Title: Data Protection Bill 2017/18 **IA No:** DCMS2017 **RPC Reference No:** RPC-4115(1)-DCMS **Lead department or agency:** Department for Culture, Media and Sport **Other departments or agencies:** Home Office, Ministry of Justice	**Impact Assessment (IA)** **Date:** 14/07/2017 **Stage:** Final **Source of intervention:** European **Type of measure:** Primary legislation **Contact for enquiries:** dataprotectionbill@culture.gov.uk
Summary: Intervention and Options	**RPC Opinion: Fit for purpose**

Cost of Preferred (or more likely) Option

Total Net Present Value	Business Net Present Value	Net cost to business per year (EANDCB in 2014 prices)	One-In, Three-Out	Business Impact Target Status
£6.08m	£4.41m	£-0.51m	In scope	Non-qualifying provision

What is the problem under consideration? Why is government intervention necessary? (7 Lines)

The Data Protection Act 1998, which provides our legal framework for data protection in the UK, is now 20 years old and needs updating to reflect the changes in the way data is generated and used in the digital world. With the increasing volumes of personal data held by businesses and government there is an increasing need to protect it. The General Data Protection Regulation (GDPR) will be directly applicable in the UK from May 2018. There are flexibilities within the GDPR which the UK can take advantage of. The Data Protection Bill will ensure the GDPR benefits the UK by exercising the available derogations in the GDPR that the UK government negotiated to minimise burdens on organisations while protecting individuals' data.

What are the policy objectives and the intended effects? (7 Lines)

The Data Protection Bill will:

- Ensure that the GDPR takes effect in a way that accommodates the UK's unique circumstances and ambitions. The government wants to make use of the flexibilities to align the GDPR with the 1998 Act to allow for a smooth transition between regimes and to minimise burdens on business.
- Ensure that we maintain a single data protection standard for general data in the UK irrespective of whether it is data that falls within EU competence or not.
- Repeal the Data Protection Act 1998 to maintain consistency and clarity in our law.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base) (7 Lines)

Option 1 (Do Nothing): The GDPR, as a directly applicable regulation, would apply in the UK but so too would the 1998 Act, causing legal uncertainty and confusion for both individuals and organisations as they struggle to apply the law effectively. Without exercising some of the available derogations in the GDPR, we would be failing to minimise burdens on organisations.

Option 2 (Preferred Option): Agree and implement the GDPR as negotiated and exercise the derogations in the best interests of the UK.

Will the policy be reviewed? It will be reviewed. If applicable, set review date: Month/Year

Does implementation go beyond minimum EU requirements?		No		
Are any of these organisations in scope?	Micro Yes	Small Yes	Medium Yes	Large Yes
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)		**Traded:** N/A	**Non-traded:** N/A	

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

Signed by the responsible Minister: Date: 30 October 2017

Summary: Analysis & Evidence - Policy Option 1

Description: FULL ECONOMIC ASSESSMENT

Price Base Year 2016	PV Base Year 2016	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: 0.68	**High:** 16.89	**Best Estimate:** 6.08

COSTS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition, Constant Price)	Total Cost (Present Value)
Low	-		-	**-**
High	-		-	**-**
Best Estimate	-		-	**-**

Description and scale of key monetised costs by 'main affected groups' (5 Lines)

No costs were monetised.

Other key non-monetised costs by 'main affected groups' (5 Lines)

There are potential costs to data subjects due to the limitation of rights if they are subject to the processing of their personal data due to public interest grounds. However, due to the lack of data and the complexities involved with valuing personal rights these costs are non-monetised.

BENEFITS (£m)	Total Transition (Constant Price)Years		Average Annual (excl. Transition)	Total Benefit (Present Value)
Low	-		£0.07	**£0.68**
High	-		£1.69	**£16.89**
Best Estimate	-		£0.61	**£6.08**

Description and scale of key monetised benefits by 'main affected groups'

The derogations enable the government to reduce the burdens involved with complying with the GDPR. We were able to monetise the costs-prevented of organisations that process data for specific public interests not having to comply with Subject Access Requests. This is estimated to save the private sector £4.4m and the public sector £1.6m over 10 years. We expect the monetised figures to be underestimates as in most cases where burdens are reduced we have not been able to fully quantify the impacts.

Other key non-monetised benefits by 'main affected groups'

There are a great variety of benefits arising from this Bill that we were not able to monetise. Some examples are: young teenagers can access information society services; organisations that are currently processing special categories of personal data on substantial public interest grounds can continue to do so, e.g. for anti-fraud activity undertaken by the insurance sector; and the balance between data protection rights and freedom of expression are maintained.

Key assumptions/sensitivities/risks	Discount rate (%)	3.5%

We provide sensitivity analysis for impacts to the insurance sector. Insurance premiums and cases of fraud could increase if the government does not intervene to allow the processing of special categories of data and criminal convictions and security related data to continue certain cases. If the evidence available were stronger the monetised benefits of government intervening may have been considerably greater.

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			Score for Business Impact Target (qualifying provisions only) £m:
Costs:	**Benefits:**	**Net:**	
£0	£0.5	£0.5	-2.5

Contents

1: Introduction

The UK is at the forefront of data innovation and the UK data economy continues to grow in both size and significance. Analysis predicts that data will benefit the UK economy by up to £241 billion between 2015 and 2020.[1] In this context, in order to guarantee the UK's continued growth and prosperity, and maximise future trading opportunities, it is crucial that we are able to guarantee effective, unrestricted data flows.

The Data Protection Act 1998, which provide the legal framework for data protection in the UK, is now 20 years old and needs updating to reflect the changes in the way data is generated and used in the digital world. With the increasing volumes of personal data held by businesses and government there is an increasing need to protect it. Data loss can often have distressing repercussions on individuals whilst risking significant reputational damage for the responsible party and the victims lose trust. In more serious cases significant financial loss can arise on both sides and there are risks of other serious harms.

Currently, an individual's personal data is protected in the UK by the Data Protection Act 1998 (the 1998 Act), internationally recognised as a gold standard. We have not, however, been complacent, and have augmented that law over time to reflect developments in the data economy. Most recently, provisions in the Digital Economy Act 2017 established a clear, transparent framework – subject to appropriate safeguards – to enable the public sector to use data to better deliver public services.

The data protection landscape has changed since the 1970s, and individuals' personal data is now subjected to a far increased level of data processing. This increase has been underpinned by the increased processing power of computers and the potential for automated decision-making both in the public and private sectors, and both trends look set to continue.

At the heart of data protection legislation have been certain key rights, such as the right of access to one's own personal data, the right to rectify inaccurate personal data, the right to have personal data deleted under certain circumstances, and the ability to have automated decisions reviewed. Equally the law has placed obligations on organisations to process personal data fairly and lawfully, to specify the purposes for which personal data is processed, and the need to put proper security measures in place.

These elements were set out in the first internationally binding data protection instrument, the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) 1981. The 1995 EU Data Protection Directive (95/46/EC) established a framework for data protection amongst EU Member States. The UK implemented the Directive with the 1998 Act which is the main piece of legislation that governs the protection of personal data in the UK.

[1] CEBR & SAS (2016), The Value of Big Data and the Internet of Things to the UK Economy, https://www.sas.com/content/dam/SAS/en_gb/doc/analystreport/cebr-value-of-big-data.pdf

Since then there have been numerous technological developments, notably the rapid expansion of the internet, the emergence of social media and the growing importance of smart phones. As a result, the European Commission and the Member States concluded that the law should be updated to reflect these changes and to provide more harmonisation across EU Member States.

In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU, which were in large part, intended to give EU citizens back control of their personal data. Negotiation influenced the final official texts of the General Data Protection Regulation (GDPR) which were published on 4 May 2016 in the EU Official Journal and shall apply from 25 May 2018[2]. The final text includes a number of flexibilities that the UK negotiated. The UK Government is keen to make best use of the derogations to bring the GDPR in line with the safeguards and exemptions embedded in the 1998 Act. This will ensure that the burden on business is kept minimal while a high standard of protection of individuals' data is guaranteed.

On 23 June 2016, the EU referendum took place and the people of the United Kingdom voted to leave the European Union. Until exit negotiations are concluded, the UK remains a full member of the European Union and all the rights and obligations of EU membership remain in force. During this period the Government will continue to negotiate, implement and apply EU legislation. The outcome of these negotiations will determine what arrangements apply in relation to EU legislation in future once the UK has left the EU.

Summary of the key changes in the GDPR:

- **Data Protection Impact Assessments (DPIAs**) - A requirement that data controllers or processors must undertake a data protection impact assessment on data processing which presents high risks. DPIAs are similar to Privacy Impact Assessments (PIAs), which are already an important part of the privacy and data protection landscape, and have proved a useful tool to help organisations which process personal data to properly consider and address the privacy risks that this entails. The Information Commissioner offers advice on how data controllers can investigate the risks associated with the personal data they hold by conducting PIAs, and provides a template for the assessment.[3] The current Information Commissioner guidance states that, "by performing a PIA early in a project, an organisation avoids problems being discovered at a later stage, when the costs of making substantial changes will be much greater".[4] Research into the effectiveness of PIAs suggests that they are beneficial because they enable privacy risks to be identified prior to programmes being put in place.[5]

- **Data protection officers (DPOs)** - A requirement that data controllers or processors must designate a data protection officer if they are a public authority or body (except for courts); or their core activities include processing operations which are regular and systematic on a large scale or including processing special categories or personal data and data relating to criminal convictions or offences. The DPO's minimum tasks are (I) to inform and advise the organisation and its

[2] General Data Protection Regulation: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[3] Read more here: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

[4] ICO (2012). *Privacy Impact Assessment Handbook*. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/

[5] Linden Consulting (2007), 'Privacy Impact Assessments: International Study of their Application and Effects'.

employees about their obligations to comply with the GDPR and other data protection laws, (II) to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits and (III) be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.). Employing data protection officers may potentially aid compliance with the legal framework and fewer infringements, leading to fewer data breaches, increase in customer confidence and less risk of enforcement action and sanctions from the Information Commissioner.

- **Demonstrating administrative compliance** - A general obligation on data controllers to maintain documentation and demonstrate compliance with the data protection legislation. This obligation includes maintaining records of certain information relating to processing activity and of all data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in order to demonstrate administrative compliance. Other obligations include obtaining prior authorisation from the supervisory authority for high risk processing as well as other activities; undertaking DPIAs; encouraging data controllers to use data protection officers on a voluntary basis and, implementing data security requirements. The proposal is intended to make it easier for the Information Commissioner to assess whether an organisation is compliant with its obligations under the GDPR.

- **Abolishing notifications** - The GDPR abolishes the current system of personal data processing notifications. Currently data controllers must notify the Information Commissioner of their data processing activities and pay a fee. A general abolition of notification for data controllers reduces the administrative burden of notifying, particularly for those operating cross-border and hence bear the cost of notifications in more than one Member State.

- **Subject access requests (SARs) -** The GDPR requires that data controllers provide the first copy of the personal data undergoing processing free of charge. For any further copies requested by the data subject, the controller may charge a “reasonable fee” based on administrative costs. Data subjects currently have a right to obtain from the data controller a copy of their personal data, together with an explanation of the categories of data being processed, the purposes of such processing, and the categories of third parties to whom the data may be disclosed. The GDPR expands on this by requiring data controllers to respond to SARs with additional information, including details of the period for which the data will be stored (or the criteria used to determine that period) and information about other rights of data subjects.

- **Data portability (DP)** – A new right to data portability, which allows for data subjects to receive the personal data, which they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit them to another data controller. Guidance from the Article 29 Data Protection Working Party explains the application of this right in more detail: [6]
    - Data collected through the tracking and recording of the data subject (such as an app recording heartbeat or technology used to track browsing behaviour) should also be considered as “provided by” him or her even if the data are not actively or consciously transmitted.

[6] Article 29 data Protection Working Party (2016), Guidelines on the right to data portability http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

- The terms “provided by” includes personal data that relate to the data subject activity or result from the observation of an individual’s behaviour but not subsequent analysis of that behaviour.
- The data controller must also include the personal data that are generated by and collected from the activities of users in response to a data portability request such as raw data generated by a smart meter. The purpose of this new right is to empower the data subject and give them more control over the personal data concerning him or her.

The purpose of this new right is to empower the data subject and give them more control over their personal data. Since it allows the direct transmission of personal data from one data controller to another, the right to data portability is seen as an important tool that will support the free flow of personal data and foster competition between controllers. It could also facilitate switching between different service providers.

▪ **Right to erasure** – The GDPR widens the existing ‘right to be forgotten’ (RTBF), including the right for data subjects to obtain erasure of personal data relating to them and the abstention from further dissemination of such data. The principle difference is a strengthening of the law from being applicable only when substantial damage or distress is likely to be caused and a court orders erasure of inaccurate data, to whenever a data subject withdraws their consent for the data to be available, as long as it is no longer necessary or legally required for the grounds on which it was originally collected. Essentially the ‘burden of proof’ for why data should be forgotten/held is transferred from the data subject to the data holder. Similar to the ‘right to data portability’ the aim of this right give back control to an individual over their personal data.

▪ **Data breach notification** – The GDPR adds a requirement for data controllers to notify the supervisory authority (in the UK, the Information Commissioner) of all personal data breaches that are likely to result in a risk to the rights and freedoms of natural persons, without undue delay, and within 72 hours where this is feasible. This requirement increases transparency and the subsequent impacts on data controllers because of this should provide an incentive for data controllers to improve their approach to personal data handling.

▪ **Administrative sanctions** – A new range of administrative sanctions for a wide range of infringements of the Regulation are introduced by the GDPR. Administrative sanctions, such as fines, serve as an important incentive for controllers and processors for compliance. Sanctions also signal data subjects that data protection violations are seriously prosecuted.

Alongside the publication of the proposals, the Commission published its Impact Assessment on the costs and benefits the proposals on Member States in 2012. The Commission estimated that the new regime would bring a net administrative benefit totalling €2.3 billion to the EU each year, mostly due to a harmonised data protection regime.[7] At the time, the Ministry of Justice conducted an impact assessment of the proposals as published on 25 January 2012 on the UK economy and estimated that the new Regulation would have a net cost to business per year of £130m. The impact assessment presented the costs to business and the administration of updating their processes and notifying breaches as well as conducting Data Protection Impact Assessments and

[7] See EU Commission Impact Assessment (2012), http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

employing a DPO. It captured mainly the benefits from the reduction in legal fragmentation and a reduction in data breaches but due to the available data did not provide a quantification of the benefits for data subjects from an increased use of their rights.

DCMS commissioned research to better understand the benefits arising from increased privacy rights for individuals. Secondary evidence and theoretical considerations underline that individuals value their personal data, and valuation increases with the quantity and the sensitivity of the data involved but despite widespread concerns about disclosure, participation in digital markets is pervasive and rising. This study's consumer choice experiment finds that individuals are willing to forego savings of roughly 5% to 10% on weekly spending on shopping, monthly spending on electricity or monthly spending on health insurance in order to have the rights described in the GDPR. This large valuation indicates that individuals are generally happy with the package of rights they have and that they should be compensated significantly for these rights to be taken away. In addition, the existence of maximum fines for non-compliance with the law is highly valued. This high valuation may be interpreted as an implicit insurance against things going wrong. Individuals are willing to pay for the existence of punitive action, which should deter non-compliance. Data rights are seen by consumers as almost as important as brand reputation, past experience and the type of data involved in the decision to give out personal data.

The research also highlighted that consumers are more optimistic about how important data rights are in these decisions than organisations' data protection officers. Benefits to consumers are not necessarily predicted to translate to increased profitability of firms, both for specific benefits and rights and for the package of rights in general. Only 21 of the 250 data protection officers surveyed predict that the package of rights of data portability, erasure and access will increase their company's profitability. Overall, DPOs show a high degree of uncertainty when asked to assess the benefits of GDPR data rights to their organisations.

The value of the GDPR rights from consumers' point of view does not depend on consumers actively using their rights, but that more widespread awareness of the scope of personal data use might make the rights even more valuable in the eyes of consumers. The report concludes that a stronger regulatory framework is likely to mitigate the effect of a localised loss of trust (i.e. a data breach affecting a specific data controller), by reassuring consumers that companies in general are incentivised (through rights that allow user control etc.) to keep data safe, and to react to a loss event by strengthening security.

Strong data protection law and appropriate safeguards enable businesses to operate across international borders. The ability for data, both personal and non-personal, to flow across borders is essential for global trade – particularly trade in services. Indeed, digitally-deliverable services comprise approximately 75 percent of products traded and delivered online.[8] Global flows, as a whole, have increased world GDP by at least 10 percent, with the sum total of around £5 trillion in 2014 alone. Data flows account for around £1.7 trillion of this effect which means that data flows are exerting a larger impact on growth than traditional goods flows.[9]

---

8 United States International Trade Commission (2014), Digital Trade in the U.S. and Global Economies, Part 2, https://www.usitc.gov/publications/332/pub4485.pdf

9 McKinsey Global Institute (2016), Digital globalization: The new era of global flows, http://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digital-globalization-full-report.ashx

The free flow of data, therefore, is essential to the UK forging its own path as an ambitious trading partner. That is why the government will be seeking to ensure that data flows between the UK and the EU, and also between the UK and third countries, remain uninterrupted after the UK's exit from the EU. Cooperation with the UK’s law enforcement and security partners, both in Europe and beyond, will also remain a priority.

2: Problems under Consideration

The Government is determined to ensure that the GDPR best supports UK interests – for citizens and businesses. In view of this, the UK will be exercising a limited number of derogations. These are flexibilities which an EU Member State, including the UK, is entitled to implement by way of national law. Although it is expected that the GDPR will benefit the UK economy, it is anticipated that there could be new administrative and compliance burdens faced by organisations as a result of the GDPR. In recognition of the concerns expressed by various stakeholders the government will seek to minimise, so far as is possible within the confines of a Regulation, any bureaucratic and potentially costly burdens on organisations while guaranteeing a high standard of data protection for individuals.

Although the GDPR is directly applicable to the UK, there are a number of articles that allow Member States to adjust the scope of the GDPR according to their own needs. If the Government does not act, organisations could face additional burdens to comply with the GDPR. Listed below are the derogations and exemptions in the GDPR that incur substantial costs and benefits. A complete table and rationale why the focus of the assessment is on the following derogations can be found in the Annex.

Table 1 - List of Derogations incurring substantial impacts

Article under consideration	Description	Government's Objective/ Policy position
Article 8	Article 8 determines the age at which a child can consent to their personal data being processed when accessing information society services. This age is set at 16, but 'Member States may provide by law for a lower age for those purposes provided that the lower age is not below 13 years'.	To allow the processing of personal data of children from the age of 13 by information society services. There is currently no minimum age requirement in the UK, although it is broadly seen at 12 and the government sees no benefit in raising it beyond 13 (see below for further consideration).
Article 9	Article 9 allows Member States, in certain circumstances, to continue processing special categories of data (sensitive personal data).	To allow organisations to continue to process special categories of personal data as set out in the 1998 Act.
Article 10	Article 10 allows Member States to legislate to allow certain organisations, beyond the official authority, to process personal data on criminal convictions and offences	To allow organisations to continue to process criminal conviction and offenses data to protect their organisations from potential criminal acts. It would also allow for the Insurance industry to continue to underwrite driving insurance.

Article 23	Article 23 allows Member States to introduce measures which exempt data controllers and processors from the transparency obligations and data subject rights of the GDPR in certain data processing situations, where it is in the public interest to do so.	Implement the restrictions available under the derogation to the extent necessary to maintain the current position under the 1998 Act, with further restrictions appropriate for new rights under the GDPR. This would ensure that businesses can continue to apply the necessary exemptions to accommodate the processing of personal data for specified purposes. These new measures will build on what has been previously available under the 1998 Act.
Article 84	Article 84 requires Member States to lay down rules on penalties for breaches of the GDPR other than administrative fines. These penalties must be effective, proportionate and dissuasive. Data protection law in the UK has always been accompanied by criminal offences. There are various provisions under the 1998 Act that provide for criminal offences, including but not limited to sections 21, 22, 24, 47 and 55, 56 and 59.	The GDPR allows the UK to specify the penalties for infringements of the law that are not subject to administrative fines. The Government will retain most but not all existing offences under the 1998 Act, with some modifications and extensions and will also create some new offences. The Government intends to: Reproduce offences in the 1998 Act which remain fit for purpose, including offences relating to unlawful disclosure of personal data obtained by the Information Commissioner in connection with their investigations, and offences relating to enforced subject access (e.g. where an employer asks a prospective employee to obtain personal data to which the organisation wouldn't normally be entitled) Extend the offence of unlawfully obtaining personal data (under s.55 of the 1998 Act) so that it covers unauthorised 'retention' of data and

		introduce a new defence for journalistic activity. Extend an offence in the Freedom of Information Act 2000 (altering records with intent to prevent disclosure) so that it applies to all data controllers and processors, not just public authorities. Amalgamate three separate offences in the 1998 Act which relate to obstructing the Information Commissioner's investigations into a single offence of obstruction. Create new offences relating to re-identifying anonymised or pseudonymised data. All the offences will become recordable crimes.
Article 85	Article 85 requires member states to reconcile the right to the protection of personal data with the right to freedom of expression and information by exercising a range of derogations and exemptions.	To broadly replicate the current exemption for journalism and the special purposes under s.32 of the 1998 Act.
Article 89	Article 89 recognises that it might be necessary for organisations to process personal data for scientific and historical research, statistical purposes or archiving in the public interest. Member States can use domestic legislation to exempt research organisations from some of the subject access provisions in the Regulation, if compliance would seriously impair their ability to complete their work.	To exempt organisations processing personal data for research purposes from certain rights as provided under Article 89 where compliance would seriously impair their ability to complete their work.

