. For instance, in the central scenario we assume that only 15% of the total potential number of checks and expected benefits estimated by Deloitte takes place in year 1. In the central scenario 100% of digital identity uptake is reached by year 7 of the appraisal period. **Low estimate scenario:** The trend in the best-case scenarios is 33% higher than the central scenario. **High estimate scenario:** The trend in the worst-case scenarios is 33% lower than in the central scenario.	There is a risk that the estimated trend lines may be incorrect. We have set three different scenarios to attempt to mitigate this risk.

SCENARIO	RISK ASSESSMENT
The trend has been estimated through conversations with the policy team based on their knowledge of the digital identity sector.	No sensitivity analysis has been undertaken.

Cost per check

SCENARIO	RISK ASSESSMENT
Central estimate scenario: We assume that the per-check fee may be 10p. The assumption has been set in agreement with the policy team based on their market knowledge. **Low estimate scenario**: We assume that the per-check fee may be 5p. The assumption has been set in agreement with the policy team based on their market knowledge. **High estimate scenario:** We assume that the per-check fee is 50p. The estimate comes from the Home Office Passport Pilot Scheme.	There is a risk these costs may not be accurate and have increased. We conducted sensitivity analysis to assess how change in cost impacts the results.

Number of checks

SCENARIO	RISK ASSESSMENT
The annual number of checks (assuming the steady state market level) for each use case has been estimated by a research project carried out by Deloitte. The values are constant across scenarios.	There is a risk that the full number of annual checks estimated by Deloitte may not be realised as soon as checks begin. To mitigate this risk, we have multiplied the annual volume of checks by the estimated trendline.
The number of digital ID checks grows over time following the estimated trendline. The trendline varies depending on the scenario.	N/A

Total annual cost of per check fees

SCENARIO	RISK ASSESSMENT
We calculate this estimate by multiplying the estimated annual number of checks (adjusted to the trend) by the estimated per check fee.	No sensitivity analysis has been undertaken.

Year the costs and benefits take place

SCENARIO	RISK ASSESSMENT
The assumptions regarding the year the digital ID checks may begin for each use case and scenario are based on information provided by the policy team based on their knowledge of the sector.	There is a risk that these assumptions may be incorrect. To mitigate this risk, we have set different years in each of the three scenarios.
The years assumed in the best and worst scenarios are variations of what is estimated in the central scenario.	N/A

Scenarios

SCENARIO	RISK ASSESSMENT
Central estimate scenario: In the central scenario we assume that the checks that rely only on passport data may start taking place from year 2 onwards. Whereas it may take 3 years for those that rely on passport data and guidance being updated. Lastly, it may take 5 years for the checks that rely on datasets other than passport data. **Low estimate scenario:** In the best-case scenario, we assume early uptake, low costs and high benefits. **High estimate scenario:** In the worst-case scenario, we assume later uptake, high costs and low benefits.	There is a risk that these assumptions may be incorrect. To mitigate this risk, we have set different years in each of the three scenarios.

Benefits

SCENARIO	RISK ASSESSMENT
The estimated benefits over the 10-year appraisal period have not been discounted.	N/A
The values used in the Deloitte methodology to calculate the benefits have been modified to align with the cost estimations. Estimated wage values have been inflated by 22% to account for overhead costs and monetary values have been inflated to 2021 prices. Where the year was unclear, we assumed the values were in 2020 prices.	N/A

First order indirect benefits

SCENARIO	RISK ASSESSMENT
The estimated annual economic value for the UK of carrying out digital ID checks has been by Deloitte.	No sensitivity analysis has been undertaken.
The estimated values assume that the steady state level of the market is	N/A

reached. Therefore, we adjusted the estimated values of the benefits by the estimated digital identity market trend over time.	
We split the total value of the benefits by the value we expect private citizens to experience and the value we expect businesses to experience.	N/A

Second order indirect benefits

SCENARIO	RISK ASSESSMENT
We assume that one proportion of the value of benefits related to faster employee mobility for people on short notice periods begins to take place when digital DBS checks are realised, the second part when digital RWT checks begin to take place and the remaining value when digital qualification checks begin to happen. Each percentage is proportional to the annual number of checks estimated for DBS, RWT and qualification checks.	No sensitivity analysis has been undertaken.
The assumption above is set for productivity improvement as well.	N/A
The total value of the indirect benefits related to reduced fraudulent applications arises when digital qualification checks begin to take place as we assume the current costs are related to hiring workers with false credentials.	N/A

Non-monetised costs to businesses: Costs to private sector businesses

SCENARIO	RISK ASSESSMENT
We expect businesses to have to pay to adapt their way they carry out ID verification to digital identity. For instance, by setting up a platform to perform digital ID checks.	No sensitivity analysis has been undertaken as we were unable to monetise these costs.

Non-monetised costs to businesses: Costs to join the Trust Framework

SCENARIO	RISK ASSESSMENT
Although being signed up to the trust framework will not be compulsory to operate in the market, we assume that private-sector access of government-held databases is only granted to the businesses signed up to the trust framework. Therefore, businesses will have to sign up to it in order to effectively operate in the market.	No sensitivity analysis has been undertaken as we were unable to monetise these costs.

Cost for public sector bodies

SCENARIO	RISK ASSESSMENT
We assume that public sector bodies face familiarisation costs, costs to digitise any IDs in paper-only form (e.g. birth certificates before a certain year), costs to	No sensitivity analysis has been undertaken.

allow private sector access to their databases and costs to set up and run the governance function. All costs except digitisation costs have been included in the net benefits calculations.	
In the central and best scenarios, we assume that 4 Departments adapt to digital identity. Whereas, in the most pessimistic scenario we assume all 43 ministerial and non-ministerial departments adapt to digital identity.	Sensitivity analysis has been undertaken by varying the number of Departments across scenarios.

Net benefits

SCENARIO	RISK ASSESSMENT
The net benefits have been discounted so they are presented in NPV.	N/A

Creation of Innovative and Secure Smart Data Schemes (DBT)

763. This section is based on analysis by DBT for the Regulatory Powers for Smart Data Impact Assessment.[314] This covers the analytical risks of the proposed preferred option.

764. The primary risks associated with the introduction of new Smart Data powers are:

a. The powers are not used to introduce schemes, and no acceleration benefits are realised;

b. Inconsistent implementation and design of secondary regulations limits the potential for coordination, efficiencies, and interoperability

765. DBT has engaged extensively with relevant stakeholders to mitigate these risks. For example, the Smart Data working group was established to bring together government departments and regulators with the aim to:

a. support the development and delivery of Smart Data infrastructure and standards for the benefit of consumers, particularly vulnerable consumers

b. where appropriate encourage commonality or consistency of approach across Smart Data initiatives to enable interoperability and cross-sector innovations

c. improve efficiency by reducing duplication across Smart Data initiatives and re-using assets or resources from prior smart-data initiatives

d. DBT continues to drive cooperation and coordination across sectors. We intend to build on the work undertaken by the Smart Data Working Group, developing an active ecosystem for Smart Data and support greater collaboration and coordination. As part of this DBT have launched two workstreams that aim to identify a variety of use cases, find ways to encourage greater cross-sector data sharing, and support wider sectors to explore future Smart Data schemes. The workstreams are:

i. The Smart Data Council[315] aims to find ways to help extend the benefits of Smart Data to new sectors. The Council is made up of key government departments,

[314] Regulatory Powers for Smart Data Impact Assessment, DBT (2024)
[315] DBT (April 2023): New Smart Data Council to drive forward savings for household acts

regulators, industry, and consumer groups. The Council will direct coordination and drive collaboration and knowledge-sharing across the key decision makers and stakeholders.

ii. The Smart Data Discovery Challenge[316] calls on innovative thinkers across industry to recommend new solutions that could benefit individuals, small businesses, and wider society. It aims to foster individual innovators and partnerships to develop their initial ideas into feasible concepts with potential to move into development. Following the Discovery Challenge, DBT are exploring launching a full challenge prize, where these ideas could be tested in a sandbox environment.

e. To identify and mitigate against any risks or unintended consequences, any secondary regulations using the Smart Data powers will go through the affirmative procedure to ensure there is robust legislative scrutiny of the measures. As part of this, a proportionate Impact Assessment and relevant Post Implementation Review requirements would need to be produced.

Reduced competition

766. There is a risk that Smart Data may unintentionally harm competition. For example:

a. ***Too strenuous compliance obligations for data holders or third parties***, leading to increased barriers to entry and reduced competition. A consultation prior to secondary legislation will help minimise this risk.

b. ***Data mobility provides dominant incumbent data holders with more market power***. Emerging research[317] suggests that increased data mobility could lead to customers becoming increasingly attracted to their existing, dominant providers who can utilise product/performance data from other providers to their advantage. However, Open Banking has been recognised by the CMA as a key step towards unlocking competition in retail banking and the evolution of the UK's fast-growing fintech sector.[318] This is evidenced in the continued growth of the Open Banking ecosystem.[319] Smart Data schemes can minimise these effects (for example by providing exemptions for smaller providers) and existing competition law should mitigate the potential for excessive market power.

c. ***Damaged incentives to differentiate on privacy and security*** if the government mandates interoperability, which is a key source of competition in markets such as digital platforms.[320] Using the tiering of standards, for instance based on risk factors or the nature of the data involved, or specific exemptions could mitigate this by ensuring proportionate approaches are used.

d. ***Lock-in to a suboptimal standard specified by the government***. This risk constraining industry from innovating beyond the standards which could improve

[316] DBT (October 2023): Government-led coalition launches open call for bold and innovative ideas using Smart Data
[317] BoE (December 2019): "Platform competition and incumbency advantage under heterogeneous switching cost — exploring the impact of data portability" paper, & Stratechery (May '18): "The Act Gates line" article
[318] CMA (November 2021): "Update on Open Banking"
[319] Number of ATPs entering Open Banking has grown by 80% in just under 2 years, and 245.
[320] FT (October 2017): "Privacy is a competitive advantage" article, among other examples such as Signal, DuckDuckGo etc.

Smart Data schemes. To minimise this risk, broad stakeholder engagement will be required when designing future schemes.

e. **A mandatory Smart Data scheme could facilitate price collusion among businesses.** Increased transparency though a Smart Data scheme which shares information in an open, free and real time basis could potentially increase the risk of price collusion and/or anti-competitive exchanges of commercially sensitive pricing information. In theory, this could lead to prices becoming higher as firms can more easily see how the other firms are pricing and match that, rather than competing. To minimise this risk, enforcement and monitoring plans for non-compliance and anti-competitive behaviour are required to be considered at secondary legislation level.

Reduced data holder incentives

767. If data holders have to share their collected data with ATPs, they may be less likely to recover the cost of data collection in the first place as any competitive advantage may be lost. This could present a free rider problem, where ATPs benefit from data collection without contributing to its provision. This risk is minimised by the fact that the majority of data in-scope of Smart Data is personal and product data, which will have been collected regardless of intervention. This risk is further minimised by the UK GDPR's data minimisation principle.

Poor security

768. Smart Data is expected to benefit consumer data security by creating strong standards and displacing less secure practices such as screen scraping. However, if security considerations behind the standards are weak, this could risk decreased security of customer data, including leakage of data.

769. In addition, increasing the use of digital services and enabling new intermediaries could present new opportunities for security risks as data is more readily transferred from one place to another. However, accreditation requirements, which would likely include security requirements, would help ensure that participants in the Smart Data ecosystem have adequate security and are trustworthy. Accreditation requirements are also expected to aid consumers, reducing the need for time spent understanding which agents are legitimate and which are not.

Lack of uptake of Smart Data schemes

770. The benefits of Smart Data would be reduced, yet the majority of costs would still be incurred, if there is a lack of uptake of Smart Data schemes. This may be because of a lack of trust in the ecosystem, a perception that there is no benefit of Smart Data enabled services, or a lack of awareness these services exist. Examining public attitudes towards potential Smart Data schemes, the Responsible Technology Adoption (RTA) unit found that schemes will need to overcome initial consumer uncertainty about the direct benefits of data sharing and concerns about potential risks[321]. Schemes will also need to win the trust of a full range of consumers, both those hesitant about using digital tools and those that are more digitally engaged. In addition, they found that consumers tend for stick with banking and telecommunications services providers that they know and have used, but that having positive previous experience with Smart Data services increased consumers' support for these types of services.

