Title: Data Protection and Digital Information (No. 2) Bill
IA No:

RPC Reference No: RPC-DCMS-5180(1)

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

Other departments or agencies:

- Department for Culture, Media and Sport
- Department for Business, Energy and Industrial Strategy
- Home Office
- Department for International Trade
- Digital Cabinet Office
- Department of Health and Social Care
- HM Treasury
- Information Commissioner's Office

Impact Assessment (IA)

Date: 13/03/2023

Stage: Final stage

Source of intervention: Domestic

Type of measure: Primary legislation

Contact for enquiries: datapolicyanalysis@dcms.gov.uk

Summary: Intervention and Options

RPC Opinion: Fit for purpose: green rated

Cost of Preferred (or more likely) Option (in 2019 prices, millions)

Total Net Present Social Value	Business Net Present Value	Net cost to business per year	Business Impact Target Status
4,721.0	2235.4	-98.3	Qualifying

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

Unlocking the power of data is one of the government's 10 Tech Priorities. As set out in the National Data Strategy, data is a strategic asset and its responsible use should be seen as a huge opportunity to embrace. The complexity of the current regulatory regime means that firms, public sector organisations and consumers are not able to take full advantage of the benefits that could be available to them through effective use of data and data sharing. As a result, the market fails and benefits are not realised. It is necessary for Government intervention to allow for the realisation of all benefits derived from more effective data use.

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

The proposals aim to deliver a data protection regime that will:

- Support vibrant competition and innovation to drive economic growth
- Maintain high data protection standards without creating unnecessary barriers to responsible data use
- Keep pace with the rapid innovation of data-intensive technologies
- Help businesses use data responsibly without uncertainty or risk, in the UK and internationally
- Ensure the Information Commissioner's Office (ICO) is equipped to regulate effectively
- Build on the high watermark for data use during Covid-19 that saw the public and private sectors collaborate to safeguard our health security, and
- Make it easier for public bodies to share vital data, improving public service delivery

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

DCMS have considered a total of two policy options, that vary in the degree of change to the current UK data policy regime, these are outlined below:

- **Option 0 - Do nothing**: this is the scenario in which no changes are made to the current legislation. All analysis carried out is compared to this baseline scenario
- **Option 1 - Data reform**: Updating and simplifying the UK's data protection framework and the role of the Information Commissioner's Office (ICO), while focusing on protecting individuals' data rights and generating societal, scientific, and economic benefits.

Is this measure likely to impact international trade and investment?		Yes		
Are any of these organisations in scope?	**Micro** Yes	**Small** Yes	**Medium** Yes	**Large** Yes
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)		**Traded:** n/a	**Non-traded:** n/a	

Will the policy be reviewed? It will be reviewed. **If applicable, set review date:** within 5 years

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

Signed by the responsible:	Dipti Bhadresa	Date:	13/02/2023

Summary: Analysis & Evidence

Policy Option 1: Data Protection and Digital Information Bill

Description: Updating and simplifying the UK's data protection framework and the role of the Information Commissioner's Office (ICO), while focusing on protecting individuals' data rights and generating societal, scientific, and economic benefits.

FULL ECONOMIC ASSESSMENT

Price Base Year: 2019	PV Base Year: 2020	Time period: 10	Net Benefit (Present Value (PV)) (£m)		
			Low: 1,210.3	**High:** 9,059.6	**Best Estimate:** 4,721.0

COSTS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low	447.6		32.2	716.5
High	1,632.8		64.2	2,073.1
Best Estimate	847.2		43.9	1,188.1

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

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

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

A qualitative assessment is provided for both direct and indirect costs where evidence is currently not available. These include the costs to LEAs of changes to public sector data handling regulations, the costs to government departments of making data sharing easier and the costs of improving interoperability of data systems across the NHS. The costs of creating robust Smart Data and Digital Identity schemes are also qualitatively assessed.

BENEFITS (£m)	Total Transition (Constant Price) Years		Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low	0		405.3	3,284.6
High	0		1,156.4	9,776.1
Best Estimate	0		711.5	5,909.2

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

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

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

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

Key assumptions/sensitivities/risks (%)	Discount rate	3.5%
Where assumptions have been made in the economic modelling we have made sure to test these either using a confidence band approach or Monte Carlo analysis.		

BUSINESS ASSESSMENT (Option 1)

Direct impact on business (Equivalent Annual) £m:			Score for Business Impact Target (qualifying provisions only) £m: n/a
Costs:	**Benefits:**	**Net:**	
8.0	106.3	-98.3	-491.7

Evidence Base

Contents

Executive Summary

Context

1. Unlocking the power of data is one of the government's 10 Tech Priorities.[1] As set out in the National Data Strategy,[2] data is a strategic asset and its responsible use should be seen as a huge opportunity to embrace. Outside of the EU, the UK can reshape its approach to regulation and seize opportunities with its new regulatory freedoms, helping to drive growth, innovation and competition across the country.

2. DCMS has worked alongside other government departments to put together an ambitious package of reforms to create a regime that is pro-growth and trusted for all citizens and businesses. This is a sovereign and pragmatic UK approach that allows data-driven businesses to use data responsibly, while keeping personal information safe and secure.

3. This impact assessment provides

    a. An outline of the existing regulatory framework and market failures

    b. The proposed policy options and preferred package of reforms in overcoming these failures

    c. The cost benefit analysis of the preferred package of reforms, comprising of:

        i. Direct costs and benefits

        ii. Indirect costs and benefits

        iii. Wider impacts

        iv. Trade modelling

        v. In depth analysis of the impact of these reforms on small and micro businesses and specific sectors within the UK economy

    d. An overview of all risks and assumptions associated with the modelling

    e. An outline of all future monitoring and evaluation activities

4. Many of the policies included in the bill have been designed by other government departments alongside DCMS, including CDDO, BEIS, Home Office and DHSC. Where this is the case, analysis has been provided directly by these departments and has been referenced accordingly. There are also reforms included in the bill which are enabling primary legislative powers and will be followed up by secondary legislation impact assessments. We have highlighted where this is the case and ensured that the analysis provided is representative of this.

Rationale and approach

5. The complexity of the current regulatory regime means that firms and consumers are not able to take full advantage of the benefits that are available to them through effective use of data

[1] Governments top 10 tech priorities, DCMS (2021)
[2] National data Strategy 2020, DCMS (2020)

and data sharing. As a result, the market fails, and benefits are not realised. Furthermore, information asymmetry exists for UK businesses that are unaware of the benefits that increased data sharing can lead to. Therefore, it is necessary for Government intervention to allow for the realisation of all benefits that can be derived from more effective data use.

6. Reform options have been designed specifically to remedy market failure in specific industries, sectors, and UK data policy more generally. DCMS set out many of these areas in Data: A New Direction. The reforms aim at achieving the following objectives:

    a. Boosting responsible innovation through the removal of barriers when using data

    b. Reducing burdens on firms, particularly small and micro firms, and deliver better outcomes for people

    c. Removing barriers to international data flows and boost trade

    d. Enabling more market competition and introduction of innovative services for consumers and firms through further adoption of smart data

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

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

    g. Helping the adoption of digital identities, enabling economic gains in the digital economy while protecting against harms and enhancing privacy

7. Balancing between ambition and pragmatism, the aim of the reforms is to create a pro-growth and innovation-friendly UK data protection regime. One that underpins the trustworthy use of data to support our world-leading science and digital ecosystems, and still maintaining the highest standards of data protection. Identifying the "right" amount of reforms to achieve this is the key driver behind the decision-making process but also the economic analysis conducted.

8. From the evidence gathered, we shortlisted down to a set of 4 options that were assessed against key critical success factors, using evidence from the consultation stage. The three options alongside the status-quo/do nothing option all seek further liberalisation of the data regime.

Findings

9. We estimate the total net present value of the preferred package of reforms to be between £1.2 billion and £9.1 billion over 10 years in 2019 prices .

Table 1: Estimated NPV of preferred option

Net Benefit (Present Value (PV)) (£m)					
Low:	1,211.5	High:	9,059.6	Best Estimate:	4721.0

10. Some of the measures assessed here are enabling only and given the uncertainty over the contents of the secondary legislation, will be assessed more fully at that stage (scenario 2 in the RPC's primary legislation guidance). The impacts of these secondary measures are either indirect or unquantifiable at this stage. Usually where this is the case, an impact assessment

would present two EANDCBs. However, in this case they are the same and therefore the EANDCB figures presented here cover the set of policies as a whole.

11. The Data Protection and Digital Information Bill is classified as a quantifying regulatory provision and therefore not exempt from the business impact target in this parliament. Many of the reforms included in the bill are pro-competition in nature. However, there are some proposals that do not qualify under these exemptions including the DHSC and Digital Identity measures. A breakdown of the competitive nature of the bill can be found later in the Impact Assessment.

12. We have ensured our analysis is robust and proportionate. We have quantified costs and benefits of the Data Protection and Digital Information Bill where possible, and otherwise provided qualitative analysis. Any evidence gaps will feature in our monitoring and evaluation plan.

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

Table 2: Estimated Net Present Value (NPV) of preferred option over 10 years in 2019 prices (£m)

	Low	High	Medium
Total NPV	1,211.5	9,059.6	4721.0
Costs			
Total Transitional	447.6	1,632.8	847.2
Average Annual	32.2	64.2	43.9
Total Cost	716.5	2,073.1	1,188.1
Benefits			
Total Transitional	0.0	0.0	0.0
Average Annual	405.3	1,156.4	711.5
Total Benefit	3,284.6	9,776.1	5,909.2

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

Impact on Trade

15. Cross-border data transfers are a key facilitator of international trade, particularly for digitised services. Transfers underpin business transactions and financial flows. They also help streamline supply chain management and allow business to scale and trade globally.[3] We

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

have conducted analysis that looks at the potential of the proposed data reforms to enable more trade between countries. The analysis however includes analytical caveats which mean that the results should be treated as merely indicative of the range and scale, rather than a granular and detailed account of the impacts. For this reason, we have decided to report these results separately to the total NPV of the package of reforms.

16. Moving to a system which allows personal data to be transferred more flexibly via data bridge regulations and alternative transfer mechanisms (ATMs) is expected to lower transaction costs and increase cross-border data flows.[4] Using a business-level approach that assesses the direct cost of using standard contractual clauses (SCCs) we estimate an annual benefit to trade of between £90m and £160m.

17. EU Adequacy decisions are adopted through a unilateral, autonomous EU process controlled and managed by the European Commission. As the UK diverges from EU GDPR, the risk that the EU revokes its Adequacy decision increases. EU Adequacy decisions do not require an 'adequate' country to have the same rules, and the Government's view is that reform of UK legislation on personal data is compatible with the EU maintaining free flow of personal data from Europe.

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

Differential impact by sector and organisation size

19. Our modelling confirms that benefits and costs from these reforms will not fall equally across the economy and society, and we expect small and micro businesses to benefit proportionally more from the reforms because they are more likely to have lower and less high-risk levels of data use prior to the reforms.

20. We expect the reforms to have distributional impacts on different sectors as a result of differing levels and types of data use between sectors.[5] For example, firms in some sectors are more likely to have processes and privacy frameworks in place already than others.

[4] Replacing adequacy, 'data bridge' is the term now used by the UK government to describe the mechanism for the trusted flow of data from the UK to another country without restrictions.

[5] Different sectors use data differently, e.g. in 2020, the two sectors most likely to say they share personal data with other organisations were Finance and Insurance (59%) and Real Estate (39%). DCMS: UK Business Data Survey (2021)

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

22. Given the estimated scale and scope of the project we will complete a Post Implementation Review (PIR),[6] within 5 years of implementation. The PIR will provide us with the opportunity to review whether the bill has met the intended objectives highlighted in this impact assessment. In order to be able to successfully measure these impacts we will also ensure that we invest in the monitoring of all key statistics that have fed into this IA with focus on the evidence gaps we have identified.

Problem under consideration and the issue being addressed

23. Data use is widespread, with more than 80% of UK firms using digitised data[7] of these businesses 12% either send data internationally or receive data from outside of the UK, which is equivalent to 10% of all UK Businesses.[8] Data-enabled trade forms the largest part of UK international services trade and is among the strongest comparative advantages of the economy, with exports estimated at £234 billion or 74% of total UK service exports - a net exporting position of about £110 billion for 2019.[9]

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

25. UK businesses identify many benefits of the UK GDPR[10] and the Data Protection Act 2018 (DPA 2018) for example, of the businesses that collect digitised personal data, 58% agreed that the introduction of the GDPR had led to increased awareness of data protection at a senior level.[11] However, the current regime can also be complex to interpret and apply, especially for small and medium businesses.[12] Such complexity is understood to be a barrier to compliance and lead to uncertainty, and potential over- or under-compliance (through strategy or error).[13] We found that 53% of those who thought the ICO guidance supporting the UK GDPR was unclear (16% of UK businesses)[14] stated they had spent a disproportionate amount of time working out its requirements.[15] Further, when asked which elements of the UK GDPR could be clearer, 42% reported the lawful bases that allow data processing.[16] There is also evidence that the current regime may reduce firm-level innovation, business creation and

[6] Producing post-implementation reviews: principles of best practice, BEIS (2021)
[7] UK Business Data Survey (2021)
[8] UK Business Data Survey (2021)
[9] DCMS internal analysis on the world total of UK services exports, based on 2019 ONS published statistics, in sectors defined as data-enabled by UNCTAD (United Nations Conference on Trade and Development).
[10] Until the end of 2020 the EU GDPR applied in the UK. Since then, the applicable legislation in the UK has been the UK GDPR. For simplicity we typically refer to the UK GDPR throughout, but where evidence relates to the earlier GDPR we refer to this as the GDPR.
[11] UK Business Data Survey (2021)
[12] The European Commission's (2020) evaluation of the GDPR identified challenges for organisations, in particular SMEs.
[13] Christensen et al.(2013) The Impact of the Data Protection Regulation in the E.U. To note, this is a forecast of the proposed GDPR rather than an ex-post impact evaluation.
[14] UK Business Data Survey (2021)
[15] UK Business Data Survey (2021)
[16] UK Business Data Survey (2021)

employment,[17] decrease investment in emerging technology firms,[18] and negatively impact data-driven industries.[19]

26. An example of this is in the case of Smart Data. Smart Data is the secure sharing of customer data with authorised third-party providers (TPPs), upon the customer's request.[20] These providers then use this data to provide innovative services for the consumer or business user, such as automatic switching or better account management. Multiple problems across markets exist which Smart Data could help to address, however current market incentives and powers are insufficient to deliver Smart Data alone. UK GDPR created a right to data portability but does not enable data sharing as envisaged for Smart Data, lacking strong standards and secure data sharing requirements. According to analysis carried out by BEIS, this complexity has cost consumers £3.4 billion a year in the loyalty penalty[21] and has led to poor consumer satisfaction, ineffective competition, and stifled innovation.[22]

27. Some businesses also view data as a liability, particularly where personal data is concerned, and take steps to curtail access and usage, implying a level of strategic over-compliance arising from uncertainty. This may come at significant opportunity cost. For example, 86% of UK businesses do not transfer data internationally, of which 18% of businesses give concerns around legal risks and uncertainty as a reason.[23] Alongside this, fewer than 10% of UK businesses use customer relationship management software to collect, store, and share customer information within their businesses,[24] meaning that most businesses do not have an easy way of using data to gain customer insights.

