Department for Science, Innovation & Technology

Overview of the Expected Impact of Changes to the Data Protection and Digital Information Bill following Report Stage

Introduction

1. This paper provides an overview of the economic impact of the amendments made at the report stage of the Data Protection and Digital Information (DPDI) Bill.

2. The existing Impact Assessment[1] provides an outline of the regulatory framework, market failures, proposed policy options and the cost benefit analysis of the package of reforms. Analysis outlining the expected impact of changes to the DPDI Bill made at committee stage can also be found in the supporting documents to the bill on gov.uk. [2]

3. In March 2023, we estimated the Net Present Social Value of the package of reforms in the Bill to be between £1.2 billion and £9.1 billion over 10 years following implementation and in 2019 prices, with a 2020 base year. Our best estimate is approximately £4.7 billion over this period. We estimated that £2.2 billion of this will be attributable to UK businesses and £2.5 billion to the public sector.

Overview of Changes

4. 22 amendments have been proposed at report stage, reflecting further stakeholder feedback and policy development in areas across government relevant to data policy. Four of these are minor or technical and do not have any additional economic or wider impacts to UK businesses. Details of these amendments can be found in the amendment pages for the bill.

5. 18 of these are substantial technical and or policy amendments that have an impact above what is already included in the original Impact Assessment. We have included an outline of the rationale, purpose and impact of these below in the analysis section. Finally, for the two most significant and substantial additions to the bill, the National Underground Asset Register and the Data access to reduce fraud amendments, separate impact assessments have been published alongside this note. The table below provides a summary of this breakdown.

[1] DPDI Bill Impact Assessment, March 2023, DSIT
[2] DPDI Bill supporting documents, DSIT

Table One: Summary of all report stage amendments

	Clause		Additional Quant Impacts?	Additional Qual Impacts?	Notes
a. i	**Digital verification service (DVS) schemes** To 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 bill to be 'supplementary code'.		X	✓	Further quant analysis will be undertaken for the enactment impact assessment.
a. ii	**Digital verification schemes** 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.		X	✓	Further quant analysis will be undertaken for the enactment impact assessment.
	References to Retained Direct EU Legislation Updating 3 references to retained direct EU legislation in the bill in light of the REUL Act.		X	X	
b	**Police retention of biometric data from INTERPOL**		✓	✓	Further quant analysis will be undertaken for the enactment impact assessment.
c	**Police retention of biometric data from other international partners**		✓	✓	Further quant analysis will be undertaken for the enactment impact assessment.
d	**Lawful ground for transferring personal data under the UK-US Data Access Agreement**		X	✓	Further quant analysis will be undertaken for the enactment impact assessment.
e	**Electoral Purposes**[3]	**Meaning of "democratic engagement"** Defining "democratic engagement" in Sch 1 (Annex 1 UK GDPR) and clause 87 and 88 (PEC Regulation).	X	✓	
		Processing political opinions data Amending exemptions in Sch 1 DPA 2018 (special category data) to permit elected representatives to process political opinions data.		✓	

[3] This collection of two amendments is analysed as a group and not separately due to substantial overlaps in impacts.

	Clause	Additional Quant Impacts?	Additional Qual Impacts?	Notes
f	**Limiting records to high-risk processing** Amending clause 16 so records required to be kept by controller/processor carrying on high risk processing should only have to cover high risk processing, rather than all processing where some of it is high risk.	X	✓	Indicative estimates have been produced but further analysis will be undertaken for the enactment impact assessment.
	SoS approval of ICO statutory codes of practice Amending clause 33 (the SoS approval power for ICO statutory codes of practice) so the ICO is no longer obliged to change a code in light of comments from the SoS but must take them into account.	X	X	
	Disclosure of information to improve public service delivery to undertakings Technical changes to how "the law of Scotland and Northern Ireland" is expressed in clause 98's amendments of s35 DEA 2017.	X	X	
g. i	**Smart Data Group 1** New provision to allow regulations to provide for an 'interface body' to play a central, technical coordinator role in a scheme	X	✓	
g. ii	**Smart Data Group 2** 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	X	✓	
g. iii	**Smart Data Group 3** 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.	X	✓	
g. iv	**Smart Data Group 4** 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	X	✓	
	Amendment to ICO's modes of serving notices. Setting out the mechanisms by which the ICO may serve notices in the DPA 2018 to reflect the modernity's of electronic communication	X	X	
h	**Reporting periods for PEC Regulation breaches** Extending the reporting period for breaches under reg 5A PEC Regulation from 24 to 72 hours	X	✓	Further quant analysis will be undertaken for the enactment impact assessment.

	Clause	Additional Quant Impacts?	Additional Qual Impacts?	Notes
i	**National Underground Asset Register** Legislation to underpin a national register of underground assets (cables etc.)	✓	✓	Impact Assessment provided
j	**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 by suspected suicide.	X	✓	Further quant analysis will be undertaken for the enactment impact assessment.
k	**Exemption for archives from further processing rules** Amending clause six to exempt archives from further processing rules where personal data was originally obtained in reliance on consent.	X	✓	Further quant analysis will be undertaken for the enactment impact assessment.
l	**Subject access requests - disproportionate searches** Clarifying that controllers are not required to make disproportionate searches in response to subject access requests - necessary because of the loss of the EU principle of proportionality under the REUL Act.	X	✓	Further quant analysis will be undertaken for the enactment impact assessment.
m	**DWP data access to reduce benefit fraud.** Better enabling DWP to access to data from third parties - particularly banks and other financial organisations to allow DWP to more proactively identify fraud or error, particularly in instances where claimants have capital (savings) above benefit eligibility limits or where claimants are spending more time out of the country than is allowed and accessing benefits fraudulently.	✓	✓	Impact Assessment provided

6. A fully updated Impact Assessment for the bill including all amendments made throughout the passage of the bill will be reviewed by the RPC and published at enactment, in line with government analytical guidelines. This is expected to be around the first half of 2024 and will include an updated summary of impacts to the ICO of all reforms and amendments.

7. The table below shows the additional impact to the estimated net present value (NPV) of the amendments at this stage. This table does not include qualitative impacts and is likely to change between now and enactment as more impacts are quantified.

Table Two: Breakdown of quantifiable impacts to the estimated NPV for the bill.

		Total Impact of preferred option (2019 prices, 2020 PV)		
		Discounted Costs (£m)	Discounted Benefits (£m)	NPV (£m)
DPDI Bill March 2023 published IA		1,188.1	5,909.2	4,721.0
Additions of quantified amendments made at report stage (as of November 2023)				
+ National Underground Asset Register		+162.1	+4,079.3	+3,917.1
		1,350.3	9,988.5	8,638.1
+DWP data access to reduce benefit fraud		+264.4	+2,145.3	+1,880.9
		1,614.7	12,133.8	10,519.0
+National Security and Law Enforcement Amendments	**Police retention of biometric data from INTERPOL**	NQ	+2.8	+2.8
		1,614.7	12,136.6	10,521.8
	Police retention of biometric data from other international partners	NQ	+1.0	+1.0
		1,614.7	12,137.6	10,522.8
Updated quantitative impact (at this stage)				
DPDI Bill & Report stage amendments		+426.5	+6,228.4	+5,801.8
		1,614.7	12,137.6	10,522.8

Analysis

a) Digital Verification Services Frameworks

i) To 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.

This summary has been provided by DSIT.

Rationale

8. Section 2 of the DPDI Bill requires the Secretary of State to establish and maintain a public register (DVS register) of digital verification service providers (DVS providers). The Secretary of State will have a duty to add DVS providers to the DVS register, as long as they have a service certified against the UK digital identity and attributes trust framework (trust framework) by an accredited conformity assessment body and correctly apply to be included.

9. While the Trust Framework describes what good digital identity services look like in general, in practice, organisations in particular sectors or use cases may need to require digital identity services to prove their compliance with rules and processes in addition to those contained within the trust framework, in order to meet needs which are particular to that sector or use case.

10. DSIT works with certifying bodies to integrate such additional rules into the trust framework certification process, and thus allow DVS providers to certify their service against additional rules as part of the same process. We call these additional rules ‘schemes.

11. Certification against schemes will allow providers to demonstrate that they can meet different sector or use case-specific needs, and thereby increase confidence in the use of digital identities in areas where more specific rules are needed.

Requirements

12. An amendment to the DPDI Bill is necessary to define these additional rules and mirror provisions for the trust framework relating to the registration of DVS providers certified against them in the DVS register. This proposed amendment will also underpin the process to establish and maintain supplementary codes and provide the Secretary of State with corresponding approval, governance and oversight powers.

Expected impact

13. The existing Impact Assessment for the DPDI bill referenced monetised costs and benefits of digitising the identity checking part of pre-employment processes. Total indirect benefits of improved employee mobility were estimated to be between £1,112.3 to 2,518.18 million over the 10-year appraisal period.

14. 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 resources to develop and assess against their own unique requirements. This will 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.

15. This will enable cost and efficiency savings beyond the estimated quantifiable benefits outlined in the initial impact assessment. This indicative assessment will be developed further as part of the bill's Enactment Stage Impact Assessment.

ii) Restricting IDVT digital Right to Work/Right to Rent Schemes checks to DVS providers noted on the register created in the DPDI Bill Part 2 as meeting the Right to Work / Right to Rent Schemes supplementary standards.

This summary has been provided by the Home Office and DSIT.

Rationale

16. All employers and landlords are required to conduct a right to work or right to rent check respectively before employing or letting a property to make sure the individual is not disqualified from working or renting by reason of their immigration status. Since 06 April 2022, employers, landlords, and letting agents have been able to obtain a statutory excuse against liability for a civil penalty where an Identity Service Provider ("IDSP") has conducted a check on a current British or Irish passport (including Irish Passport Card) on their behalf.

17. Digital checks provide a robust, resilient, secure, and efficient checking system for employers and landlords, and reduce reliance on untrained personnel examining non-secure documents. Enabling the use of an IDSP has provided many British and Irish citizens the opportunity to evidence their right to work in the UK, and right to rent in England, via digital online checking methods.

18. Requiring employers and landlords who choose to carry out a digital right to work / right to rent check to use only certified IDSPs will increase the security of the checking regime, in turn supporting possible future enhancements and creating a stronger basis on which to increase penalties for non-compliance. To note, 38 providers are already certified through the DSIT Trust Framework.