[321] RTA unit (June 2022): Part one: Examining public attitudes towards Smart Data schemes

771. However, over recent years we have seen exponential growth in Open Banking users. The pandemic has also been a catalyst for a step- change in digital skills for some participants, with 92% of UK adults using the internet at home or somewhere else.[322] Furthermore, 83% of internet users used online banking in 2021,[323] up from 51% in 2019,[324] much of which is likely facilitated by Open Banking and APIs.

Lack of demand for Smart Data services

772. Related to low user uptake is the assumption that Smart Data will enable products that customers will want to use, and an ecosystem ATPs want to join.

773. Evidence from banking shows the wide-ranging innovations offered by ATPs and high user demand for these services. There are several other examples in the energy sector:

a. The collective switching energy trial[325] featured a simplified switching process, similar to potential Smart Data use case, and found a "substantial impact on switching among customers who have not switched energy tariff for many years and can be delivered at scale".

b. Ofgem user research on midata[326] tested a functional prototype of a price comparison website. Participants were less concerned about sharing their energy data than their financial data, but were generally comfortable with sharing data when it is clear what they are consenting to. A key takeaway from this research is that clear communication and messaging is required to drive adoption, particularly around consent.

c. Previous midata[327] IA contains surveys showing demand for a better system for consumers to be informed by their own data. For example, 43% strongly agreed and a further 47% were in favour of wanting easy access to personal data. Further research from Ofcom highlights that 40% of surveyed internet users were not aware of any of the ways in which online companies collect their personal information.[328]

Changing prices for consumers

774. It is unclear how incumbent data holders will amend their pricing strategy in response to Smart Data schemes. Costs could potentially be passed onto customers, an uncertainty which Ofcom noted but stated they see no immediate competition concerns arising from Open Communications.[329]

Misuse of customer data

775. As a result of increased data sharing, there is a potential for an increase in the misuse of customer data. This could include potential risks such as an increase in 'nuisance' calls and contact, or unwelcome selling-on data.

---

[322] Ofcom (March 2023): Adults' Media Use and Attitudes report 2023
[323] Ofcom (April 2021): "Adults' media use and attitudes report 2020/21"
[324] Ofcom (May 2019): "Online Nation 2019 report"
[325] Ofgem (August 2018): "Eight times as many people get a better deal in Ofgem's collective switch trial" Press Release
[326] Ofgem (October 2020): "midata Discovery and Proof of Concept User Research Findings"
[327] Referenced in the BIS (2012): "Order making power for midata"
[328] Ofcom (April 2021): "Adults' media use and attitudes report 2020/21"
[329] Ofcom (August 2020) "Open Communications: Enabling people to share data with innovative services"

776. However, standards and security requirements would ensure that customer data can only be used for purposes as specifically requested by the consumer. There is a potential for agents to sell on customer data, but it would be at the customer's discretion whether they consent for their data to be used for these purposes.

National Security and Law Enforcement

777. This section of analysis has been provided by the Home Office. This covers the analytical risks of the proposed reforms to data use for National Security reasons.

778. Time constraints and a lack of data meant that it was not possible to monetise most costs and benefits.

779. Stakeholders were unable to provide the relevant information under the strict time constraints required by the analysis, although they responded as best they could with qualitative and some quantitative evidence. For certain proposals the data required to monetise costs and benefits simply could not be obtained as they were too specific and were not recorded.

780. Although the analysis conducted is limited, it effectively conveys the degree of uncertainty about the economic costs and benefits of these proposals, and this should be considered.

781. This analysis is also in line with previous impact assessments conducted for the DPA 2018, where data difficulties posed significant problems for monetisation of costs and benefits.

782. There are significant analytical risks given that a mostly qualitative analysis was performed resulting in a narrative based assessment.

783. A lack of data means that most costs and benefits were not monetised, and therefore the scale of the potential costs and benefits of the relevant proposals cannot be clearly demonstrated.

784. There has been an attempt to provide an idea of scale, however the information is still limited, and significant uncertainty remains.

785. There is a risk that for the proposal to remove the need to record the 'justification' for consultation / disclosing data disclosure, the number of system accesses is not constant over the appraisal period. This could lead to a reduction or increase in benefits depending on the number of times automated systems are accessed.

786. There is also the risk that after accessing a system, LEA employees perform tasks which require further logging which would increase the scale of benefits.

787. Upscaling the benefits of this proposal to the MPS so that monetised benefits are obtained for all LEAs is risky as there is no data to suggest how utilisation compares among other LEAs. This means that the values obtained should be viewed with caution.

Impact to international trade

788. HMG accepts that reforms need to comply with the UK's international legal obligations. The reforms proposed are in line with international practice. We are working with DBT legal and policy to understand whether the changes would affect our compliance with FTA measures. If

any impacts are identified through this analysis, they will be in due course reflected in the present impact assessment.

Impact of changes to EU Adequacy

789. An outline of the modelling assumptions used to estimate the impacts of EU adequacy can be found in the table below.

Table 77: Assumptions used in modelling and RAG rating of confidence in assumptions

Assumption	Description	Source	RAG Rating
Investment Horizon	Assumed a five-year investment horizon when firms decide whether or not to continue trading with the EU	Estimate	Red
Compliance Rate	The percentage of businesses that will comply with the regulations.	Estimate	Red
Profit Margin	The profit margin firms would need to continue trading with the EU	Profitability of UK Companies Data	Red
SCCs in place	The percentage of businesses that have SCC's in place	UK Business Data Survey 2021	Green
SCC Cost Rollover	The percentage of SCC costs likely to be rolled over to EU businesses	New Economic Foundation Report	Amber
SCC Cost	The cost to firms of producing SCCs	Estimate	Red

790. The table above describes analysis of the potential value of EU Adequacy. As outlined, several parameters were adjusted to capture uncertainty around business decision-making, such as the profit margin, the investment horizon as well as adjustments to SCC costs such as compliance, the number that already have SCCs in place and the proportion of costs borne by the UK business. When parameters vary by business size, the minimum and maximum of the range is used to account for uncertainty in that parameter. The three tables below outline how the parameters vary.

Table 78: EU Adequacy Parameters Sensitivity

Parameter	Best Estimate	Low	High
Profit Margin	9.6%	4.6%	14.6%
Investment Horizon (years)	5.0	2.0	10.0
SCC Compliance Rate	100.0%	100.0%	80.0%

Table 79: UK-EU SCC Cost Rollover (Borne by UK Firms)

Business Size	Best Estimate	Low	High
0	75.0%	75.0%	50.0%
1 - 9	75.0%	75.0%	50.0%
10 - 49	65.0%	75.0%	50.0%
50 - 249	60.0%	75.0%	50.0%
250 +	50.0%	75.0%	50.0%

Table 80: Percentage of UK Firms that have SCCs in place

Business Size	Best Estimate	Low	High
0	9.0%	9.0%	47.0%
1 - 9	20.0%	9.0%	47.0%
10 - 49	25.0%	9.0%	47.0%
50 - 249	31.0%	9.0%	47.0%
250 +	47.0%	9.0%	47.0%

791. The results of the updated modelling estimate an economic impact of between £190 and £460 million in one-off SCC costs and an annual cost of between £210 and £420 million in lost export revenue. Once appraised over a 10-year period, the estimated NPV of value of EU Adequacy is between £1.7 and £3.5 Billion.

Impacts of ensuring businesses are able to continue to seamlessly use their pre-bill existing transfer mechanisms

792. This reform provides for additional transitional arrangements in the Act for a wider set of current alternative transfer mechanisms (ATMs). Similar to the approach taken for pre-commencement adequacy regulations and pre-commencement standard data protection clauses, this reform introduces transitional provisions for pre-bill appropriate safeguards in Article 46 UK GDPR, Schedule 21 (paragraph 9) DPA 2018, and Section 75, Part 3, 2018 Data

Protection Act currently in operation which meet the required level of protection under the existing framework.

793. It was previously estimated that this reform will have a net zero impact, allowing businesses to continue to use their pre-bill mechanisms, however we also noted that this impact was dependent on additional transitional provisions for currently unapproved EU BCRs. The ICO have since confirmed that unapproved EU BCRs are not currently a valid legal transfer mechanism. This remains the case , and as such, additional costs will not be incurred by businesses as a result of the transitional arrangements in the Act. of final results

794. There are a significant number of assumptions made across the models used in our cost-benefit analysis. To be transparent on the potential range of uncertainty, we have undertaken a Monte-Carlo analysis varying the final results. The final results include the total costs, total benefits and net benefits. DSIT analysts have used Monte-Carlo analysis to present probabilistic results that allow us to see the likelihood of each outcome.

795. The table below shows the summary statistics for the Monte-Carlo analysis showing the mean, standard deviation, minimum and maximum for each of our results of interest. The analysis was run 50,000 times picking a random selection of each of the parameters. The costs and benefits are in present value over a 10-year appraisal period.

796. The table below shows a relatively large range of results. The net benefit of the preferred reforms varies between £7329.6 and £16075.7m with a mean of £11556.6m. The graphs below show the distribution of the final results including net benefit, total cost and total benefits. The net benefit graph shows a relatively uniform distribution, while the total cost graph shows a maximum value of £2993.0m and a minimum value of £1451.1m with a mean of £2156.2m. The total benefits graph shows a mean of £13712.8 with a minimum value of £9927.8m and maximum value of £17844.4m.

Table 81: NPV Monte-Carlo Summary Statistics

Results	N	Mean	St. Dev.	Min	Max
Net Benefit	50000	11556.6	1105.4	7329.6	16075.7
Total Cost	50000	2156.2	256.0	1451.1	2993.0
Total Benefits	50000	13712.8	1076.3	9927.8	17844.4

Chart 1: Net Benefit (£million), Final Results Monte Carlo Analysis (50,000 simulations)

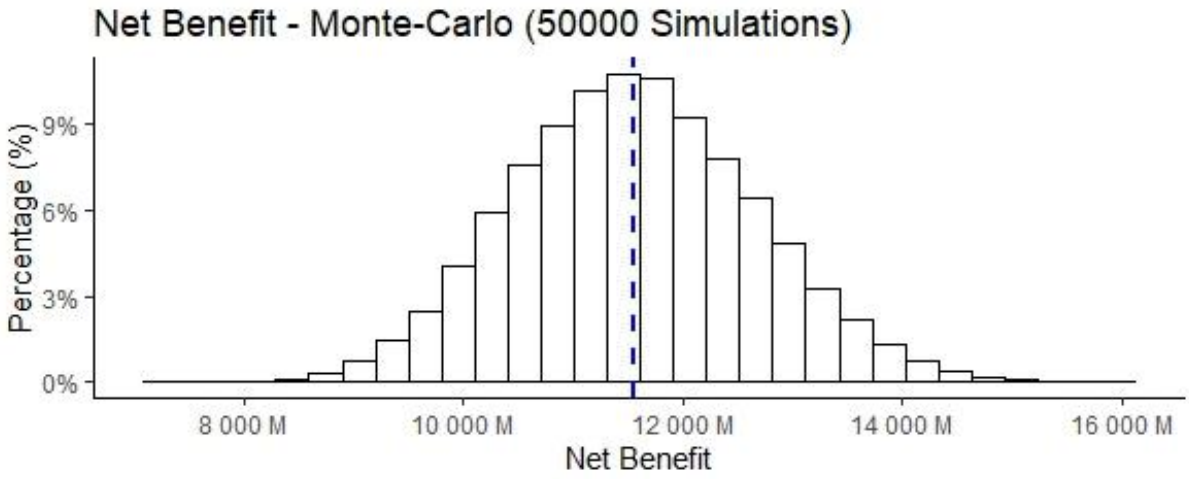


Chart 2: Total Cost, Final Results Monte Carlo Analysis (50,000 simulations)