28. From an international perspective, "uncertainty regarding legal privacy regimes" was listed across 19 OECD countries as a main barrier to transborder data flows, followed by "Incompatibility of legal regimes" by 16 countries[25] and the overall estimated compliance cost to UK businesses of using transfer mechanisms inherited from the EU for rest of world personal data transfers is estimated at about £360m annually.[26]

29. The OECD[27] highlights that achieving the benefits available from data use requires employing data-governance frameworks that incorporate whole-of-government approaches and are coherent across areas, sectors and ideally countries. Work by Frontier Economics which was published in March 2021.[28] identified a number of interrelated barriers to greater use and sharing of data in the economy, including a lack of knowledge (about potential uses of, and benefits from, data), high perceived risks (regulatory, commercial reputational); high upfront costs and misaligned incentives

30. Research shows that making data more available could help businesses improve market reach; support benchmarking and insights; drive open innovation; drive supply chain

---

[17] Christensen et al.(2013) The Impact of the Data Protection Regulation in the E.U.
[18] Jia et al. (2018) found that GDPR negatively affected venture capital investment in digital technology firms.
[19] For example, direct marketing, behavioural advertising, credit information and website analytics, as studied in Deloitte (2013). Similar findings are indicated by Arnold and Hildebrand (2017)
[20] BEIS (June 2019) – "Smart Data Review"
[21] Citizens Advice, Loyalty penalty update - progress two years on from the CMA's super-complaint investigation, 2018
market and therefore may be counted twice or more.
[22] BEIS Smart Data Impact Assessment 2022
[23] UK Business Data Survey (2021)
[24] ONS (2018) E-commerce and ICT activity Statistical bulletins, Table 25; this is even lower for micro-sized firms.
[25] OECD: Digital Economy Outlook 2020, fig 6.4
[26] Published DCMS estimate, from RoW Adequacy Umbrella IA.
[27] Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies, OECD (2019)
[28] Increasing access to data held across the economy , Frontier Economics, 2021

optimisation; address sector challenges; and build trust. Those sharing data could gain efficiency savings, develop new or improve existing products, create new or better services, solve existing or future business problems, or gain further understanding about the data they hold themselves. Businesses or organisations gaining access to data, which they or their competitors would otherwise not have, could generate new insights, develop new or improve existing products or services, and establish themselves in the market.

Rationale for intervention

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

    a. **Externalities** occur when the production or consumption of a good incurs costs or benefits on a third-party outside of the transaction. A data externality is an effect that arises from the disclosure of personal data.[29] In the data market, a negative externality occurs when the disclosure of personal data by some consumers leads to an excessive privacy loss for other consumers. The use of the disclosed personal data by businesses or organisations for activities such as targeted advertising, leads to a loss of privacy for those who consider the data to be private information. A positive externality can occur when data collected by one party is freely accessed by others and this generates positive external benefits for re-users.[30]

    b. **Public goods**, where the delivery and efficiency of public services is inefficient as a result of limited data sharing. The complexity of the regulation delays the sharing of data between public services. Also, public sector services lack the necessary framework to use data efficiently and this leads to public goods being under-utilised. The government can create open access data to provide the right framework to help improve the utilisation of public goods. [31]

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

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

    e. **Market power** refers to when the power is concentrated into too few businesses or organisations. In data markets that lack competition the complexity of the regulation deters new entrants and limits firms with relatively less power from achieving the additional benefits of effective data use. Firms with market dominance can expand into

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

complementary data markets, at a relatively low marginal cost rather than share data with complementary firms, this may deter new entrants into complementary markets.

f. **Network failure** refers to when a good or service whose value increases as the number of users increases fails to raise its value due to a lack of users. The data network effect is when a product's value grows as a result of more usage via the accretion of data.[32] In terms of data network failure, the complexity of the regulations has resulted in insufficient cooperation between UK businesses to combine datasets through data sharing and benefit from economies of scope.

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

Table 3: Summary of the market failures in data markets

	Market Failures					
	Externalities	Public goods	Information asymmetry	Imperfect information	Market power	Network Failure
Science and research (including AI)	✓	✓		✓		
Processing/ Re-use of data			✓	✓		
Subject Access Requests	✓					
Privacy and Electronic communications	✓					
Data subject rights			✓	✓		
International data transfers	✓			✓		
Using data to improve public services (including DHSC, CDDO and HO initiatives)	✓	✓		✓		
The Information Commissioner's Office (ICO)			✓			
Digital Identity Schemes[33]			✓	✓		
Smart Data[34]			✓	✓	✓	✓

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

[32] https://www.nfx.com/post/truth-about-data-network-effects
[33] More information on the rationale for intervention in the Digital Identity market can be found in the Digital Identity De Minimis Assessment - DCMS, 2021
[34] More information on the rationale for intervention in the Smart Data market can be found in the Smart Data final Impact Assessment 2022 - BEIS

34. Government intervention in the form of new legislation or changes to existing legislation will help overcome these market failures. Reform options have been designed specifically to remedy market failure in specific industries and sectors as well as UK data policy more generally. DCMS set out many of these areas in Data: A New Direction.[35]

35. The rationales for intervention to correct for the market failures currently experienced by **UK businesses** are set out below:

    a. The UK is ranked second in the world for **science and research**, and 54% of UK output is world leading.[36] Data is key to a wide range of research activities across many sectors and this is reflected in the UK GDPR. The existing legislation provides specific allowances in relation to processing for research purposes, however, the laws around personal data use for "research purposes" are complex and the current regulatory landscape has proven difficult for scientists to navigate, making it harder to establish legal certainty for vital and innovative research. This highlights how the market fails because scientists have incomplete information about personal data use and how the data value chain suffers a market failure at the collection stage. Furthermore, through the consultation process we identified that some aspects of the existing framework can place unnecessary barriers to researchers, slowing down or even stopping their progress. The barriers researchers face restrict the realisation of societal benefits from effective data use. This shows how the data value chain suffers a market failure at the impact stage.

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

    c. When used responsibly, data-driven **artificial intelligence (AI) systems** have the potential to bring substantial benefits to the lives of consumers and businesses. The development of AI and machine learning applications is contingent on data, and places specific demands on its collection, curation and use. The market failures discussed all have an effect on the current development of AI. Consumers may not be aware of their rights when subjected to automated decision making reflecting the information gaps. Uncertainty regarding these data requirements could raise barriers to realising these benefits.

[35] Data: A new direction, DCMS, 2021
[36] Study UK, Access World Leading Research

d. UK data protection legislation requires that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed - commonly known as the **data minimisation principle**. The confusion surrounding what data qualifies to be anonymised as part of this principle represents a market failure and can result in businesses facing extra time and costs to using data effectively.

e. Following on from the consultation, the government recognises that organisations face burdens because of the **accountability framework** set out in the current regime. The current accountability framework provides businesses with a list of all the activities and processes they have to do to demonstrate a high level of compliance with data regulations. Some organisations have expressed concerns over the prescriptive nature of GDPR, requesting a more flexible, outcomes-based regime. The current approach to compliance is also putting a disproportionate burden on some SMEs and organisations that undertake low risk processing, despite some current requirements being risk-based and limited exemptions applying. The current legislation represents a market failure because the disproportionate impact it has on SMEs limits competition in the market. By reducing these compliance requirements through the introduction of a new accountability framework businesses would be able to save on data processing.

f. **Subject access requests (SARs)** allow for subjects to check the accuracy of their data about them as recorded by data processors, learn more about how it is being used, and who it is being shared with, however, dealing with requests can be very time-consuming and resource intensive for organisations, placing a burden on them and secondly there are occasions whereby a subject will make a request which is not in line with Recital 63 to the UK GDPR - i.e. they will make a request not to '"be aware of, and verify, the lawfulness of processing data"' but to cause disruption to the organisation that they are requesting their data from. The process is currently inefficient and may deter businesses from handling personal data therefore restricting the wider benefits that can be achieved from effective data use.

g. The **Privacy and Electronic Communications Regulations 2003** (PECR) is complementary to the UK GDPR and the DPA. PECR prohibits an organisation from storing or gaining access to information that is held in the equipment of an individual (such as computers and mobile phones), without consent from the individual. From consultation we know that organisations have found that the ability to collect data in order to improve websites is difficult to obtain due to consent requirements, and individuals find the number of cookie pop-ups a source of annoyance and routinely accept the terms without reading them.

h. The government has highlighted its ambition for the UK to be a leader in digital trade and the world's most attractive data marketplace. Currently a number of barriers to **international data transfers** exist, including a lack of alignment in legal frameworks, transfer tools and data bridge regulations. The complexity of the regulations has contributed to information gaps for data controllers which have restricted the international transfers of data. This market failure has an impact at all levels of the data value chain. The government needs to intervene to achieve its ambition of helping domestic businesses to connect more easily with foreign markets, while attracting investment from abroad by businesses that rightly have confidence in the responsible use of data within the UK.

36. The rationales for intervention to correct for the market failures experienced by the **public sector** are set out below:

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

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

37. Rationale for intervention in the use of data for law enforcement and intelligence purposes has been provided by the Home Office.

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

    b. The Home Office has responsibility for law-enforcement and intelligence services data processing. The Bill will update the Data Protection Act 2018 (DPA 2018). It will contribute to reducing the risk from terrorism to the UK and UK interest overseas[37] and will restore confidence in the criminal justice system[38] (CJS) when it comes to data protection.

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

    d. The Home Office has two overarching aims:

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

i. Firstly, to support delivery of the manifesto commitment to empower the police to use new technologies, like biometrics, within a strict legal framework which maintains public trust;

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

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

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

38. In addition to the areas above set out in Data: A New Direction, the Government feels that the Data Protection and Digital Information Bill is a suitable legislative vehicle to pursue several reforms closely related to the UK's data protection regime - on digital identities, smart data schemes, the architecture of health databases and the registration of births and deaths.

a. An emergent marketplace in **Digital Identities** already exists, with more and more businesses and citizens preferring to verify information about themselves without needing paper documents. However, current identity proofing methods can be expensive, inefficient, and vulnerable to fraud. Digital identities can strengthen and simplify the process, however, the current landscape lacks standards which will enable interoperability and does not yet command trust. In the 2019 Digital Identity Call for Evidence,[39] respondents noted that the market required the government to step in and set these standards, create mechanisms to allow organisations to prove they follow them, and to enable checks against government-held data. More information on this market failure can be found in the Digital identity and attributes De Minimis Assessment.[40]

b. In the case of **Smart Data initiatives**, there is a failure of existing regulation to enable easy and secure data mobility. Many markets currently face low levels of consumer engagement. Consumers are unable to navigate these markets easily resulting in negative outcomes such as the 'loyalty penalty', low switching rates, poor satisfaction, and subscription traps. These negative outcomes are further exacerbated for vulnerable consumers who may have further inabilities to access and engage. Alongside low consumer engagement is a lack of trust and empowerment to utilise their own data in markets, increasing their cost of informed decision making. While already sharing data,

[39] Digital Identity: Call for Evidence Response, DCMS, 2020
[40] Digital identity and attributes De Minimis Assessment, DCMS, 2021

some customers are currently using less secure methods, such as 'screen scraping', which can lead to direct harm if this data is mishandled. Evidence also shows that in digital markets there is increasing concern that access to data is a significant barrier to entry. Intervention is therefore necessary to help address the issues arising in these markets and to alleviate wider market failures. More detail can be found on Smart data rationales in the Smart Data Impact Assessment.[41]

c. In the **health sector**, currently service users and their care teams cannot easily access or share, in real time, all the health and/or social care information that is relevant to their care. This is, in part, because IT suppliers are not uniformly providing products and services based on shared principles and architecture that incorporate or enable interoperability so that data can easily be shared in real time between organisations that use different systems. There is also stakeholder consensus that there are no existing powers that can compel IT suppliers to adopt such shared principles going forward. It is the intention of this bill to remedy this through taking primary powers to require IT suppliers of products/services to the health and care system in England to meet specified open data architecture standards to improve patient outcomes. More information on the rationale for intervention in the health and social care sectors can be found in the annex.

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

Table 4: How the legislation would overcome each market failure

Market Failure	Policy Intervention
Externalities	Implement legislation that makes it easier for personal data to be used in science and research while also providing consumers with the optimum level of privacy protection.
Public Goods	Implement legislation that makes it easier for personal data to be exchanged between public sector bodies. Introduce frameworks that encourage data use in the public sector.
Information Asymmetry	Simplify the legislation regarding data exchange and data use. Provide clarification of the rules around using personal data to benefit businesses and their consumers.

[41] Smart Data Impact Assessment, BEIS (2022)

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

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

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

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

41. Indicative analysis was previously undertaken at the pre-consultation stage. Since then, the analysis has been updated to reflect consultation responses, discussions with cross-government experts and external consultants, assessment of the latest literature, and reflections on the RPC's comments on the methodology. This engagement indicated that the reforms are largely an improvement on previous legislation, providing clearer guidance and a reduction in burdens to stakeholders. A revision of our evidence basis, considering consultation responses too, means the progressed reforms are based on a solid evidence base while the reforms that might lack at this stage the evidence to progress are disqualified. We expect these steps taken to help make a tangible improvement over previous legislation

42. Previously we conducted analysis at the collective level, looking at all of the proposed reforms as a package. Where evidence is now available we are able to analyse some policies at an individual level. Although more evidence has become available to us, there are still uncertainties and evidence gaps. However, we know that some reforms share similar channels of impact and implication so we have continued to analyse policies within groups that are consistent with the expected impacts. This ensures that the analysis remains novel, proportionate and robust.

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

44. We continue to use the approach outlined in the pre-consultation analysis note and begin by assessing the available evidence to develop theories of change for each reform, and to establish the evidence available to support either quantitative or qualitative analysis. DCMS has also worked alongside analysts from across Government to establish the rationale, options, costs and benefits, and finer detail of the impact of reforms where analysis has been led by their respective organisations and where relevant tailored towards a specific sector. These organisations are the department for Business, Energy, and Industrial Strategy (BEIS),[42] the Home Office, Cabinet Office Central Digital and Data Office (CDDO), DHSC and the Information Commissioner's Office (ICO).