This Impact Assessment considers the government's collective position on these derogations, and assesses the costs and benefits of the government's approach. We took a proportionate approach to the analysis of each derogation. We aimed to quantify costs and benefits and measure impacts whenever possible and sought data from relevant sources. The effort applied at each step of completing this Impact Assessment, in particular the estimation of cost and benefits, is aimed to be proportionate to the scale of the costs and benefits, outcomes at stake and sensitivity of the

proposal. Our focus with regard to the analysis of costs and benefits therefore lies with Articles 8, 9, 10, 23, 84, 85 and 89.

Main affected groups

- The GDPR will apply throughout the UK. Gibraltar, though a British Overseas Territory, is also subject to EU Regulations in this field. The UK has responsibility on behalf of Gibraltar for the negotiation of relevant European instruments and those instruments are directly applicable in Gibraltar.
- The Regulation is likely to affect the following sectors in the UK, although this list is not exhaustive:

- **Data controllers and processors**[10] in the public, private and third sector (e.g. charities, voluntary organisations). “Data controller” means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed. A data controller must be a “person” recognised in law, that is to say individuals; organisations; and other corporate and unincorporated bodies of persons. Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. In the impact assessment we mainly focus on organisations. In relation to personal data, “data processor” means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. “Processing”, in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.
- **Data subjects** whose personal data is processed by UK organisations and UK residents whose personal data is being processed by non-UK organisations. A data subject is an individual who is the subject of personal data;
- The **Information Commissioner**, the data protection regulator, with primary responsibility to regulate the GDPR proposals, including investigation of potential breaches and enforcement of information law;
- **The justice system** as a means through which data related disputes are resolved, particularly in relation to enforcement of new rights and contract breaches within and across Member States;
- **Wider society.**

[10] A data processor' is defined in the GDPR as a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. In most cases the data controller who controls the data will also processes the data.

3: Cost-Benefit Analysis

This section sets out the costs and benefits of the key proposals within the preferred option; and the associated assumptions and sensitivities. Analytical judgements are made about which impacts are likely to represent a cost or benefit to society which also justify the detail of the analysis of the derogations. Most of the evidence was provided by organisation through the *Call for Views* which was conducted in spring 2017.[11] Our focus with regard to the analysis of costs and benefits therefore lies on Articles 8, 9, 10, 23, 84, 85 and 89.

The counterfactual throughout the impact assessment is that the GDPR was allowed to come into force in May 2018, taking direct effect as an EU regulation, without any derogations being exercised by the UK government.

There are many available derogations under the GDPR. The government has only chosen to exercise derogations which would reduce burdens to organisations. The alternative option would have been to do nothing and not exercise the derogation. Therefore the options that have been chosen are always the minimum possible burden to organisations that are available.

The *Call for Views* provided businesses an opportunity to provide evidence about the potential costs they could face if the government did not choose the minimum burden approach to the GDPR. Given their incentive to do this, we have reason to believe that the evidence obtained and detailed throughout the impact assessment is the best available, and to obtain further evidence would have large and disproportionate resource implications, and would be likely to be burdensome for businesses to provide.

The cost of business compliance with any GDPR requirement depends on the current level of compliance with the 1998 Act. Complex businesses will make risk based judgments about establishing compliant data processing systems and there is no uniform road map common to all businesses in making systems compliant with the GDPR. Further, businesses are generally reluctant to disclose full details about their current compliance for commercial and regulatory reasons. While we have collected evidence through the *Call for Views*, the range of data disclosed by business will create limitations on the government's ability to monetise likely implementation costs. Consequently this limits the available evidence to measure the impact of any derogation.

[11] https://www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views

Table 2 - Overview of the costs and benefits of the preferred options

Article	Costs		Benefits	
	monetised	non-monetised	monetised	non-monetised
8 - Giving consent to process data and protecting children online		- the costs on organisations are smaller with an age threshold of 13 than 16		- young teenagers can access information society services (ISS) - possible increase of conversations between parents and children about data protection online -alignment of UK policy with US policy
9 - The processing of special categories of personal data		Costs include greater potential for the infringements of individuals' data protection rights, loss of privacy and opportunities for discrimination.		- organisations that are currently processing special categories data on public interest ground can continue to do so - Avoidance of greater risks and fraud costs to the insurance sector - Avoidance of potential barriers to care services and patient safety
10 - The processing of personal data relating to criminal convictions and offences		- Cost of intervening is that these data rights might make it harder for ex-convicts to find a job		- Will allow industries to process criminal data and continue completing DBS checks and processing suspicious activity reports. This saves them the cost of having to hire other businesses to complete it.

				Insurance companies will be able to continue to underwrite claims lending decisions, maintaining their risk level.
23 - Public interest exemptions for data controllers and processors from the rights and obligations under the GDPR		- limitation of rights of individuals that are subject to the processing of their personal data on public interest grounds		- organisations that are currently processing data on public interest ground can continue to do so - the public will benefits from the processing due to an increase in for example national security. The nature of the benefits for the public will depend on the reason why the exemption applies
84 - Penalties for unauthorised data decryption and data retention		- Changes to laws on retaining data and the new re-identification offence are predicted to increase the number of convictions which will be costly for the Ministry of Justice		- ensures worst breaches of data security continue to be prosecuted by Information Commissioner - Criminalise new behaviours such as decrypting anonymised files - Clarification of fine for unauthorised data retention
85 - Processing and freedom of expression and information		- limitation of rights of individuals that are subject to processing for these purposes but only to the same extent as is currently the case under the 1998		- legal certainty and the maintenance of the balance between data protection rights and the rights with regard to the freedom and expression - the inclusion of

		Act.		processing with regard to the freedom of academic expression
89 - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.		There could be problems deciding who qualifies as a research organisation, and defining what is in the “public interest”.	- Cost prevented of Subject Access Requests not having to be complied with by research organisations and archivists	- Without the derogations the work of research and archivists could be significantly impeded by individuals exercising subject access rights.

Article 8 - Giving consent to process data and protecting children online

Problem under consideration and the need for government intervention

Information society services (ISS) which offer online services to children often want to use the personal data of children visiting their sites for purposes such as targeted advertising, marketing insights, or creating an online profile. However, there is evidence that a child may not understand what he or she is agreeing to. For example, a child might not be aware of the implications of providing their contact details to a provider who might then pass them onto a third party.

In recent years, child media experts have highlighted the need for data protection safeguards to address the commercial online marketing practices directed at children and teenagers of, for example, social networking sites.[12] Children's' advocates have suggested that children's access to information society services should be ideally based on the individual competence of the child, but have concluded that this is impractical and thus an age limit needs to be fixed.[13]

Article 8 of the GDPR seeks to address this problem by requiring parental agreement before the online processing of personal data of children aged under 16. The GDPR will be directly applicable in the UK from 25 May 2018, and Member States have the discretion to set the age threshold provided it remains between 13 and 16 years. If the UK government chooses not to exercise this discretion, 16 will be the age threshold in the UK.

The government has to make a decision on whether it should keep the default age threshold - 16 years - or whether it should be set at a different age. Setting the threshold at 16 suggests that younger teenagers need greater protection as their commercial media literacy is lower than those aged 16 and above. Alternatively, setting it at 13 would grant more children the right to express their opinions online, as for example supported by Articles 13 and 17 of the United Nations Convention on the Rights of the Child (UNCRC).[14] The government's position which was supported by the *Call for Views'* evidence is to set the age for consent for data processing at 13.

Policy objectives and the intended effects

The policy aims at introducing an appropriate age threshold (13) at which a young adult has the capacity to consent to the processing of their personal data while at the same time not undermining the benefits of that ISS offer to young adults.

The provision aims at better protecting children against privacy risks arising from personal data being processed by introducing an appropriate age threshold at which a child has the commercial

[12] For example: Benjamin De La Pava et al. (2015), Children, Advertising and the Internet, LSE Media Policy Project Blog, available at: http://blogs.lse.ac.uk/mediapolicyproject/topic-guides/children-advertising-and-the-internet/

[13] LSE GDPR Roundtable 2016, a summary of the meeting is available at: http://www.lse.ac.uk/media@lse/documents/MPP/LSE-GDPR-Roundtable-14102016.pdf

[14] Find more information on the UNCRC here: https://www.unicef.org.uk/what-we-do/un-convention-child-rights/

media literacy and capacity to consent to the processing of their personal data by organisations offering information society services directly to them. If data is processed from children below this age threshold this has to be authorised by someone with parental responsibility for the child. At the same time Government is keen to not reduce children's creative, educational, civic and communicative activities online.

It should be noted that there is no clear indication from academic research that shows that setting an age for online consent increases protection for children online. Evidence from the US, for example, highlights difficulties in implementation with the parental consent measures and age verification.[15] Experts also suggest that the complexity of algorithmic processing poses challenges for children and parents to make informed decisions and agree to the processing.[16]

Policy options

The options for an age of consent vary between fixing an age threshold between 13 and 16. For illustrative reasons and due to the evidence available we focus in this assessment on the lower and upper limit of 13 and 16 respectively. If the Government does nothing, the age threshold would become 16 when the GDPR applies.

Option 1 (Do nothing): An age of child's consent for data processing of 16. The age of consent for children to agree to their data being processed is set at 16 by default in the GDPR. This will be directly applicable from May 2018 if the government did nothing. All information society services currently offering services directly to a child and processing UK citizen's data have to have systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

Option 2 (Do minimum and preferred option): An age of child's consent for data processing of 13.
Setting the threshold at 13 is the 'do minimum' option, as it is the minimum age that the GDPR allows countries to set the age of consent at. Setting the age threshold at 13 is preferred as it would bring the UK's data protection regime more closely in line with the US's Children's Online Privacy Protection Act of 1998 which places similar requirements on any company that wishes to process any personal information relating to a child under the age of 13 years. This would also keep the new law closer to the current Information Commissioner guidance on this matter that states: "Some form of parental consent would normally be required before collecting personal data from children under 12", (Personal information online code of practice, July 2010).

---

[15] Warmund (2001), Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act, Fordham Intellectual Property Media & Entertainment Law Journal., vol 1.11, Article 7, pp.189-215, available at: http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1212&context=iplj
Szoka and Thierer (2009), COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech, The Progress and Freedom Foundation, Vol.16.11, available at: http://www.ftc.gov/os/comments/copparulerev2010/547597-00052-54901.pdf,
Tierer (2011), Kids, Privacy, Free Speech and the Internet: Finding the Right Balance, Mercatus Center Working paper, available at: https://www.mercatus.org/system/files/Kids_Privacy_Free_Speech_and_the_Internet_Thierer_WP32.pdf
[16] Nathan Fisk (2016) The Limits of Parental Consent in an Algorithmic World, Media Policy Project Blog, available at: http://blogs.lse.ac.uk/mediapolicyproject/2016/11/28/the-limits-of-parental-consent-in-an-algorithmic-world/

Evidence

Main affected groups

- Children
- Parents
- Information Society Services (ISS)
    - Companies in scope: All ISS[17] that contribute to UK GDP and/or have UK employers that offer their services directly to children aged 13-16. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.

What's the current age to agree to the processing of personal data?

The Data Protection Act 1998 does not currently specify an age at which children can agree to processing by ISS - instead their level of maturity and understanding is taken as a guide to their capacity to agree. The Information Commissioner guidance[18] refers to the age of 12 as generally deemed to be the age at which children have reached that level of maturity. It also puts emphasis on the fact that is good practice for organisations to obtain parental agreement for the collection or use of information about a child aged over 12 where the processing poses great risk to a child such as the disclosure of a child's name and contact details or the publication of a child's image to a third party.

Since 2006, anyone aged 13 and older has been allowed to become a registered user of Facebook, though variations exist in the minimum age requirement, depending on applicable local law. The same minimum age applies for web-based email services including Google's Gmail and Yahoo! Mail and other social media providers such as Twitter, Instagram and Snapchat. Linkedin's minimum age is 14 whereas users have to be 16 to use WhatsApp. The reason that most social media platforms which are US companies offering their services in the UK have set 13 years as their age threshold point is due to a US law called COPPA (Children's Online Privacy Protection Act), which dates back to 1998.[19] The COPPA mandates that online services have to seek "verifiable parental consent" from younger users and would then be restricted as to how they could use the data. However, in the US not many services and apps subsequently put sophisticated age verification and consent measures in practice. Facebook, for example, use refusal messages if a user types in an underage date of birth, and also Instagram and Twitter ban under 13-year-olds.

What is an Information Society Service?

This covers a wide range of economic activities that take place online, including selling goods online, as well as video on demand and services consisting of the transmission of information via a

---

17 'Information Society service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. Also note that "remuneration" including sites that obtain their revenues from advertising e.g. YouTube.

18 ICO, Personal information online code of practice, available at: https://ico.org.uk/media/1591/personal_information_online_cop.pdf

19 US Federal Trade Commission, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

communication network, providing access to a communication network, hosting information provided by a recipient of the service or providing commercial communications by e-mail. However, the use of e-mail or equivalent electronic communications (e.g. by persons acting outside their trade, business or profession, including their use for the conclusion of contracts between such persons) is not an information society service e.g. personal e-mail exchanges or a website with no commercial content would not be covered by these Regulations. It is assumed that technically any organisation with a website could be fall under the definition of an Information Society Service. The definition of the information society services has been defined in the EU Directive for "laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services".[20]

How many children use Information Society Services?

Many children and young people use online services and social media accounts are proving popular with children younger than 13. In the UK 78% of 10 to 12-year-olds state that they have social media accounts, despite recommended minimum age limits on platforms like Facebook and Snapchat. This evidence is drawn from a survey of over 1,000 10 to 18-year-olds, conducted by ComRes for BBC Newsround to coincide with Safer Internet Day 2016.[21] The same survey found that among 13 to 18-year-olds, 96% were signed up to social media networks such as Facebook, Instagram, Snapchat and WhatsApp. Recent research from Ofcom shows similar results;[22] 3% of 5 to 7-year olds, 23% of 8 to 11-year-olds, and 72% of 12 to 15-year-olds have a social media profile. The incidence of having a profile more than doubles from 21% at age 10 to 43% at age 11.

Although many social media sites have a minimum age of 13 or older, they are still used by younger children.[23] 55% of 8 to 11-year-olds have Facebook accounts. In the same age group around four in ten (43%) use Instagram, one in three Snapchat (34%) and one in five YouTube (22%) or WhatsApp (19%). With regard to older children, more than four in five of 12 to 15-year-olds that state that they have a social media profile use Facebook (82%) and 56% use Instagram and 51% use Snapchat. Also the use of the YouTube website or app increases with age,

---

[20] Set out in 'Directive 2015/1535' - Article 4 (25) states that information society service means "a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council". Article 1(1) (b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services ('Directive 2015/1535') 'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
For the purposes of this definition:

(i) 'at a distance' means that the service is provided without the parties being simultaneously present;

(ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

(iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

[21] Comres for BBC Newsround (2016), Survey, find out more here: http://www.bbc.co.uk/mediacentre/latestnews/2016/newsround-survey-social-media

[22] Ofcom (2016) , Children and parents: media use and attitudes report, available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf

[23] The minimum age for having a profile on Facebook, Instagram, Snapchat, YouTube, Twitter and Google+ is 13. The minimum age for WhatsApp is 16. Find more here: https://www.netaware.org.uk/networks/?order=-popularity

accounting for 37% of 3 to 4-year-olds, 54% of 5 to 7-year-olds, 73% of 8 to 11-year-olds and 87% of 12 to 15-year-olds.[24]

Why do children need to be protected?

When collecting personal data it is important that the data subject properly understands how the data they provide will be used. Data from Ofcom shows that teenagers have difficulty telling the difference between search results and adverts placed around them. A minority of 8-15-year-olds can identify sponsored links in search engine results, although 12-15-year-olds are more likely than 8-11-year-olds to be able to do this.[25] This indicates that young children's knowledge of how the web works, and how their personal data is being used is not always sufficient. It can be argued that children deserve protection as they may be less aware of risks and their rights in relation to their personal data. An OECD paper highlighted that children take information privacy risks when their personal data are collected online automatically (e.g. cookies), and provide data upon request by an ISS provider, and amongst other concerns. For example, children tend to skip privacy statements of online services and they readily agree to the use of their data in order to get access to desired websites.[26]

However, many experts argue that introducing an age threshold will not necessarily tackle these issues. Critics in the US for example highlighted that the COPPA parental consent measures are difficult to implement, costly to realise and could even restrict children's free speech rights while providing little protection for children and parents[27]. Research also suggests that without widely-employed age verification techniques, age restrictions for social network use are only partially effective and parental rules affect the behaviour of younger children but are less effective with an increasing age[28].

At which age are children commercially literate?

An analysis of Ofcom data[29] from Sonia Livingstone from London School of Economics and Kjartan Ólafsson from the University of Akureyri shows that commercial media literacy increases fairly steadily from age 8 to young adulthood. There is a noticeable improvement in commercial literacy from the age of 13 to 16 when children are asked about adverts on Google search results and whether information on news media sites is true. With regard to social media sites only 2% of

---

24 Ofcom (2016), Children and parents: media use and attitudes report, p. 74-75, figures 38 and 39, available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf

25 Ofcom (2016) , Children and parents: media use and attitudes report, available at:https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf

26 OECD (2012), Report on risks faced by children online and policies to protect them, available at: https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf

27 For example: Joshua Warmund (2001), Can COPPA Work? An Analysis of the Parental Consent Measures in the Children's Online Privacy Protection Act, Fordham Intellectual Property Media & Entertainment Law Journal, available at: http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1212&context=iplj

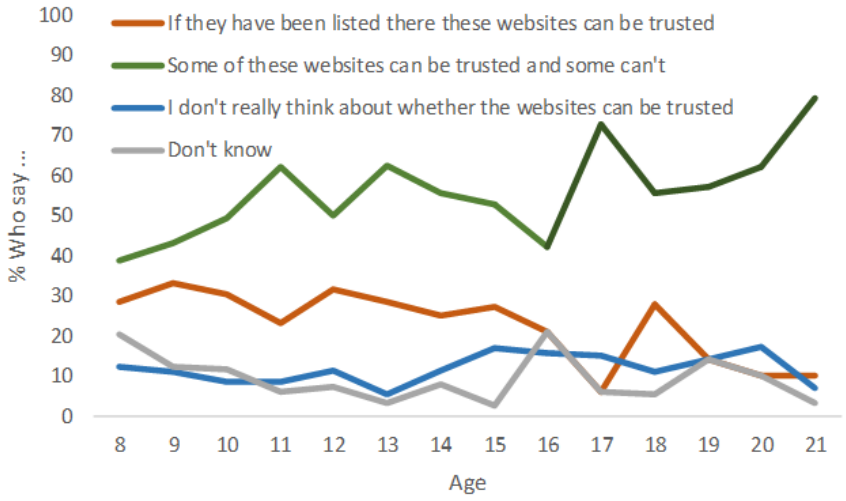
28 Sonia Livingstone, Kjartan Ólafsson and Elisabeth Staksrud (2011), Social networking, age and privacy. EU Kids Online, available at: http://eprints.lse.ac.uk/35849/

29 Sonia Livingstone and Kjartan Ólafsson (2017), Children's commercial media literacy: new evidence relevant to UK policy decisions regarding the General Data Protection Regulation, LSE Media Policy Project Blog, available at: http://blogs.lse.ac.uk/mediapolicyproject/2017/01/26/childrens-commercial-media-literacy-new-evidence-relevant-to-uk-policy-decisions-regarding-the-gdpr/

8 to 11-year-olds and 4% of 12 to 15-year-olds agreed with the statement that all information on these sites are true – less than in 2015, and less than adult respondents from the 2015 survey also.