19. The sectors have been supportive of the implementation of IDVT checks, they have provided an opportunity for quicker and more cost-effective checks, as well as removing the need for a manual check of documents. This enhances the security of the checks that are required to be completed for the schemes, providing greater confidence of their recruitment processes.

20. Home Office engagement with employers and landlords who have adopted the use of IDSPs in their pre-employment and on-boarding processes has shown that the

use of IDVT has reduced the time for completing the checks from nearly a week to estimates in the region of 5 minutes.

Requirements

21. This clause will amend the Home Office's powers in the Immigration, Asylum and Nationality Act 2006, the Immigration Act 2014 and the Immigration Act 2016 used to make regulations and orders in respect of the Right to Work and Right to Rent Scheme to allow it to make cross-reference to the DVS register established under Part 2 of the DPDI bill. The Home Office intends to amend secondary legislation so as to provide a statutory excuse against liability for a civil penalty for Employers and Landlords/Letting Agents who use a DVS provider detailed on the DSIT DVS register and noted as meeting an approved supplementary standard. There are currently 38 providers certified on the register who have been certified to provide Right to Rent and Work checks.

22. Private sector requirements will be limited to those providers listed on the DVS register and noted in that register as meeting the Right to Work / Right to Rent Schemes supplementary standards.

Expected Impacts

23. The proposal will amend existing powers to prescribe requirements by way of order. There will be no impact on employers, landlords, or digital identity verification service providers until regulations are made restricting digital identity checks carried out by a third-party to providers noted on the DVS register as meeting the Right to Work / Right to Rent Scheme supplementary standards.

24. The proposal will not impose any additional costs on providers who are already certified. There will be some costs to businesses who are not currently certified but who subsequently wish to become certified. Research is currently being conducted by DSIT to determine the scale of this cost.

25. 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.

26. Requiring employers and landlords to use only certified IDSPs 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.

27. There will also be a benefit to employers from efficiency savings brought about by this measure. This measure will reduce the time it takes to process an employee, generating time savings for both the employee and employer, as well as allowing the employers to potentially check more people in a given time. It is unknown by how much the proposal will reduce individual checks by, and so the exact scale of the time savings is an evidence gap that will be investigated further in the enactment assessment.

b) Police retention of biometric data from INTERPOL

This summary has been provided by the Home Office.

Rationale

28. In late 2022, Counter Terrorism Policing (CTP) raised their concerns regarding retention of biometrics received via INTERPOL. UK law enforcement no longer has access to the Schengen Information System. In the context of growing global cooperation on intelligence exchange post-EU Exit, the use of biometrics received via INTERPOL has become increasingly important. CTP has commented that the operation of effective tripwires, including at the border, is reliant on its robust holdings of biometrics relating to subjects of national security interest, including biometrics disseminated by INTERPOL.

29. A significant number of INTERPOL notices are being referred by the National Crime Agency to CTP: approximately 600 per month – of which approximately 50% have fingerprints attached to them. CTP highlighted that the current retention regime (set out in section 18 of the Counter Terrorism Act (CTA) 2008) presents some significant constraints for operational use of these biometrics. This includes the statutory three-year retention period, which is not aligned with the duration of INTERPOL notices (which initially last for five years but are capable of renewal), as well as the difficulties in applying the National Security Determination (NSD) regime to biometrics received via INTERPOL. The NSD regime, which allows the police to submit applications to the Biometrics Commissioner to retain the biometrics of an individual where they have not been convicted of an offence and continued retention is necessary and proportionate for the purposes of national security, can be resource intensive. The Independent Reviewer for Terrorism Legislation and the Biometrics Commissioner were consulted on these changes and are supportive of amending the CTA to mitigate these issues, which they highlighted in their most recent annual reports respectively. Processing these INTERPOL notices via the NSD regime, rather than relying on INTERPOL's processes for cancelling notices when they are no longer necessary and proportionate, or have otherwise ceased their operational utility, puts the UK at odds with the wider international law enforcement community's handling of these notices.

Requirements

30. These changes will amend the CTA to allow the police to retain biometrics disseminated by INTERPOL in national security related cases for as long as the relevant INTERPOL dissemination remains in force, rather than needing to apply to retain the biometrics under the NSD regime. The change will ensure that UK legislation is aligned with the relevant INTERPOL rules on data retention. This change will also be applied retrospectively to biometrics that were received via INTERPOL before commencement of the DPDI Bill.

Expected Impacts

31. The 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. 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.

32. CTP receives on average 300 biometrics per month disseminated by Interpol, however volumes of biometrics may fluctuate significantly due to operational factors. CTP estimates that it takes an officer approximately 4 hours to develop an NSD application. 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).

c) Police retention of biometric data from other international partners

This summary has been provided by the Home Office.

Rationale

33. Following engagement on biometrics received via INTERPOL, CTP raised separate issues relating to biometrics received from international partners outside of the INTERPOL system. These biometrics often relate to foreign nationals who are of national security interest to CTP. As in the case of the INTERPOL system, biometrics from international partners are critical for ensuring there is effective tripwire coverage for the UK, for example where a foreign national applies for a visa to enter the UK, their biometrics can be checked against those of national security interest that CTP hold.

34. The CTA does not distinguish between biometrics acquired within the UK or those that are shared by international partners. As a result, current provisions within the CTA present some challenges for CTP when they receive biometrics via these routes. In particular, the CTA sets out that biometrics can be retained for three years from the point at which they are taken – this is difficult to apply in practice when CTP receive biometrics from international partners that are older than three years or where it is not clear what date the biometrics were taken on. In addition, unlike other legislation governing the use of biometrics (in particular, the relevant provisions of the Police and Criminal Evidence Act 1984 which provides the main biometric retention regime in England & Wales), the CTA does not permit the indefinite retention of biometrics where an individual has a foreign conviction equivalent to a conviction in the UK. This inconsistency means that, under current rules, CTP would need to apply for an NSD to retain biometrics received via international partners

even if the individual had a foreign conviction, whereas if they had received the biometrics from a police force within the UK or the biometrics had been taken on arrest in the UK, they would be permitted to retain these biometrics indefinitely.

Requirements

35. These changes will amend the CTA to allow for indefinite retention of biometrics of national security interest in two specific circumstances:

    a. Where the police have received biometrics of national security interest from international partners, they will be permitted to pseudonymise this biometric data and retain it indefinitely. CTP already request biometric data from overseas to be transferred to them in a pseudonymised format. As a result, this amendment will only impact those biometrics where the biometrics are transferred with identifiable information, allowing CTP to undertake steps themselves to pseudonymise this biometric data. The existing provisions of the CTA will apply as soon as the police come to know the identity of the individual, e.g., as a result of a match against other biometric datasets, and at that point the existing retention period in the CTA (three years) will apply.

    b. Where the police have received biometrics of individuals with a foreign conviction (equivalent to a UK conviction), in line with domestic legislation in the UK, the police will be able to retain these biometrics indefinitely.

Expected Impacts

36. The NSD regime is recognised to come with high resource requirements, as it requires the police to develop a detailed national security case for retaining an individual's biometrics. Building the intelligence case, particularly to retain biometrics received from international partners where there can be 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. An application also requires sign-off by a Chief Officer, as well as by the independent Biometrics Commissioner. 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 amendment, as the amendment 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).

37. CTP have estimated that inbound biometrics received through wider international cooperation could increase to up to 200 biometrics per month over time. 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 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). 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). 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.

d) Lawful ground for transferring personal data under the UK-US Data Access

This summary has been provided by the Home Office and DSIT.

Rationale

38. The UK US Data Access Agreement (DAA) is a treaty between the UK and the US that allows each party's law enforcement bodies to directly request essential data held by telecommunications operators in the other's jurisdiction. This is solely for the purposes of preventing, detecting, investigating and prosecuting crime, including terrorism, child sexual exploitation and organised immigration crime etc. For the UK, this in particular permits access to data held by US covered providers and located in the US.

39. Therefore, we wish to fully clarify that transfers responding to US requests made in reliance on the DAA satisfy the Public Interest requirements of Article 6(3) and Article 9(2)(g) of the UK GDPR ensuring efficient functioning of the DAA.

Requirements

40. To ensure absolutely clarity around the public interests' requirements faced by UK Telecom Operator's (TO's), this amendment will update the UK GDPR and the Data Protection Act to provide absolute clarity and assurance to UK TO's that the 'public interest' lawful basis under both Article 6 and Article 9 can be relied upon for transfers of data for law enforcement and security purposes.

Expected Impacts

41. As a result of this amendment, we would expect UK TO's to have further clarity on the rules surrounding the transfer of data for public interests. As the DAA itself is strictly limited to purposes that are the prevention/detection/investigation/prosecution of crime rather than any other non-public interest considerations, we would expect UK businesses to increase their level of transfers for law enforcement purposes. Whilst we expect the quantity of transfers to increase, we do not expect this to translate into a substantial increase in direct costs for UK TOs, as many will already have the infrastructure and transfer mechanisms in place following the

establishment of the DAA. For example, the UK Business Data Survey 2022 finds that 29% of businesses in the Information and Communication sector that use digitised data transfer data overseas indicating that these mechanisms already exist.[4]

42. 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.

e) Use of data for purposes relating to electoral services

This summary has been provided by DSIT.

Rationale

43. The reforms in this section seek to reduce the regulatory constraints of data protection rules applying to political parties, MPs, and candidates. This is made up of two separate amendments.

44. The first seeks to amend the definition of democratic engagement activities within Schedule 1 to the bill, to include a more specific list of examples of certain activities which should be regarded as democratic engagement activities, similar to that set out at paragraph 691 of the bill's Explanatory Notes. The aim of this amendment is to create greater clarity with regards to what activities are covered by the democratic engagement processing condition on the face of the bill, to facilitate the use of personal data by candidates and elected representatives for this purpose by reducing uncertainty and barriers to information sharing.

45. The second amendment 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 casework.) 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.

[4] UK Business Data Survey, DCMS, 2022

Requirements

46. These amendments will update the definition of what ‘democratic engagement’ and ‘democratic engagement activities’ mean in the context of data protection law. Exemptions in Schedule 1 to the DPA 2018 will also be amended to permit elected representatives to process sensitive personal data relating to political opinions for the purpose of campaigning (which political parties are already allowed to do).