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

46. Where quantitative evidence is not available, qualitative analysis of impacts has been undertaken and expanded upon since consultation, including further literature reviews and case studies. On particularly uncertain impacts, such as trade, data bridges and Adequacy,

[42] Smart Data Impact Assessment, BEIS (2022)

complementary approaches have been used to provide more evidence of the potential scale of impacts.

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

Description of options considered

Background

48. This section discusses the approach taken to identify the various policy options to ensure that this bill of reforms delivers the government's ambition to create a pro-growth and innovation-friendly data protection regime that underpins the trustworthy use of data. This objective is part of the National Data Strategy,[43] in itself part of the government's 10 tech priorities,[44] and is the first step in establishing the UK as a global leader on data.

49. These ambitions have a strong economic rationale and the opportunity for the UK economy is substantial, given its superior starting position in comparison to many of its peers. **The data market in the UK - i.e. money made from products or services derived from digitised data - is the largest in Europe**, representing approximately 4% of GDP in 2020[45] and about 5% of the workforce[46] being employed in the sector.[47]

50. The UK data regime is already among the most comprehensive and open worldwide,[48] which is linked to its superior data governance. The UK needs to remain a pragmatic innovator, ensuring that further reforms tackle key issues and introduce net positive impacts on the economy and society. This framework underpins the reforms considered and the process through which these were agreed upon.

51. Balancing between ambition and pragmatism, the aim of the reforms is to create an ambitious, pro-growth and innovation-friendly UK data protection regime. It will underpin the trustworthy use of data to support our world-leading science and digital ecosystems, whilst maintaining the highest standards of data protection. Identifying the correct and most effective set of reforms to achieve this is the key driver behind the decision-making process and this economic analysis.

Process of shortlisting options

52. Prior to considering any specific reform options, the government gathered evidence to understand how the UK's current data protection regime is functioning in practice, identifying any gaps and raising issues. Following on from this, the approach taken was to identify the various policy levers that can be used to achieve the strategic objectives. The consultation

[43] National Data Strategy, DCMS (2020)
[44] DCMS, 10 Tech Priorities, (2021)
[45] The European Data Market Monitoring Tool (2020)
[46] Defined as a "data professional"
[47] The European Data Market Monitoring Tool, (2020). A different survey of the UK public suggests that, for those in employment, nearly three-quarters (72%) said they use 'basic' data skills either a lot or occasionally in their current role, with only 13% saying they 'never' use them. Of the people who have used 'basic' data skills, 87% are confident in using them. Fewer - but still a majority of - people use 'advanced' data skills (65%). And of people who have ever used these more advanced data skills, 74% feel confident in using them.ad hoc statistics, DCMS, data policy, (2020)
[48] As confirmed among multiple studies such as the Global Open Data Index from the Open Knowledge Foundation, and the data governance study from Washington University

stage was used to develop this understanding further and to provide further evidence around the existing and potential data landscape and the role of government intervention in this.

53. In light of this evidence, reform options have been designed to respect the key elements of the current UK GDPR, such as its processing principles, data subject rights, and mechanisms for supervision and enforcement. The options will continue to underpin a high level of protection for people's personal data and control for individuals over how their personal data is used. The Government also continues to recognise that organisations have and are continuing to invest in understanding, complying and implementing the current regime.

54. The reform options are therefore frequently clarificatory in nature, designed to address identified issues - or innovating within the current framework to better achieve the desired outcomes. Non-regulator policy levers were considered but not short listed. The main reasons being that;

    a. the original policy framework has been successful in resolving some market failures but has not achieved all its original aims, the reforms are aimed at expanding and improving existing legislation

    b. in some instances, other policy levers were considered but disqualified, such as in the case of DHSC, who considered centralising electronic patient records (EPRs) through a single-vendor, government-led solution, but rejected them as former attempts proved too costly and inefficient

    c. other policy levers might be considered by DCMS in the future that can augment and contribute to the broader national data strategy objectives, complementing this reform bill

    d. non-intrusive regulatory interventions are the preferred approach of the government, especially around data policy that remains a relatively new field and a nascent market

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

56. “Critical Success Factors” (CSFs) are the attributes that any successful proposal must have, if it is to achieve successful delivery of its objectives. The set of critical success factors used to assess each reform can be seen below:

    - Strategic fit - Does it help increase data utilisation
    - Strategic fit - Does it decrease compliance costs
    - Potential Feasibility
    - Evidence available

57. Reforms were tested against each criterion and after consultation stage grouped together into sets of reforms, presented in this assessment as options. These options can be represented by points on a hypothetical 'data - openness scale'.[49] Data Openness definitions can vary depending on the methodology followed, but here we take it to refer to transparency, accessibility, and accountability. More specifically we define it as 1) data being easy to find online, 2) data is easily usable and can be safely processed, provided the right safeguards are in place, 3) data licensing is standard practice and not jeopardised by a lack of standards. For example, to make no changes to the UK's data regime and to continue with the 'status quo' would result in the UK continuing to be a widely open jurisdiction, as defined by the OECD STRI, however unable to correct for the market failures outlined above and fully utilise data as a valuable asset.

58. The three options alongside the status -quo/do nothing option all fall on the liberalisation side of the data - openness scale when compared to the current regime. Our second option is to make minor changes to the current regime. Thirdly, we consider a moderate set of reform options and finally a more radical set of options representing an overhaul of existing legislation. More details of these packages can be seen in the table below:

Final list of options

59. From the evidence gathered, we present a set of 4 options that will be assessed against key critical success factors, using evidence from the consultation stage.

Figure 1: Outline of policy development process

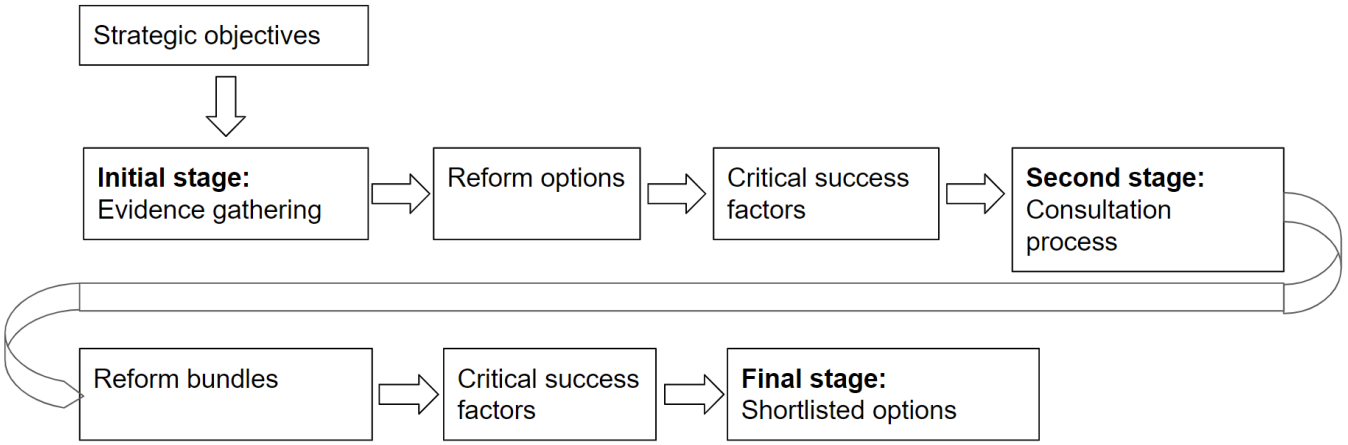


Table 5: Outline of policy options

Option	Description
Do nothing	No policy change
1. Do minimum	Minor policy changes to the current regime (UK GDPR)
2. Intermediate option	Considerable policy changes to the current regime

[49] Some such indices already exist, including the Global Open Data produced by the open knowledge foundation, available at: https://index.okfn.org/insights/

3. Do maximum	A complete overhaul of existing legislation, repealing and replacing the existing regime

Table 6: Overview of all options[50]

Reform Subheading	Reform summary	Description	Do nothing	Do min	Intermediate Option	Do max
Removing barriers to responsible innovation	Research Purposes	• Amending existing legislation to support responsible research activity using personal data. • Extend the exemptions from the regime when conducting scientific research to include when that research is carried out in a commercial setting.		X	X	X
	Further Processing	• Clarifying that further processing for an incompatible purpose may be lawful when based on a law that safeguards an important public interest (these are the laws necessary for the objectives set out in Article 23(1)) or when the data subject has re-consented.		X	X	X
	Legitimate Interests	• Creating a limited list of legitimate interests for businesses to process personal data without applying the balancing test. • List activities, such as direct marketing or ensuring network and information security, that may be in the legitimate interests of organisations handling data.		X	X	X
	AI and Machine Learning	• Enhancing the approach to explainability and accountability for fair processing in the context of profiling when using Automatic Decision Making. Amending Article 22 to clarify its meaning and ensure that any automated decisions which are made without meaningful human involvement, and which have a significant impact on the data subject are properly captured. • Clarifying the circumstances in which safeguards apply to significant decisions that are taken about individuals on the basis of profiling			X	X
	Data minimisation and anonymisation	• Put in place legislation that includes a clear test for determining when data will be regarded as anonymous (adopting the recital 26 test for anonymisation into legislation)			X	X
Reducing burdens on businesses and delivering better outcomes for people	Reform of the Accountability Framework	• Introduce an outcomes-based accountability framework. Remove prescriptive elements of existing framework and underpin the new framework with privacy management programmes. • Reducing and simplifying record-keeping requirements, for organisations that control or process low risk data.		X	X	X
	Subject Access Requests	• To amend the threshold for responding to a SAR from ‘manifestly unfounded’ to ‘vexatious’			X	X
	Privacy and electronic communications and the use of personal data for the	• PECR complements the UK GDPR and Data Protection Act 2018 and sets out more specific privacy rights on: a. Marketing by electronic means			X	X

[50] More information on all policies can be found in Annex 1

	purposes of democratic engagement	b. Confidentiality of terminal equipment c. Security of public electronic communications services d. Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services - for example, caller ID and call return - and directory listing ● These policies need to be updated to reflect increasing digitalisation.				
Boosting trade and removing barriers to data flows	Data Bridge	● Underpinning the UK's future approach to data bridge regulations with principles of risk-assessment and proportionality			X	X
	Article 27 representatives	● Removing the requirement for controllers in adequate countries to have representatives in the UK		X	X	X
	Alternative Transfer Mechanisms	● Reducing the barriers and burdens that organisations face when transferring personal data freely and safely overseas. ● Ensuring businesses are able to continue to seamlessly use their pre-Bill existing transfer mechanisms - without a requirement for further checks and avoiding additional costs			X	X
Delivering better public services	Derogations	● Clarifying that private organisations & individuals asked to carry out an activity on behalf of a public body may rely on that body's lawful ground for processing personal data.			X	X
	Digital Economy Act 2017 (CDDO)	● To extend powers aimed at improving public service delivery to business undertakings, beyond the current scope of solely individuals and households.			X	X
Reform of the Information Commissioner's Office	Strategy, Objectives and Duties	● Introduce a new, statutory framework that sets out the strategic objectives and duties that the ICO must aim to fulfil when exercising its data protection functions.		X	X	X
	Governance Model and Leadership	● The government proposed to move away from the corporation's sole structure to a body corporate, introducing a statutory board with a chair and chief executive. This change will bring the ICO in line with other UK regulators such as Ofcom and the FCA.		X	X	X
	Accountability and Transparency	● Proposals to introduce new publishing and reporting requirements for the ICO to aid transparency and external scrutiny of the ICO's performance.			X	X
	Complaints	● Proposals to create a more efficient and effective model that would require a complainant to attempt to resolve their complaint directly with the relevant data controller before lodging a complaint with the ICO.			X	X
	Biometrics Commissioner and Surveillance Camera Commissioner	● Simplify the oversight framework for police use of biometrics and police and local authority overt use of surveillance cameras.			X	
	Enforcement Powers	● Enabling the ICO to carry out more effective and efficient investigatory activity.			X	X
	Codes of Practice and	● Creating a statutory requirement for the ICO to undertake and publish impact			X	X

	Guidance	assessments when developing statutory codes of practice and statutory guidance and a process for the Secretary of State to approve statutory codes and statutory guidance ahead of laying them in Parliament.				
Home Office: Subject Access Requests	Subject Access Requests (SAR) (DPA 2018 parts 3 & 4)	● Mirror an existing UK GDPR provision that permits a two-month extension to a SAR time period when a request is particularly complex. This will introduce greater consistency across the legislation.			X	
Home Office: Intelligence Services Data Reform Proposals (part 4)	Amendments to Part 4 of the DPA 2018 - National Security Notices	● Introduce a power that would allow the Secretary of State to issue a notice authorising a law enforcement body to process data under the Intelligence Services regime in Part 4 of the DPA 2018 in specified circumstances.			X	
Home Office: Law Enforcement Data Reform Proposal	Mirror the national security exemption from Part 2 (DPA 2018 part 3)	● To mirror the national security exemption from Part 2 through amendments to the Data Protection legislation			X	
	Introduce a 'Legal Professional Privilege' Exemption (DPA 2018 part 3)	● Introduce an LPP exemption into Part 3 that is already available under the other data protection regimes (Parts 2 and 4 of the DPA 2018) which will provide greater transparency for both controllers and data subjects in relation to legally privileged material.			X	
	Introduce a definition of 'consent' to Part 3 (DPA 2018 part 3)	● Introduce a uniform definition of 'consent' that data controllers under Part 3 can refer to.			X	
	Introduce a power to allow bodies representing Part 3 controllers and processors to produce 'Codes of Conduct' (DPA 2018 part 3)	● Proposal so that codes of conduct can be produced by representative bodies to clarify the application of data protection laws under Part 3.			X	
	Remove the need to log the 'justification' for consulting/disclosing data (DPA 2018 part 3)	● Proposal seeks to remove the requirement for law enforcement agencies to record a 'justification' in the logs of consultation and disclosure.		X	X	
	Introduce the ability to actively review automated decisions (DPA 2018 part 3)	● Currently, law enforcement agencies are required to inform data subjects as soon as reasonably practicable when a decision that is based solely on automated processing is made and produces an adverse legal effect. This proposal will provide an alternative option for law enforcement agencies to provide for a human to actively review the decision as soon as is reasonably practicable thereby removing the need to notify the data subject at the time.			X	