With regard to the question on which search engine results can be trusted there is no strong increase in understanding through early teenage years, with the main gain in understanding being among younger children. The data also shows an increase in the lack of interest in whether sites can be trusted ("I don't really think about whether the websites can be trusted") and an increase in the frequency of the answer "Don't know" from the ages of 13 to 16. Looking at the same data across the adult age range shows that both younger and older people have somewhat lower levels of critical digital literacy compared with those aged around 30 to 60. The gains made through adolescence continue up to the late 20s, with no obvious cut-off in commercial literacy terms at the age of 16. Around one third of adult internet users believe that Google results can all be trusted. Livingstone and Ólafsson suggest that there is a need for greater transparency from search engines and/or greater digital literacy education for all ages, not just children.

Figure 1 - Commercial Media Literacy with regard to the Google results page



Note: Data for 8 to 15-year-olds from QC24 (When you use Google to look for something online, you are given a list of websites in the Google results page). All answer options are shown, with option 2 in green being the 'right answer'); N=748. Equivalent data for 16 to 21-year-olds from IN45; N=149.

With regard to the knowledge of how YouTube and Google make their money, Ofcom's data suggests that there is a marked increase in children's commercial literacy from the ages of 12 to 15. Livingstone and Ólafsson's analysis also shows that the answers for Google suggest that 14 and 15-year-olds have greater literacy than older teenagers and young adults. Combining children's data with data from adults across the age range gives little confidence that commercial literacy continues to increase with age, or that parents have the necessary knowledge to protect their children.

Overall, the analysis shows that there are indications that children from the age of 16 have a greater commercial media literacy compared to 13-year-olds but also highlights that the landscape is much more complex. Setting the age threshold at 16 and thus reducing children's vulnerability to

commercial and data risks has to be compared to the likely costs of teenagers' reduced opportunities for creative, educational, civic and communicative activities online[30] and, possibly, inequalities in who could obtain parental agreement as well as regarding those who might evade the need for such consent, e.g. by lying about their age online.[31]

Summary of Benefits

Option 1 (Do nothing): Age Threshold of 16

An indirect benefit could be the increase of conversations between parents and children about data protection online. This could lead to a further ensuring that parents and children make informed decisions when sharing their data and letting organisations make a profit from processing it. However, child internet safety experts have doubts that benefits from an age of consent will materialize. Whilst an increased digital age of consent might seem like a good way to protect children, online safety experts expressed their concerns in an open letter in December 2015.[32] The signatories to the letter point out that increasing the age limit for consent is artificial, as research shows that young people are adept at controlling the information they share online, more so than many adults.

Option 2 (preferred option): Age Threshold of 13

Monetised benefits: We do not currently hold the information needed to monetise the impact of this option and were unable to gather more evidence to monetise these impacts during our *Call for Views*. Furthermore, it has been difficult to put monetary values against concepts such as increase of privacy and therefore those benefits are discussed in the non-monetised section of this assessment.

Non-monetised benefits: The introduction of an age of consent of 13 would align with the US policy with an age of consent for data processing. A further direct benefit of an age threshold of 13 compared to 16 is that it does not undermine the benefits that particularly young teenagers experience from accessing ISS and also allows ISS to innovate for those young adults.

---

[30] Ofcom (2016) notes that among 12 to 15-year-olds internet users, 44% used an internet-enabled device to make a video, 18% music, 16% an animation, 13% a website, 11% a meme or gif, 9% an app or game, 6% a vlog and 4% a robot. Further, 30% of 12 to 15-year-olds have gone online for civic activities such as signing a petition, sharing news stories, writing comments or talking online about the news.

[31] For example: Sonia Livingstone (2016), The GDPR: Using evidence to unpack the implications for children online, LSE Media Policy Project Blog, available at: http://blogs.lse.ac.uk/mediapolicyproject/2016/12/12/the-gdpr-using-evidence-to-unpack-the-implications-for-children-online/ and Vicki Shotbolt (CEO of Parent Zone) (2016), Is parental consent the way forward, or is the GDPR the end of young people's freedom to roam digitally?, LSE Media Policy Project Blog, available at: http://blogs.lse.ac.uk/mediapolicyproject/2016/12/13/is-parental-consent-the-way-forward-or-is-the-gdpr-the-end-of-young-peoples-freedom-to-roam-digitally/

[32] Diana Award's Anti-Bullying Campaign (2015), Letter of concern to the draft GDPR, https://www.fosi.org/about/press/letter-european-general-data-protection-regulation/ http://www.antibullyingpro.com/blog/2015/12/11/letter-expressing-concern-to-the-draft-general-data-protection-regulation-13to16

An open letter in December 2015[33] by online safety experts highlighted the important role played by digital platforms and social media in self-development and education. Experience of age verification processes have shown that children have an 'innate curiosity, which combined with peer pressure and the appeal of exciting content on major SNS platforms has meant that large numbers of young people lie about their age to register on services that were not designed for them'. Some parents are also helping their children in this regard. They can have 'concern that their children are not left out of digital opportunities' and they may have 'a lack of awareness of the risks involved' for their children.[34]

The minimum age threshold of 13 would be the least burdensome approach and ensure that children that have the media literacy needed to reap the benefits from ISS and are not excluded from access. Setting the age threshold at 13 would be in accordance with EU law transposition principles, which state that the Government should ensure the least burdensome and most beneficial approach to EU laws are adopted by the UK. This ensures that UK businesses are not put at a competitive disadvantage relative to their EU counterparts.[35]

Summary of costs

Option 1 (Do Nothing): Age threshold of 16

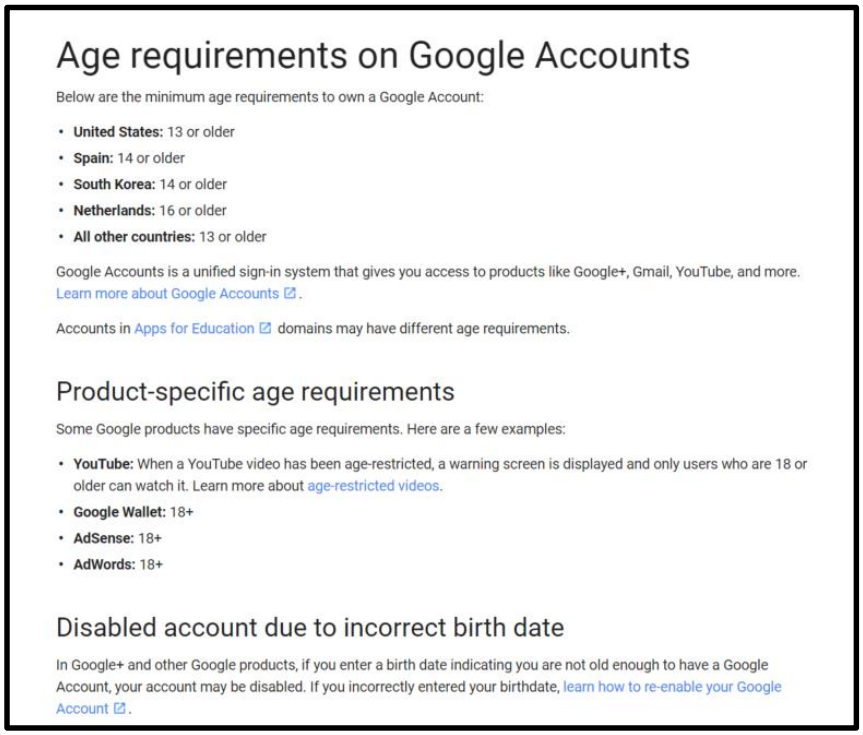
The types of costs to organisations, children and parents are very similar for an age threshold of 16 and a threshold of 13 but they are greater for an age threshold of 16 than for a threshold of 13. Many organisations that offer services directly to a children such as the social media firms Facebook/Instagram and Google have a minimum age requirement of 13 (see Figure 2 and 3).

[33] Diana Award's Anti-Bullying Campaign (2015), Letter of concern to the draft GDPR, https://www.fosi.org/about/press/letter-european-general-data-protection-regulation/ http://www.antibullyingpro.com/blog/2015/12/11/letter-expressing-concern-to-the-draft-general-data-protection-regulation-13to16

[34] Brian O'Neill (2013). Who Cares?:Practical Ethics and the Problem of Underage Users on Social Networking Sites, http://arrow.dit.ie/cgi/viewcontent.cgi?article=1055&context=cserart

[35] Read more about this in the Manual: https://www.gov.uk/government/uploads/system/Better Regulationuploads/attachment_data/file/468831/bis-13-1038-Better-regulation-framework-manual.pdf

Figure 2 - Screenshot from Google Account Help[36]



Age requirements on Google Accounts

Below are the minimum age requirements to own a Google Account:

- **United States:** 13 or older
- **Spain:** 14 or older
- **South Korea:** 14 or older
- **Netherlands:** 16 or older
- **All other countries:** 13 or older

Google Accounts is a unified sign-in system that gives you access to products like Google+, Gmail, YouTube, and more. Learn more about Google Accounts.

Accounts in Apps for Education domains may have different age requirements.

Product-specific age requirements

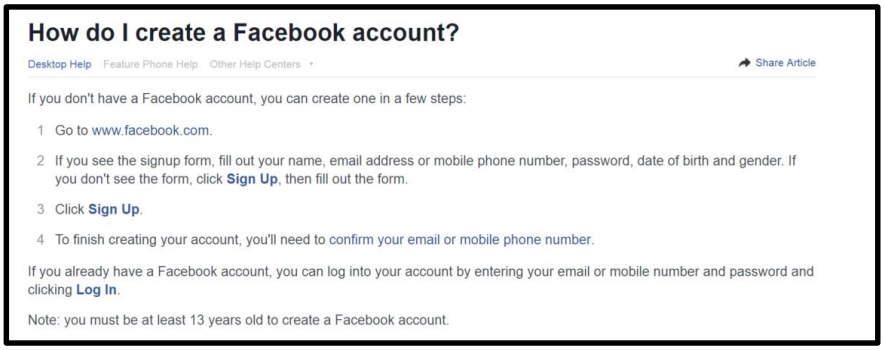
Some Google products have specific age requirements. Here are a few examples:

- **YouTube:** When a YouTube video has been age-restricted, a warning screen is displayed and only users who are 18 or older can watch it. Learn more about age-restricted videos.
- **Google Wallet:** 18+
- **AdSense:** 18+
- **AdWords:** 18+

Disabled account due to incorrect birth date

In Google+ and other Google products, if you enter a birth date indicating you are not old enough to have a Google Account, your account may be disabled. If you incorrectly entered your birthdate, learn how to re-enable your Google Account.

Figure 3 - Screenshot from Facebook's account creation help



How do I create a Facebook account?

Desktop Help Feature Phone Help Other Help Centers Share Article

If you don't have a Facebook account, you can create one in a few steps:

1. Go to www.facebook.com.
2. If you see the signup form, fill out your name, email address or mobile phone number, password, date of birth and gender. If you don't see the form, click **Sign Up**, then fill out the form.
3. Click **Sign Up**.
4. To finish creating your account, you'll need to confirm your email or mobile phone number.

If you already have a Facebook account, you can log into your account by entering your email or mobile number and password and clicking **Log In**.

Note: you must be at least 13 years old to create a Facebook account.

However, many more children and parents would be affected by an age threshold of 16 compared to 13. There are currently around 10.1 million children below the age of 13 living in the UK and around 12.3 million children below the age of 16.[37] 2.2 million children would not be able to consent to their data processing without having their parents' approval.

Organisations have to implement age verification systems and processes in order to make sure that their users are above the age threshold of 16 or their parents can provide consent for their children to use those services. For organisations that are currently processing data of children below 16 years old and for which this is part of their business model, the introduction of an age threshold might bear costs in terms of a reduction of their user base.

---

[36] find more information here: https://support.google.com/accounts/answer/1350409?hl=en

[37] Population estimates from the ONS mid-2015, https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/datasets/populationestimatesforukenglandandwalesscotlandandnorthernireland

A proportion of children below the age of 16 that fail to receive parental consent for using ISS can't access those services. Assuming that the service would be valuable for the child and his/her development, if they were not able to receive parental consent, this would have a cost with regard to the loss of information. There is possibility that those children might lose access altogether. While children under 16 could legally give out personal information with their parents' permission firms could also disallow underage users from using their services altogether. In the US for example many websites disallow underage children (children below 13 following the COPPA regulation) from using their services altogether.

Parents have to provide consent for services that require the processing of data of children and will thus incur opportunity costs for providing their consent. The extent of these costs depends on the way that consent is provided. For example reading and signing a form, providing official identification with an ID or credit card and a selfie or ticking a box are all ways to provide consent which ask for a different amount of time spent by parents.

There might also be unintended consequences when setting an age threshold at 16. Research shows that whilst there are risks for children online, there are also benefits for children from using online technologies such as greater opportunities for socialisation and communication. For example, there are opportunities for community engagement through raising money for charity and volunteering for local events as well as enhanced learning opportunities.[38] These activities could lead to improved self-esteem, perceived social support and increased social capital.[39] There are also online educational resources that can support children's learning.[40] Experts argued that setting an age threshold could limit children's rights to communicate with their peers and engage online with valuable resources online[41]. Research in the US for example suggests that instead of providing more tools to help parents and their children make informed choices, industry responses to COPPA have neglected parental preferences and have altogether restricted what is available for children to access and in some cases this has led to parents helping their children to lie about their age.[42]

John Carr, member of the Executive Board of the UK Council for Child Internet Safety, has voiced concerns that setting the age threshold at 16 could also have other unintended consequences. He highlighted that with an age of children's online agreement to processing of their data of 16, problems with laws against grooming could occur and could have adverse effects for child

[38] O'Keeffe, Clarke-Pearson and Council on Communications and Media (2011), The Impact of Social Media on Children, Adolescents, and Families, Clinical Report, American Academy of Pediatric, available at: http://pediatrics.aappublications.org/content/127/4/800.short

[39] Best, Manktelow, and Taylor (2014), Online Communication, Social Media and Adolescent Wellbeing: A Systematic Narrative Review, Children and Young Services Review, available at: http://pure.qub.ac.uk/portal/files/120352496/Final_Online_Communication_Social_Media_and_Adolescent_Wellbeing.pdf

[40] For example the tools 'Show my homework' (https://www.showmyhomework.co.uk/) and 'Firefly' (https://fireflylearning.com/)

[41] For example: Larry Magid (2015), Europe Could Kick Majority of Teens Off Social Media and That Would Be Tragic, available at: http://www.huffingtonpost.com/larry-magid/europe-could-kick-majorit_b_8774742.html and danah boyd, What If Social Media Becomes 16-Plus?, available at: https://brightreads.com/what-if-social-media-becomes-16-plus-866557878f7#.2c2btbjuh

[42] danah boyd, Eszter Hargittai, Jason Schultz, and John Palfrey (2011), Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act', available at: http://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075

protection online. Carr says that "if internet sites and services stick to their previous practice of NOT age verifying anyone or seeking parental consent instead, as now, they simply draw a line at the legal minimum age, saying you must be 16 to be a member, any third party using that site or service in future will be entitled to say they had good reason to believe everybody they engaged with on the site was at least 16 and therefore was old enough to engage in sexual activity with them."[43] In Carr's opinion this could, at the very least, compromise the operation of the grooming law and makes the work for prosecutors much harder since the age of consent for sex in the UK is 16.

Furthermore, organisations that are currently processing data of children below 16 years and made this part of their business model the introduction of an age threshold might bear costs in terms of a reduction of their user base. We weren't able to monetise these costs due to the difficulties to gather firm level evidence and did not receive any submission on these costs in our *Call for Views*.

Option 2 (preferred option): Age Threshold of 13

Monetised costs: We do not currently hold the information needed to monetise the impact of this option and were unable to gather further evidence through the *Call for Views.*

Non-monetised costs:

Direct costs to business: There are no additional costs for data controllers when setting the age at 13 rather than 16. For both options organisations have to implement age verification systems and processes in order to make sure that their users are above the age threshold or their parents can provide consent for their children to use those services. However, these costs will be limited with an age threshold of 13 since many organisations already comply with COPPA and thus don't allow children with these ages to access their services altogether. For organisations that are currently processing data of children below 13 years old and for which this is part of their business model the introduction of an age threshold might bear costs in terms of a reduction of their user base.

Impacts on the wider society:

There are no additional wider negative impacts of implementing an age threshold of 13 compared to the age of 16. A proportion of children below the age of 13 that fail to receive parental consent for using ISS can't access all services. If there are services that would be of value to a child for his/her development, and if that child is unable to gain (or is delayed from gaining) parental consent, then there is a cost to that child as they would lose access to useful information. Such resources could, for example, include educational services or online support and advice services to children suffering from abuse or online bullying. Indeed, it could actually lead to an erosion of the child's privacy as such advice and information could not be sought in confidence.[44] Experts

[43] John Carr (2016), The point about 16: implications of the GDPR for child grooming laws, LSE Media Policy Project Blog, available at: http://blogs.lse.ac.uk/mediapolicyproject/2016/12/01/the-point-about-16-implications-of-the-gdpr-for-child-grooming-laws/

[44] Recital (38) of the GDPR: Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using

highlight that enhanced protections could have the unintended consequence of "limiting children's rights to communicate with peers, engage online with educational, health and other valuable resources, or participate in the online civic and public sphere".[45]

Parents have to provide consent for services that require the processing of data of children and will thus incur opportunity costs for providing their consent. The extent of these costs depends on the way that consent is provided. For example reading and signing a form, providing official identification with an ID or credit card and a selfie or ticking a box are all ways to provide consent which ask for a different amount of time spent by parents.

Assumptions and risks

Key assumptions are it is technically feasible for ISS to implement solutions for age verification and that they will be implemented and enforced. Further, it is assumed that children won't circumvent age verification and that they won't sign-up for ISS without their parent's consent. It is also assumed that parents provide an informed consent. Risks are that children who do not obtain parental consent cannot access valuable services and that children circumvent age verification.

services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

[45] Sonia Livingstone (http://blogs.lse.ac.uk/mediapolicyproject/2015/12/18/no-more-social-networking-for-young-teens/) and argued also by Larry Magid (http://www.huffingtonpost.com/larry-magid/europe-could-kick-majorit_b_8774742.html) and Danah Boyd (https://medium.com/bright/what-if-social-media-becomes-16-plus-866557878f7)

Article 9 - The processing of special categories of personal data

Problem under consideration and the need for government intervention

Article 9 bans the processing of special categories of personal data[46] in general terms but permits it in certain specific circumstances. This includes circumstances in which Member State law permits processing for certain purposes. If we failed to exercise this Member State discretion in Article 9, special categories of personal data could no longer be processed for purposes such as scientific health research, cross-border health threats; employment law purposes and processing on specific substantial public interest grounds such as certain processing for the purpose of carrying on insurance business. Government intervention is required so that the processing of certain types of special categories of personal data in these circumstances can continue.

Policy objectives and the intended effects

The policy objective is to, as far as possible, allow organisations to continue to process special categories of personal data on the same basis as is permitted for sensitive personal data under the 1998 Act. This means we would exercise all of processing grounds in Article 9 that are subject to Member State discretion, except those that enable Member States to restrict data processing further. This approach would maintain the status quo as far as possible, thereby minimising the burden on organisations by allowing this type of personal data processing to continue. We also intend to introduce a small number of new processing grounds under Article 9.

Policy options

Option 1 (Do nothing): **Not allowing exemptions from the processing of special categories in certain circumstances. This would not take advantage of the full derogations open to the UK.** Not allowing exemptions from the processing of special categories in certain circumstances could be burdensome for businesses and the public/third sector.

Option 2 (Preferred option): **Maintaining the status quo with regard to processing special categories of personal data**. This would minimise burdens to businesses while also eliminating any transition costs. Where possible we would replicate what we have in the 1998 Act under the following: Article 9 (2) (b), (g), (h), (i) (j) and (3), and add new provisions where necessary. The Data Protection Directive 1995 included similar language to prohibit the processing of special categories of personal data unless it met a number of provisions, some of which can be created through Member State law. This was achieved through the 1998 Act. Keeping the 'status quo' would also mean not exercising the derogations within for Article 9 (a) (to ensure that individuals can still decide whether their data can be processed) and not exercising the derogation within Article 9 (4) (which would add more conditions for processing data) as they would create additional burdens above and beyond the 1998 Act.

[46] Special categories include the following; racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of genetic, biometric, health data and a person's sex life or sexual orientation.