Expected Impacts

47. 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, by providing a clearer definition of ‘democratic engagement’ it may inadvertently narrow the scope of democratic engagement by defining it on the face of the bill. For example, there may be activities that fall within the definition that are not explicitly mentioned in the list of examples and therefore discourage data users from processing data for these purposes.

48. Finally, the second amendment 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.

f) Record Keeping Activities

This summary has been provided by DSIT.

Rationale

49. This is an amendment to correct the new record-keeping provisions in Article 30A of the DPDI Bill, to make it clearer that organisations only have to keep records of the high-risk processing activities they carry out and not every processing activity if some activities are risky and some aren’t. The intent is to avoid forcing an organisation to keep records on all of their processing activities even if they are low risk. This currently creates unnecessary costs for UK businesses who are having to invest in reporting systems and in demonstrating compliance. The rationale behind this amendment is to reduce this unnecessary financial burden for businesses by increasing clarity on what is required.

Requirements

50. The way the clause is currently drafted in new Article 30A(1) is that if a controller/processor carries out any high risk processing then the duty applies for all processing, rather than just the processing that is high risk. The amendment will

make it clear that the record keeping duty only applies to the processing that is high risk.

Expected Impacts

51. The amendment is expected to reduce burdens for UK businesses which carry out low-risk data processing. It will mean that they no longer have to keep records of all their low-risk processing, therefore we expect a reduction in costs of demonstrating compliance. We also expect that the change will result in a reduction in the number of businesses seeking legal advice to clarify regulation about whether or not businesses need to keep records.

52. For example, there may be an independent shopkeeper that employs five members of staff. The shopkeeper only keeps payroll data, contact details of suppliers and email addresses of previous customers. However, due to a recent spate of shoplifting, the shopkeeper decides to install a new CCTV system which makes use of live facial recognition technology. This involves matching biometric images of visitors to the store with images of suspected offenders held on a 'watchlist'. This potentially 'high risk' activity under the new amendment would not force the shopkeeper to keep records of processing everything, but just of the CCTV processing.

53. Currently the Impact Assessment for the bill measures the cost savings to businesses of not having to keep records of low-risk processing for UK businesses that only process low-risk data. The introduction of this amendment will therefore increase the proportion of data processing impacted by this amendment, to include the low-risk processing of businesses that carry out both high and low.

54. The ICO provides examples of processing 'likely to result in high risk' [5] but the data on how many businesses carry out this processing is not available, instead the impact assessment currently uses figures from the UKBDS on 'sensitive data' as a proxy for high-risk processing. DSIT has identified this as an evidence gap and is currently developing methodology in order to measure the proportion of high risk and low risk processing activity in the future. As this is currently unavailable, we continue to use the UKBDS definition of 'sensitive data' as a proxy.

55. We are currently unable to estimate the number of firms that undertake both low and high-risk processing and the percentage of their processing which is low risk and therefore impacted by this amendment. However, we have shown the impact of 5%, 10% and 15% increases beyond the initial assumption that 50% of low-risk data usage is affected by clarification under this measure.

56. A 5% to 15% increase in the proportion of low-risk processing impacted by this amendment would increase compliance cost savings e by between £800,000 and £2.5 million, on top of what is already estimated in the Impact Assessment, with a central estimate of £1.7 million for a 10% increase. We would also expect a further increase in cost savings for firms no longer having to demonstrate compliance. We estimate the additional cost savings could be between £6.1 million and £18.2 million

[5] Examples of High Risk Processing, ICO, 2023

a year with a central estimate of £12.1 million, with the same percentage increase of between 5% and 15%.

57. We assume that this amendment will reduce compliance costs and burdens for businesses, however it is also important to consider the risks and potential wider impacts of this amendment. For example, this amendment could encourage more businesses to classify their processing activities as low risk to decrease their compliance burden, despite them having significant risk. By not recording this processing correctly and not complying with this regulation, there are risks of data not being stored correctly, being misused by businesses and breaches occurring. These risks should be balanced against the potential benefits, and this will be explored further in the Enactment Impact Assessment.

g) Changes to Smart Data Scheme Legislation

This summary has been provided by DBT.

58. The amendments will enable the government to deliver a greater range of Smart Data delivery models. The amendments allow this by changing how schemes can be designed or delivered (e.g. by allowing the Smart Data powers to be used to require the creation of a body to coordinate arrangements for data sharing interfaces and related services), or by clarifying some of the terms in the current legislation to allow explicitly for a wider range of design choices open to those making Smart Data regulations.

59. The Smart Data powers constitute Part 3 of the Data Protection and Digital Information Bill (DPDI) (No.2) Bill. This Part of the Bill provides the legislative framework for the government (the Secretary of State or the Treasury) to make regulations to establish and mandate participation in Smart Data schemes.

60. The powers in the Bill as introduced will enable regulations to, among other things:

    a. Specify who is in scope – i.e., which businesses as data holders are compelled to provide the data.

    b. Specify what data is in scope, and how it should be shared, with reference to technical standards or specific services such as APIs.

    c. Designate a public authority as an enforcer of the regulations.

    d. Designate a decision-maker to function as an accrediting body, to accredit third parties who wish to become authorised to access specific data sets (where the regulations provide that data sets may be shared with authorised third parties).

    e. Provide for levy raising powers to be raised by government or public bodies to cover the costs incurred by an enforcer and/or decision maker.

f. Set the parameters for the charges (or fees) e.g., to cover the costs of specific functions carried out by an enforcer and/or decision maker.

61. The powers as introduced enable the government to design tailored regulations for the sectors and markets where a scheme will be introduced. The amendments further enable the government to design proportionate regulations, by expressly allowing regulations to underpin a broader range of delivery models for Smart Data schemes.

62. The suggested amendments cover four main areas:

    1. Group 1: The first of these areas cover amendments that provide the Secretary of State and the Treasury with powers to include an 'interface body' within a Smart Data scheme. The 'interface body' would sit at the heart of the Smart Data scheme to coordinate arrangements (particularly standards) for data sharing interfaces and related services and make other arrangements relevant to the Smart Data scheme. Specifically, amendments in this group provide for the following:

        a) Giving the SoS or the Treasury the power to require certain participants in the scheme to establish or maintain an interface body to set standards and make other arrangements in relation to data sharing interfaces.

        b) Providing powers to the SoS or the Treasury to make regulations in relation to an interface body. These regulations may include provisions about how such bodies must carry out certain functions, including the development of interface standards and arrangements for the scheme and the monitoring of such. Regulations may also include requirements in relation to the objectives, governance, and transparency obligations of an interface body.

        c) In relation to the financial services sector specifically, providing powers for the Treasury to make regulations enabling or requiring the Financial Conduct Authority to make rules in applying to interface bodies and the people who are required to set them up and use them.

    2. Group 2: The second group of amendments change the current definition of 'customer data' in the legislation to clarify the range of information that 'customer data' relates to. The legislation originally referred to customer data as data relating to transactions between a customer and a trader. This has been widened to expressly include information relating to goods, services and digital content provided to the customer, or at the customer's request, by the trader. This includes prices or other terms on how customers are supplied with a good, service, or digital content by a trader. This is to ensure that relevant customer financial data beyond transactions between the customer and an account service provider (for example information about payments the customer has made to third parties) is within scope of the 'customer data' definition, as is currently the case in Open Banking

3. Group 3: The third group of amendments clarify the powers of enforcers to investigate and monitor compliance with the requirements of a scheme, and the process for setting fines, penalties and fees in relation to a scheme. Amendments also clarify that existing data sharing requirements in other legislation relevant to a sector can be incorporated into smart data regulations as equivalent provisions.

4. Group 4: The fourth group of amendments includes provisions that explicitly allow for a model of Smart Data delivery where regulations can be used to mandate that a specified entity collates the data from data holders and makes this available to authorised third parties ('ATPs'). Specifically, this group of amendments include:

    d) 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.

    e) Further powers that regulation makers can mandate that this specified entity must publish or make available this business data upon request.

    f) Provisions for the Secretary of State and the Treasury to make regulations to mandate that the specified entity can be funded via levies and charges from industry.

    g) Powers that 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.

63. The government is also introducing further amendments that are either clarifying amendments or have otherwise been assessed to not have any associated impacts. For this reason, this note focuses on the amendments described above.

i) Amendment Group 1 – New provision to allow regulations to provide for an 'interface body' to play a central, technical coordinator role in a scheme

Rationale

64. The Treasury has announced its intention to use powers provided through the Act to provide a long-term framework for the Open Banking regime (the current basis of which is in part provided for by an Order made by the Competition and Markets Authority (CMA))[6]. The CMA Order required the creation and regulation of the Open Banking Implementation Entity (OBIE) to develop and implement a single set of industry standards for data sharing interfaces. The OBIE standards and related services (such as its security and trust framework) have been central to the UK's success and the growth of competition and innovation in Open Banking.

[6] Retail Banking Market Investigation Order 2017 - GOV.UK (www.gov.uk)

65. Without a single set of standards, financial data holders (banks and other payment account providers) may share data in different formats and through bespoke technical interfaces (subject to certain minimum requirements in payments regulations). Such fragmentation of standards and interfaces would increase the friction and costs for authorised persons to access data from various data holders, increasing barriers to entry and hampering innovation.

66. The Joint Regulatory Oversight Committee (JROC), co-chaired by the Financial Conduct Authority (FCA) and the Payment Systems Regulator, with the Treasury and the CMA as members, has recommended that a new interface body[7], is necessary to preserve the critical standards and services currently provided by OBIE, and to coordinate the further development of Open Banking as a Smart Data scheme.

67. Noting the lessons learned in Open Banking, JROC also recommended public regulators should directly oversee any such interface body.

68. Amendments (a) and (b) would enable regulations to provide for the creation of an interface body. The amendments are necessary to reflect the structure of Open Banking as it currently exists, to ensure the ecosystem continues to operate effectively, and to achieve the recommendations for the future development of Open Banking, as set out by the JROC.

69. Beyond Open Banking, these amendments can be used to support schemes in other markets and sectors using a similar delivery model. The amendments can be used by regulation makers to establish Smart Data schemes in any sector to combat the above market failures, which are not limited to sectors where there is an existing interface body. As such, Smart Data will be able to provide customer benefits across the UK economy. It can do this by empowering customers to use their data to search for the best deals for them. This will ultimately lower prices through the higher level of competition due to higher transparency on prices. Consistent standards for data sharing interfaces allow customers to more easily access their data from different sources and to allow authorised persons to efficiently provide customers with services using this data.