Home Office: International Transfers	Clarifying use of Section 76 DPA to cover large scale transfers.	• The reform clarifies how law enforcement can legitimately use S76 which enables the transfer of personal data where 'special circumstances' are present to give confidence to the law enforcement community to use this to transfer larger amounts of data in the pursuit of the detection and prevention of crime.			X	
	Reform subsequent transfer's provision (Section 78 DPA)	• Under the current legislation, UK competent authorities must make it a condition of any transfer for a law enforcement purpose that data is not to be further transferred to a third country or international organisation without the authorisation of the transferring controller (or another competent authority). This reform considers introducing a targeted small exemption to allow competent authorities to provide a dispensation from the requirement in the case of an immediate and serious threat where authorisation cannot be obtained in good time. In such cases, the third country would be required to notify the relevant competent authority of the transfer as soon as practicable.			X	
Home Office: Births and Deaths Registration Act 1953	Remove the requirement for paper birth and death registers moving to an electronic register	• The provision for registering births, still births and deaths is contained in the Births and Deaths Registration Act 1953 (BDRA) and the Registration of Births and Deaths Regulations 1987. In 2009 the registration online system (RON) was introduced allowing registrars to register births and deaths electronically. Even though all birth and death information are held electronically, registrars are still required to also hold a record of the events in paper registers. The policy objective is to remove the requirement for paper registers to be held in 173 registration districts and make the RON system the electronic default birth and death register.			X	
Home Office: I-LEAP	Introduce delegated power to pass secondary legislation enabling the technical implementation of new international alert sharing agreements	• The International-Law Enforcement Alerts Platform (I-LEAP) will deliver real-time alert exchange with key international partners and so strengthen joint capabilities to tackle shared threats, including migrant smuggling			X	
Health and Social Care (DHSC)	New powers on providers e.g. NHS Trusts or care homes	• Amend primary legislation to create a power for the Secretary of State for Health and Social Care to direct providers to adopt an open data architecture approach, including when procuring an IT system supplier to assist. • This option increases the pressure on providers to implement the new changes, without the guarantee that the required products or services will be available for them to procure.		X		
	New Information Standard Notices (ISNs) on IT suppliers of products or services [preferred option]	• Create primary legislation for a new power for the Secretary of State for Health and Social Care to direct suppliers/suppliers to adopt an open data architecture approach through the use of ISNs. • Ensures that products and services procured by the health care system enable and support data to be accessed, interrogated and processed in real time by anyone with the			X	

		basis to appropriately access that data, irrespective of the system used by the health or adult social care provider who collated, produced or otherwise processed that data.				
	New ISNs on all health and care providers - public and private	• The new ISNs would be linked to new interoperability requirements. • This option only increases the burden on health and care providers to adhere to requirements that may be impossible to meet without IT supplier support. The options also contingent on the availability of IT products and services that meet the specified requirements. The ISNs also may not be applicable to all health and care organisations. • ISNs would arguably not be far reaching enough to ensure all suppliers adhere to the changes proposed, and may not be applicable to all health and care organisations.		X		
	No new contracts after a specific date	• All contracts between health and social care providers and IT suppliers after a set date would need to build in new open data architecture requirements/standards as a requirement from IT suppliers. • Increases the administrative burden on health and care providers to search for and procure IT products and services that meet standards that they may not have personnel to understand. It is also contingent on the availability of IT products and services that meet the specified standards, which the option cannot ensure.				X
Digital Identity	Digital Identity: Create a governance framework and enable checks against government-held data[51]	• Create a statutory governance framework to oversee the trust framework and to enable checks against government-held data.			X	X
Smart Data	Smart Data Initiatives	• Introduction of primary legislation, creating new “regulation-making” powers to enable Smart Data schemes to be introduced in any given sector. [52]			X	X
Technical reforms	• Text stating that other primary legislation is to be treated as being subject to the data protection legislation unless express provision is made to the contrary.			X	X	X
	• Enabling statutory codes requested by the SoS under this section to have the same legal effect as those issued under sections 121 - 124 of DPA			X	X	X
	• In the event that DCMS Ministers decide to ratify the Council of Europe Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (also known as C108+), outdated references to the original Convention ‘C108’, in ten articles of the Data Protection Act 2018, will need to be changed to C108+			X	X	X
	• Amending section 128 of the Data Protection Act 2018 (DPA 2018) to make sure that any new ICO codes of practice required by regulations made by the Secretary of State have the same legal effect and status as existing ICO codes			X	X	X

[51] This is the preferred option in the Digital identity and attributes - De Minimis Assessment ,DCMS (2021)
[52] This is the preferred option in the Smart Data initiatives Impact Assessment, BEIS (2022)

	issued under the DPA 2018 (the data-sharing and age-appropriate design codes are examples of existing codes).					
	• Update the definition of "direct marketing" in PECR so that it is drawn from the DPA 2018, rather than the DPA 1998. Most of the DPA 1998 was repealed when the 2018 Act came into force, so this should make the legislation easier to navigate.			X	X	X
	• Clarifying the anonymisation process by creating a test for identifiability				X	X
	• Omitting Article 27 from UK GDPR which removes the requirement for controllers and processors caught by Article 3(2) to appoint a representative				X	X
	• Privacy Management Programme - An amendment to ensure consistency in language between Clause 18 18(2)(b) and Clause 18(5)(b).				X	X
	• Research - consequential provisions - Disapply the provisions of new Chapter 8A UK GDPR (inserted by Cl 22) in relation to unstructured manual data held by FOI Public Authorities.				X	X
	• Codes of practice as to the processing of personal data - This amends section 205(2) of the Data Protection Act 2018 so as to disapply the provision about periods of time in Article 3 of Regulation (EEC, Euratom) No. 1182/71 which would otherwise apply for the purposes of section 120H(3) and (4) of that Act (inserted by clause 28 of the Bill).				X	X
	• Enforcement: Remove duplicative reference to a 'report' in this clause				X	X
	• Annual report on regulatory action - A minor amendment to clause 38 to clarify the definition of "enforcement powers" in new section 161A(6) so that it does not include section 142 to 159 DPA as applied by the EITSET and PEC Regs and section 20(2) of the Interpretation Act does not apply here.				X	X
	• Consequential amendments of The Electronic Identification and Trust Services for Electronic Transactions Regulations (EITSET Regulations) - An amendment to change the words modified, as well as the modification in this clause				X	X
	• Statutory Override - Clarification of the scope and intended effect of s183A .				X	X
	• UK GDPR Regulations - An amendment to add "made under this Regulation or another enactment that are" in order to ensure consistency with other clauses				X	X
	• Information disclosed by the Revenue and Customs - making equivalent provision for Welsh and Scottish revenue authorities				X	X
	Clause 62 establishes the primary power to establish Smart data schemes with a focus on customer data, including data sharing and action initiation by an authorised person or TPP. Further details are included	Clause 62 amendment - This amendment makes clear that the power under clause 62(3) is available in relation to all persons authorised to receive customer data, whether or not they have received such data. Clause 63 amendment - This amends clause 63(3) so that it reflects more clearly the fact that regulations under clause 62 may enable a customer to authorise a person to receive customer data and to do other things, in particular as described in clause 62(2)(b) and (3).			X	X

	around the associated regulations in Clause 63. Subsection 62 (3) is likely the focus of any amendment, although we are awaiting further legal advice.					
	● Clause 63 outlines provisions that regulations relating to customer data may, among other things, contain. ● A change to the wording in clause 63(3) to reflect the fact that the intention is that regulations may require a person who is an "authorised person" (as defined in clause 62(1)(b)) to be further authorised in order to eg. exercise a customer's rights in relation to a data holder.				X	X
	● Smart Data regulations- Deletion of redundant subsection (5) of clause 74. Subsection (5) of clause 74, which makes provision about regulations under Part 3 of the Bill, is unnecessary because equivalent provision about regulations under the Bill is made in clause 107(4).				X	X
	● Definitions in Democratic Engagement clause- definitions for “communication”, “public electronic communications service” and “call” to be made clear.				X	X
	● Co-operation between supervisory authority and overseas authorities -This inserts a consequential amendment of the heading of Article 18 of the eIDAS Regulation (cooperation with EU authorities).				X	X
	● Transfer of functions etc to the Information Commission - Adding the gloss so that "information Commissioner" and "Information Commission" are read as the same				X	X
	● Purpose limitation: processing to be treated as compatible with original purpose - To remove the exception from various provisions for journalistic, academic, artistic and literary purposes in sch 2 para 26 in light of the change to Art 36(1).					
	● Subject access requests - In clause 7(3), new Art 12A(1) (page 9, line 10) refers to “Articles 15 to 22 or 34”. Clause 11 removes Article 22 and replaces it with new Articles 22A to 22D.The amendment would ensure that article 22 should be consequently amended by Schedule 3.				X	X
	● Transfers of Personal Data to Third Countries - Transfers Approved by Regulations: Monitoring - Subsection 74B(7)(a) was removed and we believe that the connector "and" after this subsection should be also removed. In current drafting it is not determined and it looks like "and" should be kept and followed by subsection 74B(7)(b) which was preserved.				X	X
	● Transfers of personal data to third countries etc: consequential and transitional provision - This amends section 205(2) of the Data Protection Act 2018 in consequence of the repeal of section 189(9) of that Act by paragraph 19 of Schedule 7 to the Bill.				X	X
	● ICO Complaints - An amendment to ensure consistency between s.187(1)(a) and (2)(a)				X	X

	● ICO Complaints - The amendment is consequential to the repeal of Art 77 UK GDPR by batch Comp-ICO			X	X
	Privacy and electronic communications: Commissioner's enforcement powers ● The modifications in the new Schedule 1 to the PEC Regulations inserted by Schedule 10 to the Bill do not take account of the changes made by clause 13 of the Bill. In particular - ○ paragraph 3(d) modifies s.142 DPA 2018 by omitting subsections (9) and (10). Subsection (9) is repealed by clause 13(3)(a); ○ paragraph 4(1) modifies s.143 DPA 2018 by omitting subsections (1) and (9). Subsection (9) is repealed by clause 13(3)(b); ○ paragraph 24 modifies s.181 DPA 2018 by omitting the definition of "representative", as well as the definition of "certification provider". The definition of "representative" in s.181 DPA 2018 is to be repealed by clause 13(3)(c) of the Bill. ● Clause 13 is to come into force 2 months after Royal Assent (see clause 111(3)(b)) and the expectation is that Schedule 10 would come into force at that time or afterwards, ie. by the time it operates, the definition of "representative" will have been removed. ● The modifications listed above should be changed to take account of the changes made by clause 13(3).			X	X
	● ICO Governance - An amendment to ensure consistency between paragraphs 8(1) and 9(6) in reference to the Commission			X	X

Do nothing option

60. This option is the benchmark counterfactual and describes a scenario in which the current regime is continued without change. This is equivalent to the continuation of UK GDPR, all aspects of the Data Protection Act 2018 (DPA 2018) and the extended continuation of the UK and EU Adequacy agreement. As highlighted in section one, although the current regime is effective in allowing data use and data transfers, and is relatively liberal in comparison with other jurisdictions, there are certain limitations that mean the benefits from this are limited and firms are not maximising their potential gain from data use.

Do minimum

61. The do minimum option, encapsulates minor policy changes to the current regime in an attempt to resolve aspects of the market failures. This includes key reforms that aim to resolve some of the issues identified as part of the policy process. The majority of reforms have been fairly well received by stakeholders and substantial evidence exists suggesting that they would have a beneficial impact on the economy, LEAs, UK Intelligence Services, and society as a whole. The policies included in this option are listed below, the package of reforms as a whole is assessed against the critical success factors in the next section of the impact assessment.

Table 7: List of all policies in 'do minimum' category[53]

Reform Subheading	Reform summary
Removing barriers to responsible innovation	Research Purposes
	Further Processing
	Legitimate Interests
Reducing burdens on businesses and delivering better outcomes for people	Reform of the Accountability Framework
Boosting trade and removing barriers to data flows	Article 27 representatives
Reform of the Information Commissioner's Office	Strategy, Objectives and Duties
	Governance Model and Leadership
Public Safety and National Security (Home Office)	Remove the need to log the 'justification' for consulting/disclosing data (DPA 2018 part 3)
Health and Social Care (DHSC	New powers on providers e.g. NHS Trusts or care homes
	New ISNs on all health and care providers - public and private
Technical Reforms	

Intermediate option

[53] More information on all policies can be found in Annex 1

62. The intermediate option presents a package of policy options that make a substantial change and improvement to the current UK GDPR, targeted at resolving the existing market failures. The package includes a mixture of policies directed at both UK businesses and the public sector, for example specific reforms to encourage businesses to maximise their data use for research and development purposes as well as public sector reforms designed to make the sharing of data across government departments for public benefit easier. The package also includes a mixture of policies directed at both UK Intelligence Services and LEAs, for example, reforms to create consistency across the data processing regimes.

63. These reforms have all been well received at the consultation stage and substantial evidence exists on their potential impact on the economy and society as a whole.

Table 8: List of all reforms in 'intermediate policy option'[54]

Reform subheading	Reform summary
Removing barriers to responsible innovation	Research Purposes
	Further Processing
	Legitimate Interests
	AI and Machine Learning
	Data minimisation and anonymisation
Reducing burdens on businesses and delivering better outcomes for people	Reform of the Accountability Framework
	Subject Access Requests
	Privacy and electronic communications and the use of personal data for the purposes of democratic engagement
Boosting trade and removing barriers to data flows	Data Bridge Regulations
	Article 27 representatives
	Alternative Transfer Mechanisms
Delivering better public services	Derogations
	Digital Economy Act 2017
Reform of the Information Commissioner's Office	Strategy, Objectives and Duties
	Governance Model and Leadership
	Accountability and Transparency
	Complaints
	Biometrics Commissioner and Surveillance Camera Commissioner
	Enforcement Powers

[54] More information on all policies can be found in Annex 1

	Codes of Practice and Guidance
Public Safety and National Security (Home Office)	Subject Access Requests (SAR) (DPA 2018 parts 3 & 4)
	Amendments to Part 4 of the DPA 2018 - National Security Notices
	Mirror the national security exemption from Part 2 (DPA 2018 part 3)
	Introduce a 'Legal Professional Privilege' Exemption (DPA 2018 part 3)
	Introduce a definition of 'consent' to Part 3 (DPA 2018 part 3)
	Introduce a power to allow bodies representing Part 3 controllers and processors to produce 'Codes of Conduct' (DPA 2018 part 3)
	Remove the need to log the 'justification' for consulting/disclosing data (DPA 2018 part 3)
	Introduce the ability to actively review automated decisions (DPA 2018 part 3)
	Clarifying use of Section 76 DPA to cover large scale transfers.
	Reform subsequent transfer's provision (Section 78 DPA)
	Introduce delegated power to pass secondary legislation enabling the technical implementation of new international alert sharing agreements
	Remove the requirement for paper birth and death registers moving to an electronic register
Health and Social Care (DHSC)	New Information Standard Notices (ISNs) on IT suppliers of products or services
Digital Identity	Digital Identity: Create a governance framework and enable checks against government-held data[55]
Smart Data	Smart Data: Introduction of primary legislation, creating new "regulation-making" powers to enable Smart Data schemes to be introduced in any given sector[56]
Technical reforms	

Do Maximum

64. The final package of reforms assessed as part of this Impact Assessment is the 'do maximum' option. This option expands on the intermediate approach with additional reforms that seek to make complete and substantial change to the current regime. These reforms have been tested at consultation stage and while some evidence exists on their potential impact, several of them remain untested. These additional reforms are listed below:

Table 9: List of additional policy options making up 'do maximum' package of reforms[57]

Reform Subheading	Reform summary
Health and Social Care (DHSC)	No new contracts after a specific date

[55] This is the preferred option in the Digital identity and attributes - De Minimis Assessment 2021 published by DCMS
[56] This is the preferred option in the Smart Data initiatives Impact Assessment 2022 published by BEIS
[57] More information on all policies can be found in Annex 1

65. As part of the long to short listing process we have analytically assessed each set of options in order to identify the preferred package of reforms.[58] Following the consultation process we tested the options against the Critical Success Factors (CSFs), taking into consideration the interactions and interdependencies of these reforms alongside the rest within each bundle. A summary of this assessment is shown below.