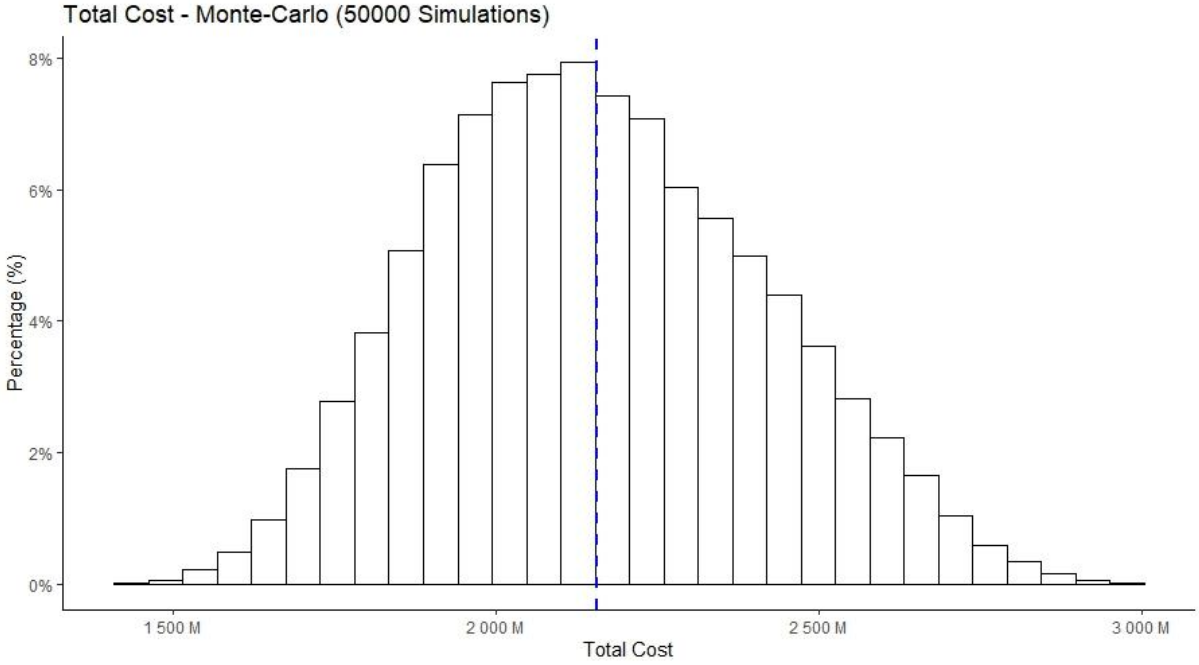
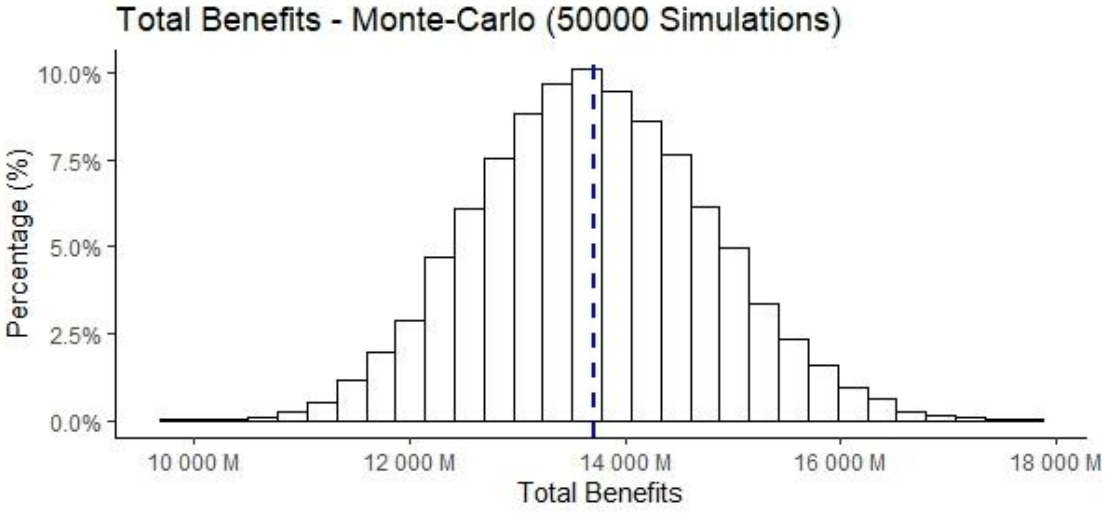


Chart 3: Total Benefits, Final Results Monte Carlo Analysis (50,00 simulations)



Impact of Criminalising the creation, or requesting the creation of, a purported intimate image (deepfake) of another person aged 18 or over without the adult's consent or reasonable belief in consent.

797. The key assumptions behind the impacts presented in this IA are described below.

Assumption	Risks / Uncertainties
The relationship between police recorded crime for intimate image deepfakes in the UK and in South Korea can be linked through i) the relationship between voyeurism offences in the two countries and/or ii) the relative number of victims of intimate image deepfakes from each country.	This has some intrinsic assumptions about behaviour and the Criminal Justice Systems in both countries, and may not hold due to differences in criminal law and culture. If this relationship does not hold, police recorded crime numbers in the UK could be different to those modelled. Voyeurism has been determined to be the closes proxy offence for which data is available.
Prevalence of intimate image deepfakes will increase for the first four years in the appraisal period (five years since last observed data point) and then reach a steady state.	Due to technological advancements and their novelty, intimate image deepfakes are becoming increasingly prevalent each year. Over time, we expect this trend to stabilise – partly due to the deterrent effects of criminal law and partly as the technology's accessibility reaches its peak. There is a serious risk that deepfake prevalence evolves in a different way, in which case the estimated numbers of police recorded crime, and therefore volumes throughout the Criminal Justice System could be different to those modelled.
50% of defendants will be eligible for Legal Aid.	This is a standard MoJ modelling assumption used for prosecutions in the Magistrates' Court. If this were to differ, costs to the LAA of this measure could change.
6-8% of police recorded crimes will result in prosecutions, and 30% of prosecutions will result in custodial sentences. The custodial sentences will be between 2-6 months. Offenders given custodial punishments will serve half of their sentence in prison.	These are taken from proxy offences and are the most reliable assumptions we could use. If in practice numbers vary from this for sexually explicit deepfakes, costs to HMPPS, LAA and HMCTS could vary.
The average annual cost of providing a prison place is £63,981 (inflated and uplifted with optimism bias) and is based on overall resource expenditure and includes staffing and estate cost.	Prison estate unit costs cover the day-to-day running costs of a prison only, and do not incorporate any capital costs associated with construction, investment and costs associated with any developing or contracted out services or rehabilitative activities these prisoners might undertake while in custody.
It is assumed that, due to on-going prison capacity issues, additional custodial sentences will require additional prison capacity. The construction cost of an additional prison place is £500,000 in 23/24	The exact construction profile will vary depending on when additional prison capacity is needed. This depends on a range of factors, primarily natural changes in the prison population and future policy changes

prices. It is assumed that the prison places will be built in the year in which the custodial sentences will be served, and the price of construction is uplifted accordingly.	that increase or decrease the prison population. Because of this, it is not possible to allocate precise prison places and costs for each additional place at this point.

798. The table below shows the varying parameters used in the low and high estimates respectively, and the resulting NPVs.

Variable	***Low***	***High***
Comparative ratio to South Korea	8.83 – the ratio of victims from each country according to the Security Hero report	3.17 – the ratio of voyeurism offences (proxy) in each country
Rate of growth of police recorded crime for first 4 years of appraisal period	13% - the growth rate if the increase from 2019 to 2023 as stated in the Security Hero report has been linear	62% - the compound growth rate of police recorded crime in South Korea from 2021 to 2024
Percentage of police recorded crimes that result in prosecutions	6%	7%
Length of custodial sentences	2 months	6 months
NPV	**-£2.6m**	**-£23.7m**

Monitoring and Evaluation

799. Evaluation is essential in evidence-based policy making. It helps policy officials understand impact, and therefore make better decisions. Effective evaluation practice is needed to credibly demonstrate the impact of governments efforts, and through building the evidence base, make better decisions.

800. The Data (Use and Access) Act plays an important role in delivering the plans set out in the King's Speech 2024.[330] The first step in the monitoring and evaluation of this area was to conduct consultation analysis in preparation for the Act. This gave us an overview of the current data landscape and the market failures currently facing UK businesses and public sector organisations. The consultation and subsequent stakeholder engagement has identified evidence gaps that will need to be monitored going forward. Work is already underway to capture this. Through the process of putting this Impact Assessment together we have identified key metrics that can be tracked that will be able to gauge the success of the measures.

801. Given the scale of intervention, we intend to perform a Post Implementation Review (PIR), within 5 years of the implementation of the Act. This would include proportionate and appropriate research including:

a. Process evaluations: to examine whether the interventions were delivered as planned and reached the right audience, and how changes are being made to improve implementation of future reforms
b. Impact evaluations: to assess the scale of effects caused by the planned changes, compared to initial ambition of the measure

802. As the legislative changes apply to all businesses, and all at the same time, we plan to use Theory Based Evaluation methods for assessing impact.[331] The impact and process evaluations will be based on more detailed versions of the Theory of Change that was presented earlier in this IA (Figure 1).

803. The Act is aimed to harness the power of data to deliver three core objectives: drive economic growth; improve public services through the enabling of modern digital government; and improve people's lives. Set out below are the measures we are taking to deliver these objectives.

c. Drive economic growth
    i. Setting up new smart data schemes

[330] https://www.gov.uk/government/speeches/the-kings-speech-2024

[331] The 'gold standard' for understanding the impact of an intervention is experimental (RCT) or quasi-experimental research. These involve two or more groups that are essentially identical, each randomly allocated to either the intervention and the status quo. This allows you to assume the only difference between the groups is receiving the intervention itself. However that is not possible for DUAA as the laws apply to everyone nationally, all at the same time.

Theory-based approaches, while not as robust as RCTs, are able to demonstrate the likely causal mechanisms of an intervention – the theory of change – and then uses evidence on the extent to which these mechanisms happened, and were driven by the intervention, to establish causality.

ii. Establishing digital verification services
iii. Developing the National Underground Asset register
iv. Simplifying data protection legislation to encourage innovation, help UK trade, and help law enforcement agencies to tackle crime

d. Enable modern digital government
   i. Changes to the digital economy act to support the delivery of public services which benefit businesses
   ii. Electronic system for registration of births and deaths
   iii. Applying NHS Information standards to IT suppliers to the health and social care system to enable interoperability and support effective and timely patient care

e. Improve people's lives
   i. Changes to how businesses handle complaints about data subject rights
   ii. Changes to the ICO to accountably promote and prioritise data subject rights

804. Many of the impacts will rely on DSIT and other departments contributing to the DUAA in developing new data sources or new modelling that will fill current evidence gaps. The evidence gaps include some aspects of the current data protection system (such as the types of legal bases that private organisations use when conducting scientific research) and also some aspects of measuring medium or long term impacts (such as how to measure public awareness of their data rights). In the risks and assumptions section of this Impact Assessment we highlight the modelling assumptions that have been made due to a lack of existing evidence.

805. DSIT will lead the monitoring and evaluation of all measures included in this Act owned by DSIT. DSIT will also lead on coordinating the monitoring and evaluation of measures owned by other departments. Where measures are being followed up with secondary legislation by different departments, M&E plans will be developed and led by the departments directly. M&E of secondary legislation is outside the scope of this IA.

An outline of the measures that are in scope of this M&E section is in Table 82.