Other options could have been Option 3 and 4 which are not subject to this impact assessment as they were ruled out as too burdensome and not achieving the government's aim:

Option 3 - **Exercising some, but not all of the derogations (2) (b), (g), (h), (i) (j) and (3) in Article 9 that allow members states to continue processing special categories of data.** As each one of these derogations reduces burdens on businesses or the public sector, there would be no reason to exercise only a subset of them.

Option 4 - **Not exercising any of the derogations that permit member states to continue processing special categories of data and exercising the derogations that would be more restrictive.** This includes exercising the derogations in Article 9 (a) which removes the right to process special categories of data even if the data subject has consented, and Article 9 (4), where we would be introducing further conditions or limitations to the processing of genetic, biometric data or data concerning health. This would be more burdensome on businesses and the public sector than doing nothing (option 1) and more burdensome than option 3, and is therefore rejected.

Evidence

Article 9 allows Member States to legislate allowing for special categories of personal data to be processed for certain purposes without the explicit consent of the data subject. These include: employment, social security and social protection law purposes, substantial public interest, various specified health, social care and public health purposes, archiving in the public interest, scientific or historical research purposes and statistical purposes. Appropriate safeguards are required.

Organisations need to process health data for employment law purposes. For example, employers process special categories of personal data to manage sickness absences and to make reasonable adjustments for individuals when they return to work.

These are some of the areas that are likely to be impacted by Article 9 derogations:

- Health Research
- Healthcare
- Private Practices (i.e. GP's)
- Health Care Professionals (i.e. contractors)
- Insurance Industry
- Sports
- Employment

Research on the Information Commissioner data controller register shows that around 57,000 organisations describe the sector they are working in as health, 72,000 as finance, insurance and credit, almost 7000 as media organisations. Overall around 480,000 data controllers are registered with the Information Commissioner.

Summary of Benefits

Non-monetised: Following our *Call for Views*, we have received widespread concern about the costs of not replicating what we have in the 1998 Act to allow special categories of personal data to continue to be processed without the explicit consent of the data subject. These costs, which could be prevented by intervening, are particularly focused in health and insurance. In the health sector not being able to process special categories of data without consent could compromise professional regulation and patient safety, while requiring patient consent for processing could create difficulty for patients with reduced mental capacity. There could be a financial impact on the insurance and underwriting sectors, as less data processing would result in an increase in their risk and could also negatively impact fraud detection.

Quantification: ONS estimates are that £22.1bn is spent per year by households on insurance. In our sensitivity analysis we show that a small rise in insurance premiums could have large cost effects, which could be prevented if the government intervene. We also obtained an estimate for the costs of fraud and provided a sensitivity analysis of the costs of an increase in fraud, which could be prevented if the government intervenes. The resource implications of estimating the extent to which insurance premiums and fraud might increase are too great for us to be able to monetise these impacts.

Monetised: Due to a lack of data on the extent of the impact we were not able to monetise the benefits that we had some quantitative data for.

Summary of Costs

Non-monetised: Costs include greater potential for the infringements of individuals' data protection rights, loss of privacy and opportunities for discrimination. We have not monetised these costs as it would be very difficult to obtain evidence about the economic impacts of these concerns. We also have evidence that the impacts would be likely to be small in scale.

Monetised: Due to a lack of data we were not able to monetise the costs

Health

Healthcare providers such as hospitals, nursing homes, GP's and health care employment agencies would no longer be able to process special categories of data without the explicit consent of the data subject if government did not replicate the legislation we have in the 1998 Act. Those offering counselling, health advice or services may no longer be able to provide it because they cannot process special categories of data.

Health researchers are looking for an approach that does not create unnecessary safeguards and burdens for the processing of special categories of personal data but an approach that replicates most of what is already in place in the 1998 Act and provides additional legal certainty for health research. Without legal certainty, health research could be delayed, which would not be in the public interest. It is important to provide greater certainty and clarity for researchers, and to support

work which builds public trust in the use of health data in research. The most effective way to do this would be to maintain the status quo set out in the 1998 Act.

These are some responses from our *Call for Views* from the health and care sector that highlight some of the issues mentioned:

- The General Medical Council make clear that 'there should be a provision which allows professional regulators, particularly in the health sector, to process sensitive personal data for the purposes of professional regulation and fitness to practise in order to safeguard patient safety'.
- Somerset County Council suggested that if we don't intervene to exercise the derogation in 9.2(h) that there 'will need to be a radical overhaul of NHS systems to ensure that explicit consent for processing by the NHS and all relevant partners is managed in accordance with the GDPR, and that this would be very expensive to support administratively to ensure it is implemented'.
- Samaritans stated that they 'would be concerned if the derogation in Article 9 is not exercised. They answer approximately 77,000 calls per week. To help understand reasons for calling and provide a better service to those in need of support they record a small number of key details from each call, for example whether a caller has experienced suicidal thoughts, creating sensitive personal data. If the derogation were not exercised, their callers would be greeted with a legalistic response asking for their consent for personal data to be processed. This could be distressing and confusing for callers who require the Samaritans listening service who are often in extreme emotional distress and may be experiencing suicidal thoughts. There is a risk that the legal statement would create a barrier to people obtaining help and introduce excessive formality to the service, endangering vulnerable people's mental health'.
- Group Risk Development explain that if derogation 2(c) were not applied, they would be unable to use family history data about someone without the individual's explicit consent. This would be problematic if, for example, the individual were in a coma and such information would be valuable.

Insurance

Organisations in the insurance sector have been vocal requesting that government continues to make it possible for them to process family history health data for insurance purposes, as is provided under the 1998 Act. Without intervention they would no longer be able to process this data without seeking the consent of the individuals which could have a financial impact on the insurance and underwriting sectors as well as a lack of health cover for individuals. It could also negatively impact fraud detection.

Listed below are some of the issues raised in our *Call for Views* from the insurance sector:

- Lloyds Market Association stated that the processing of special categories of personal data, 'in particular health data, and criminal records data, is essential to provide many types of insurance. Without it, policies cannot be arranged by brokers, underwritten at realistic and accurate rates, or claims processed'. They also explain that currently under the GDPR, relying on consent as a precondition of providing insurance 'would at best be an unnecessary additional step in the sales, renewals or claims process. At worst, if it prevented personal data passing up the insurance chain, it could reduce insurance cover

(for example if policies could not be issued until all consents were directly received), impact the accuracy of underwriting and pricing, and limit the spread of risk and stability of the insurance market'.

- AXA UK state that 'without an exception for using sensitive data for insurance contracts, the process of providing an insurance contract, whether for health, travel and motor (pre-existing health, or dealing with motor accidents) would be complex and disruptive for the policyholder'.
- Investment & Life Assurance Group explained that 'insurers often process special category personal data, for example to price and underwrite according to the level of risk presented'. It's important to 'ensure that the industry can continue to provide products and services that allow individuals to manage financial risks and provide security'.
- The Association of British Insurers explain fully why insurers need to process personal data:

- To accurately calculate the level of risk posed by an individual entering into a contract. Insurers use historical behaviours and data to predict future risk. This allows insurers to charge a fair price for insurance that reflects the level of risk being insured. The more accurate this risk profiling, and the data that it is based on, the more efficient and stable an insurance company will be, leading to better value for customers and greater access to insurance products. This benefits wider society by enabling individuals to take risks, such as driving a car, travelling abroad, or running a business, knowing that the risks are covered by the protection benefits provided by insurance products.
- Provide customers with risk-reflective insurance cover: Without the ability to use historical data to understand and quantify risk, the likely consequence would be that insurers inflate premiums in order to account for 'unknown' risk, for all customers, even those who would in practice represent a low risk.
- Harness the power of data, allowing them to manage individuals' risks and innovate. Insurers are beginning to use big data to innovate and provide customers with insurance products that are better suited to their needs. For example, fitting cars with telematics devices has enabled insurers to develop insurance products which are more accurately priced by profiling customers' driving behaviours.
- Retain data for long-term liabilities of individuals. Insurers must retain data in order to comply with legislation and regulation relating to complaints, liability, record-keeping and a number of professional requirements (e.g. Anti-Money Laundering requirements). For long-term insurance such as life policies or personal pension schemes, firms have specific requirements to retain records for a minimum of five years from the end of a business relationship. As such, firms constantly review the data they hold and process to ensure compliance with their legal and regulatory obligations.

Insurance Premiums

Many respondents to our *Call for Views* have suggested that insurance premiums may rise as a result of insurers not being able to process special categories of data without explicit consent. They may need higher premiums because having less information available about clients increases the risks of insuring them, and because of an increased risk of fraud. ONS statistics from the Living Cost and Food Survey show that for the financial year to 2016, weekly household expenditure on insurance products was approximately £425m. Multiplying this for 52 weeks gives an annual estimated spend of £22.1bn. The table below provides a breakdown of insurance expenditure in the UK 2015-16:

Insurance Type	Total Weekly expenditure £m	Annual expenditure £m
Household insurances	124	£6,448
Medical insurance premiums	44	£2,288
Vehicle insurance including boat insurance	250	£13,000
Non-package holiday, other travel insurance	7	£364
Total	**425**	**£22,100**

The table below provides a sensitivity analysis of the possible additional costs to consumers if premiums were to increase because insurers were unable to process special categories of data:

If premiums increased by:	0.10%	0.50%	1.00%	2.50%	5.00%	10.00%	25.00%
Cost per year: (£m)	£22	£111	£221	£553	£1,105	£2,210	£5,525

Unfortunately we are unaware of evidence that would enable us to estimate the percentage increase in insurance premiums and therefore how much household insurance expenditure would be likely to go up. We considered household insurance costs rather than business insurance as household insurance is more likely to involve personal data, and would therefore be more likely to experience a change in premiums if Article 9 were not exercised.

Insurance Fraud

Many of the *Call for Views* responses also mentioned insurance fraud which might increase if not exercising the relevant derogations. This analysis could also relate to Article 10. It is not clear to which the extent fraud prevention will be affected by this provision specifically, but we have listed some of the concerns we have received from industry:

- Motor Insurers' Bureau explained that 'by enabling insurers to access details of incidents it makes it harder to successfully commit claims fraud or misrepresent claims history', and therefore 'helps to keep down the cost of insurance for honest policyholder'. Without the derogation MIB claims 'the Industry and customers will be heavily impacted'.
- Insurance Fraud Bureau 'help insurers identify fraud and avoid the financial consequences of insurance fraud'. They express concern about the impact of being unable to share sensitive data for anti-fraud purposes.

- The Association of British Insurers explained that if individuals were able to object to the processing of their data, it could prevent insurers from identifying and preventing fraudulent activity and cross-reference information with other fraud databases. At underwriting stage, insurers rely on automated decision-making processes and profiling to identify fraudulent activity and to cross-reference information with other fraud databases. Furthermore, insurers are required to carry out this processing in order to comply with The Proceeds of Crime Act 2002 and 4th Money Laundering Directive, and in doing so firms coordinate with a number of fraud databases including the Insurance Fraud Register (IFR) and the Health Insurance Counter Fraud Database (HICFG). So at the claims stage, 'insurers need to process personal and sensitive data to assess whether a claim is likely to be fraudulent'. This benefits honest customers, insurers and wider society by detecting crime and reducing premiums by lowering levels of fraudulent claims. In 2015, fraud screening by insurers detected claims fraud with a value of £1.3bn[47].

Based on the £1.3bn annual detected fraud cost figure, the table below provides a sensitivity analysis of the possible costs to the economy if fraud were to increase because insurers were unable to process special categories of data:

If fraud increased by:	0.1%	1%	5%	10%	50%	100%	250%
Cost per year: (£m)	£1.3	£13.0	£65.0	£130.0	£650.0	£1,300.0	£3,250.0

These figures are based on the level of detected fraud. Actual fraud might be significantly above the £1.3bn figure we have used in this analysis. We have not included these figures in our overall net present value in this Impact Assessment. There is little evidence about the extent of the causal relationship between fraud and the processing of special categories of data. The potential cost is wide ranging from possibly no increase in fraud to additional fraud costs of billions. Unfortunately we are aware of little evidence that can suggest what the increase in fraud costs might be.

Further Business Concerns

- The Confederation of British Industry (CBI) made it very clear that 'processing sensitive personal data is fundamental to the services and products that businesses deliver for consumers. For example, the ability for insurance firms to offer health insurance, retailers to provide tailored services based on lifestyle information or businesses to conduct due-diligence checks'. They recommended that 'the government should ensure that existing legal justifications from the 1998 Data Protection Act are carried forward under the GDPR'.
- techUK point towards the need not to gold plate, stating that they 'do not believe that the Government should seek to place additional restrictions on the processing of these categories of data, as the GDPR already provides appropriate protections'.

47 https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2016/keyfacts/keyfacts2016.pdf

Sports

Sport governing bodies are concerned that explicit consent is not an appropriate legal basis for ongoing regulatory data processing. They have highlighted that anti-doping activities require a participant's consent, however this must be freely given and is invalid if the individual has no genuine free choice or is unable to refuse or withdraw consent without detriment. If it is not possible for sports bodies to process special categories of data for drug testing without consent then competitors would no longer be able to compete. This could impact UK sporting events which draws in spectators and creates tourism.

Costs

There could be concerns that individual's personal data is not being adequately protected, resulting in for example higher levels of anxiety, especially for vulnerable people. People may fear that their personal data could be used by processors (insurers in particular) to discriminate against them. We have not monetised these costs as it would be very difficult to obtain evidence about the economic impacts of these concerns. We also have evidence that the impacts would be likely to be small in scale.

Some organisations addressed these concerns. The Association of British Insurers for example explained that they believe that the risks to consumers having their data protection rights infringed upon would be limited by a number of factors:

- The UK insurance market is highly regulated with oversight from Financial Conduct Authority (FCA)
- The FCA's operational objectives are to ensure consumer protection, integrity and competition and it regularly reviews insurers' processes to ensure that these conditions are met.
- UK legislation such as the Equalities Act 2010 and the Rehabilitation of Offenders Act 1974 legally protect individuals from discriminatory profiling and pricing.

The European Digital Rights (EDRi) and the Open Rights Group highlighted in their analysis[48] and submission[49] that it is important that this exception is applied only in such clearly defined areas. In case of misuse this article can lead to serious abuses of sensitive data for anything labelled "archiving in the public interest" or "scientific" uses, including use of such data for commercial research. The Open Rights Group emphasised that "there is a risk that private and public sector research bodies (which are increasingly intertwined) will try to stretch the provision to allow them to do anything they want with sensitive data they can obtain, certainly also for commercial "research" purposes".

Assumptions and risks

The main assumption in this assessment is that the provisions that we are planning to enact strike an appropriate balance between the public interests listed in the exemptions and individuals' data protection rights.

[48] see here: https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf
[49] see here: https://www.openrightsgroup.org/assets/files/pdfs/submissions/OpenRightsGroup-GDPR-derogations-consultation.pdf

Further Information

Please see below a list of the eight derogations found in Article 9:

- Article 9 (2) (a) The exception in this part of the article states that Member States can legislate to set out types of processing of special categories of personal data that is prohibited, even when the data subject has given explicit consent.

- Article 9 (2) (b) Member State law can authorise and provide appropriate safeguards for the processing of special categories of personal data in the field of employment, social security and social protection, where it is necessary.

- Article 9 (2) (g) Member States can legislate to allow for special categories of personal data to be processed which falls within the substantial public interest so long as it is necessary and proportionate.

- Article 9 (2) (h) Member States can legislate to allow for processing of special categories of personal data for the purposes of preventative or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

- Article 9 (2) (i) Member State can legislate to allow special categories of personal data to be processed in the public interest with additional safeguards in the area of public health, such as protecting against cross-border threats to health of ensuring high standards of quality and safety of health care and of medicinal products of medicinal devices.

- Article 9 (2) (j) Member States can allow for the processing of special categories of personal data if it was necessary and proportionate and had appropriate safeguards for archiving purposes in the public interest, scientific or historical research purposes of statistical purposes.

- Article 9 (3) sets out the conditions and safeguards for the processing of special categories of personal data for Article 9 (2) (h), these conditions and safeguards must be created through Member State law or rules established by national competent bodies.

- Article 9 (4) Member States can introduce further conditions or limitations to the processing of genetic, biometric data or data concerning health.

Article 9 (2) (b), (g), (h), (i) (j) and (3) are all concerned with allowing member states to legislate to allow the processing of special categories of data to continue in different circumstances.

Article 9 (2) (a) and (4) are concerned with allowing member states to further restrict the processing of special categories of data to continue in different circumstances. Invoking Article 9 (2) (a) would mean in certain circumstances organisations could not use personal data even if data subjects had consented. This would be restrictive to any organisation for whom such data would be of value, and to any individuals who would benefit from the prohibited data being processed. Invoking Article 9 (4) would be restrictive to any organisation that would value genetic or biometric

data or data concerning health. The sections above on Health, Insurance and Further Business Concerns give relevant examples of ways in which this derogation could be prohibitive. Invoking these derogations would also take the UK's data protection regulations beyond the minimum requirements set out by the GDPR. It is for these reasons that they were not included in the preferred option.

Article 10 - The processing of personal data relating to criminal convictions and offences

Problem under consideration and the need for government intervention

Article 10 allows Member States to legislate to allow certain organisations, beyond official authorities[50], to process personal data on criminal convictions and offences. Currently this data can be processed under the 1998 Act as sensitive personal data, but if we do not take advantage of the Member State discretion in Article 10, wholly private organisations will not be able to process these data when the GDPR comes into force. Not being able to process this data will mean, for example, that pre-employment and insurance checks for criminal convictions or offences by private bodies can no longer be made.

Policy objectives and the intended effects

The policy objective is for all organisations to be able to continue to process criminal conviction and offences data as they do under the 1998 Act to protect their organisations from potential criminal acts.

Policy options

Option 1 (Do nothing): **Not legislate to allow certain organisations, beyond official authorities, to process personal data on criminal convictions and offences**. This would mean that private organisations would no longer be able to legitimately process criminal conviction and offence categories of personal data.

Option 2 (Preferred option): **Replicating the position in the 1998 Act in so far as we can to allow the processing of criminal conviction and offence personal data with appropriate safeguards.** This would make it possible for organisations to continue to process criminal conviction and offences data as they do under the 1998 Act to protect their organisations from potential criminal acts.

Evidence

These sectors could for example be impacted by this Article:

- Finance
- Insurance
- Pension Scheme and Charity Trustees
- Health

[50] There is no definition of official authority but the concept of official authority encompasses bodies which, in domestic law, are not public authorities per se but are vested with special powers beyond those ordinarily available in private law.

Most of the evidence we have is from our *Call for Views* in spring 2017. A common theme from the *Call for Views* responses was the concern that not exercising the derogation could lead to an increase in fraud.

Summary of Benefits

Non-monetised: Taking advantage of the derogation in Article 10 will have noticeable benefits across industries including banking, finance, insurers, pension schemes, media and the health industry. In the *Call for Views* many respondents touched on the additional costs they would face if they were not allowed to process criminal conviction and offences data. The derogation will allow industries to process suspicious activity reports, complete bank employee screening, including DBS checks, and allow them to underwrite claims management and lending decisions, all of which would increase costs for businesses if the government did not intervene. Some mentioned they would incur costs through management time, possible payment to specialised recruitment agency and set up costs / training etc. In the *Call for Views* there was concern in many industries, but most noticeably in the insurance sector who explained that without government intervention, they would have no legitimate basis to underwrite according to the level of risk and price of insurance premium. We believe that the costs to insurers would increase due to an increase in their risks and a negative impact on fraud detection.

Quantification: One organisation said that they pay approximately £40,000 per year for employment checks for 1,000 people. This provides a clue as to how much organisations value this data. Unfortunately we have not been able to monetise the impacts of organisations not being able to conduct employment checks because of difficulty in obtaining further required evidence. Organisations were not able to share further insights since these specific scenario analysis were not conducted by industry.

ONS estimates are that £22.1bn is spent per year by households on insurance. A small rise in insurance premiums could therefore have large cost effects, which could be prevented if the government intervene. We also obtained an estimate for the costs of fraud and provided a sensitivity analysis of the costs of an increase in fraud, which could be prevented if the government intervenes. The resource implications of estimating the extent to which insurance premiums and fraud might increase are too great for us to be able to monetise these impacts.

Monetised: Due to a lack of data we were not able to monetise the benefits that we had some quantitative data for.

Summary of Costs

Non-monetised: If the government did not intervene, firms would find it harder to screen employees for a criminal record or conviction. This could make it easier for ex-convicts to find a job if the derogation does not come into force, and could result in increased employment and rehabilitation across the country. However, there could be negative effects on the job market, for example ex-convicts may be able to become employed in jobs which they are not suited for, such as childcare.