Table 10: Ranking of packages against CSFs

Policy Option	Strategic Fit - Does it help increase data utilisation?	Strategic Fit - Does it decrease compliance costs?	Potential Feasibility?	Evidence available?
Do nothing	No	No	High	N/A
Do minimum	Low	Low	High	Sufficient
Intermediate option	Medium	Medium	High	Sufficient
Do maximum	High	High	Low	Limited

66. The preferred option is the intermediate package of reforms, outlined above. This set of options are expected to meet the Government's objectives of increasing data utilisation, creating a flexible and non-burdensome compliance environment for businesses whilst maintaining an environment that efficiently regulates the use of personal data for all purposes including research and development and AI and Machine Learning. These reforms are also both feasible to implement at this stage without risking delays, introducing unforeseen risks or creating further costs for UK businesses, consumers and government as indicated by the limited evidence on their ability to deliver efficiently the objectives expected. Some of the reforms in the "Do maximum" option, while remaining of interest to the Government, were deemed to not currently meet the bar set in terms of available evidence or feasibility to progress at this stage. Amassing the evidence and balancing priorities would introduce delays and the Government is prioritising making progress quickly on the issue of data policy. Going forward in this impact assessment we assess the costs and benefits of the preferred option only compared to the baseline 'do nothing' scenario.

Policy objective

67. The proposed set of reforms that form part of the preferred package are designed to benefit the UK as a whole. These include policies targeted at resolving market failures for both the private and public sector as well as creating a framework for effective oversight of the UKs data protection regime These sets of reforms largely reflect and align with the NDS and the priorities set as part of it.

68. The first group of reforms focuses on the **removal of barriers to responsible innovation** when using data. There is untapped potential for linkage and re-use of datasets across organisations, domains and sectors in order to enhance the development and

[58] The Green Book, 2020, HMT (2020)

commercialisation of new products, services and solutions, and to deliver wider public benefits[59] the UK GDPR provides an important regulatory framework for access, use and re-use of personal data that protects the rights of individuals.

69. An effective data protection regime requires active interpretation and application to new and emerging technologies. The UK's data protection regime should be an adaptable and dynamic set of rules that are flexible enough to be interpreted quickly and clearly in order to fit the fast-changing world of data-driven technologies.

70. This set of reforms is designed to create a regulatory framework that encourages and reduces barriers to data use. With the support of the ICO, organisations have been learning how to apply the UK GDPR to their data processing activities and new data-driven technologies over the last three years. This is an important and ongoing process that is not without challenges: there is complexity both in regulatory concepts and rules, and the huge variety of data processing activities to which they should apply. Persistent uncertainty about how to operationalise our data protection regime risks creating barriers to data access, use and sharing that stifle innovation and competition.

71. The second group of reforms is centred around **reducing the burdens on businesses and delivering better outcomes for people.** These policies are designed to incentivise organisations to invest more effectively in the governance, policies, tools, people and skills that protect personal data, so individuals can have even greater confidence that their personal data is being used responsibly.

72. These reforms are designed to reduce burdens on organisations by, for example, equipping them with tools to more effectively respond to subject access requests and providing greater flexibility on compliance within the **accountability framework**. Proportionate and flexible compliance activities will help organisations unlock the value of their data assets rather than being seen as a regulatory burden. The privacy management programme approach would be based on a number of elements at the core of accountability, such as: leadership and oversight, risk assessment, policies and processes, transparency, training and awareness of staff, and monitoring, evaluation and improvement

73. These policies are designed to **boost trade and remove barriers to international data flows.** Consumers and businesses collect, share and process personal data internationally in order to use or trade digital products and services. According to the World Trade Organisation, trade in data-enabled services grew from $1.0 trillion in 2005 to $2.4 trillion in 2017.[60] Data flows have a larger impact in raising world GDP than the trade in goods.[61] In 2019 the UK exported £234 billion in data enabled services (74% of total UK services exports) and imported £124 billion in data-enabled services (57% of total UK services imports).[62]

74. The bill is designed to encourage a more collaborative approach to working with international partners and to remove unnecessary barriers to cross-border data flows, including by agreeing to commitments in bilateral and plurilateral trade agreements, by changing the UK's approach to data bridge regulations and looking at the use of alternative transfer mechanisms.

[59] Public Health Research Data Forum: 'Enabling Data Linkage to Maximise the Value of Public Health Research Data' (2015)
[60] World Trade Report 2019: The Future of Services Trade, Figure D.6: Global exports of ICT-enabled services
[61] McKinsey 2016, Digital Globalisation: The New Era of Global Flows
[62] DCMS, 'Understanding and measuring cross-border digital trade Final Research Report', 14th May 2020

75. The UK's experience of the COVID-19 pandemic has demonstrated the power of using personal data responsibly in the public interest, and of collaboration between the public and private sectors. The preferred package of policy options is designed to build on this experience in order to **deliver better public services** in more agile, innovative, effective and efficient ways.

76. **By creating a more efficient data sharing framework for the delivery of public services,** there are a number of barriers to effective data use in government that could be reduced. These barriers include; data infrastructure that is not interoperable; legal and cultural barriers to data sharing; inconsistent data capability in the workforce; and financial disincentives that discourage investment.

77. The proposed package of reforms will make changes to the laws applying to all data processing in the UK including those relating to law enforcement and national security. The overarching **Home Office policy objective** for the Data Protection and Digital Information Bill is to maintain high data protection standards, that preserve and improve confidence in public sector use of data; and to maintain the UK's international standing as a responsible user of personal data.

78. The legislative changes that are being implemented by the Home Office are specific to Law Enforcement and Intelligence Services, as any changes to these regimes would not be reflected under Part 2 (General Data Processing regime). For example, the Home Office aims to provide flexibility to support the use of new and innovative technology specific to Part 3 and Part 4 reforms surrounding Artificial Intelligence (AI). It also aims to support LEAs in making better use of Automated Decision Making (ADM). The Home Office will mirror DCMS proposals where it is appropriate to do so.

79. Additionally, the Home Office seeks to simplify the legislation by removing unnecessary complexities and minimising differences across all the data processing regimes: UK GDPR, Law Enforcement, and Intelligence Services. This includes reforms such *as Introducing the definition of Consent to Part 3* and *Mirroring the National Exemption from Part 2* which aims to create consistency across regimes. The Home Office will also seek to improve international data flows and shape new agreements for law enforcement data transfers, as well as delivering reforms to substantially simplify the oversight framework for police use of biometrics and overt surveillance, ensuring lines of accountability are clear for data controllers and the wider public.

80. These reforms will allow LEAs and National Security partners to carry out their duties more effectively and support operational outcomes, whilst maintaining high data protection standards. The commencement of these reforms will take place two months after Royal Assent.

81. The objective of 'removing the requirement for paper birth and death registers moving to an electronic register' is to introduce a change to the legislation which will remove the requirement for paper registers to be held in 173 Local Authorities. Local Authorities within England relate to county, district or parish councils, London borough councils, the Common Council of the City of London and the Council of the Isles of Scilly. In Wales Local Authorities relate to any county, county borough or community council in Wales. This removes the requirement for records of births, still-births and deaths to be held in two mediums (paper and online). There will be no requirement for registrars to store paper registers in the future reducing the risk of loss or theft

of those registers for those seeking to commit identity fraud, therefore resulting in public protection and counter fraud benefits. The move to an electronic register will provide savings to central and local governments and remove the duplication of processes.

82. **Reform of the Information Commissioner's Office** will empower the Information Commissioner to protect data rights and promote trust in the data protection system in order to unlock the power of data. The Information Commissioner's Office (ICO) is the independent supervisory authority with responsibility for monitoring and enforcing the application of data protection legislation in the UK. Reforms in this group are designed to support the ICO's existing transformation programme, which aims to increase its valuable, upstream support to help organisations comply with the law, and develop its consultative approach to guidance with a greater emphasis on how organisations may use and share data responsibly.

83. In order for these policy objectives to be realised the correct regulatory framework needs to be in place. This includes **technical policy reforms** that allow for changes to occur, for example including a new provision to make it clear that other primary legislation is to be treated as being subject to the data protection legislation unless express provision is made to the contrary, will help to strengthen the trust in the new regulatory framework.

84. Current identity proofing methods can be expensive, inefficient, and vulnerable to fraud. **Digital identities** can strengthen and simplify the process, however, the current landscape lacks standards which will enable interoperability and does not yet command trust. The objective of this policy is to allow people to prove things about themselves as quickly and securely as possible. As a result of enabling this, the following objectives could be met:

    a. **Economic gains associated with a functioning digital identity system, enabling the full realisation of the digital economy.** The current lack of widespread digital identity use in the UK is preventing end-to-end digital transformation at scale. Britain's tech industry currently adds nearly £184bn a year[63] to our economy, with 74% of people in the UK saying they cannot live without the internet.[64] Individuals in the UK expect to be able to carry out their transactions online and, as services increasingly move online to meet demand, an individual's ability to provide their identity digitally has become essential.

    b. **Protection against fraud, for both businesses and people.** Identity fraud is at a high level within the UK with just over 180,000 cases reported in 2020.[65] Digital identity can play a crucial role in reducing crime and fraud, both online and offline. The wide scale adoption of secure digital identity solutions has the potential to reduce the opportunity to steal and use stolen documents.

    c. **The enhancement of privacy and enablement of data minimisation.** Use of physical identity documents often involves the oversharing of personal data which can then be misused. The wide scale adoption of secure digital identity solutions has the potential to reduce the opportunity to steal and use stolen documents. Digital alternatives will also be able to minimise data to safeguard privacy,[66] reducing the risk of data misuse.

[63] TechUK, (2019)
[64] Onwards, The People's Study. (File available from GDS)
[65] CIFAS Fraudscape (2021)
[66] The Information Commissioner's position paper on the UK Government's proposal for a trusted digital identity system https://ico.org.uk/media/about-the-ico/documents/2619686/ico-digital-identity-position-paper-20210422.pdf

d. **The promotion of inclusive solutions and removal of barriers to inclusion.** According to the last census in 2011, 17% of people in England and Wales do not have a passport[67] (a key document for identity proofing). DWP research has also found around only 34% of prison leavers have a primary form of ID,[68] making it difficult for them to access benefits or open a bank account. Digital identity presents a unique opportunity to allow people without common identity documents to use a digital alternative. A secure way to share basic identity information digitally could give excluded groups access to the services most people take for granted.

85. More information on how the proposed policy will overcome market failures in the digital identity market can be found in the Digital identity and attributes - De Minimis Assessment.[69]

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

87. The overarching policy objective for changing data use in the health and social care sector is to ensure systems are interoperable to facilitate the appropriate access to information needed by health and care staff, to aid the quality of care they provide and improve outcomes for people accessing the health and care system. The secondary objectives are to facilitate population wide research and analysis, operational planning and promote innovation within the health and care IT supplier market. The intended effects are improved clinical outcomes for patients, improved clinical/care decision making enabled by access to accurate and complete information, better procurement and commissioning by health and care providers, and a more dynamic and responsive health and care IT market.

[67] https://webarchive.nationalarchives.gov.uk/20160107124139/http://www.ons.gov.uk/ons/dcp171776_310441.pdf
[68] Presentation by Ministry of Justice at a Cross-Government Data Sharing Group, 5th March 2020
[69] Digital identity and attributes - De Minimis Assessment, 2021 DCMS
[70] Smart Data Impact Assessment 2022 - BEIS

Summary and preferred option with description of implementation plan

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

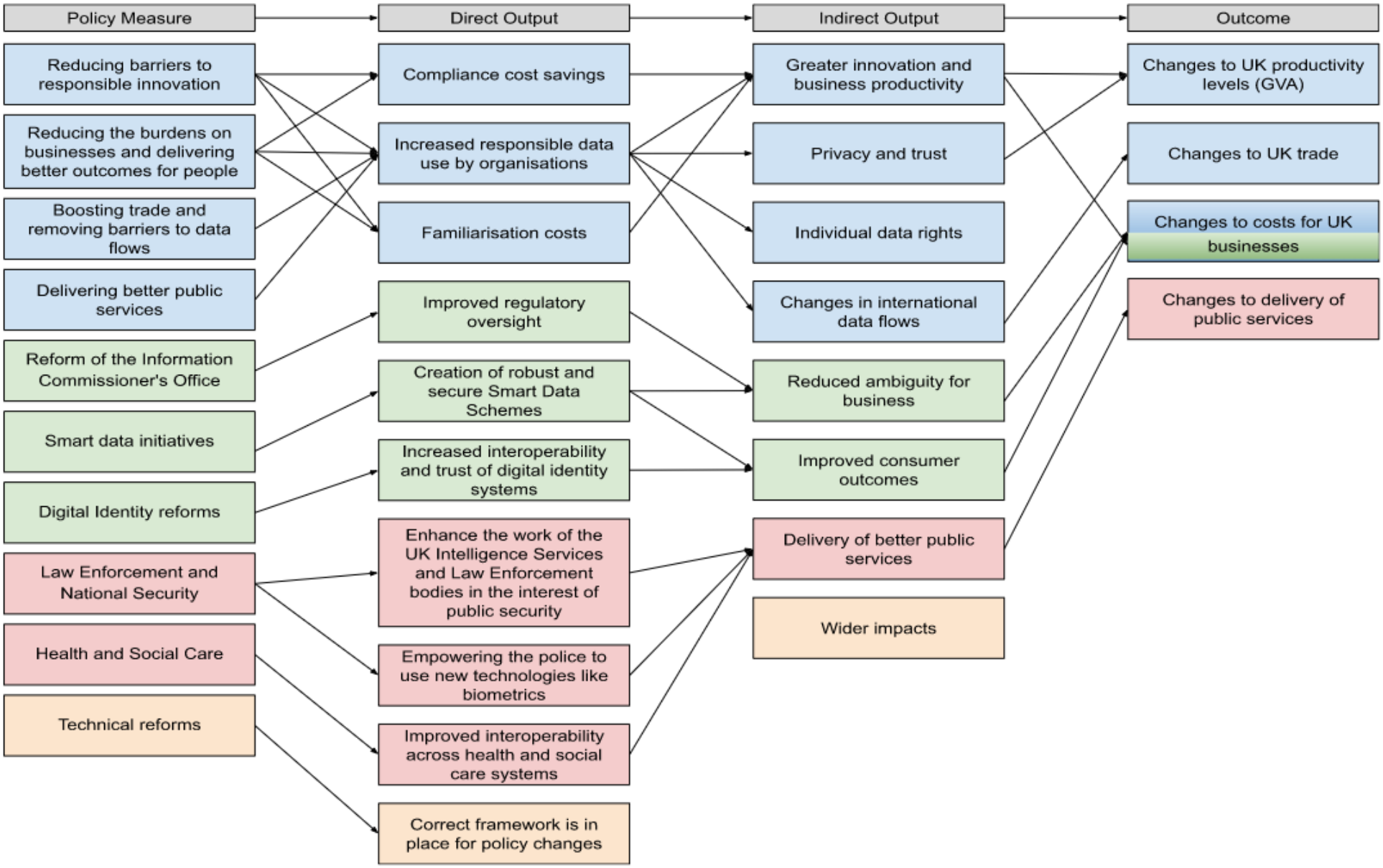
89. The figure below sets out the theory of change for the group of reforms. Where we have sufficient evidence and we have been able to make reasonable assumptions, we have quantified the net impact in terms of changes relative to the baseline. We assume the baseline is where the status quo remains in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

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

91. More detailed theory of change for the Smart Data initiatives[71] and Digital Identity[72] reforms can be found in their respective impact assessment. We have simplified both here to provide an overview of the impacts and outcomes.