Table 82: areas of DUAA that are in scope of this M&E section

Measures in scope of this Monitoring and Evaluation	**Leading Government Department**
the Information Commissioners Office • ICO governance changes • New strategic framework of principal objective and duties • Accountability and transparency measures • Consultations on ICO statutory codes • Improvements to the law enforcement regime • Modernisation of ICO enforcement powers • Responding to complaints from data subjects	DSIT, Digital and Data Policy

- Minor clarifications on dealing with subject access requests

Science and research
- Simplification of scientific research provisions
- Clarification of further processing rules

Solely Automated Decision Making (SADM)
- Expanded legal bases on which SADM can be done
- Consolidates and clarifies existing obligations on controllers

Data re-use
- Removal of consent requirements in relation to non-intrusive cookies
- Direct marketing by charities and the "soft opt in"
- Data protection by design: children's higher protection matters
- Adds Recognised Legitimate Interest as a lawful basis for data processing personal data

International data shares

Digital Identity (some is primary)	DSIT, Digital Identity
NUAR (some is primary)	DSIT, Geospatial Centre
AI and copyright	IPO
Smart Data powers	DBT, Smart Data
Deepfakes and intimate image abuse	MoJ
Electronic births and deaths register	HO,
Data Protection, changes to law enforcement data use	HO, Data and Identity Directorate
Public Safety and National Security (Home Office)	HO

For each area in Table 82, we will take broadly the same approach to planning M&E:

1. Develop a theory of change for how the measures are expected to work in practice

2. Review the literature and perform secondary analysis, talk to stakeholders and or sector experts to build the evidence base on likely type, scope and scale of impacts.

3. Collate data on how the system looked or worked before the DUAA came into effect, or collect new metrics where data not already available

4. Consider how to collect data on these changes (normally through administrative data, surveys, or interviews with key stakeholders) and fill evidence gaps

Work is underway to create detailed M&E plans for each of the areas of the Act outlined in Table 82. We will publish updates with more details periodically, including the first post implementation review report within five years of Royal Assent.

Table 83 shows the sections of the DUAA that are out of scope.

Table 83: All reform areas that will need secondary legislation Monitoring and Evaluation plans, and are out of scope of this section.

Measures that will require secondary legislation Monitoring and Evaluation	Leading Government Department
AI and Machine Learning	DSIT (AI)
Privacy and electronic communications	DSIT (Data Policy)
Changes to Digital Economy Act 2017	DSIT (GDS)
Digital Identity (some is secondary)	DSIT (GDS)
Smart Data schemes	Sector specific
DHSC Open Data Architecture	DHSC
NUAR (some is secondary)	DSIT (GDS)
Access to research data	DSIT (SOH)
Smart meter data	DESNZ

Table 84: Long run impacts of the package of reforms and how these will be monitored and evaluated

Long Run Impact	How this will be monitored and evaluated
Increase in consumer trust	Consumer trust and privacy will be monitored through use of surveys such as the public attitudes to data and AI and successor survey instruments[332] and the ICO public attitudes and information rights survey.[333] There are a number of inputs into consumer trust of business data use that are out of the remit of this Act, and qualitative research would be needed to explore the impacts of the Act on consumer trust.
Improved regulatory oversight	Changes to ICO functions will be measured using a time cost approach in which ICO will report to DSIT any additional costs and benefits of changes to their organisational structure. In terms of ICO performance this will be measured by the existing KPIs in place at the ICO.

[332] https://www.gov.uk/government/publications/public-attitudes-to-data-and-ai-tracker-survey-wave-4/public-attitudes-to-data-and-ai-tracker-survey-wave-4-report
[333] https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/views-of-the-public/

Long Run Impact	How this will be monitored and evaluated
Lower compliance costs for UK businesses	DSIT will endeavour to estimate compliance costs for UK businesses using the UK Business data survey. This includes the number of full-time equivalent members of staff employed whose primary role is to undertake activities related to complying with UK data protection laws (or time spent a month for sole traders), and the activities undertaken in the last 12 months', which can be used to produce estimates of costs. The average cost of compliance activities is also taken from a variety of published academic sources. Going forward we will track the changes in these estimations using future iterations of the UK Business Data survey and compare them to pre-implementation costs. Estimating detailed costs using a survey based approach is difficult therefore we will attempt to complement the approach using other sources if available.
Increase in UK business productivity	The relationship between productivity levels and data use is a relatively new and complex area of research. Academic literature is limited, and the definition of data use and productivity varies across much of it. DSIT is looking to monitor this relationship going forward by carrying out its own longitudinal study across sectors on the relationship between data use and firm level productivity. This might allow us to track the changes in productivity that are due to an increase in data use or availability as a result of the Act. Disentangling exact impacts of the reforms will be challenging but the work might allow us to identify the broader context within businesses operate.
Introduction and take up of digital identity schemes	As this is primary and enabling legislation, costs and benefits will vary by sector and use case. The monitoring and evaluation of each should be specific to each reform accordingly. However, there are metrics that can be used to monitor and evaluate the impact of the enabling legislation; these include the number of organisations certified, the number of checks made in total, the number of people signed up to the trust framework and the growth in numbers of service providers. Going forward these will be monitored by DSIT.
Criminalise the creating, or requesting the creation, of a purported intimate image (deepfake) of another person aged 18 or over without the adult's consent or reasonable belief in consent.	The Act places a duty upon the Secretary of State to undertake a review within the next 24 months of the operation of the reasonable excuse defence for both offences. We will publish the outcome of the review. We will also continue to keep this area of the criminal law under review to ensure it is working effectively and as intended. This includes engagement with stakeholders including the Police and Crown Prosecution Services.
Specific to the National Underground Asset Registry: Improved data sharing and on-site efficiencies, and reduced accidental asset strikes due to poor or incomplete information	Changes to data sharing efficiencies will be monitored and evaluated through primary qualitative and quantitative data collection and stakeholder engagement to understand how enforcing data providers to upload and update data on NUAR has changed their data sharing behaviours and the impact this has had on their organisation. We will also assess how the platform has changed the data sharing process from the service users' perspectives. Changes to on-site efficiencies and accidental asset strikes due to poor or incomplete information will also be

Long Run Impact	How this will be monitored and evaluated
	assessed by primary data collection and stakeholder engagement, supported by secondary data and literature reviews to understand the impact had.

806. The table below summarises these assumptions and the proposed ways forward in terms of their monitoring and evaluation:

Table 85: Evidence gaps and proposed monitoring and evaluation approach

Long Run Impact	Evidence gap	Proposed Monitoring and Evaluation
Lower compliance costs for UK businesses	How much data use is affected by clarification of when businesses need to seek legal advice under the proposed policy changes	This can be proxied as part of the UK Business Data Survey going forward, using the number of businesses 'prevented from using or sharing data due to legal restrictions' or because 'they were unsure if it was permitted under the data protection laws'. More robust quantification of 'data use' is conceptually and practically very challenging.
Increase in UK business productivity	The number of firms that would increase data use because of these measures	Further DSIT work to identify the link between data use and productivity is being developed
Increase in UK business productivity	% of firms that would not increase AI use based on the AI measures in the Act	Further DSIT work to identify the link between data use and productivity is being developed. For AI measures we will also work with the Office of AI.[334]
Increase in UK business productivity	Proportion of businesses for which improving standards would lead to additional sharing	Further DSIT work to identify the link between data use and productivity is being developed
Increase in UK business productivity	Accounting for the fact that this is about data shared across organisations rather than all data	Further DSIT work to identify the link between data use and productivity is being developed
Increase in Familiarisation costs	Wage assumptions of those responsible for familiarising themselves with new legislation - across firms of different sizes	This will be monitored as part of the UK Business Data Survey going forward.
Competition in the Data Economy	The Act is designed to decrease the barriers to data use for UK firms and public sector organisations, we expect the market to become more competitive.	DSIT will work with CMA on a programme to define and measure the competitiveness of data markets

[334] https://www.gov.uk/government/publications/ai-activity-in-uk-businesses/ai-activity-in-uk-businesses-executive-summary

Long Run Impact	Evidence gap	Proposed Monitoring and Evaluation
Changes to how organisations carry out R&D	Clarifications in how science is defined and data is permitted to be used for research in commercial settings	This will require research that is targeted at specific parts of organisations. DSIT is looking into how this study could work
Changes to how organisations carry out ADM	DUA changes which legal bases can be used when an organisation does ADM. We might therefore expect behaviour to change. We also expect the number of organisations carrying out ADM to change.	This will require research that is targeted at specific parts of the economy. DSIT is looking into how this study could work

Smart Data proposals (DBT) - Monitoring and Evaluation

807. Part 1 of the Act creates an enabling framework for Smart Data schemes through regulation-making powers. We do not expect there to be direct impacts from the enactment of Part 1. Instead, these impacts will be realised at the secondary legislation stage.

808. With regard to a monitoring and evaluation plan, DSIT and DBT will assess Part 1 of the primary legislation against the key objectives of the primary legislation and will use the following metrics:

a. **Reduction in regulatory duplication**: This should be measured by the number of Smart Data schemes using the primary legislation

b. **Acceleration of schemes:** The length of time taken for DBT to develop primary legislation could be taken as a proxy for the amount of time saved for relevant sectors, assuming sectors would have independently sought primary legislation otherwise. The number of Smart Data schemes implemented or in the implementation stage using the primary legislation. The baseline scenario assumes that Smart Data schemes would materialise after 10 years without legislation, so if there are Smart Data schemes implemented within the 5-year review period then the benefits have been realised earlier.

c. **Cross-sector coordination:** This could be measured by the number of ATPs operating successfully across multiple sectors, or the marginal costs to ATPs entering a second scheme, compared to the counterfactual.

809. Across all these objectives, and in evaluating the quality of Smart Data schemes, a key challenge is establishing a strong counterfactual for what would have occurred in the absence of primary legislation. There is no plausible way to separate what extent of the scheme's outcomes are a result of the coordinating work of Smart Data and what are the results of the scheme itself.

810. DBT will supplement its monitoring and evaluation of the primary legislation as a whole described above, by monitoring the output of each evaluation of the secondary legislation.

811. The counterfactual will vary by scheme and should reflect the sector specific circumstances. While Open Banking could be used as an example, it is not underpinned by this primary legislation, and it is expected that learnings from Open Banking can help accelerate the implementation of other Smart Data schemes. Examples of schemes where the counterfactual is likely no scheme emerging:

a. **Open Finance** - In the Open Finance consultation response[335], FCA said that a legislative framework would be needed for Open Finance to develop fully. In this consultation response, respondents also pointed out that coverage for existing initiatives for Open Finance-type arrangements will inevitably be partial, limiting the potential benefits.

b. **Open Comms** – Without government intervention, DSIT do not think industry would take forward the development of a voluntary scheme in the foreseeable future, which affords consumers easy access to, and the sharing of their data. Intervention is required to ensure that relevant data sets and types are in open formats, and to standards which would allow effective use by third-party providers. In the Open Communications consultation response, Ofcom said that they did not envisage that industry would introduce customer data mobility voluntarily.[336]

Enhance the Work of the UK Intelligence Services and Law Enforcement Agencies in the Interest of Public Security (Home Office) - Monitoring and Evaluation

812. The impact of the new arrangements will be monitored through existing stakeholder forums. Engagement with impacted groups takes place on a regular basis to consider the impact on these communities and their operations. Assessment of the new arrangements will be extended to these forums and any suggested amendments will also be considered through these channels. Any arising issues will continue to be flagged through internal data protection practitioner networks and escalated through data policy working groups, and boards, if required. This reflects existing structures that are in place to manage data protection related matters.

Improved interoperability across health and social care systems – Monitoring and Evaluation

813. As outlined in the monitoring and evaluation section of the Open Data Architecture Information Standards Impact Assessment, DHSC have identified further evidence gaps that will need to be monitored going forward, including the cost of compliance activities, how they vary by firm and the time spent by businesses familiarising themselves with the legislation. Through the process of putting the Impact Assessment together we have also identified key metrics that can be tracked and measured going forward that will be able to gauge the success of the proposed measures.

[335] FCA (March 2021): "Open finance – feedback statement"
[336] Ofcom (July 2021): "Update on Open Communications: Enabling people to share data with innovative services"

Annex

1. List of all recommended policies
2. Impact of preferred option (2024 prices, 2024 PV)
3. EU Adequacy Monte-Carlo Analysis
4. List of ICO guidance updates
5. Gravity trade modelling
6. Differences in previous DPDI Bill against DUA Act
7. List of measures removed from the do max option.

1. Full list of policies in preferred package of reforms

Table 86: All policy reforms included in the preferred package and whether they will likely be followed by secondary legislation.