Monetised: Due to a lack of data we were not able to monetise the costs

Employment and Pre-employment Checks

Many of the responses from the sectors below touch on the costs they could face if they are no longer able to process personal data related to criminal convictions or related security measures about their employees or for pre-employment checks. Some of the responses on this issue included:

- The CBI stating that 'the processing of personal data related to criminal convictions or related security measures is crucial to many industries such as financial services, insurance, credit and professional services'. Criminal data is 'essential in both employment contexts (employee vetting, employee security monitoring) and due-diligence (anti-money laundering, crime prevention, KYC checks, fraud prevention)'. They recommended that 'where possible, the government should ensure that existing legal justifications from the 1998 Data Protection Act are carried forward under the GDPR'.
- techUK stated that the 'government must make sure that there are sufficient lawful bases for processing criminal offence data, such as the fraud prevention one currently found in Schedule 3 of the Data Protection Act 1998'.
- Essex County council said 'that at the very least the same protections and requirements of the DPA should be in place'. They expressed concerns that there would be a 'gap' in protections over the processing of Personal Data for the prevention and detection of crime if the 1998 Act were repealed. The Information Records Management Society also stated that 'legislation should be drafted to cover this gap', and that it should 'at least' provide the same protections and requirements of 1998 Act.

Banking

The Association for Financial Markets in Europe and the British Bankers Association stated 'this derogation is particularly important, as the GDPR puts in place an absolute prohibition on the processing of such data in the absence of enabling legislation.' They suggest that not only do 'core financial service activities' need to be set as being in the public interest, but that in the context of Article 10, this must be a 'substantial public interest'.

They provided a list of examples of where the processing of criminal data is particularly necessary:

- Processing & disclosure of Suspicious Activity Reports
- Bank employee screening, including Disclosing and Barring Service (DBS) checks
- Know Your Customer screening
- Negative News / Adverse Press Screening - performing adverse press checks on clients and third party suppliers and their directors using third party databases (e.g. Worldcheck, RDC, LexisNexis) or public negative news repositories)
- Politically Exposed Persons Screening - screening customers/clients records against external databases to establish connections to Politically Exposed Persons (PEPs) as part of customer due diligence and onboarding
- Sanctions Screening - screen customers and beneficial owners against sanction lists (including US, EU, UK, and UN lists).
- Underwriting, claims management and lending decisions – fraudulent activity is factored into pricing models and decisions.

Finance, Fraud and Employment Checks

This section provides evidence on the costs of employment checks. However, we have not been able to monetise the impacts of organisations not being able to conduct employment checks because of difficulty in obtaining further required evidence. Some problems are that it is not clear how representative our figures are; how many organisations would be affected, and; how many organisations see checks as a compulsory burden or whether they do so voluntarily. We were unable to obtain further evidence through the *Call for Views.*

The Finance & Leasing Association (FLA) stated that the 'derogation is required to support employment screening in relation to jobs where a previous conviction or offence would be an issue of serious concern'. A particular issue is that there may be situations where there is no legal requirement for criminal checks but such checks are 'clearly justified'. This would be in any areas 'where roles have the capability to facilitate fraud or other offences, and working with vulnerable persons'. Equifax Limited made a similar point in their response.

Providing further evidence, the FLA stated that 'pre-employment checks are especially important for fitness checks on those in a position of influence or control', and that 'it is commonplace for firms to perform credit and criminal checks on their employees on a regular basis e.g. every year or two, depending of their level of seniority'. An association member 'estimated the cost of processing this for a business employing 1000 people at £40,000 per year'. This gives an indication of the value of pre-employment criminal record checks (and therefore the derogation) to financial firms, as it indicates that they are willing to forego at least £40,000 per year per 1,000 people in order to have them. This gives a cost of approximately £40 per employee (though this will probably be less for large companies; more for smaller companies). We have not quantified the effects of firms no longer being able to conduct employment criminal checks because:

- It's not clear how much these costs should be scaled up. We don't know how many firms (both in finance and all other sectors) would be affected by no longer being able to conduct employment checks if the derogation were not exercised.
- We don't know whether the figures quoted are representative of other firms the FLA represents, or firms from other sectors (the costs could vary considerably according to the size of the organisation conducting them). The FLA suggested that it would not be appropriate to extrapolate based on the figures from one member.
- We are not sure how not being able to conduct employment/criminal checks would affect businesses. If businesses conduct these checks through compulsion (e.g. authorities such as the Financial Conduct Authority (FCA) require it), then failing to exercise the derogation would save them money in the short run, as they would not legally be able to conduct the checks. Alternatively, if businesses conduct these checks voluntarily (e.g. they are willing to spend £40,000 per 1,000 employees to reduce the costs of fraud faced by them), then we could deduce that being able to conduct the checks is of value to firms by an order of at least £40,000 per 1,000 employees, and that this would therefore be a lost benefit if the derogation were not exercised. We are thus unable to quantify the number of businesses that employment checks are a cost and for whom they are a benefit. Nonetheless, the FLA indicated that many firms conduct subsequent checks to the ones that are required (e.g. by the FCA), with a view towards reducing reputational risk. The implication is that many financial organisation choose to conduct employment checks, so therefore not being able to conduct criminal checks as part of this process would be a concern to them.

- For some firms there could be considerable opportunity costs that would be difficult to quantify. The FLA said that although 'identifying the costs of not conducting criminal checks is quite difficult because if you were unable to process relevant data and recruited somebody who later turned out to have a criminal history and therefore wasn't (arguably) fit for purpose, the business would have incurred costs in respect of management time, possible payment to specialised recruitment agency and set up costs / training etc. This is without estimating the cost of the crime committed which could involve money or data stolen. In essence, firms process this [employee criminal] data to mitigate the costs of fraud and reputational damage'.
- One member of the FLA which processes data on behalf of lenders has indicated that 'if they could not carry out checks on staff as per FCA requirements, the cost of losing their FCA authorisation and FCA regulated customers would come in at around £10m per annum'.

Finally, the FLA said that if certain organisation could not process personal data on criminal convictions and offences, 'firms will be unable to protect themselves against fraud', and that that would put themselves 'at odds with FCA requirements'.

Insurance and Fraud

Insurers use fraud databases, including the Insurance Fraud Register (IFR) and the Health Insurance Counter Fraud Database ("HICFG"), with referrals to the National Crime Agency (NCA). Not being able to process criminal conviction data would mean that Insurers would no longer be able to use these databases which are important tools in the fight against money laundering and other organised crime.

The responses from our *Call for Views* allow us to set out the problems the insurance industry would face if the UK did not exercise the Article 10 derogation and the impacts that could follow. A large volume of respondents have expressed the importance of the derogation in Article 10 being exercised.

Concerns

Several organisations brought forward concerns about forming contracts, calculating risk and identifying fraud:

- Coop Insurance explain that without government intervention insurers like themselves will 'not have a legitimate basis' to:
    - 'Underwrite according to the level of risk and price the insurance premium accordingly.
    - Detect and reduce fraud, both by screening for previous fraud at point of quote/sale, and by assessing whether a claim is likely to be fraudulent.
    - Prevent fraud: via their own internal fraud registers and the Insurance Fraud Bureau, [where] insurers keep data relating to individuals and their conviction and offence data'.
- Motor Insurance Bureau explain that the insurance industry currently processes data relating to criminal convictions and offences as these are used to assess the risk of a potential policyholder. Processing this data is important for them so that they provide

‘accurate risk profiling, accurate pricing for consumers, a better customer experience and combating insurance fraud.’

- Cunningham Lindsey stated that ‘a common requirement for insurance is that a policyholder discloses any current criminal convictions’, and that if convictions are not disclosed contracts ‘may be void’. They therefore feel that they, and the rest of the insurance market, ‘have to process details of criminal convictions. Presently, Article 10 prevents us from doing so and some form of derogation is needed allowing the insurance market to process this data’.
- Aviva explained that they ‘require legislation to allow us to process data relating to criminal convictions for employment vetting purposes, insurance underwriting and anti-fraud purposes’.
- BGL Group stated that ‘Many businesses across the insurance industry, including BGL, rely heavily on processing personal data relating to criminal convictions or offences (in compliance with all legal requirements) to detect fraud, verify claims and to assess risk in order to ensure that insurance premiums are set at an appropriate level. It is therefore of vital importance to us and to the insurance industry as a whole for there to be appropriate derogations which allow insurance providers, intermediaries, underwriters, price comparison sites etc. to process this type of data for these purposes’.
- Direct Line Group also explained that for insurers the ‘processing of conviction information is necessary to perform a contract; can form part of an insurer’s legal obligations and it is a legitimate interest of insurers to process such data to prevent or detect fraud’.
- The Association of British Insurers said that ‘if no domestic legislation is introduced, then insurers will not be able to use criminal conviction and offences data to identify risk, underwrite, price accurately, handle claims and to help detect and prevent fraud. The processing of such data by insurers also helps act as a disincentive for criminal behaviour, and contribute to a safer environment and society with less of a burden on public service resources. They seek UK legislation for a derogation from the GDPR, ‘so that insurers can process criminal conviction data for the purposes of identifying risk and preventing fraud, and ensure that any such authorising legislation provides appropriate safeguards for data subjects’.

Impacts

Some organisations also expressed their opinion on the impact that not exercising this derogation could have on their business. They explained that there could be increases in insurance premiums and increases in insurance related fraud:

- Coop Insurance stated that ‘Insurance premiums for honest law-abiding customers are likely to increase’. They explain that ‘the majority of consumers will end up paying higher premiums to cross-subsidise payments made for fraudulent claims’.
- Concerning wider society impacts, Coop Insurance expressed concern that ‘criminals and would-be criminals will have a reduced disincentive to offend, as they will be treated in the same way as law-abiding citizens’. ‘This is likely to lead to a greater number of offences and fraudulent activity, including offences that put people’s lives and safety at risk. These activities, for example, “crash for cash”, in turn create an avoidable burden on public services (e.g. police, emergency services and NHS) to investigate the treat injured parties’.

- On Fraud: from Coop: 'The Association of British Insurers (ABI) estimates UK insurers, like ourselves, had detected over 130,000 fraudulent general insurance claims, worth £1.3bn in 2013. These frauds could only have been detected using sophisticated data analysis, which combines thousands of individual cases of fraud to detect patterns and trends on a large scale, and therefore enable an accurate identification of crimes'.

Quantification of Insurance Impacts

Premium increases:

- Office for National Statistics' Living Cost and Food Survey figures show that annual household spending on insurance products for the financial year to 2016 was £22.1bn.

Fraud Prevention:

- The ABI estimated in 2015 that through fraud screening by insurers, claims fraud with a total value of £1.3bn had been detected.

We explored the potential consequences of these costs increasing if we do not exercise the derogations in Article 9 to allow the processing of special categories of data. We believe the costs of insurance premiums and fraud would also increase if we do not exercise the derogation in Article 10, but similarly as there are evidence gaps we are unable to suggest the extent of the increases that might be caused by organisations not being able to process criminal convictions and security related data.

Pensions

Some members of the pensions sector expressed concern in our *Call for Views* about what could happen if they did not know of fraudulent/criminal activities an individual has committed. An example of this would be if someone was convicted of killing their spouse and then made a claim to the trust. They could profit from the offence if the trust could not process criminal conviction data. Independent Transition Management Limited explained that Pension schemes 'need to process data on criminal convictions' in case of examples like this.

Crimes Affecting Businesses

Intu Properties plc, who are largely focused on shopping centre management and development, highlighted the importance of the ability for them and other retailers to collect, share and receive information relating to criminal activity for their own crime prevention activities or to then share that information through organisations such as National Business Crime Solution (NBCS) to support private sector efforts to tackle crime and threats.

They further explain that NBCS is a not-for-profit initiative supported by the Home Office and the National Police Chiefs Council (NPCC) who provide a collaborative solution to tackle serious and organised crime affecting businesses, particularly in the retail sector. Intu highlights that "by working collaboratively and sharing data/intelligence on offences, businesses can take preventative action and better manage resources in relation to the risks". They also added that "by enabling the NBCS (as a nationally focused partnership) to coordinate the linked offences, especially when spanning numerous force areas this helps to ensure police only respond to

offences having the most harm and risk and also then ensures that those posing the most harm receive sentences for the full extent of their offending, rather than being dealt with in isolation". The latest statistics from the NBCS over the past 3 years show that NBCS member business collaboration resulting in the positive identification of over 419 suspects; the successful arrest of 309 offenders resulting from NBCS investigations; and sentences of over 200 years being imposed over that time for those having most harm and impact on member businesses.

Further Cases of Crime Prevention

- Employee vetting processes of many organisations could be majorly impacted
- Reducing the ability of companies to check criminal records reduces the consequences to convicts of having criminal records. The incentive against offending are therefore reduced, so an increase in crime may result.
- The National Society for the Prevention of Child Cruelty (NSPCC) is sometimes required to disclose personal data relating to criminal offences for the purpose of evidence in criminal proceedings. They also process data about criminal offences allegations in the course of providing their ChildLine confidential counselling service and their social work with children and families.
- Intu Properties PLC encourages the derogation for Article 10 to be invoked, and to 'introduce more specific provisions to cater for instances where the processing of data relating to preventing or detecting crime by the private sector (for example to investigate suspected criminal behaviour in retail centres and ban potential offenders) would clearly be in the public interest'.
- The Information Records Management Society stated that they wanted legislation with 'clear provision around the processing of special categories personal data for the purpose of DBS checks'.

Health

The General Medical Council explained in the *Call for Views* that it is 'crucial' that they are able to process information relating to criminal convictions and offences, as it is part of their process of determining an individual doctor's fitness to practise, and 'would also be relevant to the decision on whether an applicant should be granted registration'. They said that 'the government should ensure that criminal conviction and offence information can be processed by medical and professional regulators as it is clearly relevant to fitness to practice [of health professionals] and patient protection'.

The Department of Health gave a list of cases where legislation is 'required' to authorise the processing of personal data:

- Pre-employment checks on criminal convictions
- Counter-fraud
- Regulatory purposes - e.g. in deciding whether to register someone to carry on a health or social care service
- Serious case review
- Investigation of mental health related or domestic homicide
- Multidisciplinary reviews
- In the context of safeguarding boards

- Offender management e.g. someone is being released from prison and needs mental health input.
- Risk management and public protection in care settings

Impacts for Ex-Convicts

This derogation could also impact ex-convicts as data subjects.

- For example, they could waste time by applying for jobs for which they are not suited for due to their criminal record. It is helpful for employment seekers to know about the requirements that need to be fulfilled to be eligible for a certain position. If prospective employers would not be able to conduct employment checks, there could be lack of clarity over whether an employee is required to have a clean record. Alternatively not exercising the derogation could make it easier for ex-convicts to find employment.
- Some respondents in our *Call for Views* have pointed out that the consequences of committing crime would be reduced if organisations were not able to check their employees. Thus making it easier for ex-convicts to find employment could help to increase employment across the country, but reducing the consequences of committing crime could result in an increase in crime.

Assumptions and risks

The main assumption in this assessment is that exercising the derogations strikes an appropriate balance between individuals' data protection rights the specific public interest cases for the processing of personal data relating to criminal convictions and offences or related security measures.

Further Information

Article 10 states that processing of personal data relating to criminal convictions and offences or related security measures based on Article 6 (1) can only be carried out by an official authority unless Member States legislate to allow appropriate safeguards for this data to be processed by others. A comprehensive register of criminal convictions can only be kept and held by the official authority.

Article 6 (1) sets out a list of when processing of personal data can be lawful; therefore, personal data relating to criminal convictions and offences or related security measures cannot be processed under Article 10 without a lawful purpose under Article 6(1).

Article 23 - Public interest exemptions for data controllers and processors from the rights and obligations under the GDPR

Problem under consideration and the need for government intervention

Article 23 allows Members States to introduce legislation that restricts the scope of the rights for data subjects and obligations for organisation under the GDPR in certain circumstances. The test for applying restrictions to the obligations and rights in Articles 12-22, 34 and 5 of the GDPR requires that the restriction in question "respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society…" The restrictions are available for important objectives of general public interest, including for crime prevention and taxation purposes, the protection of judicial independence and judicial proceedings and the protection of the data subject or the rights and freedoms of others and for the purposes of important economic, budgetary and financial interests. Intervention is required to set out a range of measures in domestic law that safeguard these public interests.

Policy objectives and the intended effects

The government's objective is to maintain the effect of the exemptions currently contained in the 1998 Act to the full extent permitted under the GDPR, and to extend them to any new rights introduced under the GDPR where necessary. A number of new exemptions will be introduced where these are justified by the changes to the existing data protection regime made by the GDPR. The government intends to maintain the approach adopted under the 1998 Act whereby the exemptions exist for various purposes only, and not entity or sector. The UK already provides a comprehensive data protection regime, with appropriate exemptions that. We therefore propose to give full effect to the GDPR requirements which afford enhanced protection to data subjects without putting unjustified additional burdens on data controllers. The government intends to keep the burdens on businesses and other organisations as light as possible, giving organisations clarity and certainty where possible but beyond that allowing them the freedom to operate efficiently.

Policy options

Option 1 (Do nothing): **Not exercising the derogation.** Domestic legislation is required to give effect to the derogations under Article 23. If no action is taken, full compliance with the GDPR will not be achievable as there are specific processing purposes which require restrictions to the rights and obligations under the Regulation.

Option 2 (Preferred option): **Create domestic legislation which will allow us to exempt data processors and controllers from the key rights and obligations in the GDPR in certain circumstances.** This will entail reviewing existing exemptions and implementing them under the GDPR, suitably modified to ensure compatibility, therefore causing no disruption to business' current data policies, with necessary changes.

<u>Another option was dismissed due to its impact and concerns about the feasibility. This option was therefore not analysed in the impact assessment:</u>

Option 3 - Implement the derogation partially by introducing legislation that covers a selection of the exemptions from the key rights and obligations in the GDPR that currently exist under the 1998 Act. This would not minimise disruption to current business practices and would prevent certain data processes that would be in the national interest.

Evidence

As the government's objective is to maintain the effect of the exemptions currently contained in the Data Protection Act 1998 to the full extent permitted under the GDPR, the approach should be seen as deregulatory. It minimises the extent to which GDPR could restrict activities, and also minimizes any transition costs that could have been incurred if the 1998 Act were significantly departed from. The full information section lists the areas exemptions can be made.

Summary of Benefits

Non-monetised benefits: Organisations that are currently processing data and exercising exemptions under the 1998 Act will retain the ability to continue to rely on those exemptions. The impact to organisations of taking the preferred option is minimal as it would retain the approach adopted under the 1998 Act. The main impacts therefore are the avoidance of the costs from additional regulatory burden for organisations that would result if the derogation was only partially exercised (option 3) or not exercised at all (option 1). These costs would result mainly from the obligation that organisation would need to follow in order to process data and the administrative actions organisations have to take with regards to the rights of individuals. It is difficult to measure the amount of organisations in the public, private and third sector that would not be able to process data with regard to the exemptions and would experience a greater burden.

Monetised benefits: Due to a lack of data and the difficulties of obtaining the data from organisations we were not able to monetise the benefits. During our *Call for Views* we did not receive substantive evidence that would have supported a monetisation of benefits and also following up on specific issues did not provide any further insights because organisations were not able to provide detailed evidence for different scenarios.

Examples of cases where exercising exemptions could lead to benefits which stakeholders highlighted in the *Call for Views:*

- **Preventing crime**: Without exemptions to the regulation, there could be circumstances where subject access and disclosure of personal data would be likely to prejudice crime prevention. An example for this is the exercising core financial service activities which are in the public interest. Industry stakeholders highlighted that exercising this derogation does not mean that firms should be able to avoid informing data subjects that their personal data will be processed for the purposes of preventing financial crime but the exemptions ensure that data subjects are not given details about specific relevant processing that would impede the core financial service activities. For example, where a firm has a suspicion that a customer is engaged in illegal activity and must pass information to law enforcement agencies, firms cannot provide a 'just in time' fair processing notice to the customer advising them of this data sharing, as this would amount to a 'tipping off' offence and would put an investigation at risk.

- **Keeping trade secrets and intellectual property safe**: ability to withhold information about the logic involved in automated decision- taking if, and to the extent that, the information constitutes a trade secret for example with regard to the right to data portability.