70. Amendment (a) gives the Secretary of State and the Treasury the power to require data holders to establish or maintain an interface body. The interface body can then develop and implement a single set of industry standards for data sharing: reducing friction and fragmentation in data access.

71. This amendment helps to alleviate the network failure, as a central standard body enhances the ability of schemes to be designed to establish and utilise standards. Standardised interfaces benefit customers by ensuring that they can access data, through authorised persons or ATPs, in a consistent, reliable manner enabling access to better services, deals and tailored advice.

72. In the current legislation, a decision-maker can accredit authorised persons and ATPs to ensure secure data sharing with regulatory oversight. Amendment (a)

[7] Referred to as the “future entity” in the Open Banking context.

further allows for an interface body to be created for the schemes, or for the data and interface standards to be designed specifically for each sector, raising the quality of specific schemes. This further addresses the network failures associated with setting data standards and potentially makes them more efficient for data holders to implement.

73. Amendment (b) allows for regulations to be made that apply to interface bodies including in relation to their functions, funding, governance, and transparency requirements.

74. Amendment (b) further strengthens the ability for the interface body to address this network failure, as it allows these specific requirements to be conferred to it in regulations. In the absence of these specific requirements, the individual participants would have to separately fund and coordinate the functions of the interface body.

75. Without regulations, in some markets, there is a risk that larger players dominate the decisions around the design of the interface body. This can create a spillover effect, where the decisions around the design of the interface body may be dominated by larger players but will impact all players including the larger and smaller firms. Amendment (b) therefore addresses these market failures by giving the power for regulation makers to set out these specific requirements in regulation.

76. Amendment (c) allows for a specific model to be used exclusively in the financial services sector, whereby the power to set detailed rules can be sub-delegated to the FCA, within certain parameters and in the pursuit of certain objectives as specified by the Treasury in regulations. This is to facilitate a Smart Data scheme for Open Banking, where the FCA is the existing regulator of data holders and authorised persons, and exercises delegated rulemaking, supervision and enforcement powers under established financial services legislation.

77. The group of amendments promotes competition to combat market power. Having an ‘interface body’ to coordinate secure, efficient, and standardised data sharing, will ensure that data standards in Smart Data schemes are not monopolised by a small number of incumbent, larger firms. Regulation of interface body arrangements can also ensure that the interests of authorised persons and customers are adequately represented in data standards development. Allowing for oversight of the interface body and requiring it to publish documents enables accountability of these standards, ensuring they are of a high quality and developed in the interests of customers and a competitive ecosystem.

Requirements

78. Amendment (a) allows for an interface body to be established to play a technical coordination role to facilitate the secure, efficient and standardised sharing of customer data.

79. Amendment (b) provides powers to the SoS or the Treasury to make regulations in relation to an interface body. These regulations may include provisions about how such bodies must carry out certain functions, including the development of interface standards and arrangements for the scheme and the monitoring of such.

Regulations may also include requirements in relation to the objectives, governance, and transparency obligations of an interface body.

80. Amendment (c) allows for the Treasury to sub-delegate to the FCA powers to make rules and issue directions in respect of the interface body for schemes in financial services, those persons required to set it up and those required to use (or who are otherwise using) specified facilities, services and / or arrangements such as Application Programming Interfaces (APIs).

81. Amendment (c) is intended to be akin to the rule-making powers the FCA has available to it under the Financial Services and Markets Act 2000, although aimed specifically at financial services Smart Data schemes and subject to additional limitations.

82. It will be for the Secretary of State and the Treasury to use the provisions as necessary to design the envisaged Smart Data scheme. This may include full, or partial use of the powers as amended.

Expected Impacts

83. The preferred Option is Option 1. As Smart Data has the potential to be economy wide, there may not be an established regulator or 'interface body' that covers the scope of every sector where there could be a Smart Data scheme. By allowing the Treasury or the Secretary of State to require the establishment of a new private industry body, or designate an existing one, to take on the role of the interface body, it will allow for consistency between different schemes. It will also reduce the risk of the fragmentation of data sharing which would create difficulties and costs for customers and authorised third parties to access data from various data holders. Reducing this risk, will therefore decrease barriers to entry, encourage innovation, and ultimately increase the benefits to customers and authorised persons.

84. These amendments allow for a degree of flexibility in regulation-making, ensuring regulations can be tailored to specific sectors. This will likely improve the effectiveness of Smart Data schemes and increase the likelihood that each individual scheme leads to net benefits.

85. The additional impacts of including the amendments into the primary legislation are expected to be:

    a. Increasing legislative consistency: increasing the overall benefit by allowing different sectors to use the legislation to design different schemes that have sector specific data standards.

    b. Enabling new types of schemes: an interface body allows for a broader range of Smart Data schemes. This creates new benefits for customers, new opportunities for businesses to innovate but it may create new costs for industry in relation to funding the interface body. However, this cost to industry may be offset as interface bodies could reduce the overall costs to operationalise schemes by allowing alignment on aspects of interface development and central services.

86. As mentioned in the introduction, we expect minimal direct impacts to businesses from the primary legislation alone, due to impacts being presented as broad in the Smart Data Impact Assessment (SDIA).

87. As the specific features of the schemes will be established in secondary legislation, there will be no change in the primary legislation impacts due to the amendments.

88. We do not expect extra estimated costs at scheme level due to the amendments compared to those estimated in the SDIA because the impacts estimated in the SDIA were based on Open Banking. As part of Open Banking, a private entity (Open Banking Limited) was created to be the interface body. As the SDIA does not isolate specific costs and instead re-scales them to fit the telecommunication sector, the cost of creating an interface body is already included in the impacts.

89. Since the SDIA was published, the Treasury has committed to using the Smart Data powers in Part 3 of the DPDI Bill to provide a long-term regulatory framework for Open Banking.[8] However there will be no meaningful changes to impacts as estimated in the SDIA as the sum of costs are unlikely to change and instead could be spread amongst more participants.

Summary of Costs

90. As stated in the original SDIA, costs to operationalise the schemes and to ensure adequate regulatory oversight will fall on the sector regulator, or any other administrator, who will be named in the secondary regulations as responsible for specific roles. By including the amendments in the legislation, these costs will either fall on either an existing public or private body or on a new private body established in accordance with regulations made by the Secretary of State or the Treasury to become the interface body.

91. Resources to cover the costs (set up and ongoing costs) incurred by the interface body will not come from central government and instead will be recouped from industry in accordance with regulations, possibly through levies, charges or another funding model.

Summary of Benefits

92. The amendments allow the Secretary of State or the Treasury to establish an interface body to provide technical coordination within Smart Data schemes. This allows for the data standards to be coordinated efficiently to fit the needs of the sector and allows for easier innovation and lower barriers to entry for authorised third party providers, creating higher quality schemes. This then allows for a wider range of services, allowing customers to use their data more effectively to better navigate the market.

93. Overall, amendments in this group are therefore likely to lead to an expansion of the benefits described in detail in the SDIA. This because these benefits primarily stem

[8] **Economic Secretary to the Treasury speech**, HM Treasury, 2023

from Smart Data enabling services, which are likely to be improved and expanded in higher quality Smart Data schemes.

Net Impacts

94. These amendments broaden the range of options available to regulation makers, meaning that they are better equipped to oversee development of data standards that meet the requirements of the specific market. This will mean that regulations may be used in a broader range of markets, leading to an increased number of schemes, or the amendments may facilitate broader or better designed schemes.

95. Ultimately, it will be for the Secretary of State and the Treasury to decide whether and what type of interface body is needed when designing a Smart Data scheme. There is a small risk that allowing for a broader range of Smart Data delivery models leads to regulation makers selecting a less efficient model. This risk is mitigated by the requirement to undertake scheme specific impacts analysis at the point of designing the secondary legislation that enables Smart Data schemes[9].

96. Overall, there is therefore a strong likelihood that the amendments allow for an expansion of net benefits, with only a limited risk of the amendments allowing schemes with net disbenefits compared to the counterfactual.

ii) Amendment Group 2 – 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.

Rationale

97. The government’s intention for Smart Data implementation is to develop schemes that can be interoperable. The primary legislation needs to provide a framework to allow for bespoke regulations in specific sectors, to facilitate the appropriate use cases that will address the relevant customer harms.

98. Amendments in this group expands the definition of ‘customer data’ to clarify that transactions between customers and third parties are within scope, including financial transaction data, as is currently the case in Open Banking

99. Amendments in this group clarifies that Smart Data action initiation applies to all actions a customer can carry out and not just actions that are underpinned by an express customer right. This removes the risk that some ‘actions’ a customer is entitled to make may not be covered by the previous scope of ‘customer rights’.

[9] For example, as set out in the Better Regulation Framework and Green Book https://www.gov.uk/government/publications/better-regulation-framework , https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-governent/the-green-book-2020

Ultimately, this enables a broader range of future schemes, and by extension, a broader range of use cases for authorised persons to develop.

100. Both amendments promote competition to combat market power and information asymmetries. Enabling access to a wider range of information to customers under ‘customer data’, allows customers to understand more about their behaviour and consumption patterns. This allows customers to better navigate the market and find a deal that is better suited to them.

101. More informed decisions may lead to increased customer switching between service providers, and therefore more competition between firms on factors such as price and service quality. This encourages lower prices and greater transparency on prices between firms so it is easier for customers to see when they could be getting a better deal with a different company. Amendments in this group allow authorised persons to create innovative services that involve actions on the customers behalf. This can make markets easier for customers to engage with, increasing their ability to make informed decisions in line with their own preferences, wants and needs. These actions may include authorised persons offering more efficient / faster switching methods or offering more efficient forms of payment.

Requirements

102. Amendments in this group expand upon the current definition of ‘customer data’ in the legislation to clarify the range of information that ‘customer data’ relates to. The legislation originally referred to customer data as data relating to transactions between a customer and a trader. This has been widened to expressly include information relating to goods, services and digital content provided to the customer, or at the customer’s request, by the trader. This includes prices or other terms on how customers are supplied with a good, service, or digital content by a trader. This is to ensure that relevant customer financial data beyond transactions between the customer and an account service provider (for example information about payments the customer has made to third parties) is within scope of the ‘customer data’ definition, as is currently the case in Open Banking.