Reform measure	Reform Summary	Will this policy be followed up with secondary legislation? (Y/N)
Research Purposes	● Consolidating research provisions into a single chapter	N
Research Purposes	● Creating a statutory definition of scientific research	N
Research Purposes	● Incorporating broad consent for scientific research into legislation	N
Research Purposes	● Extending the “disproportionate effort” exemption on information provision requirements for further processing for research purposes of personal data collected directly from the data subject	N
Research Purposes	● Extending the exemptions from the regime when conducting scientific research to include when that research is carried out in a commercial setting.	N
Further Processing	● Clarifying how personal data can be further processed for research purposes	N
Further Processing	● Clarifying that further processing for an incompatible purpose may be lawful when based on a law that safeguards an important public interest or when the data subject has re-consented	N
Further Processing	● Exempt archives from further processing rules where personal data was originally obtained in reliance on consent.	N
Legitimate interests	● Recognised Legitimate Interests. The act will introduce a new lawful ground for non-public bodies when processing personal data for “recognised legitimate interests”. This is limited to a small number of public interest objectives, such as the prevention of crime, safeguarding vulnerable individuals and responding to emergencies. Under the current law, data controllers have to do a detailed assessment of whether their interests are outweighed by the rights of data subjects when processing personal data for such purposes	N
AI and Machine Learning	● Future proofing Article 22	Y

Reform measure	Reform Summary	Will this policy be followed up with secondary legislation? (Y/N)
AI and Machine Learning	● Enhancing the approach to explainability and accountability for fair processing in the context of AI	Y
AI and Machine Learning	● Clarifying the circumstances in which safeguards apply to significant decisions that are taken about individuals on the basis of profiling.	Y
Data Adequacy	● Underpinning the UK's future approach to data adequacy regulations with principles of risk-assessment and proportionality	N
Data Adequacy	● Relaxing the requirement to review data adequacy regulations every 4 years	N
Alternative Transfer Mechanisms	● Power for SoS to formally recognise new ATMs	N
Alternative Transfer Mechanisms	● Changes to the standard approach to alternative transfer mechanisms. (Art 46)	N
Alternative Transfer Mechanisms	● Ensuring businesses are able to continue to use their pre-bill existing transfer mechanisms without a requirement for further checks and avoiding additional costs.	N
Public Interest (join DSIT/HO measure)	● Lawful ground for transferring personal data under the UK-US Data Access Agreement	N
Public Interest (join DSIT/HO measure)	● Clarifying that private organisations & individuals asked to carry out an activity on behalf of a public body may rely on that body's lawful ground for processing the personal data under Art 6(1)(e)	N
Digital Economy Act 2017 (CDDO)	● To extend powers under section 35 of the Digital Economy Act 2017 aimed at improving public service delivery to business undertakings, beyond the current scope of solely individuals and households	Y
Public Safety and National Security (Home Office): Part 4	● Amendments to Part 4 of the DPA 2018 - Joint processing by intelligence services and competent authorities	N

Reform measure	Reform Summary	Will this policy be followed up with secondary legislation? (Y/N)
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● National security exemption (DPA 2018 part 3)	N
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Data subjects' rights to information: legal professional privilege exemption (DPA 2018 part 3)	N
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Consent to law enforcement processing (DPA 2018 part 3)	N
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Law enforcement processing and codes of conduct (DPA 2018 part 3)	N
Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	● Logging of law enforcement processing (DPA 2018 part 3) Automated decision making (DPA 2018 part 3)	N
Public Safety and National Security (Home Office): International Transfers	● Transfers based on special circumstances (Schedule 6 DPA, Section 76)Subsequent transfer's (Section 78 DPA)	N
Public Safety and National Security (Home Office): International Transfers	● Clarify conditions on the use of international processors by UK competent authorities (Part 3 DPA)	N
Public Safety and National Security (Home Office): Biometrics	● Retention of biometric data and recordable offences	N
Public Safety and National Security (Home Office): Biometrics	● Retention of biometric data from INTERPOL	N
Public Safety and National Security (Home Office): Biometrics	● Retention of biometric data from other international partners	N

Reform measure	Reform Summary	Will this policy be followed up with secondary legislation? (Y/N)
The National Underground Asset Register	● National Underground Asset Register Legislation to underpin a national register of underground assets (cables etc.)	Y
The National Underground Asset Register	● Create powers to ensure the full participation by all owners of underground assets in NUAR and enable a sustainable charging regime.	Y
Data Preservation Notices	● Establishing a data preservation process which will require OFCOM, following instruction by a coroner, to issue data preservation notices to online service companies to ensure they retain data that may later be requested by a coroner when carrying out an inquest into a child's death.	N
Smart Meter Data (DESNZ)	● Create new power to give Ofgem more flexibility in the process it needs to follow to identify the successor holder of the Smart Meter Communication Licence.	N
Smart Meter Data (DESNZ)	● Enable Ofgem to modify conditions of existing licences and industry codes if it considers that it is necessary or expedient to do for the purpose of granting a Smart Meter Communication Licence.	N
Online safety researchers access to data	● Create powers for the Secretary of State (SoS) to place a duty on platforms to comply with any regulations later passed by SoS allowing researchers access to certain data held by platforms.	Y
Electoral Purposes	● Amend Schedule 1 of the Data Protection Act 2018 so that the 4 day threshold in which outgoing elected representatives have to process special category data on behalf of their constituents without explicit consent, is changed to 30 days, to overcome these operational barriers.	N

Reform measure	Reform Summary	Will this policy be followed up with secondary legislation? (Y/N)
Electoral Purposes	● Amending exemptions in Sch 1 DPA 2018 (special category data) to permit elected representatives to process political opinions data.	N
Subject Access Requests (Joint DSIT/HO measure)	● Clarifying that controllers are not required to make disproportionate searches in response to subject access requests - necessary as a result of the loss of the EU principle of proportionality under the REUL Act. (Home Office measure)	N
Subject Access Requests (Joint DSIT/HO measure)	● Time limits for responding to requests by data subjects (SAR) (DPA 2018 part 3/4)	N
Privacy and electronic communications	● To add three low privacy risk exceptions to the prohibition on storing information, or accessing information stored, on a user's connected device. For example, collecting statistical information to improve the service/website requested by the user.	Y
Privacy and electronic communications	● Empowering ICO to take action against organisations for the number of unsolicited direct marketing calls 'sent' as well as calls 'received' and connected.	Y
Privacy and electronic communications	● Amending the regulations' enforcement tools and actions so that it is aligned with the regime under the Data Protection Act 2018, including fine levels, whilst keeping bespoke tools such as third-party information notices.	Y
Privacy and electronic communications	● Extending approved code of conduct provisions under Article 40 UK GDPR to the PEC Regulation	Y
Privacy and electronic communications	● Extending the reporting period for breaches under reg 5A PEC Regulation from 24 to 72 hours	Y
Updating Special Category Data	● Create a new power for the Secretary of State to add new types of data to the list of special categories of data that get extra protection. This will provide the flexibility to add new types in the future including in response to new technological developments, to ensure heightened protections for citizens.	N

Reform measure	Reform Summary	Will this policy be followed up with secondary legislation? (Y/N)
Digital Identity	● eIDAS/trust services	Y
Digital Identity	● Data checking gateway	Y
Digital Identity	● Trust framework accreditation and certification	Y
Digital Identity	● Trust framework governance	Y
Digital Identity	● Validity of digital identity	Y
Digital Identity	● Mutual recognition of digital identities	Y
Digital Identity	● Mutual recognition of trust services	Y
Digital Identity	● Welsh and Scottish safeguards for Digital Verification Services	Y
Digital Identity	● Include a power for DSIT SoS to approve additional rules for particular sectors or use cases which build on the rules in the UK digital identity and attributes trust framework; to make provision for organisations to be certified against those additional rules; and to make provision for the DVS Register to note which sets of additional rules (if any) an organisation has been certified against in addition to the trust framework. In policy terms, we refer to a set of additional rules as a 'scheme', and we expect the equivalent term in the Act to be 'supplementary code'.	Y
Digital Identity	● To amend the Immigration Act 2014 and the Immigration Asylum and Nationality Act 2006 to permit regulations to specify that, where digital checks are undertaken, these are undertaken by a DVS provider on the DVS register.	Y
Smart Data (DBT)	● Smart Data: Introduction of primary legislation, creating new "regulation-making" powers to enable Smart Data schemes to be introduced in any given sector.[1]	Y

Reform measure	Reform Summary	Will this policy be followed up with secondary legislation? (Y/N)
Smart Data (DBT)	● Expanding the definition of ‘‘customer data’’ to include transactions between the customer and third parties, and clarify the scope of action initiation, or ‘write access’ services	Y
Smart Data (DBT)	● Provisions to clarify the powers of enforcers to investigate and monitor compliance, and the process for setting fines, penalties and fees and to allow existing data sharing requirements in other legislation to be incorporated into Smart Data regulations.	Y
Smart Data (DBT)	● Clarification of the power to make provision in connection with business data – to expressly facilitate a Smart Data delivery model where data holders provide business data to a specified third party, who then provides (or publishes) the business data to other third parties	Y
Smart Data (DBT/HMT)	That the Smart Data primary legislation includes the four groups of Smart Data amendments introduced throughout the Data (Use and Access) Act’s passage through parliament, as set out in Table 8.	Y
Data Architecture (DHSC)	● Enabling legislation to prepare, publish and mandate standards that apply to the products and services provided by IT suppliers, to ensure that those products and services enable and support data to be accessed, interrogated and processed in real time by anyone with the basis to appropriately access that data, irrespective of the system used by the health or social care provider who collated, produced or otherwise processed that data.	Y
Public Safety and National Security (Home Office): Birth and Deaths	● Remove the requirement for paper birth and death registers moving to an electronic register	N
Strategy, Objectives and Duties	● ICO's Objectives and Duties	N
Strategy, Objectives and Duties	● Statement of Strategic Priorities	N
Governance Model and Leadership	● Remove the Information Commissioner corporate sole structure. Introduce a Board structure with Chair/CEO.	N

Reform measure	Reform Summary	Will this policy be followed up with secondary legislation? (Y/N)
Governance Model and Leadership	● Remove the requirement for Parliament to agree to a change to the IC salary.	N
Accountability and Transparency	● Accountability and Transparency - require publication of key documents	N
Accountability and Transparency	● Statutory codes of practice - ICO required to undertake and publish an impact assessment and consult with a panel of experts when developing or updating statutory codes of practice, unless exempt	N
Complaints	● Complaints - organisations required to have a complaint handling process	N
Enforcement Powers	● Enforcement - power to commission technical reports	N
Enforcement Powers	● Enforcement - power to compel witnesses to attend interview	N
Enforcement Powers	● Enforcement - notice of intent extension	N
Enforcement Powers	● Enforcement - without attending premises clarification	N
Express reference to children meriting specific protection with regard to their personal data	Provides ICO with a duty to consider that children may be less aware of the risks of consequences of processing and their rights in relation to it in all its data protection activities where relevant.	N
Data protection by design: children's higher protection matters	Provides ICO with a duty to consider that children may be less aware of the risks of consequences of processing and their rights in relation to it in all its data protection activities where relevant.	N
Creating, or requesting the creation of, purported intimate image of an adult	Criminalising the creation, or requesting the creation of, a purported intimate image (deepfake) of another person aged 18 or over without the adult's consent or reasonable belief in consent.	N
Copyright works and artificial intelligence systems	The Act requires that a set of reports on the use of copyright works in the development of AI systems are published within 9 months, and that a statement of progress is provided within 6 months	N
Direct Marketing	Allowing charities to send direct marketing for the purposes of furthering one or more of their charitable purposes.	N

2. Impact of preferred option (2024 prices, 2024 PV) (£m)

	Discounted Costs	**Discounted Benefits**	**Net Present Value (NPV, £m)** (Benefits – Costs)	**Equivalent Annual Net Direct Cost to Business** (minus sign indicates net direct benefits)	**Net Present Value NPV to businesses**
DUA act	1,959	12,562	10,604	-281	4,967
Breakdown of impact by group of measures					
NUAR	225	4,833	4,608	-189	2,542
Impact on the ICO	22	8	-14	-	-
Digital Identity	1,485	5,737	4,253	-	1,266
Home Office	2	400	398	-	-
DHSC	203	341	138	7.1	-61
Data Protection and privacy	22	1244	1222	-106	1222

3. EU Adequacy Monte-Carlo Analysis

814. There are a significant number of assumptions in the EU Adequacy model that we have varying degrees of confidence in. To be transparent on the potential range of uncertainty, we have undertaken Monte-Carlo analysis which varies the assumptions in the model providing an indication of the potential range of results. Only services export results can be adjusted. The goods result is constant across the scenarios (£200m in lost revenue and £40m in SCC costs). Table 85 shows the summary statistics for the Monte-Carlo analysis showing the mean, standard deviation, minimum and maximum for each of our results of interest. The analysis was run 50,000 times picking a random selection of each of the parameters including for those parameters which vary by business size. These are: profit margins, investment horizon, SCC compliance, the proportion of firms that already have SCCs in place and the proportion of costs borne by the UK firm.