Also other stakeholders highlighted the importance of maintaining the current restrictions. The Information Commissioner for example believe that "it is important that a number of restrictions as currently set out in the DPA are maintained". The CBI also "supports government legislating in specific situations to restrict the applicability of data subject's rights" and explain that "existing exemptions within the 1998 Data Protection Act ensure that the rights of data subjects do not go unfettered but are necessarily and proportionately balanced against the public interest of a properly functioning tax and judicial system." The ABI stated that government should legislate to continue similar restrictions that exist under the current Directive and which were used in the 1998 Act, to shape appropriate exemptions from the requirements of the 1998 Act where that was permissible. The Charity Commission would welcome an exemption to the right of access similar to that in the 1998 Act. The Manufacturing Society comment that, "save where the Government considers that Article 23 might allow for broader exemptions (i.e. greater restriction of individual rights, more freedom for data controllers/ processors), we would recommend maintaining the existing exemptions that apply under the DPA where possible"

Summary of Costs

Non-monetised costs: The exemptions for data controllers and processors from the rights and obligations limit the rights of data subjects. Digital rights organisations replied to the *Call for Views* and highlighted with regard to Article 23, for example, the following: EDRi note that the provision is not limited to exemptions for the benefit of public authorities only, but can also be used to exempt private-sector controllers (companies) from the normal requirements relating to data subject rights, e.g., in relation to online fraud detection by banks which the association sees critically. Privacy International agree that, the list is largely the same as the corresponding one in the 1995 Data Protection Directive (Article 13(1)). While the discretion under this provision is significant, it should be noted that any restrictions must "respect […] the essence of the fundamental rights and freedoms" and must be "a necessary and proportionate measure in a democratic society" to safeguard the listed interests.

Monetised costs: Due to a lack of data and the difficulties of gathering further evidence for specific scenarios we were not able to monetise the costs.

Assumptions and risks

The main assumptions with regard to this Article are that the exemptions being introduced provide an appropriate balance between individuals' data protection rights and the safeguarding of the public interests mentioned in the derogation (these are listed in the 'further information' section). Risks include the non-application of relevant exemptions in the required processing circumstances and the abuse of the exemptions by data controllers to justify processing of personal data.

Further Information

Members States can restrict the scope of the rights and obligations provided for in Articles in the GDPR to safeguard the following interests:

- National security
- Defence
- Public security
- The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security
- Other important public interests, in particular economic or financial interest, such as monetary, budgetary and taxation matters, public health and social security;
- The protection of judicial independence and judicial proceedings
- The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- A monitoring, inspection or regulatory function connected to most of the cases above
- The protection of the data subject or the rights and freedoms of others
- The enforcement of civil law claims.

The exemptions can relieve the data controller (or processor) from all or some of the obligations of transparency, notice, subject access requests, rectification, erasure, restriction on processing, notice of rectification, erasure or restriction, portability, objection, control of automated decision-making and notice of the personal security breach to the data subject as well as the data protection principles to the extent that they correspond to the aforementioned rights and obligations. The rights and obligations set out in the GDPR are designed to apply generally, but some of the exemptions being proposed are designed to accommodate special circumstances. If an exemption applies, then (depending on the circumstances) a data controller or processor will be exempt from the requirements relating to, but not limited to, granting subject access to personal data and giving privacy notices. The entitlement to an exemption depends in part on the purpose for processing the personal data in question. Each exemption has to be considered on a case-by-case basis because the exemptions will only permit departure from the GDPR's general requirements to the minimum extent necessary to protect the particular functions or activities the exemptions concern.

Article 84 - Penalties

Problem under consideration and the need for government intervention

The 1998 Act includes a range of criminal offences to deal with the worst cases of misuse of personal data. We need to make sure that these are transferred into the new legislation that implements the GDPR. This exercise provides us with an opportunity to modernise those offences that are no longer fit for purpose and address new offending behaviour which has become possible in recent years due to developments in technology.

Policy objectives and the intended effects

The government will retain most but not all existing offences under the 1998 Act, with some modifications and extensions and will also create some new offences. The aim of this policy is to ensure that offenders who, for example, unlawfully obtain, disclose or sell sensitive data or obstruct the Information Commissioner in carrying out her activities, continue to be liable to effective sanctions. Although most of the penalties for offences in the 1998 Act will remain unchanged, all offences will become recordable for the first time, so that convicted offenders are left with a meaningful criminal record.

Policy options

Option 1 (Do nothing): Not exercising the derogation. If the government doesn't act to reproduce offences in the 1998 Act, offenders responsible for the worst breaches of people's privacy could no longer be criminally prosecuted. The Information Commissioner could only rely on administrative fines which would not be sufficient to reflect the seriousness of the offending in some extreme cases. Furthermore, new types of offending behaviour, such as re-identifying data which has been encrypted in digital files would continue to go unpunished by the criminal.

Option 2 (Preferred Option): Reproducing, extending, amalgamating and creating new offences:

a. Reproduce offences in the 1998 Act which remain fit for purpose. Maximum penalties (fines) would remain the same as now. These include: i) offences relating to enforced subject access, e.g. where an employer asks a prospective employee to obtain data to which the organisation would not normally be entitled (s.56 of the 1998 Act); and ii) powers for the Tribunal to commit to the High Court any conduct on the part of the defendant that would amount to contempt of court (Sch. 6, para 8 of the 1998 Act). These offences would continue to be triable either way and the maximum penalty on indictment would be an unlimited fine. The offences would become recordable;

b. Extend the offence of unlawfully obtaining personal data (under s.55 of the 1998 Act) so that it covers unauthorised 'retention' of data and create a new defence for journalistic activity. The offence would continue to be triable either way and the maximum penalty on indictment would be an unlimited fine. The offence would become recordable. Extend the offence in s.77 of Freedom of Information Act 2000 (altering records with intent to prevent disclosure) so that it applies to all data controllers and processors, not just public authorities. The penalty for the offence on summary conviction (currently a fine) would remain unchanged.

c. Extending offences relating to unlawful disclosure of personal data obtained by the Information Commissioner in connection with their investigations (s.59 of the 1998 Act) to cover material obtained by the Information Commissioner under certain other statutory regimes that it regulates.

d. Amalgamate three separate offences (in sections 47, 54A and Sch.9, paragraph 12 of the 1998 Act) relating to the obstruction of the Information Commissioner's investigations into a single recordable offence of obstruction. The offence would be triable either way and the maximum penalty on indictment would be an unlimited fine. The offence would be recordable;

e. Create new offences relating to re-identifying anonymised or pseudonymised data. This responds to one of the recommendations in the National Data Guardian for Health and Care's "Review of Data Security, Consent and Opt-Outs".[51] Given that patient data is now increasingly held in encrypted digital files, both Dame Caldicott and the Information Commissioner consider that an offence of intentionally decrypting such data would increase confidence in the NHS and provide a powerful disincentive. The offence would be triable either way. The maximum penalty on indictment would be an unlimited fine and the offence would be recordable.

Proposals b, c and e above may have a new impact on business insofar that they widen existing offences or criminalise new behaviour and are therefore the focus of the assessment. However, businesses which have good data protection practices in place are unlikely to be affected by these changes.

Evidence

The government committed to introduce a re-identification offence as part of the UK Digital Strategy. This followed recommendations in the National Data Guardian for Health and Care's "Review of Data Security, Consent and Opt-Outs" about the importance of safeguarding sensitive patient data, which is increasingly held in digital format.

There have been repeated calls by Parliamentary Select Committees,[52] the Information Commissioner[53] and in the Leveson Report to strengthen the offence of unlawfully obtaining, disclosing or selling personal data under s.55 of the 1998 Act.

Most of the criminal offences will be capable of being committed by any person. There will be an impact on the, Information Commissioner, police and the Crown Prosecution Service, who may be required to investigate and prosecute the offences, and the courts who will need to determine sentence. Enforcement agencies and the courts may need guidance on the changes we are making to existing offences and on the new offences relating to re-identifying encrypted personal data. As we are not proposing to introduce any custodial sentences, there will be no impact on the prison service.

---

[51] https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs
[52] https://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/46809.htm#_idTextAnchor035
[53] https://ico.org.uk/media/about-the-ico/consultation-responses/2016/1625324/ic-evidence-public-bill-committee-on-digital-economy-bill.pdf (paragraph 33) and https://ico.org.uk/media/about-the-ico/consultation-responses/2017/2013384/digital-economy-bill-lords-committee-briefing-20170202-pdf.pdf (paragraph 8)

Summary of Benefits

Non-monetised: These new offences will ensure that the worst breaches of data security continue to be prosecuted by the Information Commissioner and/or other relevant prosecuting agencies and protect the rights of data subjects. The proposals widen existing offences and criminalise some new behaviours, such as intentionally decrypting anonymised files. The belief is this will increase confidence in systems, including the NHS, and provide a powerful disincentive for this kind of cyber-attack. There is also an extension which criminalises the unauthorised retention of data, providing a deterrent to people who might be permitted to access data initially but are not permitted to retain it indefinitely.

Monetised: Due to a lack of data and the difficulties in gathering further evidence after our *Call for Views* we were not able to monetise the benefits. Organisations were able to provide illustrative examples but were not able to share insights which were needed to conduct an analysis of the overall impact of this derogation option.

Summary of Costs

Non-monetised: Three streams summarised below:

Unlawfully obtaining and retaining data: The offence of unlawfully obtaining data under section 55 of the 1998 Act is the most prosecuted data protection offence. In 2016-17, the Crown Prosecution Service prosecuted 39 cases and in 2015-16 the figure was 69. The Information Commissioner report that they prosecuted 33 such cases between January 2014 and March 2017. If the offence were widened to cover the unlawful retention of data (e.g. where somebody may have accessed the data lawfully but held onto it for longer than permitted), this might lead to a marginal increase the overall number of prosecutions under s.55. The offence is being widened primarily in light of the first instance decision in ICO v Adair, Robert and Evans[54] which suggested acts of retaining data were not covered by the offence, even where the defendant knew he or she was no longer permitted to hold it. It is worth noting that many prosecutions under s.55 occur alongside prosecutions for more serious offences (such as misconduct in a public office, fraud, bribery or offences under the Computer Misuse Act 1990. The Criminal Proceedings Database records very few convictions for s.55 as the principal offence in either of the last two years. This could mean that even if the offence were widened to include the unlawful retention, the impact on the overall caseload in the courts is unlikely to be significant.

Extending the offence in s.77 of the Freedom of Information Act 2000 of altering records to prevent disclosure and frustrate subject access requests: Extending the offence so that it also applies to data controllers in the private sector could also lead to some additional prosecutions. It is difficult to estimate with any precision how many individuals in the private sector would be prosecuted for this offence due to a lack of data. The MoJ's Court Proceedings Database shows no prosecutions or convictions of public officials in the last 5 years (although that database records convictions on a principal offence basis and it is possible that defendants may have been prosecuted for more

[54] https://www.ncoa.org.uk/media/3741/ICO-v-Adair-Evans-and-Roberts-dismissal-judgment-final.pdf

serious offences at the same time). We therefore anticipate the number of additional prosecutions would be very small.

New re-identification offence: This offence is not expected to immediately result in a significant number of new prosecutions. There is no data on the prevalence in the UK of this offence currently. Evidence from Australia and New Zealand suggests that anonymous data can be decrypted by criminals with the technological knowhow, but it is difficult to predict how widespread this issue might become. We are seeking to modernise our legislation to guard against unquantifiable future threats.

Monetised: Due to a lack of data and the difficulties we experienced in gathering further evidence on this specific derogation and the cost implications we were not able to monetise the costs.

Assumptions and risks

The main assumption is that it is already good practice to neither unlawfully retain data nor altering records with intent to prevent disclosure, nor deliberately or recklessly re-identify anonymised or pseudonymised data.

Article 85 - Processing and freedom of expression and information

Problem under consideration and the need for government intervention

Article 85 requires Member States to provide exemptions or derogations from certain rights and obligations in the context of processing personal data for journalistic, academic, artistic and literary expression purposes (together referred to as the special purposes), if such exemptions or derogations are necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information. If the government does not act the special purposes would be subject to all the obligations and responsibilities on data controllers in the GDPR. This is likely to have an adverse impact on freedom of expression.

Policy objectives and the intended effects

The focus of the policy is around preserving the status quo as far as this is possible, to maintain the correct balance between personal data rights and freedom of expression in the public interest. Relevant responses to the *Call for Views* generally support this approach.

Policy options

Option 1 (Do nothing): Not exercising the derogation. If the government does not act the special purposes would be subject to all the obligations and responsibilities on data controllers in the GDPR.

Option 2 (Preferred option): Fully exercising the derogation by preserving the s.32 exemption in the 1998 Act and the limited enforcement regime in sections 44, 45 and 46 of the 1998 Act. This also includes making these exemptions available for academic expression, which was not part of the special purposes under the 1998 Act.

Evidence

The GDPR is substantively similar to the 1995 Directive in its treatment of the freedom of expression carve out. The GDPR provides that Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities, including where processing relates to freedom of expression and information. Member States should reconcile the rules governing freedom of expression and information (formerly just ‘freedom of expression’ under the 1995 Directive), including journalistic, artistic, literary and (the newly added) academic expression, with the right to the protection of personal data (formerly ‘privacy’ under the 1995 Directive). The GDPR provides that the primary objective of any exemptions or derogations in this area should be the balancing by Member States of the two competing sets of rights.

The main affected groups are data controllers and processors that process data because of journalistic, artistic, literary and or academic expression and data subjects whose data is processed for these special purposes.

Data controllers and processors that are part of the creative sector, which includes almost 250,000 businesses in the UK[55], may be impacted by this policy. More specifically the Annual Business Survey 2015 shows that there are about 11,000 businesses in the UK that are classified as carrying out publishing activities and about 430 that are involved in publishing newspapers. With regard to the data controller register, Information Commissioner research shows that about 6,600 organisations could be classified as media organisations. Around 29,000 organisations are classified as creative, arts and entertainment activities of which around 16,000 are categorised as artistic creation. Furthermore, Universities UK estimates that the number of higher education institutions in 2014-15 in the UK was 164[56] which can be used as a lower estimate of the organisations impacted by this article in relation to academic expression. These statistics show that between 6,600 and up to 250,000 organisations could process personal data for journalistic purposes and the purposes of academic, artistic or literary expression.

Summary of Benefits

Non-monetised: Exercising this derogation brings a benefit to controllers and processors that process data for journalistic purposes and the purposes of academic, artistic or literary expression and the society as a whole. This is supported by a number of responses in the *Call for Views* as set out below:

- **Journalism and media:** *The Guardian* for example noted that this exemption is critical for freedom of expression and journalists. The organisation further underlines that the current exemption for the special purposes set out in s.32 of the 1998 Act is generally considered to be a broad protection and provides a good framework for the new derogation under the GDPR. *The Guardian* also highlighted that "Journalism, by its very nature, requires the processing of large volumes of personal data, for instance through the gathering, collation, storage and retention of information. In many cases, only a tiny fraction of this information will be published, after careful consideration with regard to editorial standards and wider legal obligations. It is an integral part of many very important stories, from Panama Papers to investigations of the corporate and tax affairs of Sports Direct and Boots". The *News Media Association* also indicated that "it is imperative that the UK government implements Article 85 to the widest possible extent, in addition to the derogations and exemptions to individual Articles which would also benefit freedom of expression and freedom of information including journalistic processing". The *Media Lawyers' Association* and its member *Which?* emphasise that the journalism exemption in the 1998 Act has been important "in enabling *Which*? to process personal data during the course of undercover investigations if, as a publisher, we believe it's in the public interest". Without this exemption it would be difficult to conduct and publish investigations which helped identify, expose and amplify areas of consumer detriment and harm. *Which?* therefore argues that a restriction of the ability to process personal data in the public interest could have a considerable impact on the protection of consumers across markets.
- **Academic freedom of expression:** The *British Academy and Economic & Social Research Council*s submission to the *Call for Views* underlines the benefits for data controllers in the field of academic research. They also indicate that this submission was "the result not least of sustained advocacy by UK civil society such as the ESRC 2013

[55] DCMS (2016), DCMS Sectors Economic Estimates, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/544103/DCMS_Sectors_Economic_Estimates_-_August_2016.pdf
[56] Universities UK, https://www.hesa.ac.uk/data-and-analysis

Statement[57] but also repeated inclusion of the issue in Wellcome Trust submissions". The Wellcome Trust 2015 statement put emphasis on the importance of the academic freedom of expression derogation "because research in areas such as politics and history is unlikely to be compatible with the research model set out in Article 83 [now Article 89] and may not be permitted otherwise"[58]. Furthermore, the *University of Cambridge* indicated that explicit addition of processing for academic expression in Article 85 is beneficial for the university.

- **Further evidence of benefits:** Also other organisation such as *Tech UK* are of the opinion that government must maintain the exemption set out in section 32 of the 1998 Act.

Monetised: Due to the lack of extensive data on the monetary benefit of freedom of expression no benefits have been quantified. We were unable to gather further evidence to monetise the impacts through the *Call for Views*, and to obtain further evidence would require a disproportionate use of resources.

Summary of Costs

Non-monetised: There has to be a balance between the rights of individuals and the exemption of data processors with regard to freedom of expression and information. Human rights advocates generally support the exemptions that support freedom of expression and information[59]. However, there could be a cost to individuals through the reduction of privacy rights if their personal data is processed subject to exemptions for journalistic purposes and the purposes of academic, artistic or literary expression.

Monetised: Due to the lack of data of how many people are subject to processing under these circumstances and what the monetary consequences for them due to this type of processing would be, no impacts were quantified. After the *Call for Views* we conducted further research to answers these questions but no comprehensive overview of the situation from organisations was available.

Assumptions and risks

The main assumption in this assessment is that the current balance between the right of freedom of expression and information and the rights with regard to data protection is adequate.

---

[57] ESRC (2013), Response to the European Commission's proposed European Data Protection Regulation, http://www.esrc.ac.uk/files/about-us/policies-and-standards/esrc-response-to-the-european-commission-s-proposed-european-data-protection-regulation-2013/

[58] Wellcome Trust (2015), Academic research perspective on the European Commission, Parliament and Council texts of the proposal for a General Data Protection Regulation, https://wellcome.ac.uk/sites/default/files/research-perspective-data-protecton-regulation-proposal-wellcome-jul15.pdf

[59] see EDRI (https://edri.org/files/1012EDRi_full_position.pdf) and Open Rights Group's (https://www.openrightsgroup.org/assets/files/pdfs/submissions/OpenRightsGroup-GDPR-derogations-consultation.pdf) statements

Article 89 - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Problem under consideration and the need for government intervention

Article 89 recognises that it might be necessary for organisations to process personal data for scientific and historical research, statistical purposes or archiving in the public interest. Processing is permitted for such purposes under Article 89(1) if appropriate technical and organisational safeguards are in place to protect personal information from misuse. Article 89(2) and (3) gives Member States the discretion to use domestic legislation to exempt research organisations from complying with some of the rights people have to access or amend their data, or to prevent further processing, if responding to such requests would seriously impair their ability to complete their work. Government intervention is therefore needed to ensure that the derogations available for research organisations are set out clearly in UK law so that valuable research and archiving projects are not compromised.

Policy objectives and the intended effects

The government intends to replicate the position under the current law as far as possible. Section 33 of the 1998 Act exempts processing for research purposes from the subject access provisions in section 7 of the 1998 Act, providing that the processing does not support decisions about individuals or cause them substantial damage or distress. By ensuring that all the derogations available for research organisations under Articles 89(2) and (3) are set out clearly in UK law the government will be providing research organisations and archiving services with a similar degree of flexibility as they currently have under the 1998 Act.

Specifically, the government intends to exempt research organisations from having to comply with the subject's rights to access (Article 15), rectification (Article16), restriction of processing (Article 18) and objection to processing (Article 21), where this would seriously impede their ability to complete their work, and providing that appropriate organisational safeguards are in place to keep the data secure. Two further exemptions are available for organisations which are responsible for archiving in the public interest, namely from the obligation to alert third parties with whom the data might have been shared of any changes made in response to a rectification request (Article 19), and from the right of data subjects to data portability (Article 20).

Policy options

Option 1 (Do nothing): The government would not invoke any of the derogations from subject access provisions and all other rights and obligations in respect of research organisations. This would mean that they would have to comply with the subject access provisions in the same way as any other organisation, even if this seriously impaired their ability to do their work.

Option 2 (Preferred option): The government's preferred option is to replicate section 33 of the 1998 Act as far as possible. This will involve exempting all research organisations from those subject access provisions specified in Article 89 of the GDPR, where compliance would seriously impair their ability to complete their work. This option would exercise all of the exemptions available, and would mean the UK would be meeting the minimum requirements the GDPR allows for Article 89. Research organisations would still need to ensure that adequate safeguards were in place to protect personal information from misuse and they would still have to comply with subject access provisions from which they were not exempt, including the duty to tell people at the outset how information about them would be used (see Article 13 which doesn't form part of the derogations).