[71] Smart Data Impact Assessment 2022 - BEIS
[72] Digital identity and attributes - De Minimis Assessment, 2021 DCMS

Figure 2: Theory of change for preferred option



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

Table 11: List of all reforms that are being followed up with secondary legislation

Reform Heading	Reform subheading	Will secondary legislation include direct costs and benefits to UK businesses?	Who will be responsible for the secondary legislation IAs?
AI and Machine Learning	Future proofing Article 22 Enhancing the approach to explainability and accountability for fair processing in the context of AI	Yes	DCMS
Privacy and electronic communications and the use of personal data for the purposes of democratic engagement	Requiring websites to respect preferences set by individuals through their browser. The Bill would set out the main principle, but we may need regulations to set out further detail about how the provision would work (e.g. including what technologies are in scope).	Yes	DCMS
Delivering better public services	To extend powers under section 35 of the Digital Economy Act 2017 aimed at improving public service delivery to business undertakings, beyond the current scope of solely individuals and households (CDDO)	No	CDDO
Digital Identity	Digital Identity: Create a governance framework and enable checks against government-held data[73]	No	DCMS
Smart Data	Smart Data: Introduction of primary legislation, creating new “regulation-making” powers to enable Smart Data schemes to be introduced in any given sector[74]	Yes	This will be sector specific
Health and Social Care	Create primary legislation for a new power for the Secretary of State for Health and Social Care to direct suppliers to adopt an open data architecture approach[75]	Yes	DHSC
National Security and Law	Introduce delegated power to pass	No	Home Office

[73] This is the preferred option in the Digital identity and attributes - De Minimis Assessment 2021 published by DCMS
[74] This is the preferred option in the Smart Data initiatives Impact Assessment 2022 published by BEIS
[75] An overview of how this policy will be implemented can be found in the Annex.

Enforcement	secondary legislation enabling the technical implementation of new international alert sharing agreements		

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

Impact analysis

Changes following consultation

94. We have made significant progress with the economic analysis of our reform package since the consultation stage. This has been helped by evidence gathered through the consultation process, and the additional time provided to fill evidence gaps. The main changes are in the following areas:

95. **Trade modelling:** In the pre-consultation analysis note a proposed methodology was outlined for measuring the impact on trade of the package of reforms. DCMS has invested in expanding its trade modelling capabilities and developed an in-house gravity trade modelling approach[76] with the help of other government departments. A gravity modelling annex can be found in annex 6.

96. **EU Adequacy assessment:** Revising the modelling of the costs and benefits of retaining Adequacy. Similarly, to the trade modelling section, a consistent and varied methodological approach is employed to produce robust results. Key assumptions are adapted and tested of our SCC-based approach to produce realistic estimates of SCC costs faced by UK businesses if Adequacy is not renewed.

97. **Familiarisation costs:** When faced with the proposed policy changes firms will encounter up front familiarisation costs. This methodology has been updated by revising the key parameters used within the modelling. The modelling continues to use a time-cost approach but the number of pages of relevant guidance by sector and firm size has been revised, based on further research and conversations with policy leads. The cost of the training firms faces already and how these costs might alter going forward has also been investigated.

98. **Compliance costs:** A number of these reforms will impact the total costs businesses face by complying with UK data policy. We have updated our previous methodology to ensure we avoid any double counting of legal fees that firms may face. Previously we considered the ‘Establishing a legal basis for data processing’ compliance activity both separately but also as part of ‘Legal fees’ when looking at a firm's compliance costs. We have now separated these two activities to avoid double counting. We are also stress testing key model assumptions, including the number of firms impacted by the reforms and the cost of individual compliance activities using UKBDS data and consultation responses.

[76] The gravity model of international trade states that the volume of trade between two countries is proportional to their economic mass and a measure of their relative trade frictions. The gravity model has been commonly used in international trade analysis for several decades due to its intuitive appeal.

99. Analysis of proposals led by **Other Government Departments**: Many of the policy proposals in the preferred package are designed by other government departments and include policies that alter data use for Law Enforcement and National Security organisations, health and social care firms and other public sector departments. DCMS has worked alongside these departments to provide an in-depth assessment of the costs and benefits of these policies.

100. **Impact by business size (Small and Micro Businesses):** The analysis focuses on how the costs and benefits change across businesses of different sizes and within different sectors. There is a particular focus on small and micro firms and any potential impact the proposed reforms might have on them, based on an extensive literature review and drawing insights from the UKBDS.

101. **Benefits to UK productivity:** The analysis of quantifiable benefits has been expanded by looking closer at the relationship between UK business productivity levels and data use, by further reviewing the literature and by carrying out sensitivity analysis to test our modelling assumptions.

102. Using the UK Business Data Survey[77], the total number of firms that analyse data to gain insight and knowledge is ascertained, and the proportion of these that find current guidelines hard to follow and have therefore been stopped from implementing a change or a new product into business practices. The likely increase in data use stemming from the change in legislation is then calculated using informed assumptions from the literature, and ultimately what this means for a firm's productivity level. In order to ensure the estimates are as accurate as possible these assumptions have been tested to assess their impact. Furthermore, using this data, a breakdown of benefits by sector and size of business has been provided.

103. On **qualitative benefits**, more evidence from the literature has been collected to inform our evidence base. This includes assessing whether any of the policies have a material impact on consumer trust and privacy. The potential benefits to consumer switching that may come from the proposed reforms, and any sector specific impacts on data-intensive sectors such as financial and business services.

Changes following publication in June 2022

104. Additional Reforms have been added to the bill since its initial submission in 2022, following further discussions with stakeholders and industry. The list of policy reforms that have since been added to the bill are as follows:

a. Extending the exemptions from the regime when conducting scientific research to include when that research is carried out in a commercial setting.

b. Reducing and simplifying record-keeping requirements, for organisations that control or process low risk data.

c. Clarifying activities that fall under legitimate interests, by listing activities such as direct marketing or ensuring network and information security.

d. In an international transfers regime context, ensuring businesses are able to continue to seamlessly use their pre-Bill existing transfer mechanisms - those which meet the

[77] DCMS: UK Business Data Survey, 2021

required level of protection under the current transfer framework - without a requirement for further checks and avoiding additional costs.

e. Clarifying the circumstances in which safeguards apply to significant decisions that are taken about individuals on the basis of profiling.

105. These additional reforms have been added to the package of reforms as a whole and their impact has been assessed qualitatively and quantitatively where possible.

106. We estimate there will be a net positive impact on the total NPV for the bill with the addition of these policies. However we stress that there are substantial non-monetisable costs and risks that also must be considered and that are set out in the following sections.

107. We estimate that the additional reforms could add an extra £0.1 to £0.8 billion to the NPV with the central estimate of the impact being £0.4 billion (2019 prices, 2020 base year). Since publication we have also worked to redefine some of our compliance cost modelling assumptions using the UKBDS 2021. As a result this has also altered the estimated NPV as outlined in the table below.

108. The NPV previously published for the bill in June 2022 was estimated to be between £1.3 billion and £8.5 billion, with a best estimate of approximately £4.7 billion, over 10 years following implementation. These estimates were reflected in 2019 prices, with a 2020 base year, and costs and benefits starting in 2022. In this latest assessment we changed the year that costs and benefits begin to 2024, which discounts the NPV to £4.3 billion. This we have done to better reflect when we expect the changes to take effect (post royal assent).

109. Accounting for these additional reforms and updates to our modelling assumptions, we estimate the new NPV of the bill to fall between £1.2 billion and £9.1 billion with a central estimate of £4.7 billion, in 2019 prices, with a 2020 base year, and a cost and benefits starting year of 2024.

Table 12: Step changes to the Net Present Value of the bill since publication

NPV, over 10 years in 2019 prices, with a 2020 base year and costs and benefits starting in 2024 (£bn)[78]			
	Low Scenario	Medium Scenario	High Scenario
DP&DI Bill as of June 2022 with benefits and costs starting in 2024	**1.2**	**4.3**	**7.9**
Updates to existing analysis[79]	-0.1	0.0	0.4
Additional reforms (a-e)	**0.1**	**0.4**	**0.8**
1. Scientific Research	0.04	0.08	0.13
2. Record Keeping	0.08	0.27	0.54
3. Legitimate Interests	0.01	0.03	0.09

[78] Rounding to 1 decimal place may mean that totals in table do not sum absolutely
[79] These changes are to compliance cost modelling assumptions outlined in the relevant section of the IA.

4. ITR reform	No quant estimates		
5. ADM and Profiling	0.00	0.01	0.00
Total	**1.2**	**4.7**	**9.1**

110. The ICO have confirmed that the additional six policies are likely to only have a minimal impact on their resources and costs. The ICO expects the total impact to stay within the original bands presented in the original impact assessment. This includes annual cost savings of between £1.1 and £1.8 million, upfront costs of between £0.8 and £3.0 million over the first two years, and between £0.9 and £2.0 million in the third and fourth years. Annual costs are also estimated to be between £0.8 and £2.8 beginning from year three. These figures will be updated between now and the Impact Assessment at Royal Assent to reflect all relevant changes and additional amendments that impact the ICO.

111. The Home Office have confirmed the following three policies to be in scope of having impacts on Law Enforcement and National Security Impacts. We do not expect any other government department to face direct impacts as a result of these additional reforms.

a. Record Keeping Requirements: The Home Office does not envisage this amendment having any additional impact on law enforcement organisations. Data stored and processed by law enforcement agencies is routinely assessed as high-risk. Only in very limited circumstances will law enforcement processing fall below the high-risk threshold under the UK GDPR framework and subsequent opportunities for those bodies to benefit from these changes in the UK GDPR will be further limited. This amendment will not result in any changes to law enforcement compliance or implementation processes.

b. ITR transfer tools:

i. DCMS would like to amend the ATM4 transitional provisions in Part 2 of Schedule 7 of the Data Protection and Digital Information Bill (the DPDI Bill) to include additional transitional provisions regarding pre-commencement appropriate safeguards under Article 46 of the UK GDPR. The Home Office is also seeking an equivalent transitional provision regarding pre-commencement appropriate safeguards agreements (legally binding instruments) made under section 75(1)(a) of the Data Protection Act 2018 (the DPA).

ii. Consistent with the instructions above, the Home Office wants Schedule 7 of the Bill to be amended to provide a transitional provision to ensure any current section 75(1)(a) of the DPA (legally binding agreements) can continue to be relied upon following commencement of the Bill. Such transfers should be taken as satisfying the requirements of section 75 as amended, including the DP test in new section 75(5).

iii. The Home Office does not expect there to be significant familiarisation costs associated with this amendment. The HO does expect there to be some small costs that are avoided as a result of the amendment. This is because, in the absence of the amendment, controllers would be required to re-assess existing section 75(1)(a) agreements under the new test which will be introduced by the

DPDI Bill. Therefore, the amendment will avoid imposing additional costs on law enforcement which would be associated with the time required for re-assessing each of the agreements. These avoided costs are expected to be small and have not been quantified.

c. Automated Decision Making:

i. This amendment also introduces a third power to Section 50D as part of reforms to Part 3 of the Data Protection Act 2018, enabling the Secretary of State to specify that certain decisions are, or are not, to be taken as having had meaningful human intervention. Given that this amendment will simply require law enforcement agencies to give additional thought to the degree of meaningful human involvement there has been in taking a decision, and the role that profiling has played in reaching it, the Home Office would anticipate minimal changes to the existing economic impact are required. This might include costs arising from familiarisation, guidance and training as well as potential minor updates to existing processes. Although it is not possible to quantify any such costs, we expect them to be minimal.

ii. No economic impact is anticipated as a result of the introduction of the power for the Secretary of State to specify that certain decisions are, or are not, to be taken as having had meaningful human intervention until such a power is exercised. We expect the use of this power to be rare; however, if the SoS does exercise it, it could result in costs as outlined above. As above, although it is not possible to quantify any such costs, we expect them to be minimal.

Assumptions and methodology

112. The preferred package of reforms has been analysed and estimations of the potential costs and benefits can be found below. These are assessed over a period of 10 years from 2024 to 2033, and are discounted using the Green Books suggested discount rate of 3.5%.[80]

113. Where analysis has already been published with respect to some of the policies included in the bill, this is referenced accordingly. This is the case for the Digital Identity measures[81] and the Smart Data policies.[82] In both cases all costs and benefits have been appraised over 10 years and the same base year has been applied. Where other government departments have fed into this analysis, this is also the case.

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

[80] HMT: The Green Book, 2020
[81] DCMS: Digital identity and attributes - De Minimis Assessment (DI DMA), 2021
[82] BEIS: Smart Data Impact Assessment, 2022

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

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

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

118. We expect the package of reforms to have a net positive impact overall, however we provide an overview of the direct and indirect costs that could be faced by UK businesses as a result of these policies. These costs are likely to consist mainly of familiarisation costs faced by businesses and public sector organisations having to update any processes and systems to be in line with the new guidance.

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

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

121. As there is a wide array of reforms in the package the cost benefit analysis is split out in table 12 and the reforms are classified as being either monetisable or not, having direct or indirect impacts, whether or not they will be followed by secondary legislation or not, and who is likely to be impacted.