103. Amendments in this group clarify the provision of action initiation, or ‘write access’, that allows an authorised third party to carry out actions on a customer’s behalf. This amendment clarifies that the Smart Data action initiation applies to all actions a customer can carry out and not just actions that are provided for by a right.

Expected Impacts

104. Smart Data has the potential to be economy wide and therefore the powers included in the Bill need to be broad enough to allow effective schemes in all sectors. These amendments do this, by expanding the definition of ‘customer data’ to include the relevant financial transaction data between the customer and third parties and clarifying that the authorised third party can carry out actions that the customer can take for them.

105. The additional impacts of including the amendments into the primary legislation compared to the ‘do nothing’ scenario is expected to be:

    a. Increasing legislative consistency: Now that the description of ‘customer data’ has been expanded and the authorised person can act on the customer's behalf, more policies can use the legislation. Therefore, Smart Data schemes that would have originally had to occur under different legislation, if the definition was not expanded, can now use this legislation. This increases the overall benefit through more consistent schemes.

    b. Enabling new schemes: Broadening the legislation will allow a wider range of data to be used in Smart Data schemes, which also enables wider use cases that could benefit customers.

    c. Broadening scheme scope: By expanding the definition of ‘customer data’ and clarifying how an authorised person can act on a customer’s behalf it allows schemes to have more functions and partake in cross-sector innovation that may not have been possible before.

106. The impact analysis presented in the SDIA was broad and illustrative as there is uncertainty about the specific features of the schemes that will be established in secondary legislation. As a result, there will be no change in these estimated impacts due to the amendments. This is because, although we expect small impacts from these amendments, they are likely too specific to be captured in the modelling undertaken in the SDIA. Instead, we expect these impacts to be considered at the secondary legislation stage where the modelling will be more specific.

Costs

107. Expanding the definition of customer data and how an authorised person can act on a customer’s behalf allows for a broader range of data and services. As the original illustrative estimates were left high level to account for variation of services delivered by authorised persons and different data requirements across sectors, the amendments do not have an extra impact on the estimated costs.

Benefits

108. It is likely the amendments will create benefits. The amendments allow for a wider range of data and a wider range of services, allowing the customer to use an authorised person to access their data and navigate the market.

109. However, as the original illustrative estimates were left high level to account for variation of services delivered by authorised persons and different varieties of data sets across sectors, we do not predict the expected impacts of the amendments to be different to those already in the SDIA.

Net Impacts

110. These amendments broaden the range of options available to regulation makers, meaning that they are better equipped to design regulations that meet the requirements of the specific market. This will mean that regulations may be used in

a broader range of markets, leading to an increased number of schemes, or the amendments may facilitate broader or better designed schemes.

111. Ultimately, it will be for the Secretary of State and the Treasury to decide which data to include in scope when designing a Smart Data scheme. There is a small risk that explicitly allowing for a broader range of design options to be used in Smart Data schemes leads to greater uncertainty to regulation makers and increases the chance that one or more schemes are established with less efficient features. This risk is mitigated by the requirement to undertake scheme specific impacts analysis at the point of designing the secondary legislation that enables Smart Data schemes.

112. Overall, there is therefore a strong likelihood that the amendments allow for an expansion of net benefits, with only a limited risk of the amendments allowing schemes with net disbenefits compared to the counterfactual.

iii) Amendment group 3 – 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

Rationale

113. Currently, the Bill has provisions that allow regulation makers to appoint an ‘enforcer’ of a Smart Data scheme, who can be given powers to monitor compliance and set fines, financial penalties, and fees. However, the current legislation does not explicitly provide for the ability for regulation makers to give investigative or monitoring powers to the enforcer to aid in this monitoring role. The current powers also do not provide for the ability of regulation makers to explicitly provide the enforcer with information gathering powers.

114. Amendments in this group, explicitly allow regulation makers to give powers to the enforcer to require the provision of documents and compel individuals to answer questions in relation to its enforcement role. This will allow for more effective enforcement of the Smart Data regime, as enforcers will have further explicit methods for monitoring compliance with the regulations.

115. Effective enforcement is important for a Smart Data scheme to function, and so that all participants are complying effectively with the regulations. These amendments therefore enhance the ability for Smart Data schemes to effectively address each of the market failures identified earlier in this note. Specifically, these amendments also address an information asymmetry whereby participants have more information about their actions than the enforcer by requiring participants to share information with the enforcer.

116. This group of amendments also clarifies that fines, financial penalties and fees must be set out in regulations, but these regulations do not have to refer to a specific

maximum value. Instead, the regulation can refer to a published index, such as the consumer price index, or other methods commonly used in other legislation to identify the maximum fee.

117. This allows the maximum fines, penalties and charges set out in regulations to be updated in a consistent manner, without the need for further regulations. This allows for the maximum fine, financial penalty, and charge to be updated over time without the regulations themselves being updated. This increases the effectiveness of fines, financial penalties, and charges as key components of an enforcement mechanism by ensuring that they continue to be set at the right level and updated over time in line with economic and market condition changes. These amendments therefore enhance the ability for Smart Data schemes to effectively address each of the market failures identified earlier in this note.

118. Finally, this group of amendments allow regulation makers to incorporate existing data sharing requirements in other legislation within Smart Data regulations. This allows for consistent regulation within each sector, by allowing regulation makers to design regulations and enforcement arrangements which are consistent with the wider regulatory framework.

119. This allows regulation makers to create a more streamlined, and consistent regulatory environment in each sector. This is likely to increase the effectiveness of Smart Data schemes and their enforcement and therefore increase their ability to address each of the market failures identified earlier in this note.

Requirements

120. This group of amendments enables regulation makers to expand the monitoring and compliance powers that regulation makers can give to the ‘enforcer’ of the Smart Data scheme. They specify that regulations can make provision for the monitoring of compliance by an enforcer and clarify that an enforcer can require the provision of documents and compel individuals to answer questions in interviews in relation to this.

121. This group of amendments also clarifies that fines, financial penalties, and charges must be set out in regulations, but these regulations do not have to refer to a specific maximum value. Instead, the regulation can refer to a published index, such as the consumer price index, or other methods commonly used in other legislation to identify the maximum fee.

122. Finally, this group of amendments allow regulation makers to incorporate existing data sharing requirements in other legislation within Smart Data regulations.

Expected Impacts

123. For Smart Data schemes to be as effective as possible at addressing the market failures identified earlier in this note there needs to be a clear, and robust enforcement procedure. This group of amendments clarify these procedures and give explicit routes for enforcers to gather information necessary to monitor

compliance with the regulations and to update the fines, penalties and charges that act as incentives for compliance with the regulations.

124. Overall, this qualitative analysis identifies that there is a strong likelihood that the amendments allow for an expansion of net benefits, with only a limited risk of the amendments allowing schemes with net disbenefits compared to the counterfactual. The amendments explicitly allow for a more effective system of compliance, and therefore are likely to increase the likelihood of individual schemes enabled by the broader Smart Data clauses to realise the potential benefits. This is because these benefits are largely reliant on compliance by individual participants, which would be ensured by an effective enforcement arrangement. There is a small chance that these amendments lead to disbenefits in individual schemes, for example if they lead to less efficient enforcement mechanisms but this is mitigated strongly by the requirement for departments to undertake scheme specific impacts analysis at the point of designing the secondary legislation that enables Smart Data schemes.

125. We expect minimal direct impacts to business from the primary legislation alone. Whilst it enables the government to mandate the participation of data holders and to establish enforcement procedures, the secondary legislation will make use of these powers. There is a small chance that amendments in this group increase the signalling impacts associated with the primary legislation, described in earlier sections. By explicitly allowing for a clearer enforcement mechanism, businesses may respond more strongly to the signal caused by primary legislation.

126. Nevertheless, by explicitly allowing for a clearer enforcement mechanism this group of amendments is likely to increase the effectiveness of individual Smart Data schemes. Specifically, the additional impacts of including the amendments in the primary legislation compared to the ‘do nothing’ scenario is expected to be:

    a. Enabling more clearly enforced schemes: by explicitly enabling a broader range of enforcement tools this group of amendments is likely to increase the effectiveness of enforcements in individual Smart Data schemes. This will increase the benefits associated with these schemes, which are reliant on compliance by participants. This will come at a cost for enforcers who will have to undertake this enforcement and participants who will have to comply.

    b. Regulatory consistency: by allowing regulation makers to incorporate existing data sharing requirements within Smart Data requirements this will lead to a clearer, and more consistent regulatory environment for participants. This is likely to reduce the familiarisation and administrative costs associated with Smart Data schemes, by aligning Smart Data regulation with existing requirements where possible.

Costs

127. Amendments in this group increase the range of enforcement mechanisms available to enforcers. These are likely to come at an administrative cost to enforcers, as there will be some costs associated with requesting documents and attendance at meetings by participants and interpreting this information.

128. In addition, there is likely to be a cost to participant business in a Smart Data scheme as they would have to provide this information and attend these meetings.

129. The change in the way that the maximum financial penalties, fines, and fees can be specified in regulation, is likely to have an impact on the value of the financial penalties, fines and fees paid by participants to the body specified in regulations, such as the enforcer, that receives these payments. This represents a transfer from participant businesses to other bodies specified in Smart Data regulations, such as the enforcer, which may either be a public or private sector body.

130. It is not possible or appropriate to quantify or monetise these costs and transfers as they will depend on how the powers are used by regulation makers and the structure of the specific sector or market in question. The SDIA discusses the best available evidence on the scope of the costs that would be associated with enforcement of Smart Data schemes.

Benefits

131. The primary benefit of this group of amendments is to increase the effectiveness of monitoring, compliance and ultimately enforcement of Smart Data schemes. As Smart Data schemes require participation to provide benefits this will increase the likelihood that Smart Data schemes achieve each of the benefits identified and discussed in detail in the SDIA.

132. 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. This will reduce the administrative cost associated with finding alternative solutions to undertaking a particular task that relied on this coverage and seeking redress if they were harmed by this lack of coverage.

133. In addition, the increased regulatory consistency is likely to decrease the administrative and familiarisation cost for participants who already comply with existing data sharing requirements.

Net Impacts

134. Overall, this qualitative analysis identifies that there is a strong likelihood that the amendments allow for an expansion of net benefits, with only a limited risk of the amendments allowing schemes with net disbenefits compared to the counterfactual.