Table 87: Summary Statistics EU Adequacy Monte Carlo Analysis Results

Statistic	N	Mean	St. Dev.	Min	Max
Business that cease trading	50,000	5,043	933	2,817	9,601
Business that continue trading	50,000	95,062	933	90,503	97,287
Annual Lost Export Revenue	50,000	£240m	£17m	£211m	£378m
SCC Costs	50,000	£352m	£29	£240m	£458m

815. The number of businesses that cease trading varies between 2817 and 9601 with a mean of 5043. The three graphs below show the distribution of our main costs (including goods). SCC costs are more uniform in distribution with a mean of £352m with a minimum of £240m and maximum of £458m. Annual export revenue lost has a left-skew with a mean of £240m with a minimum of £211m and maximum of £378m, the result indicates the non-linearity of the two main assumptions for the export decision, investment horizon and profit margin for businesses interact, as both approach their minimum values, results become larger than the mean but this is unlikely.

816. These results have a lower maximum when compared to the simpler scenario analysis described above. Similarly, whilst the mean of lost export revenue is similar, SCC costs mean is lower £352m compared to the £410m central estimate. These divergent results show the unlikelihood of getting all parameters at their absolute minimum or maximum (even when parameters are chosen a large number of times). Even in scenarios where Export Revenue loss is high, where profit margins and investment horizons are low, it does not necessarily mean that SCC costs are similarly high as other assumptions such as the compliance rate, the number of businesses that have SCCs and costs borne by UK firms all vary. The Monte-Carlo analysis was proportionate and took simple draws from triangular distributions based on the minimum, maximum and mean of each. In reality, it is likely certain parameters are highly correlated with

each other for example profit margins and investment horizons which both reflect business risk aversion and decision-making.

Chart 4: Export Revenue Lost, EU Adequacy - Monte-Carlo Analysis (50,000 runs)

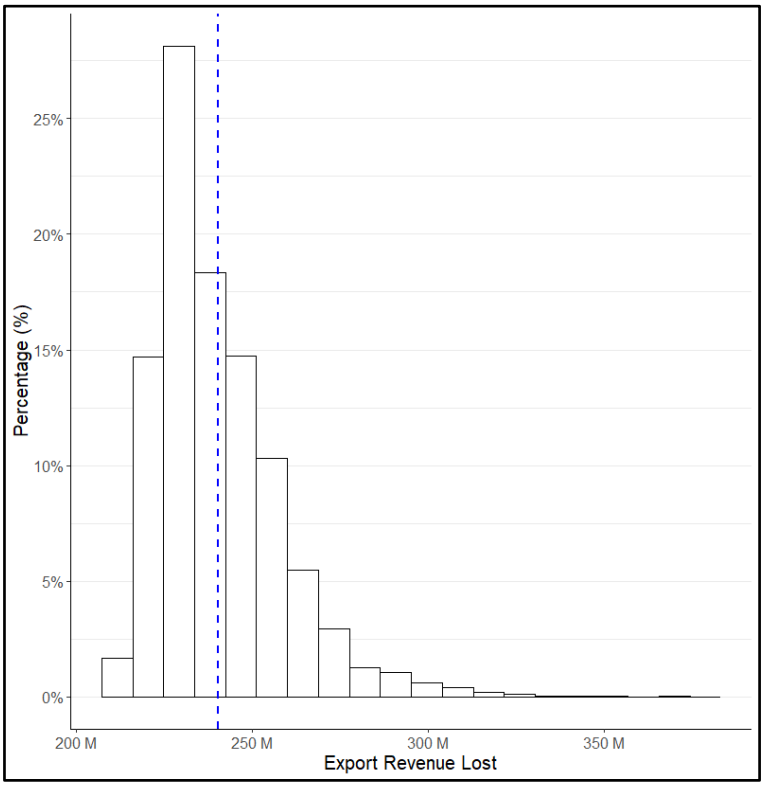
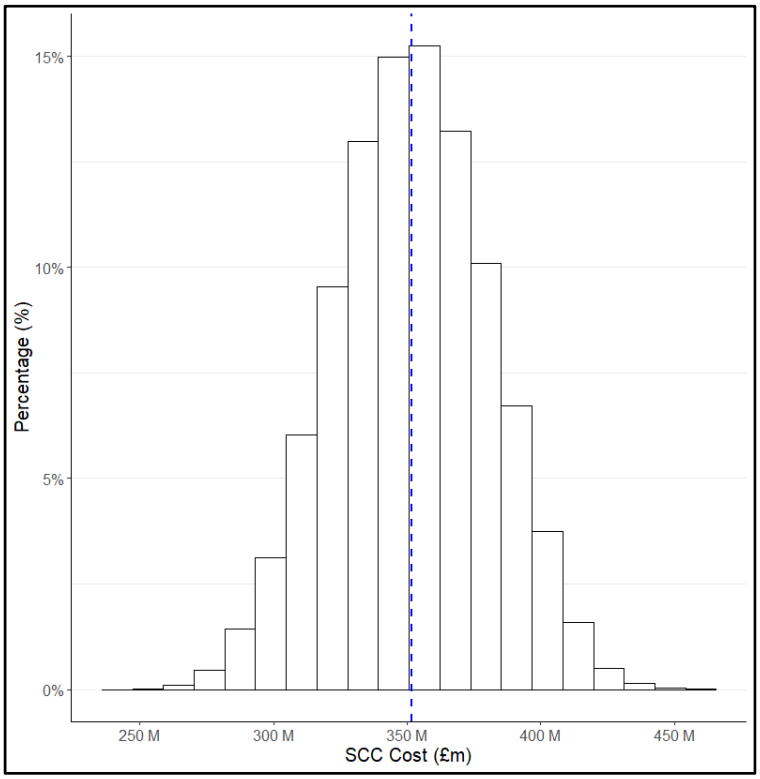


Chart 5: SCC Cost (£m), EU Adequacy Monte-Carlo Analysis (50,000 runs)



4. Guidance proposals for the ICO

Guidance Proposals

There are currently approximately 20 areas where we have identified the need for either significant revisions to or production of new guidance by the ICO.

Guidance which has been set out as needed in the consultation includes:

Chapter 1
- Guidance on schedule 1 processing conditions for AI and machine learning – section 1.5, para 91.

Chapter 2
- New guidance on reforms to regulation 6 of PEC Regulation, section 2.4, para 201.

Chapter 3
- Changes to the international transfers framework to be supported by the ICO through practical guidance on determining risks, section 3.3 para 259.
- International transfers: proposal to allow organisations to create or identify their own alternative transfer mechanisms in addition to those listed in Article 46 of the UK GDPR. Guidance is likely to be required from the ICO and could impact on our ability to enforce infringements in these transfers, section 3.3 para 263.

Guidance identified by the ICO as likely to be needed, but not included in the consultation:

Chapter 1
- Research and re-use of data, reviewing all guidance for consistency with legislative changes.
- ICO guidance on legitimate interests, section 1.4. Need to update guidance to reflect legislative changes and address questions about LIAs for activities not on list and handling of related queries by ICO. Requires, policy, legal, and economic input.

Chapter 2:
- PEC Regulations – cookies: new guidance based on changes to Regulation 6.

Chapter 3
- Derogations: guidance on changes to derogations, dependent on final proposals.
- Certifications: potential guidance on the use of certifications for transfers, depending on final proposals.

Chapter 5
- Enforcement Powers: New guidance on ICO's updated enforcement powers, updates to RAP and enforcement manual.
- Guidance on new complaints process, section 5.6, para 385.

5. Gravity trade modelling annex

STRI modelling

1. At consultation stage of the previous DPDI Bill we outlined a potential modelling approach which included estimating the impact of these policy changes on the OECD's Services Trade

Restrictiveness Index (STRI)[337] which sets out a series of sector-specific restrictions to services trade which forms a parameter in an economic gravity model to estimate the impact on trade.[338]

2. DSIT has since then expanded its gravity modelling capabilities and developed its own in-house approach with the help and expertise of other government departments. We have used the Department for Business and Trade) Services Trade Model as the basis for our modelling approach[339]. This ensures greater cross-government consistency in our approach.

3. STRIs are used to assess how restrictive, or open and closed to international trade and economic competition, a jurisdiction is to foreign services providers. Barriers to services trade are defined in terms of restrictions to foreign entry, movement of people, discriminatory measures, barriers to competition, and regulatory transparency. STRIs are calculated by the OECD using a scorecard approach; each restriction carries a weight and if in place is added to the score. STRIs are calculated by the OECD for 22 sectors across all OECD countries.[340] The overall modelling approach is to simulate the impact on trade of turning the data specific restrictions 'on' or 'off'. The proposed package of reforms involves restrictions being turned on or off by the UK, EU+ and other trade partners.

Model specifications

4. Full detail of the underlying model's methodology and specification is published in DIT's Services trade modelling working paper. The model works in several stages[341]. Firstly, a standard gravity model is estimated for each sector with controls such as physical and cultural distance, GDP and tax regimes. Fixed effects are also employed to control for unobserved heterogeneity.[342] The key parameter being the sensitivity of trade flows within a sector to the OECD's 2021 STRI. As a result, the model captures only countries with STRIs.[343] The second is an estimate of how changes to trade costs in a given country affect trade costs for the rest of the world.

5. The final stage is the general equilibrium simulation exercise[344]. By feeding the scenario back into the structural model estimated in the first stage, directly affected flows adjust in accordance with the sensitivity of trade flows to the STRI but also have an impact on third countries. These effects feed back into the initial relationship. The results do not account for cross-sector impacts or the reallocation of factors of production. 80% confidence intervals are used to account for uncertainty in the STRI parameter.

6. To model the potential impact of the reforms, we need to appropriately model the STRI position both in the baseline, and as a result of implementing new measures. Currently the UK has among the most liberal data trade regimes worldwide, with the OECD setting only 1 out of

[337] Services trade in the global economy, OECD
[338] The gravity model of international trade states that the volume of trade between two countries is proportional to their economic mass and a measure of their relative trade frictions. The gravity model has been commonly used in international trade analysis for several decades due to its intuitive appeal.
[339] Services trade modelling, DBT Analysis Working Paper
[340] ibid.
[341] ibid and for further detail on the methodology underpinning the model please see An Advanced Guide to Trade Policy Analysis: The Structural Gravity Model. WTO iLibrary.
[342] By using importer-year and exporter-year fixed effects the model controls for all importer and exporter specific characteristics.
[343]
[344] ibid and for further detail on the methodology underpinning the model please see An Advanced Guide to Trade Policy Analysis: The Structural Gravity Model. WTO iLibrary

5 data-sector relevant STRIs in place with its international trade partners - including the EU, with which it also has data adequacy.

7. We have identified the reforms most likely to impact trade through changing data restrictions. These are;

    a. Underpinning the UK's future approach to data adequacy regulations with principles of risk-assessment and proportionality,

    b. Relaxing the requirement to review data adequacy regulations every 4 years

    c. A new power for SoS to formally recognise new ATMs and,

    d. Changes to the standard and approach to alternative transfer mechanisms. (Art 46)

8. The most relevant STRI 2021 measures are 1.20.3 (cross-border transfer of personal data is possible to countries with substantially similar privacy protection laws) and 1.20.2 (cross-border transfer of personal data is possible when certain private sector safeguards are in place) respectively. As the OECD already defines 1.20.2 being available in the UK, the only available measure for modelling changes is 1.20.3. Therefore, turning this off between the UK and a priority country is used to represent data adequacy regulations. For testing reciprocation, both 1.20.2 and 1.20.3 are relevant as some partner countries do not have alternative transfer mechanisms in place.