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

Table 13: Breakdown of all costs and benefits by category

	Reform	Monetised?	Direct?	Followed by secondary legislation?	Who is impacted?
Benefits					
Compliance cost savings	Removing barriers to responsible innovation	Monetised	Direct	No	UK Businesses
	Reducing burdens on businesses and delivering better outcomes for people				
Improved Regulatory Oversight	Relaxed requirement to review data bridge decisions	Monetised	Direct	No	Government (ICO)
	Enforcement Powers				
	Complaints				
Empowering the police to use new technologies like biometrics (HO): Efficiency Benefits	Oversight Reform	Non-Monetised	Direct	No	Government and LEAs
Impact on UK Business Productivity and innovation	Removing barriers to responsible innovation	Monetised	Indirect	No	UK Businesses
Creation of Robust and Secure Smart Data Schemes (BEIS): Increase in use of Smart Data schemes indirect benefits	Introduction of primary legislation, creating new “regulation-making” powers to enable Smart Data schemes to be introduced in any given sector	Non-Monetised	Indirect	Yes - to be followed up with sector specific legislation	Consumers, businesses, data holders and data recipients
Increased Interoperability and Trust of Digital Identity Systems	Create a governance framework and enable checks against government-held data	Monetised for four examples use cases	Indirect	Yes - to be followed up with sector specific legislation	UK businesses and consumers
Privacy, trust and individual data rights	Removing barriers to responsible innovation	Non-Monetised	Indirect	No	UK consumers

	Reducing burdens on businesses and delivering better outcomes for people	Non-Monetised	Indirect	No	UK consumers
Delivery of better public services	Clarifying that private organisations & individuals asked to carry out an activity on behalf of a public body may rely on that body's lawful ground for processing the personal data under Art 6(1)	Non-Monetised	Indirect	No	UK businesses and public sector organisations
	To extend powers under section 35 of the Digital Economy Act 2017 aimed at improving public service delivery to business undertakings, beyond the current scope of solely individuals and households (CDDO)	Non-Monetised	Indirect	Yes	UK businesses and Government
Improved Customer Outcomes	All reforms	Non-Monetised	Indirect	No	Consumers
Improved Interoperability across Health and Social Care Systems	Create primary legislation for a new power for the Secretary of State for Health and Social Care to direct suppliers/suppliers to adopt an open data architecture approach through the use of ISNs. [83]	Non-Monetised	Indirect	Yes	Healthcare providers, patients and third-party providers
Enhance the work of the UK intelligence services and law enforcement bodies in the interest of public security (HO): Benefits	Removing the need to log the 'justification' for consulting / disclosing data disclosure	Monetised	Direct	No	Government (LEAs) and private sector LEAs
	Introduce a 'legal professional privilege' exemption	Non-Monetised	Direct	No	Government (LEAs and UK Intelligence Services)
	Public Safety and National Security (Home Office): Subject Access Requests	Non-Monetised	Indirect	No	
	Mirror the national security exemption from Part 2 (DPA 2018 part 3)	Non-Monetised	Indirect	No	
	Amendments to Part 4 of the DPA 2019 - National Security Notices	Non-Monetised	Direct	No	
	Introduce a definition of 'consent' to Part 3 (DPA 2018 part 3)	Non-Monetised	Indirect	No	
	Clarifying use of Section 76 DPA to cover larger scale transfers. (International	Non-Moneti	Indirect	No	

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

	Transfers)	sed			
	Reform subsequent transfer's provision (Section 78 DPA)	Non-Monetised	Indirect	No	
	Introduce delegated power to pass secondary legislation enabling the technical implementation of new international alert sharing agreements	Monetised but not included in total NPV	Direct	Yes	
	Remove the requirement for paper birth and death registers moving to an electronic register	Monetised	Indirect	No	
		Non-Monetised	Indirect	No	
Costs					
Familiarisation costs	Removing barriers to responsible innovation	Monetised	Direct	No	UK businesses
	Reducing burdens on businesses and delivering better outcomes for people				UK businesses
	Enhancing the work of the UK intelligence services and law enforcement bodies in the interest of public security (HO)				Government (LEAs and UK Intelligence Services)
Improved Regulatory Oversight	Accountability/DPIAs	Monetised	Direct	No	ICO
	SARs				
	New ICO Duty to consult				
	Mandatory IAs for statutory codes and guidance				
	Setting up expert panels for statutory codes and guidance				
	Governance changes				
Enhance the work of the UK intelligence services and law enforcement bodies in the interest of public	Introduce the ability to actively review automated decisions	Monetised but not included in calcs	Direct	No	Government (LEAs) and UK businesses

security (HO): Costs	Introduce delegated power to pass secondary legislation enabling the technical implementation of new international alert sharing agreements	Monetised but not included in total NPV	Direct	Yes	
	Subject Access Requests (SAR)	Non-monetised	Direct	No	Government (ICO, LEAs and UK Intelligence Services)
	Introduce a power to allow bodies representing Part 3 controllers and processors to produce 'Codes of Conduct'				
	Amendments to Part 4 of the DPA 2018 - National Security Notices				
	Remove the requirement for paper birth and death registers moving to an electronic register	Monetised	Indirect	No	
Creation of Robust and Secure Smart Data Schemes (BEIS): Increase in use of Smart Data schemes indirect costs	Introduction of primary legislation, creating new "regulation-making" powers to enable Smart Data schemes to be introduced in any given sector	Non-Monetised	Indirect	Yes - to be followed up with sector specific legislation	UK businesses and consumers
Increased Interoperability and Trust of Digital Identity Systems	Create a governance framework and enable checks against government-held data	Monetised for 4 examples use cases	Indirect	Yes - to be followed up with sector specific legislation	UK businesses and consumers
		Non-Monetised			
Delivery of better public services	To extend powers under section 35 of the Digital Economy Act 2017 aimed at improving public service delivery to business undertakings, beyond the current scope of solely individuals and households (CDDO)	Non-Monetised	Indirect	Yes	UK businesses and Government
Empowering the police to use new technologies like biometrics (HO): Costs	Oversight Reform	Non-Monetised	Indirect	No	Government (ICO, Investigatory Powers Commissioner Office (IPCO))

Improved Interoperability across Health and Social Care Systems	Create primary legislation for a new power for the Secretary of State for Health and Social Care to direct suppliers/suppliers to adopt an open data architecture approach through the use of ISNs. [84]	Non-Monetised	Indirect	Yes	Healthcare providers, patients and third-party providers
			Direct	Yes	Healthcare providers, patients and third-party providers

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

Benefits

Summary

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

1. Direct Benefits
    a. Monetised
        i. Compliance cost savings
        ii. Improved regulatory oversight
        iii. Enhancement of the work of the UK intelligence services and law enforcement bodies in the interest of public security
    b. Non-monetised
        i. Enhancement of the work of the UK intelligence services and law enforcement bodies in the interest of public security
        ii. Empowerment of the police to use new technologies like biometrics
2. Indirect Benefits
    a. Monetised
        i. Impact on UK business productivity and innovation
        ii. Increased interoperability and trust of digital identity systems
        iii. Remove the requirement for paper birth and death registers moving to an electronic register
    b. Non-monetised
        i. Creation of robust and secure Smart Data schemes
        ii. Privacy, trust and individual data rights
        iii. Delivery of better public services
        iv. Improved customer outcomes
        v. Improved interoperability across health and social care systems
        vi. Enhancement of the work of the UK Intelligence Services and Law Enforcement Bodies in the Interest of Public Security
        vii. Remove the requirement for paper birth and death registers moving to an electronic register
        viii. Increase in data use for research purposes

123. Benefits arise from a variety of impacts including an estimated increase in responsible data use and a reduction in compliance costs. We estimate the whole package of reforms will generate benefits of between **£3.3 billion and £9.8 billion over ten years, discounted and in 2019 prices**. These benefits arise mostly from the measures relating to reducing barriers to responsible innovation, and reducing burdens on business and delivering better outcomes for people. The rest of this section sets out our approach and evidence used to quantify these benefits.

Direct benefits - Monetised

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

Compliance cost savings

125. Several of the measures included in the bill will change compliance requirements for organisations, typically lowering the current compliance burden while continuing to require businesses to be accountable for delivering key outcomes for data protection.[85] Compared to the current data protection regime, the proposed measures will reduce administrative costs owing to fewer staff or less time spent on unnecessary compliance activities.

126. We have identified the reforms within the package that are likely to impact UK business compliance costs and updated these to reflect any post-consultation stage policy changes. Using data from the UK Business Data Survey, 2021,[86] we have estimated the total number of firms likely to be impacted following implementation.

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

128. The full list of legal activities, estimated costs and sources can be found in the table below. We have updated our modelling to use a more up to date exchange rate,[87] other than this, these remain unchanged from the consultation stage where they were not challenged and remain our best estimates. Since the consultation stage we have updated the definition of legal costs to avoid any double counting in our analysis. These are derived from the best available evidence, there remains a large degree of uncertainty. For example, we assume that the baseline cost of some compliance activities varies depending on the size of the organisation (e.g. establishing a lawful ground for data processing) whereas others do not (e.g. cost of seeking legal advice).

Table 14: A list of all compliance activities and their estimated cost

Activity	Description	Annual cost per activity per business (£)
Seeking legal advice	Businesses often require external legal advice in order to maintain their compliance with regulation. This includes advice on how and whether data can be used. (Excludes the cost of establishing a legal basis for data processing)	£935/year cost of legal advice (equivalent to 4 hours of a legal professional and 2 hours of a clerical worker)[88]

[85] Data: a new direction: Analysis of expected impact, 2021, DCMS
[86] DCMS: UK Business Data Survey, 2021
[87] We assume that 1 EUR = £0.85 which is the 2021 Q4 Bank of England average
[88] Proposal for an EU Data Protection Regulation, Ministry of Justice, (2012)

Acquiring consent for data processing	Businesses must acquire consent to process personal data as consumers have the right to prevent processing of their data. They often fulfil this requirement by having 'opt-in' and 'opt-out' functionality on their website	£63.75 cost per business per year to run opt-in/opt-out[89]
Responding to SARs	Consumers have the right to access their personal data which is met through a Subject Access Request (SAR). When these are raised, businesses have to collate information on what data they hold on the individual, how it is used, who it is being shared with and where they obtained the data from. Compiling a response to each SAR takes time for the business to complete	Around 9 SARs on average per year at a cost of £75/SAR[90] for SMEs and £375/SAR for large businesses[91]
Notifying data breaches to ICO	If an organisation is involved in a data breach of a certain severity, they must report the details of this to the ICO no longer than 72 hours after becoming aware of it.	£1,500[92]
Providing privacy notices	Businesses that process personal data must provide a privacy notice. Privacy notices are public documents that explain how the business processes personal data and how it applies data protection principles	Assume cost per request similar to cost of SARs: £75/SAR[93] for SMEs and £375/SAR for large businesses[94]
Preparing Data Protection Impact Assessments (DPIAs)	DPIAs must be completed by businesses where data processing is likely to result in a high risk to individuals. They describe the nature and scope of processing, identify the risks to individuals of processing and ways to mitigate those risks. DCMS confirmed that under each of the measures a DPIA would still be required	£935/year cost of legal advice (equivalent to 4 hours of a legal professional and 2 hours of a clerical worker)[95]
Other internal compliance activities	Other internal compliance activities not listed above include, but are not limited to, notifying the authorities of processing of data which might represent specific risks to individuals, and responding to consumer questions about how the business is following data protection principles	Annual wages for DPO (medium and large enterprises): £50,000 for medium and large enterprises; annual labour costs for

[89] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data - Impact Assessment, European Commission (2016)

[90] Proposal for an EU Data Protection Regulation, Ministry of Justice, (2012)

[91] DSARs and the impact of Covid-19, Guardum, (2020)

[92] This is a mid-point estimate of the cost of notifying the ICO of a data breach, which the MOJ's 2012 Impact Assessment estimated to be between £1,000 - £2,000. This includes initial incident analysis and fact finding, drafting the letter to the ICO, and analysis and response to replies and questions from the supervisory authority

[93] Proposal for an EU Data Protection Regulation, Ministry of Justice, (2012)

[94] DSARs and the impact of Covid-19, Guardum, (2020)

[95] Proposal for an EU Data Protection Regulation, Ministry of Justice, (2012)

		DPO-type functions: £900 for small and micro enterprises[96]

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

Table 15: Estimated compliance cost savings by reform, 2021 prices

Average Annual Compliance Costs (£m)			
Reform	Low Scenario	Medium scenario	High scenario
Legitimate Interests	0.6	4.5	14.8
AI and Machine Learning	0.3	2.6	7.3
Research Purposes	1.4	8.7	25.8
Accountability Framework: Record Keeping	13.8	38.7	71.0
Privacy and electronic communications and the use of personal data for the purposes of democratic engagement	7.9	15.8	23.7
Subject Access Requests	9.3	59.1	153.0
Total	33.3	129.3	295.6

130. These results can be broken down by reform and compliance activity. For example, the table below sets out the estimated annual compliance cost saving from creating a limited non-exhaustive list of legitimate interests for which businesses can use personal data without applying the balancing test. We also estimate the savings for businesses by clarifying that activities, such as direct marketing or ensuring network and information security, fall into the scope of the legitimate interests basis for processing personal data. We estimate these reforms to result in a total cost saving for businesses of between £0.6 and £14.8 million and the central estimate is presented in the table below.

[96] Data Protection Officer Salaries - Glassdoor (2021)

Table 16: Breakdown of compliance cost saving calculations as a result of creating a limited non-exhaustive list of legitimate interests, 2021 prices

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations actually affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
Effect on legal advice costs	1.3 million firms that use data to generate new insights or knowledge[97]	50%[98] of the total organisations that have sought legal advice because of UK GDPR/DPA2018[99]. On average 34% of these transfer data to the public sector and 41% use data to improve marketing or sales performance[100]	£70.4 million annual cost of legal advice for these organisations	6.3%: assuming that 25% of legal advice costs are related to issues clarified by this measure[101], and that for those issues the cost of legal advice will fall by 25% as a result of the measure[102]	4.4
Reduction in customer complaints about data use relating to non-permissible uses of data	Number of customer complaints: 2,976, according to ICO - data on number of complaints to		Cost of responding to legal complaints: £725[104]	6.3%: assuming that 25% of all data uses are affected and there is a 25% reduction in complaints as a result of the measure[105]	0.1

[97] DCMS: UK Business Data Survey, 2021
[98] 50% is an assumption that takes account of the fact that UKBDS question is: "have you sought legal advice as a result of GDPR…". But many of these cases may have been one-off (resulting from the need to check compliance when GDPR came into force. This 50% is tested in the risk and assumption sector of this IA
[99] DCMS: UK Business Data Survey, 2021
[100] ODI - YouGov 2020 - Data Sharing
[101] This is an assumption made in the model. As there is currently a lack of evidence available of the true number of issues this is something that is tested in the sensitivity analysis section and a proposal of how this will be measured going forward will be included in the Monitoring and Evaluation plan.
[102]In the model we assume that clarification can reduce costs in around 25% of cases where legal advice would have been sought. As this is an assumption we test this in the sensitivity analysis section and propose a way of monitoring this in the M&E plan.
[104] Average cost of each ICO investigation (2016/17)
[105]We assume that 25% of data uses will be affected by this measure and that the measure will impact 25% of these. We understand that this measure will not eliminate all of the complaints under the categories listed above. Businesses are less likely to do things that break the law and if the guidance is clearer but we assume this will be minimal based upon consultation responses. We test this assumption in the sensitivity analysis section.