135. The amendments explicitly allow for a more effective system of compliance, and therefore are likely to increase the likelihood of individual schemes enabled by the broader Smart Data clauses to realise the potential benefits which are reliant on compliance by individual participants. There is a small chance that these amendments lead to disbenefits in individual schemes, for example if they lead to less efficient enforcement mechanisms, but this is mitigated strongly by the requirement for departments to undertake scheme specific impacts analysis at the point of designing the secondary legislation that enables Smart Data schemes.

iv) Amendment group 4 – 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

Rationale

136. Currently, the Bill provides for the Secretary of State and the Treasury to make provisions in regulations, to require data holders to publish business data or to provide business data on request to a customer of a trader, or to a specified third-party recipient. Regulations may require this business data to be provided using specified facilities or services, such as APIs.

137. However, in some markets business data sets may be held by a large number of small and technologically underdeveloped data holders, such as micro businesses, which do not have access to funding to upgrade their IT systems[10]. This data could be beneficially accessed if the Smart Data scheme could specify a single third party (being a public body or an entity appointed by a public body) for data holders to provide the business data to. A single third party, likely appointed by the government or a regulator, would be tasked with collecting the data from the data holders, likely through a range of methods depending on the business data sets. The specified third party could then be required to aggregate and clean the business data, so that it could be published and/or provided to other third parties upon request, likely via an API or similar. Essentially, the specified third party would act as a middleman between the data holders and the typical ATPs looking to utilise the business data sets.

138. This single third party could unlock data that could not ordinarily be supplied in a standard format by data holders. Where data is not supplied in a standard format (as APIs enable), ATPs, who are generally private sector businesses, are less likely to be incentivised to make use of the available business data sets. In short, ATPs may require a range of APIs, and other methods of receiving the data, to access the full range of data being shared. This would be costly, inefficient and would ultimately lead to this data not being available to ATPs within some Smart Data schemes. Where ATPs are not accessing the business data, they will be unable to provide innovative services for customers and customers will not be receiving the full benefits associated with Smart Data schemes.

139. There is therefore a rationale to unlock these benefits by amending the existing legislation so that this model of Smart Data delivery is more explicitly allowed for.

140. For schemes where there are a diverse range of dispersed, and potentially technologically underdeveloped data holders each of the following market failures is

[10] This problem is less likely to occur for customer data, as smaller, less technologically developed businesses are less likely to gather this data at all.

better addressed by a Smart Data delivery model that uses a specified third party to collate data from data holders. Specifically:

a. Information failure and information asymmetry: for markets where some of the data is held by small, technologically underdeveloped data holders there may be insufficient private incentive for ATPs to invest in gathering and collating this data. This means that customers would not have information easily available on all the potential businesses in the market, and the information failures and asymmetries would partially persist.

b. Network Failure: similarly, where there is insufficient private incentive for ATPs to gather and collate information from all data holders relevant for the market then this reduces the potential positive impacts of setting common standards across the market.

c. Market Power: it is likely that it is the smaller or newer entrants to a market that ATPs will be least incentivised to collate information from. There is a large initial set up cost to set up the data infrastructure to collate data from each data holder. This means that it will be more profitable for the ATP to collate data from larger firms, which will lead to more sales by the ATP collator, and more established firms that may be more likely to stay in the market for a longer time. In these instances, Smart Data schemes may counterintuitively decrease competition, as they only enable services when a customer is already using a larger, older firm at the expense of new entrants or smaller players. Using a specified data collator, as enabled explicitly by these amendments addresses this potential risk to competition.

141. There may also be whole markets where the market failures identified apply but all or many of the data holders are small and not technologically developed enough to easily provide data in a specified format to ATPs. This means that ATPs, who are generally private sector entities, would not be sufficiently incentivised to collate the data. In these instances, there is a rationale for a Smart Data scheme, but it could only be developed through the model enabled by these amendments. There is therefore a rationale to include these amendments to enable these schemes and to address the identified market failures in these markets.

Requirements

142. Amendments included in this section:

d. 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.

e. Further powers that regulation makers can mandate that this specified entity must publish or make available this business data upon request.

f. Provisions for the Secretary of State and the Treasury to make regulations to mandate that the specified entity can be funded via levies and charges from industry.

g. Powers that 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.

143. These amendments explicitly allow for an increased range of models for Smart Data delivery, where business data can be securely shared directly from data holders to a specified third party. In this model, this specified third party collates, and makes this data available to ATPs, for example via an API, or published in a specified format. ATPs offering services can then access this data through the specified third party rather than through intermediary ATPs. The specified third party that collates this data in this model can either be a private sector entity, such as a consortium of business, or a public sector body, such as a regulator.

144. Amendment (d) further gives regulation makers the power for the specified third party to participate or comply with specific data standards or arrangements. This is to ensure that there is a common understanding of the format that the data is collected, so that regulation makers can ensure interoperability across schemes, and so that ATPs know in advance the structure of the data.

145. Amendments (e) and (f) clarify that regulation makers can use the existing funding mechanisms in the Bill to fund the activities of the specified entity. In particular, they clarify that the specified entity can be funded via levies recouped from industry, and that financial assistance may be provided for the purposes of meeting expenses incurred under the regulations. This ensures regulation makers can design schemes to be ‘self-funding’ and reduce reliance on public money, in line with the principles underpinning the regulation-making powers in Part 3.

146. Importantly, the Smart Data powers do not prescribe a particular delivery model. The specific delivery model will be chosen by the Secretary of State and the Treasury when they use secondary legislation to create a Smart Data scheme. The amendments expand the range of models explicitly allowed for by the Bill, but the option will still be available to use any other delivery model enabled by the Smart Data clauses as they currently stand.

Expected Impacts

147. This option explicitly allows for a broader range of Smart Data delivery models, where business data can be collated and made available through a specified third party rather than through market driven ATPs. This option therefore allows for Smart Data schemes to be implemented more comprehensively, and effectively in instances where the business data involved means that there is not sufficient market incentive for private sector ATPs to collect this data without intervention.

148. Overall, this qualitative analysis identifies that there is a strong likelihood that the amendments allow for an expansion of net benefits, with only a limited risk of the amendments allowing schemes with net disbenefits compared to the counterfactual. The amendments explicitly allow for a broader range of Smart Data delivery models and therefore gives more options for regulation makers when designing regulations to establish specific Smart Data schemes. This leads to a larger potential for net

beneficial regulation design choices, increasing the quality, breadth and number of net-beneficial Smart Data schemes that may be enabled through the Smart Data clauses. There are a narrow range of instances where explicitly allowing a broader range of Smart Data delivery models may decrease the net benefits, but this risk is mitigated strongly by the requirement for departments to undertake scheme specific impacts analysis at the point of designing the secondary legislation that enables Smart Data schemes.

149. We expect minimal direct impacts to businesses from the primary legislation alone. Whilst it enables the government to mandate the participation of data holders, the secondary legislation will make use of the power to mandate. The primary legislation could potentially have a signalling impact if businesses respond in advance of secondary legislation. For example, by preparing for data sharing upgrading technology, which would incur a cost to the business.

150. Nevertheless, by explicitly allowing a broader range of delivery models these amendments are likely to accelerate and increase the range of Smart Data schemes available. They are also likely to lead to a change of impacts for schemes that are set up via secondary legislation using the model that is explicitly allowed for under these amendments. Specifically, the additional impacts of including the amendments into the primary legislation compared to the 'do nothing' scenario is expected to be:

    a. A shift in impacts from private sector ATPs to the appointed entity: for schemes that would have been established under a different model of Smart Data delivery under the 'do nothing' counterfactual but are now set up using the model explicitly allowed by these amendments. In these instances, the costs of collating business data from data holders are transferred from private sector ATPs to the specified third party, which may be a public or private entity. There may also be associated efficiency savings or losses from this transfer of activity.

    b. Enabling new and broader schemes: some schemes or some aspects of some schemes may not have been possible under other models of Smart Data delivery. Expanded the models of Smart Data delivery explicitly allowed in the primary legislation may allow for more, and broader Smart Data schemes that may have been less likely to have been established under the 'do nothing' counterfactual.

Costs and transfers

151. There will be different cost impacts associated with these amendments, depending on whether they are used by regulation makers to design new and broader schemes or whether they are used to establish schemes that would have been created under a different Smart Data delivery model in the counterfactual.

152. Where the amendments create new or broader schemes there will be an expansion of each of the costs associated with using the Smart Data powers. These are highlighted in full in the SDIA.

153. For schemes that are established under the model that is explicitly allowed by these amendments there are two potential costs and transfers compared to schemes established using a different model of Smart Data delivery:

    a. The costs of collating business data are transferred from ATPs, who are generally smaller private sector businesses, to the specified third party. This specified third party may be a private sector or public sector entity, so initially this transfer may either be between different businesses or be a transfer of costs from business to government. As stated in the original SDIA, it is likely that costs incurred by the government will be recouped from data holder businesses through levies and charges. Therefore, after the initial cost outlay the overall impact will be a transfer of costs from ATPs who are typically smaller businesses to the larger data holders that typically pay levies in Smart Data schemes. For smaller data holders that are less technically capable this model may ease data burdens, as it transfers the cost of collating this data from these data holders to the collation body.

    b. There may be efficiency losses or gains from collating business data using a specified third party rather than ATPs, who are generally private sector businesses. On the one hand, private sector ATPs may be driven to innovate, and deliver more efficient services by the forces of market competition. On the other hand, there is a large initial, fixed cost for collating data and a small incremental cost incurred each time this data is made available to others. This means that there is a 'natural monopoly' in the market for data collation, and in both models, there is likely to be only one provider in the long term. In this instance, the specified third party may be less incentivised to use this monopoly power to increase the price that ATPs pay for access to data than a private sector monopoly ATP. As a result, there may be increased data access and Smart Data benefits under the model with a specified third party.

Benefits

154. The benefits associated with these amendments will be different depending on whether the amendments enable schemes that would have happened anyway through another model of Smart Data delivery or whether they enable additional or expanded schemes.

155. Where the amendments create new or broader schemes there will be an expansion of each of the costs associated with using the Smart Data powers. These costs are highlighted in full in the SDIA.