9. Whilst these measures do closely relate to the policies, this lack of specificity indicates a limitation of the STRI in measuring policy changes. How data adequacy regulations and alternative transfer mechanisms work in practice differs by country. As above, this indicates how results may overestimate the impacts.

Table 88: Reforms that will impact trade

Reforms	**Most relevant STRI measure**
● Underpinning the UK's future approach to data adequacy regulations with principles of risk-assessment and proportionality ● Relaxing the requirement to review data adequacy decisions every 4 years ● A new power for SoS to formally recognise new ATMs and, ● Changes to the standard and approach to alternative transfer mechanisms. (Art 46).	● 1.20.2: Cross-border transfer of personal data is possible when certain private sector safeguards are in place ● 1.20.3: Cross-border transfer of personal data is possible to countries with substantially similar privacy protection laws

10. Given the uncertainty as to the point at which trading partners might make changes, we have set out 'medium', 'high', 'low' and 'high with EU adequacy loss' scenarios to illustrate impacts under a range of different combinations of responses:

a. A **Medium** scenario which assumes that the UK, moving unilaterally, will become less restrictive with all priority countries as a result of these reforms but all else will stay the same.

b. A **High** scenario which assumes that the countries that are within the UK's priority list for data adequacy regulations will become less restrictive in response to the UK becoming less restrictive with them as a result of these reforms. This scenario assumes that countries with which the UK already has data adequacy will stay the same. This scenario is optimistic in that data adequacy regulations are unilateral and reciprocation is not assumed. 1.20.2 is also switched off, where possible[345], as the two measures are modelled together. The need for private sector safeguards between the country and the UK is assumed to be overruled by having data adequacy.

c. A **Low** scenario, where we assume the UK still becomes less restrictive with priority countries as in the medium scenario, but that the EU+ bloc becomes slightly more restrictive in response to the implementation of these reforms. This reflects the framework outlined in the summary that a decrease in requirements with 3rd countries might be accompanied with more friction in UK-EU trade.

d. A **High with EU Adequacy Loss** scenario which assumes the same as the 'High' scenario but that the EU bloc also becomes slightly more restrictive in response to the wider set of reforms.

e. An EU Adequacy Loss scenario which assumes that the EU bloc becomes slightly more restrictive. To model a scenario where the UK's EU adequacy decision is discontinued, solely focusing on the UK-EU trade relationship.

11. For the purposes of modelling responses, the countries considered are placed into three groups:

- EU+EEA. These are countries the UK already has data adequacy with, and they may impose additional restrictions with respect to the UK, in response to a deviation from UK GDPR.

- 'Priority countries',[346] that the UK previously has identified as key countries for future partnerships. These countries may further liberalise with respect to the UK, in response to deviations from UK GDPR. This group comprises[347] Australia, Brazil, India, Indonesia, Republic of Korea and the United States. Since the priority group was introduced in 2021, the UK has concluded data adequacy regulations with the Republic of Korea[348] and the United States[349]. The modelling has been updated to not include the Republic of Korea and the United States trade impacts in the results.

- Other countries where a STRI parameter exists but are not priority countries or in the EU+. These are affected by the general equilibrium impacts but are not directly

[345] India and Indonesia have 1.20.2 ON in the do-minimum. All other priority countries have this measure off already.
[346] UK approach to international data transfers (2021), DSIT
[347] Dubai International Finance Centre, Colombia, Singapore and Kenya are also in the 'priority' group. However, owing to lack of STRI or trade data they have not been modelled.
[348] UK-Republic of Korea data adequacy supporting documents, DSIT (2022)
[349] UK-US data adequacy: explainer, DSIT (2023)

affected by the policy changes. This group includes: Canada, China, Israel, Mexico and Malaysia amongst others.

Table 89: Summary table of all modelling scenarios

Scenarios	UK Policy	Changes to UK STRI	Partner Policy	Changes to Partner STRI
Baseline	As is	As is	As is	As is
EU Adequacy Loss	As is	As is	EU+ countries become more restrictive	1.20.3 ON for EU+
High	UK becomes less restrictive with priority countries	1.20.3 OFF for priority countries	Priority countries become less restrictive	1.20.3 OFF and 1.20.2 OFF for Priority countries
High with EU adequacy loss	UK becomes less restrictive with priority countries	1.20.3 OFF for priority countries	Same as above EU+countries become more restrictive	1.20.3 OFF and 1.20.2 OFF for Priority countries 1.20.3 ON for EU+
Medium	UK becomes less restrictive with priority countries	1.20.3 OFF for priority countries	No changes	No changes
Low	UK becomes less restrictive with priority countries	1.20.3 OFF for priority countries	EU+ countries becomes more restrictive All other countries remain the same	1.20.3 ON for EU+

Caveats

12. Since the submission of this impact assessment, the UK government's list of priority partners for data adequacy agreements has changed following a ministerial steer. This means the potential trade impacts from data adequacy decisions are likely to change. Our model is caveated and for this purpose our modelling assumptions remain conservative therefore we have decided to keep the list of priority partners within this section as they are important for the context of the 'Gravity trade modelling annex'.

13. The policy changes have been made on the set of priority countries before final assessments and decisions have been made. For each individual country, a full technical assessment will be undertaken before a decision to establish data adequacy is made. Prioritising countries for assessment are not a guarantee to receiving a positive decision. Additional countries may be

announced as being assessed in the future. The full group of non-priority countries represents 22% of UK services exports. Whilst it is unlikely that the UK will establish data adequacy with all of these countries, the benefits identified in this Annex will be underestimated at least to some degree, as more countries than the initial priority list are assessed, and data adequacy is established.

14. The high scenarios test full reciprocation from priority countries. Although establishing a data adequacy is likely to increase the likelihood of a priority country reciprocating, it is not assumed. It is likely some level of reciprocation will occur but the benefits to trade in these scenarios may be overestimated.

15. The model covers only certain sectors.[350] As above, cross-sector effects are not captured. Similarly, the model captures a subset of countries although it captures about 76% of UK services trade and 2/3s of global services trade.

16. How data adequacy operates on a bilateral basis may mean the 1.20.3 measure and its assigned weight may not be specific enough.[351] Whilst the OECD assigns differential weights for each country, bilateral-specific STRIs are not used i.e. how data adequacy functionally works between two countries may be different for another. For example, sector-specific restrictions may still be in place, or some compliance activities may still be required, for example with the United States, UK companies may need to verify that the business they are sending personal data to has signed up to a certification scheme. Similarly, risk aversion of businesses may mean even with regulations, alternative transfer mechanisms are still widely used as an additional form of protection when transferring data.

17. How data and trade interact is a nascent field. The understanding of how data as an input into production due to its intangible and non-rivalrous nature affects trade requires more research in the future.

18. DSIT will continue to develop its methodologies to better understand the relationships and drivers of data-dependent trade and work with X-HMG colleagues to develop methodologies.

Results

19. Below is a break-down of the results, which represent the medium-term impact on UK exports and imports from the first set of priority countries for data adequacy.[352] In reality, decisions will be made over several years. The difference in results compared to the previous Act IA is driven by the UK agreeing data adequacy regulations with the United States of America and the Republic of Korea, therefore we have removed their respective trade impacts.

20. For full detail of the underlying model, please refer to DBT's published Services Trade Modelling paper[353]. Results are presented on a country grouping level and for a subsection of sectors. It should be noted that the model does not account for cross-sectoral impacts and so results should be caveated that they do not cover whole-economy effects.

[350] It does not cover Manufacturing, Maintenance and Repair, Intellectual Property, Personal, Cultural and Recreational and Government sectors. These omitted sectors represent about 12% of UK services exports.
[351] The effect of the STRI on trade may vary by country pair. Due to a lack of degrees of freedom, however, the model cannot estimate country- or pair-specific STRI coefficients. The estimated STRI parameter of interest represents the average effect of the STRI across countries.
[352] For this model medium-term means results post adjustment for third-party effects.
[353] DIT Services trade modelling working paper

Table 90: Overall Results (£million), 2024 prices

Activity	Medium	High	Low	High with EU Adequacy Loss
Total UK Exports	477.4	745.7	-2,804	-1,561.3
Total UK Imports	-1.9	75.4	-383.6	-801.4

21. The overall results show an increase in both exports and imports in the high scenario. In the medium scenario exports are expected to increase and imports face a slight decrease. Both exports and imports are estimated to fall in the low scenario. Reciprocation of a data adequacy decision has a large impact on exports but not imports in the high scenario.

22. The results are further split out by sector and country grouping below.

Table 91: UK Exports Impact by Sector (£m), 2024 prices:

Sector	Medium	High	Low	High with EU Adequacy Loss
Transport	67.4	108.3	-421.9	-267.4
Construction	5.2	10.1	-68.5	-57.4
Insurance	20.7	76.5	-160.6	-7.0
Financial Services	118.7	152.1	-679.3	-334.7
Telecoms, Computer, and Information	158.2	256.8	-801.5	-461.5
Other Business Services	97.3	131.5	-608.8	-378
Distribution	10.0	10.5	-63.8	-55.2
Total	**477.4**	**745.7**	**-2,804.5**	**-1,561.3**

23. For UK exports, the largest affected sectors are Financial Services, ‘Telecoms, Computer and Information’ and Other Business Services. At the aggregate, the medium scenario sees an

increase of £477.4m compared to the baseline. Scenarios testing reciprocation by priority countries show an increase in the impact to £745.7m compared to the baseline.

24. Each of the medium and high scenarios have been tested for what happens when EU adequacy is lost as a result of the wider set of reforms. In the most pessimistic scenario, UK exports would fall by £2,804.5m relative to the baseline driven by the 'Telecoms, Computer and Information', 'Financial Services' and 'Other Business Services' sectors. All other sectors see a decrease in exports. In the scenario with reciprocation but EU adequacy loss, the net impact is net-negative with a decrease of £1,561.3m. 'Telecoms, Computer, and Information' and 'Other Business Services' sectors see the greatest fall in exports in this scenario.

Table 92: UK Exports Impact by Country Grouping (£million), 2024 prices

Country grouping	Medium	High	Low	High with EU Adequacy Loss
Priority	57.2	438	72.7	557.4
EU+	346.9	252.7	-2,966.5	-2,354.2
Other	73.2	55.0	89.2	235.5
Total	**477.4**	**745.7**	**-2,804.5**	**-1,561.3**

25. The above results break-down the results by country grouping showing the changes in exports in each scenario. Across the scenarios, priority countries see an increase in exports. The increase in exports for the priority countries is higher following the loss of EU adequacy than the direct impact of awarding adequacy due to the general equilibrium effects. Exports to other countries also increase due to trade creation. The general equilibrium effects consider the relative size of the EU+ group and their trading relationships with the UK and all other countries. A proportion of the UK's exports to the EU+ are diverted to priority and other countries partly reduce the negative impacts of the loss of EU adequacy.

Table 93: UK Imports Impacts by Sector (£million), 2024 prices

Sector	Medium	High	Low	High with EU Adequacy Loss
Transport	-71.8	-54.1	-168.8	-291.7
Construction	1.2	5.0	-41.5	-50.6
Insurance	5	14.4	-16.7	-53.0
Financial Services	-11.0	-3.8	-20.8	-71.4
Telecoms, Computer, and Information	32.7	41.7	-13.6	-95.7
Other Business Services	43.7	73.4	-89.3	-202.7

Sector	Medium	High	Low	High with EU Adequacy Loss
Distribution	-1.6	-1.1	-32.8	-36.3
Total	**-1.9**	**75.4**	**-383.6**	**-801.4**

26. In the medium scenario imports decrease by £1.9m and in the high scenario imports increase by £75.4m, with reciprocation having a positive impact on imports. When testing the impact of the loss of EU adequacy leads to a decrease in UK imports £383.6m to £801.4m across the two scenarios compared to the baseline.