The following options were not further assessed in the impact assessment as they were dismissed due to the burden they would put on organisations and their failure to achieve the government's objective:

Option 3: The government would exercise derogations under Article 89 (2) but not Article 89 (3), or vice versa. This option was considered and rejected. It would either mean that organisations involved in scientific, historical or statistical research would benefit from the derogations from subject access rights and other rights and obligations, and archiving services would not; or that archiving services would benefit from the derogations and the other research organisations would not. There would be no good reason to make such a distinction when the activities of either could be seriously impeded if they were required to comply with subject access rights and other rights and obligations. The burden of complying with subject access rights has been quantified.

Option 4: The government would exercise some, but not all, of the derogations under Article 89(2) and (3). For example, the government could require organisations processing for the purposes of archiving in the public interest, scientific or historical research or statistical purposes to give people access to any data held on them (under Article 15) but provide that they do not have to rectify it (Article 16) or restrict processing (Article 18) if doing so would seriously impair the achievement of such purposes. This option was considered but rejected as being unworkable. The challenge for many research organisations is locating the data in the first place. Where it is being used for scientific or statistical research, personal identifiers might have been removed and re-identifying individuals who had originally provided the data might be very difficult and time consuming. Where it is held in an archive, it might be found in a wide range of source material spanning many years. In these circumstances, it would be disproportionate for such an organisation to comply with the initial subject access request.

Option 5: The government would invoke specific derogations in Articles 89(2) and (3) in respect of some research organisations and not others. For example, research organisations that were doing work which would have clear benefits for the public (e.g. research into cures for cancer) could be given more leeway than other types of research organisation. This option was considered and rejected because it would be disproportional to the scale of the measures involved. It would be very difficult to assess with objectivity which causes were the most worthy and such a proposal could arbitrarily favour or disadvantage certain organisations.

Evidence

The government's favoured option is to invoke the derogations for research organisations. As this minimises the extent to which GDPR could restrict research activity, this measure should be seen as deregulatory. In contrast, the other options could seriously impair the ability of some research organisations to complete their work and are consequently not favoured by government.

Summary of Benefits

Non-monetised: In response to the government's *Call for Views* many research organisations (including a wide range of businesses and business groups, universities and groups, the General Medical Council, county council, Sport England and more) expressed concern about the consequences of the government not exercising the derogations. Their activities would be seriously impeded if they were frequently expected to locate a person's information from a wide range of research material where direct identifiers might have been removed in order to comply with rights under the GDPR. In the case of archives, data about an individual might be held in numerous collections over considerable time spans from multiple sources, many of which will be paper based with limited index information. Finding somebody's personal data that might have been created decades ago would be hugely resource-intensive.

Monetised: In the case of Subject Access Requests (where an individual has the right to request a copy of the data an organisation has about them), we have produced a monetised estimate of what the costs would be in the 'administrative costs prevented' section.

Summary of Costs

Non-monetised: There are risks that data protection rights could be infringed upon, particularly as it could be unclear who in some cases who when personal data is processed for research purposes and what qualifies as being in the 'public interest'. However, replicating the existing legislation (which is nearly 20 years old) as far as possible should reduce these uncertainties as affected organisations will be familiar with the legislation and its definitions.

Monetised: Due to a lack of data and the difficulties of gathering further evidence that was not provided in our *Call for Views* we were not able to monetise the costs.

Research

A substantial amount of *Call for Views* responses supported the retaining the current position as far as possible:

Business organisations:

- The Direct Marketing Association made clear that the 'UK is an attractive research base and in order to enhance this position the UK should implement the derogation in Article 89 (3)'.

- techUK explained that 'the Government should invoke this derogation by maintaining the research exemption in Section 33 of the Data Protection Act 1998', as it would 'prevent a barrier to innovation and allow organisations to conduct big data analytics, modelling and statistical analytics which do not lead to decisions or measures about individuals, or which do not cause damage or distress'.

Higher education:

- Universities UK, the Russell Group, the Universities of Cambridge, Manchester and Birmingham and JISC (providers of IT in universities) all suggest that subject access provisions could conflict with the aims of research or objectives of archiving, and that in these cases derogations should be invoked. Individuals (especially if acting together) could affect the outcomes of important research by applying the Rights in Articles 15, 16, 18 and 21.

Health:

- The General Medical Council explained that failing to exercise the derogations in Article 89 could seriously impede their research. Their concern is that much of their research 'relies on having a complete cohort in the dataset – if individuals could opt out in significant numbers or prevent the processing, this would reduce the value of the data or make it unusable'. In relation to one of their most significant research projects, UKMED, they explain a number of relevant concerns:
    - SARs, Article 15 - they estimate that there are currently 60,000 individuals in their dataset, but since the data is anonymised, SARs would cause a significant administrative burden to them.
    - Restriction of processing, Article. 18 - 'If large numbers of individuals exercised their right not to be included in the research, it would have less value. This would in turn make the processing of other individuals' data more difficult to justify, as it would not necessarily result in worthwhile research outcomes'.
    - Right to object, Article 21 - 'Research projects can have a long lifespan and contain interlinked data. It would not be practical to remove an individual's data from a dataset halfway through a research project, or to pause a project while considering an individual's objection'.
    - Conclusion: they have 'serious concerns that without the derogations, large scale research projects such as UKMED would not be viable because the reduced quality of the output could not be justified by the increased burdens. This would leave the GMC less able to improve standards of medical training and less able to assist the government's workforce planning objectives'.

Other organisations:

- The Information Commissioner stated that 'the exemption in s.33 of the 1998 Act should be replicated as far as possible under the GDPR'. Their rationale is that 'the basic principle that rights can be dis-applied where the collection of data has no direct effect on any individual remains valid'.
- Essex County Council and Sheffield City Council - support use of derogations where this would seriously impede research-based activities

Archiving

- Archives and Records Association have said that as far as possible, current approach to archiving under s.33 of the 1998 Act should be preserved.
- National Library of Scotland and British Library stated that 'all the derogations under Article 89(3) are essential for proper operating of the library', and that the 'derogations under Article 89(2) should be invoked for research purposes'.
- Many organisations (including the National Library of Scotland and British Library, Cultural Heritage Institutions Privacy Alliance, Royal College of Physicians and more have pointed out that many archiving services (possibly with the National Archive being a single exception), may not have a 'legal basis' for being carried out, but that they should still be protected i.e. by invoking the derogation. The Natural History and Imperial War Museums feel that subject access rights could undermine their objectives to maintain permanent archives, while the Heritage Alliance supported the use of derogations to all for effective archiving.
- The NSPCC archive cases where it has been involved in protecting children. They explained in their response that 'the NSPCC processes personal data and special categories of personal data in order to evaluate the effectiveness of its services in protecting children from harm. We also conduct research in order to establish policy and campaigning objectives, for example our research into the prevalence of sexual abuse of children. These research objectives are in the substantial public interest. Where practicable and fair, we obtain the consent of data subjects but there are circumstances where we rely upon the provisions of s33 of the 1998 Act and safeguards such as our research approval process'. It is therefore vitally important for the protection of children that the derogations in Article 89 are exercised.

Preventing Criminal Activity

- Cifas, a UK fraud prevention service, collects information on fraudulent activity and shares it with credit card companies, insurers, police etc. Derogations for archiving and research functions would reduce barriers to their fraud prevention work.

Avoidance of administrative costs

Office for National Statistics Case Study

While the Office for National Statistics currently only receive, on average, between 10 and 20 SARs a year, this is likely due to the current exemption for data processed for statistical purposes within the 1998 Act. It is impossible to say how this number would increase were the exemption to be lost. ONS explained that the cost associated with complying with a single SAR in the absence of the exemption would be disproportionately high due to the effort that would be required to locate information. ONS currently hold information in approximately 600 administrative datasets from many different sources, in addition to information obtained from 100 different surveys, including the census. All of this information can be held in different formats, in different secure locations and, for the most part, will have had direct identifiers removed, while still remaining personal data. All of which will make it both difficult and time consuming to find all the personal data held in relation to a single individual. For example, finding one individual's return, from one census, could take a single

staff member a number of hours, and that's assuming that the individual can recall their address for that particular census night. ONS also note that the cost of losing the exemption would not be limited to complying with individual requests; they would need to completely re-assess how personal data is held across the organisation. There would be considerable cost and resource implications in complying with GDPR in the absence of the Article 89 derogations. However ONS emphasise the primary reason for the exemptions is the fact that processing for statistical purposes benefits society by informing policy making and public debate, but has no impact upon individuals.

Quantification of Admin Costs

It is difficult to quantify what the costs would be if the derogation were not exercised, as currently section 33 of the 1998 Act exempts processing for research purposes from the subject access provisions. We can, however, in some cases assume what the cost would be to research organisations if they did have to face subject access provisions. We have done this for subject access requests.

Subject Access Requests (SARs) Costs:

- **Estimates of the costs for firms from answering a SAR:** the 2011 Post Implementation Review of the 1998 Act estimated a SAR to cost between £100 and £500. In response to the UK's 2012 Call for Evidence, Mobile Broadband Group reported this estimate to be correct, stating that with 'most responses' estimated an average of between £100 and £500'.[60] We don't know what the mean cost overall would be for an SAR, so we have taken the mean of this range, £300, to be our expected estimate, and used the £500 - £100 range to provide our maximum and minimum estimates. All of these estimates could be considered to be conservative given the evidence we have received from suggesting that SARs would be particularly costly for them to comply with (such as the ONS case study). We have assumed that this cost is representative of all sectors, given that the 2012 Call for Evidence also states that 'there was no clear evidence to equate the cost of compliance with a SAR with whether the data controller was a public authority or a private company'.
- **Estimates of the number of research organisations that would have to comply with them:** In June 2017 there were 477,278 organisations on the Information Commissioner's Data Controller Register.[61] Splitting these into different sectors, based on Information Commissioner research[62] we've estimated that:
    - 68.3%, of these are from the private sector (325,982)
    - 28.2% are public (134,593) and
    - 3.5% are charities (16,705).
- Information Commissioner Analysis on the data controller register also suggests that for those that hold personal data for research purposes there are:
    - 1.2% of organisations from the private sector (3,912)
    - 0.4% of organisations from the public sector (538)

60 Call for Evidence on EU Data Protection Proposals: https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/supporting_documents/eudataprotectionproposalscallforevidence.pdf

61 Information Commissioner register: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/download-the-register/

62 BDRC Continental for the ICO (2015), Data Controller Registration Fee Research

- 0.08% of organisations from charities (13)

This gives us estimates for each sector of the number of research organisations that would might have to comply with SARs if they were not exempt from them (i.e. if the derogations in article 89 were not exercised).

- Estimates of the number SARs research organisations would expect to have to comply with without the derogation: research based on Information Commissioner figures suggests the percentage of data controllers in the UK that receive at least one SAR per year for each sector is:
  - 14% of all private sector data controllers (45,637).
  - 38% of the public sector received SARs (51,145).
  - 20% of the third sector (charities) received SARs (3,341).
- We make the assumption that these aggregate figures are representative of UK research organisations, as we are not aware of any figures that are for research organisations alone.
- This research also provided estimates for the number of organisations that had received more than 1 SAR. Based on these, we assume that of those research organisations that receive an SAR, the average number they receive is:
  - In the minimum estimate, all of them receive only 1;
  - The expectation is that they on average receive 3;
  - The maximum estimate is that they on average receive 5.

The table below presents the annual costs for each of our estimates for each sector, using the assumptions described above.

Estimate	Sector	Number of research organisations	Cost Per SAR	Percentage receiving at least 1 SAR/ year	Average number of SARs received	Total Annual Cost (2011 prices)
Expected	Private	3912	£300	14%	3	£492,884
Expected	Public	538	£300	38%	3	£184,123
Expected	Charities	13	£300	20%	3	£2,405
Max	Private	3912	£500	14%	5	£1,369,123
Max	Public	538	£500	38%	5	£511,452
Max	Charities	13	£500	20%	5	£6,682
Min	Private	3912	£100	14%	1	£54,765
Min	Public	538	£100	38%	1	£20,458

Min	Charities	13	£100	20%	1	£267

Please note that some of the numbers presented were rounded. The figures for the cost of SARs were estimates from 2011. We have had to assume that the costs in 2011 are representative of what the costs would be today and for the future. For the final NPV figures we have used the HMT GDP deflator to inflate the 2011 figures in the table above to 2016 prices.

Costs

Monetised: Due to the lack of data and the complexities in monetising individual rights we were not able to monetise the costs.

Non-monetised: There were a small number of expressions of concerns in the government's *Call for Views*:

- Open Rights Group were concerned that Article 89 'creates dangerous loophole and provides exemptions which won't be needed all of the time'. They felt that 'organisations should only be exempt where the use of personal data is necessary and in the public interest'. Their concern highlights the difficult trade-off between what is necessary and in the public interest, compared to the value of individuals' data rights. London Economics explored this, finding that although 60% of consumers said they're unlikely to use their rights more than once a year, the value of the GDPR rights stems from the knowledge that they can use them if needed.
- Big Brother Watch were similarly concerned that 'research organisations will rely on exemptions on grounds of public interest when there are no good reasons to do so', and that this could result in the erosion of data subjects' rights.

Assumptions and risks

The monetised benefits are all within the 'avoidance of administrative costs'. The assumptions used to construct those numbers are explained in that section.

The main assumption in this assessment is that the derogations strike an appropriate balance between the public interests for scientific and historical research, statistical purposes or archiving, and individuals' data protection rights.

Further Information

Article 9 of the GDPR permits processing of special categories of data when this is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1). Article 89(1) provides that processing for such purposes should be subject to appropriate safeguards. Safeguards should ensure that technical and organisational measures are in place to respect the principle of data minimisation. Where appropriate, this might include through pseudonymisation or by ensuring that further processing does not permit the identification of the data subjects. Articles 89(2) and 89(3) allow Member States to use domestic legislation to exempt research organisations from certain subject access

provisions in the Regulation, if compliance would seriously impair or render impossible their ability to complete their work.

Under Article 89 (2), data processed for scientific or historical research purposes or statistical purposes would be exempt from the following subject access rights:

- Right of access (Article 15). Under the GDPR, individuals will have the right to obtain: confirmation that their data is being processed; access to their personal data; and other supplementary information such as the purposes of the processing or who else will access the data.
- Right to rectification (Article 16). Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
- Right to restriction of processing (Article 18). Individuals have a right to 'block' or suppress processing of personal data in certain circumstances. When processing is restricted, controllers are permitted to store the personal data, but not further process it.
- Right to object (Article 21). Individuals have the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Data processed for archiving purposes in the public interest under Article 89(3) would also be exempt from the subject access rights above, and with two additional rights:

- Notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19). If controllers have disclosed the personal data in question to third parties, they must inform them of the rectification where possible. They must also inform the individuals about those third parties if the individual asks.
- Right to data portability (Article 20). The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

When research organisations receive a SAR, for example, they will need to consider whether a particular activity would be seriously impaired or rendered impossible by responding to the request. If the answer was 'no', they would still need to comply. Organisations may also have other obligations to data subjects which are not covered by Article 89 - for example, Article 89 has no bearing on the obligations in Article 13 which require organisations, at the time data is collected from an individual, to provide him or with details about how the data will be used and how long it will be kept.

Small and micro business assessment (SaMBA)

There is no distinction in the GDPR between large data controllers and SME or micro enterprises or sole traders since the aim is to protect data in particular when the data is sensitive and high risks are associated with the processing. Small and medium firms that qualify for this assessment won't be excluded from the analysed derogations. The provision will apply for all data controllers in the UK to meet the aim of the bill. This is in line with the risk-based approach of the GDPR which focusses of the risk of processing and the sensitivity of the data, not the size of the firm that does the processing.

Benefits by organisation size:

Based on Information Commissioner research, we were able to breakdown the organisations on the Information Commissioner's Data Controller Register:

	Micro	Small	Medium	Large	Total Number
Private	71.7%	18.8%	5.6%	3.8%	325,982
Public	45.5%	28.2%	12.8%	13.5%	134,593
Charity	52.7%	23.8%	13.4%	10.1%	16,705

The number of data controllers currently on the Information Commissioner's register is 477,279. The figures show that micro and small businesses are the two groups that are expected to benefit the most from the cost savings from exercising the most significant derogations.

For Article 89, we monetised what the expected saving would be to research organisations not having to comply with subject access requests (SAR). The figures show that micro and small businesses are the two groups that are expected to benefit the most. This is because the majority of organisations on the Information Commissioner's Data Controller Register are micro or small businesses. However, these figures assume that a small business is just as likely to receive an SAR as a larger one. We would not expect that to be the case as larger organisations have greater potential to be asked for SARs as they are likely to hold more people's personal data. The figures below are therefore likely to overstate the savings to smaller organisations and understate the savings to larger organisations.

Annual cost saving	Micro	Small	Medium	Large	Total
Private	£353,572	£92,865	£27,574	£18,872	£492,884
Public	£83,746	£51,962	£23,625	£24,790	£184,123
Charity	£1,267	£573	£322	£243	£2,405

4: Annex - Summary of GDPR derogations

The majority of the provisions in the General Data Protection Regulation (GDPR) will automatically become UK law on 25 May 2018. However, the Data Protection Bill gives government the opportunity to implement a number of flexibilities and derogations. The government intention is to ensure the whole data protection system is tailored to meet the UK's specific circumstances and ambitions.

The following table sets out each flexibility and derogation, the article of the GDPR to which it corresponds, and the UK's reason(s) for choosing, in this way, to deviate from the GDPR's default position and the rationale why the decision was made to include the analysis of this derogation in the impact assessment. Generally, the impact assessment focuses on those derogations that state implementation options for the UK.

GDPR Article	**Description**	**The government intention**	**Rationale why or why not this derogation is included in the impact assessment**
Article 4 - definitions	Article 4 contains definitions of terms used in the GDPR. These include what is meant by terms such as 'controller', 'processor' and 'consent' as well as many others. Article 4(7) sets out the definition of 'controller' which is the legal or natural person that determines the purposes and means of the processing of personal data. The current wording of Article 4(7) may make it operationally harder to identify the data controller in certain circumstances.	The GDPR allows the UK to specify who the controller should be, or the criteria to nominate a controller in specific circumstances. We will ensure it is straightforward to identify the data controller by maintaining the 1998 Act as far as possible whilst remaining consistent with the GDPR definition.	This provision will not impact organisations as government has no intention to deviate from the definition of data controller in the 1998 Act.
Article 6 - lawfulness of processing	For an organisation to process an individual's personal data, there are certain conditions that need to be met. This article lays down those	Article 6(1) of the GDPR is directly applicable and offers little by way of derogation. However, it does allow Member States to make more	This derogation will not impact organisations as government has no intention to deviate from the 1998 Act and the Freedom of Information Act

	conditions for the processing to be considered 'lawful'. For example, the conditions include an individual giving consent, entering into a contract or an organisation processing data in the public interest. Schedule 2 to the 1998 Act contains equivalent provision to Article 6 of the GDPR.	specific rules regulating the processing of data for public interest purposes. The policy aim is to reflect the 1998 Act as far as possible and continue to provide clarity as to what processing for 'public interest purposes' means, to ensure that organisations are able to continue lawfully processing data. The government will do this by replicating the wording of paragraph 5 of Schedule 2 to the 1998 Act. The term 'public authority' is not defined in the GDPR. A number of respondents to the *Call for Views* asked for a definition of public authority to be provided. For clarity and legal certainty we plan to base the definition on that in the Freedom of Information Act 2000.	2000.
Article 8 - conditions applicable to child's consent	Article 8 sets out the conditions applicable for a child's consent in relation to 'information society services'. Where a child is under 16, processing will be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. The 1998 Act is silent on this matter.	The GDPR allows the UK to set the age at which a child may consent to the processing of their personal data by those offering information society services to an age between 13 and 16. The government will set the age at which a child can consent to the processing of data for the purposes of the provision of information society services at 13 years old.	There is currently no age threshold for children's consent for data processing in the UK and this new regulation will impose costs and benefits on organisations, children and parents.