156. As mentioned in previous sections where the amendments enable Smart Data schemes that would have been delivered via a different Smart Data model, there is a transfer of activity from the private sector to the specified third party. Depending on the market where the Smart Data scheme in question is being established there may or may not be efficiency savings associated with this model compared to different Smart Data models. This may have knock-on impacts in terms of the price and quality of business data that is offered by the collator of business data to the ATPs that deliver Smart Data enabled services. This may have an impact on the number

and quality of services available and therefore the total benefits of the Smart Data scheme itself.

Net Impacts

157. These amendments broaden the range of options available to regulation makers, meaning that they are better equipped to design regulations that meet the requirements of the specific market. This will mean that regulations may be used in a broader range of markets, leading to an increased number of schemes, or the amendments may facilitate broader or better designed schemes.

158. Ultimately, it will be for the Secretary of State and the Treasury to decide which model to use when designing a Smart Data scheme. There is a small risk that explicitly allowing for a broader range of Smart Data models leads to greater uncertainty to regulation makers and increases the chance that one or more schemes are established under a less efficient model. This risk is mitigated by the requirement to undertake scheme specific impacts analysis at the point of designing the secondary legislation that enables Smart Data schemes.

159. Overall, there is therefore a strong likelihood that the amendments allow for an expansion of net benefits, with only a limited risk of the amendments allowing schemes with net disbenefits compared to the counterfactual.

h) Reporting periods for PEC Regulation breaches

This summary has been provided by DSIT.

Rationale

160. 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”.

161. 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’. They are also required to keep a log of all those breaches. There is currently no threshold for how serious the breach must be – all breaches must be notified. This is seen to be an additional burden on UK businesses who experience low-impact breaches, who currently have to report these to the ICO within 24 hours. Failure to do so incurs a fixed monetary penalty notice (MPN) under PEC Regulation 5C. However, there is provision in the legislation to allow businesses to notify the ICO within 24 hours and then submit a full report within a further 72 hours.

162. In February 2023, the ICO published a statement advising that it no longer planned to issue fines to service providers for reporting personal data breaches, as required under Reg 5A, after the 24-hour deadline, as long as the reports are still received

within 72 hours. There is an exception for high-risk incidents which still need to be reported within 24 hours.

163. The ICO changed their approach as the vast majority of received reports were low-risk incidents and communications providers advised that the 24-hour reporting timescale resulted in significant burdens. Therefore, by extending this timescale to 72 hours, the ICO felt it would be less burdensome for service providers to gather the necessary evidence required.

Requirements

164. By amending regulation 611/2013 which sets out the data breach reporting rules for PEC Regulation 5A and extending the reporting period for low-impact personal data breaches under PEC Regulation 5A from 24 to 72 hours, this will reduce the burden of reporting breaches for UK businesses.

Expected Impacts

165. 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[11] 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.[12] 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[13] and short-term direct cost[14] for the most disruptive breach or attack for all businesses is £630. However, we are looking specifically at 'low impact' breaches, so we assume that £630 would be the upper limit of the cost of reporting for these firms.

166. As a result of this amendment, we expect that UK businesses who experience low-impact 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.

167. It is expected that the amendment 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.

168. Whilst this amendment may make the process of reporting breaches more achievable for businesses there may be some providers who may not wish to take

[11] ICO (2022). Data security incident trends. https://ico.org.uk/action-weve-taken/data-security-incident-trends/

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

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

[14] 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.

the regulatory risk to report beyond the current statutory timescales, limiting the potential impact of the reform. We are working to provide robust estimates of these potential cost savings, and these will be presented in the enactment Impact Assessment.

i) National Underground Asset Register (NUAR)

This summary has been provided by the Geospatial Commission who have also produced a standalone Impact Assessment for this reform. More detail and information can be found in the IA published alongside this note.

Rationale

169. A significant proportion of UK utility, building and transport infrastructure is buried underground, including over 4 million kilometres of pipes, electricity and telecoms cables, and sewers. It is estimated that a hole is dug every seven seconds to install, operate, maintain and repair buried pipes and cables - assets that are critical for keeping the water running, gas and electricity flowing, and our telecommunications lines connected. This busy and usually unseen environment suffers from an estimated 60,000[15] accidental strikes per year, leading to injury, project delays, and disruption to traffic and local economies, resulting in costs to the UK economy of £2.4bn per year.[16]

170. Existing legislation[17] outlines obligations on asset owners to:

    1. Record all underground assets that belongs to them when undertaking works in and along the street.

    2. Make these records available for inspection for free (at a cost to the asset owner) to certain companies and agencies (including some exceptions to sharing).

171. There are no services in England, Wales or Northern Ireland which provide comprehensive access to data in a standardised, immediate and digitally interactive format. While there are a small number of businesses who provide helpful services in connecting data requestors with asset owners and providing some data to requestors, these services are incomplete, and often share data in numerous documents in a range of formats, and to various timescales.

[15] A widely quoted industry statistic, found in reputable industry publications. See: (1) https://www.ceca.co.uk/wp-content/uploads/legacy-media/172382/ceca-communicates-91-may-2015.pdf & (2) USAG 2014 Strike Damages Report: https://www.utilitystrikeavoidancegroup.org/reports/.

[16] https://www.gov.uk/government/publications/national-underground-asset-register-unlocking-value-for-industry-and-the-wider-economy/national-underground-asset-register-nuar-economic-case-summary

[17] Relevant legislation to date includes the New Roads and Street Works Act (NRSWA) 1991 for England, Wales and Scotland, the subsequent The Street Works (Records) (England) Regulations 2002, and The Street Works (Northern Ireland) Order 1995 for Northern Ireland.

172. There are a limited number of existing search providers that charge asset owners to service this complexity, by managing queries regarding underground assets in partnership or on behalf of asset owners. These services are incomplete and do not provide access to the data in a standardised, immediate and digitally interactive format.

173. Despite the value that improved access to underground asset data could bring, there is a clear need for government intervention as the market has failed to overcome commercial, security and other barriers. These barriers must be overcome to take full advantage of the benefits that could be available through effective use of data and data sharing via a centralised platform with data from all asset owners. The key market failures and other barriers to reaching a viable solution are economic externalities, coordination failure, national security concerns, commercial sensitivities, differing appetites for liability risk between businesses and set-up and ongoing costs.

Requirements

174. The Geospatial Commission (part of the Department for Science, Innovation & Technology) is building a digital map of underground pipes and cables that will revolutionise the way we install, maintain, operate and repair our buried infrastructure - the National Underground Asset Register (NUAR).

175. NUAR 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 are as follows:

    a. Increased efficiency of data sharing;

    b. Reduced asset strikes;

    c. Reduced disruptions for citizens and businesses; and

    d. Expedited delivery of projects like new roads, new houses and broadband roll-out.

176. Current legislation does not compel the efficient sharing of these records in a uniform way making it insufficient to meet policy objectives.

177. New primary legislation is therefore required for NUAR to be fully operational to meet these objectives.

178. The powers sought are described in detail below:

    a. **Data sharing requirements** - requiring asset owners to share their data on the NUAR Platform in a prescribed way, giving workers access to complete and comprehensive data from all asset owners across England, Wales and Northern Ireland;

b. **Charging** - ensuring the service is sustainable in the long-run by establishing a charging regime that is limited to cost recovery and proportionate to those who will benefit most, resulting in no ongoing cost to the taxpayer;

c. **Enforcement** - enabling enforcement mechanisms to be put in place to promote data sharing compliance and payment of fees;

d. **Delegation of running NUAR** - ensuring that the NUAR service is provided by the public body(ies) best positioned to run and manage them.

e. **Licensed access** - enabling the exploration of licensed access to NUAR data to support other use cases beyond excavation planning and safe digging, and by a wider pool of end users.

f. **Spending powers** – giving the Secretary of State authority to use public funds where necessary to achieve government outcomes related to NUAR (exercised in line with the wider spending framework set by HM Treasury).

Expected Impacts

179. Figures shown here are in 2019 prices discounted over 10 years to 2020 present value, in line with RPC guidance.

180. NUAR will reduce the number of utility strikes and improve data sharing and on-site efficiency for utility asset management, resulting in industry and public sector cost savings estimated to deliver £420m[18] per annum of economic growth. Other indirect benefits such as reduced traffic delays and disruption, programme overruns, costs to local businesses and costs to local highways from closing/redirecting traffic, as well as improved worker safety. It also underpins the government's priority to get the economy growing; expediting projects like new roads, new houses and broadband roll-out.

181. Costs associated with the NUAR include transition costs such as data transformation, data vectorisation and familiarisation costs (this includes for both Asset Owners and Data Consumers), and ongoing costs such as continually adhering to new legislative requirements and implementing organisational administrative changes. These costs are expected to total £16.7m[19] per annum and accrue both in the transition phase and once NUAR is fully operational.

j) Data preservation Notices

[18] Note that the full NUAR Impact Assessment quotes circa **£491m per annum** in the main body of the analysis, as it was initially conducted in a 2021 price base and 2021 present value. To be consistent with the analysis of other DPDI measures, the impacts and costs of NUAR were subsequently converted into 2019 prices and 2020 present value (expressed in the Summary & Evidence tables of the Impact Assessment). These are just alternative ways of expressing the same benefit and cost estimates.

[19] As per previous footnote about price base and present values. When expressed in a 2021 price base and 2021 present value, costs per annum are estimated to be £19.5m.

This summary has been provided by DSIT.

Rationale

182. This amendment is seeking to build on the provisions in the Online Safety Bill, which aim to alleviate challenges facing coroners who seek access to children's data and information from online services to support their investigations into whether social media and other online services activity played a contributing role in their death by suicide. While the Online Safety Bill provisions seek to strengthen coroners' abilities to gather information, the policy intent behind this amendment is to establish a data preservation mechanism to ensure online service companies retain all relevant data that may later be requested by a coroner when carrying out an inquest into a child's death by suspected suicide.

183. In a number of recent high-profile cases, coroners that have requested information as part of their investigation from online service companies about a child's online activities have struggled to access this. One of the challenges reported by coroners and tech companies is that the storage limitation principle, set out in Article 5(1)(e) UK GDPR, prevents companies from keeping personal data for longer than is actually needed. In order to comply, online service companies' routine processes delete this data at regular intervals, and therefore important data may no longer be available when required by coroners as part of an investigation into a child's death.