27. The largest affected sectors depend on the scenario. For the medium and high scenarios, 'Transport' is the most negatively affected sector and 'Other Business Services' is the most positively impacted sector. . In scenarios that account for EU adequacy loss, 'Transport' is the most affected sector with all other sectors negatively impacted.

Table 94: UK Imports Impacts by Country Grouping (£million), 2024 prices

Country grouping	Medium	High	Low	High with EU Adequacy Loss
Priority	262.6	286.3	250.2	201.2
EU+	-233.2	-186.4	-595.5	-918.9
Other	-31.2	-24.5	-38.3	-83.7
Total	**-1.9**	**75.4**	**-383.6**	**-801.4**

28. When looking at the imports results by country grouping, the results show that in the medium and high scenarios imports increase relative to the baseline by £262.6m and £286.3m respectively for priority countries. In these scenarios, imports from the EU+ fall by £186.4m to £233.2m and in all other countries by £24.5m to £31.2m compared to the baseline. The result differs from the exports results where EU+ and other exports also increase in these scenarios.

29. In the EU Adequacy loss scenarios, priority country imports still increase by £201.2m to £250.2m, the size of the increase is relatively similar to the scenarios without EU adequacy loss. EU+ imports fall by £595.5m to £918.9m and other countries imports fall by around £38.3m to £83.7m relative to the baseline.

30. Imports divert from EU+ and other countries even in positive scenarios. The additional restrictions placed by the EU+ in the EU adequacy loss scenarios further reduce imports in the EU+ and other groupings but also negatively impact the increase in imports for priority countries.

Table 95: Overall Impact on UK-EU Trade if EU Adequacy is discontinued (£m), 2024 prices

Total UK Exports to EU+[354]	Total UK Imports from EU+[355]
-2,531.1	-685

31. When isolating the impact on trade between the UK and EU of the UK losing its EU adequacy decision, the results show that UK exports to the EU+ fall by £2531.1m and UK imports from the EU fall by £685m relative to the baseline. UK exports to the EU/EEA are estimated to fall by a greater magnitude in comparison to UK imports from the EU/EEA.

Table 96: UK-EU Trade Impact if EU Adequacy is discontinued by sector (£m), 2024 prices

Sector	UK Exports to EU+ Impact	UK Imports from EU+ Impact
Transport	-407.6	-221.4
Insurance	-124.4	-60.4
Financial Services	-563.2	-55.5
Telecoms, Computer and Information	-787.4	-111.7
Other Business Services	-570.8	-208.9
Distribution	-77.7	-27.1
Total	-2531.1	-685

32. In the scenario where the UK's EU adequacy decision is discontinued, all sectors see a decrease in exports to the EU+ with 'Telecoms, Computer and Information', 'Other Business Services' and 'Financial Services' being the most affected.

33. Similarly, all sectors see a decrease in imports from the EU+ when EU adequacy is discontinued. The 'Transport' and 'Other Business Services' sectors are expected to face the largest decrease in imports from the EU+.

Sensitivity Testing

34. To account for uncertainty in the STRI parameter, including the specificity for each bilateral country and business' behavioural reaction to policy changes, the 80% confidence interval is used. Due to the sector-specific STRI parameters, the range of impact depends on the sector of interest.

35. For changes to UK exports, the results show a range of £209m to £642.7m in the medium and £314.1m to £1079.1m in the high scenarios respectively. When testing the impact of EU adequacy loss, the results show a range of -£1054.41m to -£4275.2m in the low and -£576.2m to £2481.8m in the high with EU adequacy loss scenarios respectively. In the EU adequacy loss scenario, UK exports to the EU/EEA show a range of -£997.1m to -£3927.1m.

36. For changes to UK imports, the results show a range of -£13.2m to £92.3m in the medium and £15.3m to £215.4m in the high scenarios respectively. When testing the impact of EU adequacy loss, the results show a range of -£89.6m to -£752.4m in the low and -£271.8m to -

[354] Top 10 most impacted EU+ nations: Germany (-£382m), Ireland (-£315m), France (-£309m), Netherlands (-£292m), Switzerland (-£239m), Luxembourg (-£180m), Spain (-£163m), Italy (-£120m), Sweden (-£86m), Denmark (-£79m)
[355] Top 10 most impacted EU+ nations: Germany (-£86m), France (-£84m), Ireland (-£75m), Spain (-£69m), Netherlands (-£56m), Switzerland (-£53m), Luxembourg (-£46m), Sweden (-£45m), Italy (-£34m), Poland (-£33m)

£752.4m in the high with EU adequacy loss scenarios respectively. In the EU adequacy loss scenario, UK imports from the EU/EEA show a range of -£245.5m to -£1169.8m.

37. As with the central results, the results do not account for cross-sector impacts or the reallocation of factors of production.

6. Measures in the do maximum option

817. Below illustrates the additional measures to the do intermediate policy for the discounted do maximum option. Throughout the development of the Data (Use and Access) Act changes were proposed reflecting stakeholder feedback and ongoing policy development. These developments led to a better understanding of implicit costs and policy risks not previous considered which led to the data protection and ultimately Do maximum option not being suitable for implementation.

Table 97: Additional measures to the do intermediate policy for the discounted do maximum option.

Measures removed
Data Protection - information relating to identifiable living individual
Data Protection - vexatious or excessive requests
Data Protection - obligations of controllers and processors
Data Protection - vexatious or excessive requests to IC
Data Protection - IC refusal to act on complaints
Data Protection - Codes of practice: approval by the Secretary of State
Data Protection - Electoral purposes Exemption to further processing rules in UK GDPR for contact details collected by MPs during constituency casework to be reused for political campaigning
PECR - use of electronic mail for direct marketing
PECR - direct marketing for democratic engagement
PECR - meaning of expressions in section 116
Home Office: Public Safety and National Security, Implementation of law enforcement information sharing agreements
Home Office: Meaning of "appropriate national authority"
Home Office: Public Safety and National Security, Retention of biometric data
Home Office: Public Safety and National Security, Oversight of biometric data

7. Measures added via amendment during passage of the DUA Bill and included in the Bill at Royal Assent

Table 98: Summary of all Lords Committee, Report and Third Reading stage amendments included in the Bill at Royal Assent.

Amendment summary
Information Commissioner's Office This amendment adds an express reference to children meriting specific protection with regard to their personal data in new section 120B(e) of the Data Protection Act 2018 (Information Commissioner's duties in relation to functions under the data protection legislation).
Information Commissioner's Office - Privacy by design: children's higher protection matters This amendment builds on existing duties under Article 25 of the UK GDPR to design their processing activities in a way that complies with the data protection principles. It requires Information Society Services that are likely to be accessed by children (and are already subject to the Age-Appropriate Design Code) to consider how best to protect and support children when designing their services; and to take account of the fact that children merit specific protection because they may be less aware of the risks of the processing, and may have different needs at different ages.
Direct Marketing Regulation 22 of the PEC Regulations prohibits the transmission, by means of electronic mail, of unsolicited communications to individual subscribers. This amendment creates an exception from the prohibition for direct marketing carried out by a charity for charitable purposes.
Lawfulness of Processing & Rights of Data Subjects This amendment adds an express reference to children meriting specific protection with regard to their personal data when the SoS is considering whether to use regulations to add to the list of 'recognised legitimate interests'
Purported intimate images offences This amendment makes it an offence to create a purported intimate image of an adult without their consent or reasonable belief in their consent and provides that deprivation orders can be made under the Sentencing Code in connection with the offence
Purported Intimate image offences Clarification from "creating" to "soliciting the creation of" is to make consequential amendments to the long title of the Bill, and the headings of the new provisions inserted into the Sexual Offences Act 2003 by Government amendment 2.
Purported Intimate image offences: This amendment provides that the new Clause "Creating purported intimate image of adult" extends to England and Wales only.
Government Minor and Technical: Clause 89 of the Bill amends section 82 in Part 4 of the Data Protection Act 2018 (intelligence services processing). This amendment makes a consequential change to a definition in the Investigatory Powers Act 2016 which cross-refers to section 82.
Government Minor and Technical: section 124B(11) of the Data Protection Act 2018 provides that the Information Commissioner's duty to establish a panel to consider draft codes of practice may be disapplied or modified by regulations. This amendment ensures that regulations can make provision in relation to a particular code or amendment or a type of code or amendment.
Government Minor and Technical: The immigration legislation amended by Clause 55 may be extended to the Channel Islands or the Isle of Man. This amendment provides that the amendments made by Clause 55 may be extended to the Bailiwick of Guernsey or the Isle of Man.
Government Minor and Technical: This amendment provides that amendments of the Online Safety Act 2023 made by the Bill (see Clauses 124 and 125) may, like the other provisions of that Act, be extended to the Bailiwick of Guernsey or the Isle of Man.
Government Minor and Technical: Cybersecurity and Government Registers These two amendments address a duplicate reference to "the undertakers employees" by replacing it with a correct reference to "the contractor's employees" in Clause 56, page 52, line 13 and Claire 58, page 62, line 34.
Government Minor and Technical: Terms used in Chapter 1 – Data Protection This amendment provides that the clause defining "the 2018 Act" and "the UK GDPR" for the purposes of Chapter 1 of Part 5 of the DUA Bill comes into force on Royal Assent.

Table 99: Summary of all Commons Committee and Report stage amendments included in the Bill at Royal Assent. This excludes the following 12 Commons Committee amendments which removed non-Government amendments made during Lords passage:

Amendment numbering (HL Bill 100 Commons Amendments)[1]	**Amendment summary**
Commons Amendment 32	Clause 28, page 30, line 32, leave out subsections (3) and (4)
Commons Amendment 33	Clause 45, page 43, line 12, leave out subsection (6)
Commons Amendment 34	Clause 56, page 54, line 1, leave out lines 1 to 3
Commons Amendment 35	Clause 56, page 58, leave out lines 10 and 11 and insert "obtain the consent of the Welsh Ministers in relation to any provision which would be within the legislative competence of Sendd Cymru if contained in an Act of the Senedd (ignoring any requirement for the consent of a Minister of the Crown imposed under Schedule 7B to the Government of Wales Act 2006)
Commons Amendment 43	Clause 67, page 75, line 26, leave out "and that is conducted in the public interest"
Commons Amendment 44	Clause 95, page 120, line 31, leave out subsection (1)
Commons Amendment 47	Page 170, line 2, leave out Clause 135
Commons Amendment 48	Page 170, line 23, leave out Clause 136
Commons Amendment 49	Page 171, line 15, leave out Clause 137
Commons Amendment 50	Page 171, line 37, leave out Clause 138
Commons Amendment 51	Page 173, line 1, leave out Clause 139
Commons Amendment 52	Page 173, line 13, leave out Clause 140

1[1] Data (Use and Access) Bill [HL], Parliament (2025)

Table 100: Amendments made during ping-pong

Amendment text
The Secretary of State must produce guidance for persons described about how to protect information kept in, or obtained from, NUAR. The persons are persons who, pursuant to regulations made under section 106C, are able to access information kept in NUAR. The Secretary of State may revise or replace the guidance. The Secretary of State must publish the guidance (and any revised or replacement guidance) in such manner as the Secretary of State considers appropriate for bringing it to the attention of persons described in subsection (2). The same guidance may discharge the obligations of the Secretary of State under this section and under Article 45CA of the Street Works (Northern Ireland) Order 1995 (S.I. 1995/3210 (N.I. 19)). And The same guidance may discharge the obligations of the Secretary of State under this Article and under section 106CA of the New Roads and Street Works Act 1991.
It is a defence for a person charged with an offence under this section to prove that the person had a reasonable excuse for creating the purported intimate image.
The Secretary of State must review the operation of subsection (7A), publish the outcome of the review in a report before the end of the period of two years beginning with the day on which this section comes into force, and lay the report before Parliament.
The Secretary of State must, before the end of the period of 6 months beginning with the day on which this Act is passed, lay before Parliament a statement setting out what progress has been made towards the publication of— (a) the economic impact assessment required by section (Economic impact assessment), and (b) the report required by section (Report on the use of copyright works in the development of AI systems). (2)
The duty in subsection (1) does not apply where the economic impact assessment and the report have been published before the end of the period described in that subsection.”