		The government is not persuaded that setting the age at 16 would create any additional protections for children for the reasons given in Chapter 3 of this document.	
Article 9 - processing of special categories of personal data	Article 9 sets out the circumstances under which 'special categories' (sensitive personal data under the 1998 Act) of data can be processed. Processing these 'special categories' is generally prohibited as they cover sensitive personal matters including racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership. The GDPR has introduced two additional 'special categories'; genetic and biometric data. Schedule 3 to the 1998 Act permits the processing of sensitive personal data in certain listed circumstances. Examples are where the processing is on the basis of explicit consent, or without consent for medical purposes by health professionals.	The GDPR allows the UK to expressly set out the conditions and safeguards that will allow the processing of 'special categories' of data to continue. The UK will provide for processing under Article 9 so that, in so far as possible, all 'special category' processing currently carried out in reliance on Schedule 3 1998 Act, currently known as 'sensitive personal data' can continue. The policy aim is to reflect the 1998 Act as far as possible. The government will implement the derogations available to ensure that organisations that currently process sensitive personal data in compliance with the 1998 Act can continue to do so under the GDPR.	This derogation limits the rights of data subjects but not exercising this derogation would put substantial burden on organisations and therefore the costs and benefits of data subjects and data controllers are analysed in the impact assessment.
Article 10 - processing of personal data relating to criminal convictions and	Article 10 restricts the 'processing of personal data relating to criminal convictions and offences' Criminal convictions and	The GDPR allows the UK to authorise the processing of personal data relating to criminal convictions	This derogation limits the rights of data subjects but not exercising this derogation would put substantial burden on organisations and prevent

offences	offences or related security measures based on Article 6(1) can only be processed 'under the control of official authority', or if processing is specifically authorised, with the necessary safeguards to protect individuals' rights and freedoms. A full register of criminal convictions can only be kept under the control of official authority. In the 1998 Act, criminal convictions data is incorporated into the definition of sensitive personal data and is subject to the processing conditions for sensitive personal data in Schedule 3. Any person or organisation can process the data provided conditions in Schedule 3 are met.	and offences otherwise than by a public body or authority The government intends to exercise the derogation as there are many organisations that would not be classed as an 'official authority' who currently process criminal convictions data. For example, employers process criminal convictions data as part of their pre-employment checks and insurers process criminal convictions data for anti-fraud purposes. These bodies will need legal certainty to ensure they can continue the processing of criminal convictions and offences data under the new law. The policy aim is to reflect the 1998 Act as far as possible. The government will therefore implement Article 10 by mirroring relevant provisions under Article 9(2) in order to provide grounds for processing otherwise than under the control of official authority.	them from processing personal data relating to criminal convictions and offences. Therefore, the costs and benefits of data subjects and data controllers are analysed in the impact assessment.
Article 22 - automated individual decision making	Article 22 gives individuals the right to object to decisions made about them solely on the basis of automated processing, where those decisions have legal or other significant effects. Solely automated processing means where there is no human intervention, for example, when data is entered into a computer	The GDPR allows the UK to specify additional circumstances and safeguards when solely automated processing may take place. With a fast moving pace of technology driving automated decision making with algorithms and artificial intelligence, It is important to maintain a narrow list of exemptions that protect	This provision will not impact organisations as government has no intention to deviate from the1998 Act's position.

	about an individual's spending habits and debt, which then processes the data to calculate creditworthiness. The 1998 Act provides similar safeguards against automated decision making. These include an individual being informed about and being able to object to solely automated processing, as well as ask that a decision made through that process be reconsidered.	individuals' rights. The government believes that safeguards within the 1998 Act (Section 12 of the 1998 Act) could be adapted to be applied to circumstances where a person does not consent to processing and where it is not necessary for the purpose of a contract. We will therefore apply these additional safeguards which GDPR does not otherwise provide for.	
Article 23 - restrictions	Article 23 allows Member States to introduce restrictions to the rights and obligations in the GDPR where it is a necessary and proportionate measure required to safeguard an important public interest objective. The 1998 Act has similar restrictions on rights and obligations where in the public interest.	The GDPR allows the UK to introduce exemptions from transparency obligations and an individual's rights. The government's objective is to preserve the effect of the exemptions in the 1998 Act to the extent permitted under the GDPR. We consider that most are compatible with GDPR requirements, subject to necessary adjustments. Where it is considered necessary we will extend those exemptions to any new rights. We will maintain the approach adopted under the 1998 Act whereby the exemptions exist for various purposes only, and not entity or sector.	This derogation limits the rights of data subjects but not exercising this derogation would put substantial burden on organisations and introduce barriers for processing personal data required to safeguard an important public interest objective. Therefore, the costs and benefits of data subjects and data controllers are analysed in the impact assessment.
Article 43 - certification bodies	Certification schemes exist to encourage and demonstrate compliance	The government intends to make the Information Commissioner and the	UK National Accreditation Service (UKAS) is responsible for certification

	with data protection standards. Article 43 sets the criteria and procedure for accrediting certification bodies. Article 43(1) requires Member States to 'ensure' that certification bodies are accredited by a supervisory authority. There is no current equivalent provision to Article 43 in the 1998 Act.	UK National Accreditation Service (UKAS) the certification bodies. Certification bodies shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification and need to notify the Information Commissioner and/or UKAS of the reasons why certifications have been granted or revoked.	schemes.
Article 49 - derogations for specific situations	The GDPR imposes restrictions on the transfer of personal data outside the European Union to other countries or international organisations where there is no 'adequacy decision' in place or appropriate safeguards. This is in order to ensure that the level of protection of individuals provided by the GDPR is not undermined. The 1998 Act similarly restricts data transfers. Schedule 4 to the 1998 Act sets out instances where the transfer of personal data to third countries can occur. This includes where the transfer is necessary for reasons of substantial public interest. An 'adequacy decision' is when the EU Commission determines that a non-EU country ensures an adequate level of protection of personal data.	The UK can permit the transfer of personal data to a third country in the absence of an adequacy decision when this is done for 'important reasons of 'public interest'. The government will legislate to provide an order making power that allows the Secretary of State to specify circumstances where a transfer of data is necessary for reasons of substantial public interest, as well as circumstances in which a transfer of data is not deemed to be necessary for reasons of substantial public interest.	The 1998 Act already allows for data transfers in similar circumstances if it is in the substantial public interest.
Article 52 -	Article 52(4) to (6) relate	The GDPR allows the UK	Equivalent provisions

independence	to resourcing, staffing and financial control of supervisory authorities. The article imposes a requirement on Member States to ensure that supervisory authorities are properly resourced. The 1998 Act provides for similar measures in this area.	to lay down specific rules on the resourcing, staffing and financial control for the Information Commissioner. We will make provision to ensure the Information Commissioner has adequate resources.	already exist in the 1998 Act.
Article 53 - general conditions for the members of the supervisory authority	Article 53 requires the appointment of members of supervisory authorities to be appointed by way of a transparent procedure, each member to meet the conditions required for the performance of their duties and for a member's dismissal to occur only in specific cases. Equivalent provision exists in the 1998 Act including grounds for dismissal.	The GDPR allows the UK to determine the conditions required for the performance of Information Commissioner. The existing grounds for dismissal in the 1998 Act will be amended to avoid conflict with the GDPR. The government will impose a duty on the Secretary of State to determine what the conditions required for the performance of the role of the Information Commissioner should be.	Equivalent provisions already exist in the 1998 Act.
Article 54 - rules on the establishment of a supervisory authority	Article 54 concerns the rules on the establishment of the supervisory authority. The 1998 Act provides for the establishment of the Information Commissioner and other areas relating to the appointment of the Information Commissioner. The 1998 Act does not currently provide for suitably qualified Commissioners.	The GDPR allows the UK to make rules in several areas relating to the Information Commissioner and members. The aim is for the Information Commissioner to continue to be the sole supervisory authority for data protection in the UK, and the designated national supervisory authority for the UK. The government will	Equivalent provisions already exist in the 1998 Act.

		ensure that future Commissioners are suitably qualified in terms of the GDPR to perform their role effectively, and make it a requirement for the Secretary of State's preferred candidate to appear before the relevant select committee for a pre-appointment hearing. The government will retain the term of office for the Information Commissioner as a maximum of seven years, and prohibit reappointment. Further the government will impose a duty on the Information Commissioner to issue a code of conduct.	
Article 57 - tasks	Article 57 provides a comprehensive list of tasks given to the supervisory authorities of Member States. These include things like enforcing the law, handling complaints and conducting investigations. Section 51 of the 1998 Act provides equivalent provision.	The GDPR allows the UK to ensure that the tasks of the Information Commissioner currently provided by the 1998 Act are incorporated into the new law. The government will legislate to reflect section 51(7) 1998 Act (voluntary audits) and section 42 1998 Act (requests for assessment) to allow the Information Commissioner to continue performing fundamental tasks. The policy aim is to reflect the 1998 Act as far as possible.	Equivalent provisions already exist in the 1998 Act.
Article 58 - powers	Article 58 concerns the powers afforded to a supervisory authority.	The GDPR allows the UK to establish civil sanctions and penalties	Equivalent provisions already exist in the 1998 Act.

	Article 58(2) provides for a supervisory authority's corrective powers, which are wide ranging. 58(4) provides for safeguards to be put in place under domestic law in respect of all of the Information Commissioner's powers listed. These powers are fundamental to the Information Commissioner's functions, and include issuing warnings, reprimands and orders to organisations in breach of the law. 58(6) gives Member States a discretion to provide by law for supervisory authorities to have additional powers. The 1998 Act has provision for the large majority of the powers conferred by the GDPR.	which can be exercised by the Information Commissioner or the courts for the enforcement of the new law. The policy aim is to reflect the 1998 Act as far as possible. The government will include provision in the new bill under Article 58(4) (linked to Article 90) that outlines the safeguards which apply to the Information Commissioner and use of investigatory powers. The government will also insert a clause replicating the position set out in section 58 of the 1998 Act, in order to ensure continuity in terms of the status of the Information Commissioner's powers to request personal data/information when carrying out its investigatory role as against other enactments and rules of law which prohibit disclosure of information. Outlining the safeguards which apply to the Information Commissioner's use of its investigatory powers should provide real clarity for the Information Commissioner as to the extent of their powers.	
Article 59 - activity reports	Article 59 states that each supervisory authority is required to present an annual report to Parliament, government and other	The UK will need to ensure that the new law provides obligations for the delivery of annual reports.	Equivalent provisions already exist in the 1998 Act.

	authorities as designated by member state law. The reports are also to be made public.	The government will legislate to ensure that annual reports be laid before each House of Parliament. The Information Commissioner will also continue to be able to lay before each House other reports relating to Information Commissioner functions as appropriate.	
Article 78 - right to an effective judicial remedy against a supervisory authority	Article 78 provides that all individuals, controllers and processors have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision. Article 78 has two key parts: ● Article 78(1) gives an individual the right to an effective judicial remedy against a legally binding decision of the Information Commissioner which concerns them; and ● Article 78(2) gives an individual the right to an effective judicial remedy where the Information Commissioner does not handle a complaint, or does not inform them within 3 months of the progress or outcome of the complaint. The right under Article 78(2) does not have an equivalent in the 1998	The UK is required to ensure there is a specific right to a judicial remedy if the Information Commissioner does not update an individual on progress with their complaint within three months, or does not handle their complaint. The right for a controller or processor to appeal to the Tribunal over certain decisions, with other decision subject to challenge by judicial review will be retained through Article 78(1). The policy aim for Article 78(2) is to create a statutory right for an individual to apply to the Tribunal for an order that the Information Commissioner must handle their complaint and/or update them on the progress or outcome of the complaint within three months, if the Information Commissioner has failed to do so. The government will create a statutory right to	Similar provisions already exist in UK law and we do not expect great additional costs and benefits.

	Act.	apply to a Tribunal if the Information Commissioner fails to take any action to investigate an individual's complaint, or the Information Commissioner fails to inform the individual of the progress or outcome of their complaint.	
Article 79 - right to an effective judicial remedy against a controller or processor	Article 79 gives an individual the right to an effective judicial remedy against a data controller or data processor where the individual considers that the processing of their personal data has infringed their rights under the GDPR. The 1998 Act gives individuals the right to apply to court for an order against a data controller in certain circumstances.	The UK is required to ensure that individuals have an effective judicial remedy where he or she considers that his or her rights have been infringed as a result of the processing of his or her personal data in non-compliance with the GDPR. The policy aim is to reflect the 1998 Act, as individuals currently have a right to an effective judicial remedy. The government will ensure that individuals are able to bring a claim before the courts when their rights under the GDPR have been infringed, in the same way as they can currently bring a claim before the courts for infringements of certain sections of the 1998 Act. The courts before which the claim must be brought will be, the county court or High Court in England and Wales and Northern Ireland, and the Court of Session or sheriff in Scotland.	Equivalent provisions already exist in the 1998 Act.
Article 80 - representation	Article 80 allows individuals to have the	The policy aim is to ensure that individuals	The basic right in Article 80(1) is non-derogable and

of data subjects	right to mandate a not-for-profit body, organisation or association (such as a consumer protection body) to exercise rights and bring claims on their behalf. These rights include the right to lodge a complaint with the Information Commissioner (Article 77); the right to an effective judicial remedy against the Information Commissioner (Article 78); and the right to an effective judicial remedy against a data controller or processor. Article 80 is a new provision, with no direct equivalent in the 1998 Act.	are able to exercise their rights to authorise non-profit organisations to deal with claims on their behalf, and that such organisations can collect damages awarded on individuals' behalf. The government will legislate to ensure that individuals are able to exercise their rights to authorise non-profit organisations to deal with claims on their behalf.	directly applicable.
Article 82 - right to compensation and liability	Article 82 gives any person who has suffered material or non-material damage as a result of an infringement of the GDPR the right to receive compensation from the controller or processor. Section 13 of the 1998 Act provides that an individual who suffers damage by reason of a data controller's contravention of the 1998 Act is entitled to compensation for that damage.	The policy aim is to reflect the 1998 Act as far as possible. The UK will ensure that a person is able to claim compensation for material or non-material damage in the county court or High Court in England, Wales and Northern Ireland and the Court of Session or sheriff in Scotland, in the same way as they can currently claim compensation under the 1998 Act.	This provision will not impact organisations as government has no intention to deviate from the current setup under the 1998 Act.
Article 83 - general conditions for imposing administrative fines	Article 83 makes provision in relation to the imposition by the Information Commissioner of administrative fines for the infringements of	The GDPR allows the UK to make rules to fine public authorities and bodies if domestic law does not provide for administrative fines, and specify to what extent	This provision will not impact organisations as government has no intention to deviate from the current setup under the 1998 Act.

	certain provisions of the GDPR.	they might be fined. The government will replicate the existing processes and safeguards applicable to civil monetary penalties under the 1998 Act.	
Article 84 - penalties	Article 84 requires Member States to lay down rules on penalties for breaches of the GDPR other than administrative fines. These penalties must be effective, proportionate and dissuasive. Data protection law in the UK has always been accompanied by criminal offences. There are various provisions under the 1998 Act that provide for criminal offences, including but not limited to sections 21, 22, 24, 47, 55, 56 and 59.	The GDPR allows the UK to specify the penalties for infringements of the law that are not subject to administrative fines. The government will retain most but not all existing offences under the 1998 Act, with some modifications and extensions and will also create some new offences. The government intends to: Reproduce offences in the 1998 Act which remain fit for purpose, including offences relating to unlawful disclosure of personal data obtained by the Information Commissioner in connection with their investigations, and offences relating to enforced subject access (e.g. where an employer asks a prospective employee to obtain personal data to which the organisation wouldn't normally be entitled) Extend the offence of unlawfully obtaining personal data (under s.55 of the 1998 Act) so that it covers unauthorised 'retention' of data and introduce a	This provision reproduces, extends and creates a new offence and the costs and benefits are analysed in the impact assessment.

		new defence for journalistic activity. The offence will become a recordable crime. Extend an offence in the Freedom of Information Act 2000 (altering records with intent to prevent disclosure) so that it applies to all data controllers and processors, not just public authorities. Amalgamate three separate offences in the 1998 Act which relate to obstructing the Information Commissioner's investigations into a single offence of obstruction. Create new offences relating to re-identifying anonymised or pseudonymised data	
Article 85 - processing and freedom of expression	Article 85 requires Member States to introduce exemptions to the GDPR where necessary to 'reconcile the right to the protection of personal data with the right to freedom of expression and information.' The article makes provision for processing that is carried out for journalistic purposes, or for the purposes of academic, artistic or literary expression. Exemptions or derogations are permitted for a similarly	The GDPR allows the UK to provide exemptions to Article 85 to find the right balance between the protection of personal data and the right to freedom of expression. The policy aim is to reflect the 1998 Act as far as possible. The government believes that section 32 of the 1998 Act sets a good standard and should be used as a baseline for implementing the GDPR. This view was supported	This provision limits the rights of data subjects but not exercising this derogation could have an adverse impact on freedom of expression and therefore the costs and benefits of data subjects and data controllers are analysed in the impact assessment.

	defined category under section 32 of the 1998 Act. The two GDPR additions that Article 85 provides are protection to the freedom of expression *and information* and also academic expression alongside the other purposes.	by the majority of respondents to the *Call for Views* that commented on the derogation. Section 45 of the 1998 Act will be amended to allow the Information Commissioner to make a determination in respect of each of the conditions in section 32 of the 1998 Act, which is the current journalistic exemption. This would enable the right balance to be struck between data rights and freedom and expression and information, whilst retaining the additional freedom of expression safeguard of requiring a court to authorise the issue of an enforcement notice.	
Article 86 - Processing and public access to official documents	Article 86 allows the principle of public access to official documents to be taken into account when applying the GDPR. The rights and protections afforded under the GDPR, and in particular under Article 15 and Chapter III, are therefore balanced by the acknowledgement that Union or Member State law may nonetheless permit the disclosure of personal data held by public entities or private entities performing public tasks. These opposing rights, on the one hand the protection of personal data and on the other hand the disclosure of that personal data, are	The policy aim is to reflect the 1998 Act and Freedom of Information Act 2000 as far as possible. The current UK public access regimes provide public entities with the duty to disclose personal information in the public interest and this will continue as we consider it is compatible with the GDPR under Article 86.	This provision will not impact organisations as government has no intention to deviate from the current setup under the 1998 Act.

	already enshrined in several UK laws, particularly the Freedom of Information Act 2000.		
Article 89 - safeguards relating to processing for archiving purposes	Article 89 permits processing of personal data for scientific and historical research, statistical purposes or archiving in the public interest, if appropriate technical and organisational safeguards are in place to protect personal information from misuse. Section 33 of the 1998 Act exempts processing for research purposes from the subject access provisions in section 7 of the 1998 Act, providing that the processing does not support decisions about individuals or cause them substantial damage or distress.	The government intends to replicate the position under the current law as far as possible. By ensuring that all the derogations available for research organisations under Articles 89(2) and (3) are set out clearly in UK law the government will be providing research organisations with a similar degree of flexibility as they currently have under the 1998 Act. The government intends to exercise derogations in Articles 89(2) and (3) so that research organisations do not have to comply with an individual's rights to access (Article 15), rectify (Article16), restrict further processing (Article 18) and object to processing (Article 21) where this would seriously impede their ability to complete their work, and providing that appropriate organisational safeguards are in place to keep the data secure. The government will also invoke two further derogations which are only available for archiving organisations, namely the obligation to alert third parties with whom the data might have been shared of any changes made by an individual (Article 19), and	This provision limits the rights of data subjects but not exercising this derogation would put substantial burden on research organisations and archivists and therefore the costs and benefits of data subjects and data controllers are analysed in the impact assessment.

		the right of individuals to transfer their data to another provider (Article 20).	
Article 90 - obligations of secrecy	Article 90 is concerned with obligations of secrecy (confidentiality) in relation to investigations by supervisory authorities. It allows Member States to pass national rules that reconcile the protection of personal data (in the form of powers of access) with confidentiality obligations. These rules can only apply in relation to personal data which a controller or processor has received as a result of an activity covered by an obligation of confidentiality. UK law does not have an obligation of secrecy, however there are equivalent obligations in the form of duties of confidence and legal professional privilege. If the Information Commissioner or Information Tribunal needs information for the discharge of their duties under the 1998 Act, there is no law that prohibits the person who has that information from disclosing it.	The policy aim is to reflect the 1998 Act as far as possible. The Information Commissioner is subject to a statutory prohibition against disclosure of information disclosed to them. The government does not want to introduce national law under Article 90 as this would limit the Information Commissioner's power to obtain information and reduce the Information Commissioner's ability to effectively regulate the sector. Article 90 could apply to a large number of organisations e.g. health service bodies, the police, legal profession and social work bodies. The government believes that the current practice adopted by the Information Commissioner achieves a fair balance between the need for the Information Commissioner to be able to regulate effectively and individuals' rights. The government will replicate existing provisions in the 1998 Act and will legislate to include a provision equivalent to section 58 of the 1998 Act, to clarify	This provision will not impact organisations as government has no intention to deviate from the current setup under the 1998 Act.

		that those asked to provide the Information Commissioner with information under Articles 58(1) (a), (e) or (f) can do so without being found to have breached existing duties of confidence or non-disclosure requirements in other legislation. The existing rule set out in section 58 of the 1998 Act overrides any law which would otherwise prevent the disclosure of data to the Information Commissioner such as Legal Professional Privilege.	