184. This is particularly the case when a coronial request for information includes third party data. As UK GDPR only applies to 'living persons', storage limitation principles do not apply to deceased children's personal data. Various types of non-personal data, including metadata, which is also important for coroners to access to determine the role of online services and social media in a child's death by suicide (including algorithms that influence what content is shown to children), is also not covered by UK GDPR. This enables online service companies to retain or delete this data as they see fit, and stakeholders have raised concerns that 'bad actors' may use this ambiguity to delete relevant, and potentially incriminating data, if they are made aware of a child's death prior to a coroner issuing a request for this information.

Requirements

185. This amendment is therefore seeking to establish a fast-acting data preservation process that would be initiated as soon as possible, following the event of a child's death (where suicide is suspected) to ensure relevant data is captured and retained by social media companies and online services, before it is erased through routine processes. It would enable Ofcom, following an instruction by a coroner, to issue a data preservation notice to relevant online service companies in instances where are child is suspected to have died by suicide.

186. Our data preservation provision will also provide online services companies with a clear lawful basis for the retention of third-party personal data under Article 6(1)(c) UK GDPR.

Expected Impacts

187. The ONS reports that during 2021, 14 suicides were reported across the 10- 14 age bracket and 215 deaths in the 15-19 bracket. Of these cases, not all would require the power to be used by Ofcom and of the proportion in which it is, we would expect compliance with the reform to be high and therefore the impact to the Justice system to be zero.

188. We estimate that the addition of this measure could result in minor additional costs for companies that are required to store data that previously would have been deleted. The scale of this cost will depend on the size of the business, the storage method used and how often they update their databases. The coroners' Courts Support Service states that on average an inquest will take 6 to 9 months to complete and at a firm level this means that data storage costs would increase. However, given the scale of operations and the high number of subscribers of the social media companies that would receive these requests we would expect the maximum costs of retaining this data to be minimal compared to their total data storage costs.

189. In line with the changes proposed in the Online Safety Bill this additional measure could also increase resourcing costs on Ofcom, however we would not expect this to be above those estimated in the Online Safety Bill Impact Assessment for an information request. Alongside additional costs to businesses the measure is expected to increase the success rate for coroners gaining access to relevant information on deceased children from platforms. This could have cost savings for coroners, as well as wellbeing benefits for the families of deceased children. It has not been possible to monetise these benefits at this stage. We will look into these costs in more detail in the Enactment Impact Assessment.

k) Exemption for Archives from further processing rules

This summary has been provided by DSIT.

Rationale

190. Clause 6 in the DPDI bill inserts the new Article 8A into 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.

191. 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.

192. 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.

193. 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 (and 8A(2) of the DPDI Bill), 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).

194. 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 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.

195. The Bill 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 Bill contains a power for the Secretary of State to add to this list.

196. The provisions in the Bill 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.

197. 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.

198. Our provisions in the new Article 8A make clear that archiving (alongside research purposes or compatibility) is not exempt from the prohibition on re-using data originally collected on consent.

199. This clarification has caused issues for certain archives, i.e., privately run archives or local charities (examples are outlined below in 'extent of gap' section) who rely on donations of material containing personal data from controllers who may have originally collected it on consent. These archives also tend to be less GDPR literate and do not necessarily have the agency to comply with it.

200. The aim for the amendment is therefore to ensure that archiving in the public interest is not obstructed by the new provisions as set out in Article 8A(4) around re-using personal data originally obtained on an individual's consent.

Requirements

201. The amendment 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 amendment 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.

Expected Impacts

202. As a result of this amendment, 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.

203. This amendment 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.

204. By exempting archives from the further processing rules laid out in the bill, 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.

205. 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.[20] 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 amendment.

l) Subject access requests - disproportionate searches

This summary has been provided by the Home Office.

Rationale

206. The current position regarding the level of search that a data controller is expected to undertake in response to a subject access request is that of a "reasonable and proportionate search". This is a position which is adopted by domestic courts in line with the EU law general principle of proportionality (which applied on the basis that the data protection framework had an EU law origin). This expectation is not currently provided on the face of the Data Protection legislation. With the Retained EU Law Act 2023 coming into force, UK courts will no longer be able to rely on general principles of EU law from 1 January 2024, and there is a concern that domestic courts may diverge from the EU law based proportionality principle and from the current position that data controller need only to conduct a reasonable and proportionate search for the information requested by a data subject. As such, DSIT is seeking to codify this position on the face of the Data Protection legislation to maintain the status quo and clarify this position for data controllers. In order to ensure that the principle also continues to apply to subject access requests under Part 3 and Part 4 and to retain consistency across Data Protection legislation, the Home Office is mirroring this provision in both Parts 3 and 4 of the DPA 2018. It should be noted that in Part 4 the principle is not directly EU law derived, but it applies by way of consistent interpretation with comparable provisions in Part 2 and Part 3.

Requirements

207. The proposal will amend Article 15 UK GDPR given that this article provides for rights of access to data subjects. For Parts 3 and 4 of the DPA 2018, the proposal will amend sections 45 and 94 (as these sections relate to rights of access for their

[20] Participation Study (2021-22) DCMS, 2022

relevant parts) to make this requirement clear on the face of the legislation (i.e. a data controller need only to conduct a reasonable and proportionate search for the information requested by a data subject).

Expected Impacts

208. It is expected that there will be minimal, if any, impact upon data 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 data controllers when responding to subject access requests. It will also provide similar assurance to data subjects that data controllers are explicitly required, by legislation, to conduct a consistent level of search when in receipt of an access request from the data subject. These assurances are shown to be in an area of importance to data subjects, as of the rights that focus on protection of personal information, the right to access personal information is deemed to be of greatest importance to the public.[21]

m) DWP data access to reduce benefit fraud

This summary has been provided by DWP who have also produced a standalone Impact Assessment for this reform. More detail and information can be found in the IA published alongside this note.

Rationale

209. In 2022/23, Government lost a total of £8.3bn to welfare fraud and error, a figure that increased during the pandemic and remains high compared to historic levels (2010-2019)[22]. The majority of this loss is claimant fraud; Capital fraud and error, as one example, accounted for £894m of losses in Universal Credit alone[23]. Current legislation relies on claimants to self-report changes of circumstances and the Department has no power to independently verify information received. The Government has committed to take action to tackle this, as outlined in the May 2022 Fraud Plan[24], including taking new powers for Third Parties to share information with DWP to improve the accuracy of payments and reduce key areas of loss, including capital and abroad fraud and error.

210. This loss of taxpayer's money is preventable and could be stopped more effectively with new powers. Banks/building societies and the financial sector know how much capital their customers have, or when people make transactions abroad, and they will always know if those customers are benefit claimants. New powers on Third Party data gathering would enable us to access targeted data at scale to signal if a claimant might be breaching benefit rules, allowing us to detect and prevent fraud proactively. As well as preventing loss to the exchequer and rooting out fraud in the

[21] ICO, Information Rights Strategic Plan: Trust and Confidence, 2021
[22] Fraud and error in the benefits system. Financial Year Ending (FYE) 2023. Link
[23] Ibid.
[24] Fighting Fraud in the Welfare System, 2022, Link

welfare system, this measure is also positive for claimants affected by overpayments caused by error; stopping them receiving more than they are entitled to earlier thus reducing the total amount they must subsequently have to repay through recovery once the overpayment has been detected.

Requirements

211. The Policy objective of DWP is to deliver better public services by enhancing the government's access to information from Third Parties on a larger scale where data is signalling potential fraud and error in the benefit system, improving efficiency and payment accuracy in the benefit system. This measure will deliver better public services by enabling DWP to better detect and prevent fraud and error, ensuring a greater proportion of claims are paid correctly and reducing the burdens on the welfare state associated with overpayments building up and associated debt recoveries.

212. DWP will protect privacy, ensuring appropriate use of the power – only looking at data that is signalling potential benefit fraud and error. DWP will create a system for third parties that is effective, simple, and secure and data will be transferred, received and stored safely.

213. Through primary legislation we aim to set the broad framework for this power, including:

    a. **Definition of data holder:** The type of data holder is likely to evolve over time. Initially, for the purposes of detecting fraud and error, we want the data holder for this measure to be defined as any third party as prescribed by the Secretary of State via secondary regulations.

    b. **Definition of the type of data we will be looking for:** the minimum data to establish identity of the data-matched claimant and the 'relevant data' which signals potential fraud/error i.e., the reason they have been matched. We will ensure we are able to demonstrate compliance with the data-minimisation principle of the General Data Protection Regulation (GDPR).

    c. **The purposes for which we are asking the information:** data request notices will be defined to ensure DWP requests only the data items required for the purpose of identifying specific types of potential fraud and error. The specific type of fraud and error and precise data items to be requested will be detailed in the data request notice to the third party, at the time of request.

    d. **Who is authorised to use this power:** this will set out the authority for DWP to use the power.

    e. **Introduce the new statutory Code of Practice required to support the legislation:** and explain that the detail of Disputes, Appeals and Fines procedures will be included in secondary legislation.

Expected Impacts

214. The proposed measures will directly impact DWP and Third-Party Data holders. Implementation will necessitate the recruitment, reallocation, and training of staff for DWP to build systems and act on the data provided. It is estimated that the department requires current and additional FTE to operate the policy, costing around £370m (including overheads). From 2031/32 staffing costs are estimated to be around £30m per year (including additional non-staff costs). The majority of this is focused on processes DWP currently follow when they have a suspicion of fraud or error.

215. Third-Party Data holders, specifically financial institutions (banks/building societies) are the main affected group by the initial use of this power. There are likely to be implementation and administration costs involved with the setup and delivery.

216. The measure is expected to generate around £500m in Annually Managed Expenditure[25] (AME) savings over the scorecard period (2025/26 to 2028/29), and £500m per year when fully rolled out (2030/31). There will be a phased roll-out of the policy that will affect AME savings in the first few years, but this will allow DWP to scale the work at a sensible rate. While the new powers for DWP to detect fraud and error may deter criminals from attempting to defraud the benefit system, saving the taxpayer money[26]. Claimants will benefit from the measure as 'error' will be identified earlier. This will reduce the total amount of debt, ensuring that repayments are manageable. The long-term impacts of the measure may deter serious and organised criminals from targeting the benefit system.

217. All figures are correct at the time of submitting to RPC and are subject to change as per the usual scrutiny process applied to government spending.

[25] See here for a definition of AME: How to understand public sector spending - GOV.UK (www.gov.uk)

[26] It has not been possible to monetise the deterrent effect of the measure.