	ICO on how data is being used/collected[1] [03]				
Total annual reduction in compliance costs					4.5

131. The table below shows the average annual decrease in compliance costs from all of the AI and machine learning reforms in the bill. We estimate these savings to be approximately between £0.3 and £7.3 million a year.

132. By including the additional reform that clarifies that profiling is only subject to the safeguards associated with solely automated decision-making when significant decisions are taken about an individual on its basis without meaningful human involvement, firms that use data for AI-driven ADM will have more clarity on the use of data for profiling activities within solely automated decision-making processes. This clarification will reassure firms that may currently be unsure about using data for this purpose and that spend money and time seeking legal advice on the matter. This increase in confidence could therefore lead to a decrease in costs of compliance and employing legal assistance. We make the assumption that there will be a 10% further reduction in the legal advice requested because of the additional measure. Evidence is limited to suggest the exact percentage however we have remained conservative in our estimates as we acknowledge this is not the only reason why these firms would seek legal advice. Because of this the assumption is tested using sensitivity analysis.

133. Assuming that approximately 375,000 firms use personal data with AI and 15% of these do not find current Article 22 UK GDPR and related ICO guidance clear[106] applying the assumption above we estimate that this additional reform could lead to an increase in compliance cost savings of £1.3 million a year.

Table 17: Breakdown of compliance cost saving calculations as a result of AI and Machine learning measures, 2021 prices

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations actually affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
Effect on legal advice costs	375,000 businesses that use personal data and use AI	15%: organisations that don't find UK GDPR and related ICO guidance clear and easy to	£56m annual costs of legal advice	5%: assuming that 20% of legal advice costs for affected organisations are related to processing personal data to improve accuracy of	2.5

[103] ICO Complaints and concerns data sets
[106] DCMS (2021) UK BDS. https://www.gov.uk/government/statistics/uk-business-data-survey-2021

		understand[107]		AI systems, and that 25% of legal costs in these cases could be saved as a result of the measure[108]	
Reduction in customer complaints about data use	Number of customer complaints: 2,976, according to ICO - data on number of complaints to ICO on how data is being used/collected[109]	8% of organisations associated with research purposes	Cost of responding to legal complaints: £725[110]	6.3%: assuming that 25% of all data uses are affected and there is a 25% reduction in complaints as a result of the measure[111]	0.0
Total annual reduction in compliance costs					2.5

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

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

136. Using the 2021 UK Business Data Survey (UKBDS), we estimate that the number of businesses that use data to generate new insights or knowledge, employ someone who leads on R&D and have sought legal advice because of UK GDPR or the DPA 2018 is approximately 110,000. Assuming a constant cost of legal advice of £935 for these firms we estimate that the total cost is approximately £350m a year.

137. Initially we assumed that policies designed to amend existing legislation to support responsible research activity using personal data, constitute 10% of the legal costs faced by

[107] DCMS: UK Business Data Survey, 2021 Businesses that responded "Strongly disagree" and "tend to disagree" to the question "My business finds the regulatory GDPR and DPA 2018 guidance published by the ICO clear and easy to understand?"
[108] We assume that AI is a smaller subset of use cases than with the legitimate interest measure hence only 10% is applied. We understand that even with clearer guidance, some legal advice will still be required. The amount of time spent seeking legal advice is an assumption due to the current lack of data. Because of this we test these assumptions in the sensitivity analysis section and make plans for their measurement going forward.
[109] ICO Complaints and concerns data sets
[110] Average cost of each ICO investigation (2016/17)
[111] We assume that 25% of data uses will be affected by this measure and that the measure will impact 25% of these. We understand that this measure will not eliminate all of the complaints under the categories listed above. Businesses are less likely to do things that break the law and if the guidance is clearer but we assume this will be minimal based upon consultation responses. We test this assumption in the sensitivity analysis section.

these firms. By adding this additional reform that further clarifies the businesses that can rely on 'research purposes' we assume that an extra 25% of legal costs will be impacted.

138. The total savings are estimated to be approximately between £1.4 and £25.8 million a year.

Table 18: Breakdown of compliance cost saving calculations as a result of research purposes measures, 2021 prices

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations actually affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
Effect on legal advice costs	110,000 organisations that use data to generate new insights or knowledge, have sought legal advice in the last year and that employ someone who leads on R&D[112]	50% of the organisations that have sought legal advice because of UK GDPR/DPA2018[113]	£349m annual cost of legal advice	9%: assuming that 35% of legal advice costs are related to issues clarified by this measure, and that for those issues the cost of legal advice will fall by 25% as a result of the measure[114]	8.7
Reduction in customer complaints about data use	Number of customer complaints: 2,976, according to ICO - data on number of complaints to ICO on how data is being used/collected[115]	3.7% of organisations associated with research purposes	Cost of responding to legal complaints: £725[116]	6.3%: assuming that 25% of all data uses are affected and there is a 25% reduction in complaints as a result of the measure[117]	0.0
Total annual reduction in compliance costs					8.7

139. Reducing and simplifying **record-keeping requirements**, for organisations that control or process low risk data. This reform is designed to reduce the burden on businesses keeping records of their data usage, storage and processing. This reform ensures this exemption will

[112] DCMS: UK Business Data Survey, 2021
[113] DCMS: UK Business Data Survey, 2021
[114] We assume that Research purposes are a smaller subset of use cases than with the legitimate interest measure hence only 10% is applied. We understand that even with clearer guidance, some legal advice will still be required. The amount of time spent seeking legal advice is an assumption due to the current lack of data. Because of this we test these assumptions in the sensitivity analysis section and make plans for their measurement going forward.
[115] ICO Complaints and concerns data sets
[116] Average cost of each ICO investigation (2016/17)
[117] We assume that 25% of data uses will be affected by this measure and that the measure will impact 25% of these. We understand that this measure will not eliminate all of the complaints under the categories listed above. Businesses are less likely to do things that break the law and if the guidance is clearer but we assume this will be minimal based upon consultation responses. We test this assumption in the sensitivity analysis section.

now be based on risk rather than business size or frequency of data processing. Organisations will not have to keep records unless the processing is likely to result in a high risk to the rights and freedoms of individuals. This aligns with the threshold for carrying out a data protection impact assessment, as currently defined by the ICO.

140. The reform also seeks to expand on current Article 35(4) and Article 35(5) such that it applies across to clause 14 senior responsible individuals and clause 15 duty to keep records. This will provide greater flexibility and clarity in guidance on what constitutes high risk processing and will help firms identify which of their data processing activities fall into which category.

141. We estimate that this simplification will reduce costs for businesses who currently need to clarify record keeping requirements and demonstrate that they are compliant with them. We also expect that reducing this burden might encourage some firms to increase their data utilisation and subsequently raise their productivity. However, the scale of these impacts are dependent on several factors, including the current and expected level of compliance.

142. For the purpose of estimating the impact of the reduced burden on businesses keeping records for low risk activities, we note that businesses typically incur costs for the following activities:

a. Maintaining documentation of all processing activities (article 30);

b. Maintaining documentation of data protection impact assessments that are carried out (Article 35); and

c. Obtaining prior authorisation from the supervisory authority for processing (article 36).

143. As a result of this reduction in burden, firms will spend less time and money on ensuring they are compliant with the current guidelines and paying for legal advice. We estimate that 2.3 million businesses in the UK process ‘less sensitive’ personal data. Using data from the 2021 UKBDS and internal assumptions, we estimate that 6.2% of these businesses seek legal advice annually to establish record keeping requirements, resulting in an aggregate £66m cost to businesses. We expect the clarifications to reduce the scope for seeking legal advice for low risk activities, assuming a 25% reduction and applying this to only half of all data usage taking place in these companies.These assumptions remain conservative as we do not expect all firms that currently seek legal advice to change their behaviour, and that some of their activities might still be “high risk” activities. We also test these assumptions using scenario analysis.

144. As well as removing the need for certain businesses to pay for legal advice, firms will also have to spend less demonstrating their compliance. Of the 2.3m businesses processing less sensitive data we assume all of these businesses face this demonstration cost. We estimate this cost to be approximately £50 per business, and we assume that 25% of this cost will be saved. Once again we remain conservative as we make the assumption that there will still be a cost for demonstration of compliance.

145. We estimate the total compliance saving to be between £13.8 million and £71.0 million a year, with a central estimate of £38.7 million a year in 2021 prices.

Table 19: Breakdown of compliance cost saving calculations as a result of record keeping policies, 2021 prices

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations actually affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
Effect on legal advice costs	2.3 million businesses that process less sensitive personal data	6.2% of these businesses have sought legal advice within a year	£66m annual cost of legal advice	12.5%, assuming 50% of data usage is affected by clarification under this measure (i.e. how much of low risk data will no longer be within scope of legislation) and a 25% reduction in legal advice required in these cases.	8.3
Effect on demonstration of compliance		All business demonstrate compliance	£53 per business	25% share of demonstrating compliance saved as a result of measure.	30.4
Total annual reduction in compliance costs					38.7

146. The table below shows how allowing organisations to use cookies for low-risk processing without consent could achieve between £7.9 and £23.7 million cost savings on average each year. There could be additional savings when the government commences provisions to move from an opt-in to an opt-out model in relation to the placement of cookies via websites.

Table 20: Breakdown of compliance cost saving calculations as a result of PECR measures, 2021 prices

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations actually affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
Obtaining opt-in consent	826,726 organisations that	All businesses	£49m	30% of businesses will no longer offer	15.8

	collect personal data through website analytics [118]			opt-in consent[119]	
Total annual reduction in compliance costs					15.8

147. The table below shows how limiting the time and threshold for responding to subject access requests could lead to cost savings for businesses of between £9.3and £153.0 million each year.

Table 21: Breakdown of compliance cost saving calculations as a result of SARs measures, 2021 prices

Compliance Activity	Number of organisations potentially impacted	Proportion of these organisations actually affected	Baseline Cost	Percentage change in compliance cost resulting from measure	Estimated effect (£m per year on average)
Decrease in SARs	600,000 organisations that receive SARs in a year. assumed to be ~75% of organisations that have received a SAR according to UKBDS. [120]	All businesses	£819m annual cost	6.25%: assuming that 25% of all SARs are sent are speculative in nature, and that 25% of these will take less time and resource to respond to as a result of the measure[121]	59.1
Total annual reduction in compliance costs					59.1

148. The estimated figures above rely on many modelling assumptions as a result of the level of evidence available being restrictive at this time. We go on to test these assumptions in our sensitivity analysis section later on in this report. By modelling a low and high scenario where we flex these assumptions we estimate that the total compliance cost saved will fall between £33.3 and £296.6 million.

[118] DCMS: UK Business Data Survey, 2021

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

[120] Assumed to be ~75% of organisations that have received a SAR according to DCMS: UK Business Data Survey, 2021

[121] This is an assumption used in the model due to a lack of available data. We have therefore tested this assumption in the sensitivity analysis section and have created a plan for its ongoing monitoring in the M&E section.

Improved Regulatory Oversight - ICO analysis

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

a. Strategy, Objectives and Duties

b. Governance Model and Leadership

c. Accountability and Transparency

d. Codes of Practice and Guidance

e. Complaints

f. Enforcement Powers

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

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

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

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

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

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

Table 22: Expected impact on ICO of changes to data bridge regulations decision making process, 2021 prices

Reform	Impact	FTE Estimate		Cost Saving Estimate (£m)	
		Low	High	Low	High
Relaxed requirement to review data bridge regulations	Small	1	5	0.0	0.2

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

Table 23: Expected impact on ICO of changes to Enforcement Powers, 2021 prices

Reform	Impact	FTE Estimate		Cost Saving Estimate (£m)	
		Low	High	Low	High
Enforcement Powers	Medium	6	15	0.3	0.7

157. Based on the proposals set out in the government response to the consultation and subject to transitional arrangements, the introduction of a criteria by which the ICO can decide not to investigate a given complaint, potentially has a large positive impact in the long term. This is entirely contingent upon the ICO retaining wide discretion to determine whether to investigate a complaint, even after a period of 45 days during which an individual can complain directly to a controller to try to resolve the matter, has elapsed. Realising this benefit will take some time given the work required in the short-medium term to support organisations to put in place effective complaints resolution processes. As an all-economy regulator the ICO receives a high volume of cases which they handle directly, which is not true of many other regulators. A significant number of complaints relate to organisations that receive a small number of SARs per year, and we would expect they would need substantial support with the new provision/requirement. However, the ICO notes that conversations in this area are ongoing and will keep this assessment under review.

Table 24: Expected impact on ICO of changes to the complaints process, 2021 prices

Reform	Impact	FTE Estimate		Cost Saving Estimate (£m)	
		Low	High	Low	High
Complaints	Large	16	20	0.7	0.9

158. Total cost savings are likely to start in year 2 after implementation, once processes have been established and are likely to be annual benefits of between £1.1 million and £1.8 million.

Table 25: Expected positive impact on ICO of all policy changes, 2021 prices

Reform	Impact	FTE Estimate		Cost Saving Estimate (£m)	
		Low	High	Low	High
Relaxed requirement to review data bridge regulations	Small	1	5	0.0	0.2
Enforcement Powers	Medium	6	15	0.3	0.7
Complaints	Large	16	20	0.7	0.9
Total cost savings	Total	23	40	1.1	1.8

Enhance the work of the UK intelligence services and law enforcement bodies in the interest of public security (HO)

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

Removing the need to log the 'justification' for consulting / disclosing data disclosure

160. Currently, law enforcement agencies (LEAs) are required to keep logs of several processing activities that they carry out. This proposal seeks to remove the requirement to record a 'justification' in the logs of consultation and disclosure. This is because it is technologically challenging for LEAs to automatically log a 'justification' as it requires human input to 'justify' the reason for accessing/disclosing data. As such, it holds limited value in maintaining accountability, especially in police misconduct investigations, as an individual misusing the database is unlikely to record an honest justification. We are only removing the 'justification' element; the other requirements to monitor compliance will remain in legislation.

161. The LEAs will no longer have to record a 'justification' when accessing automated systems. This will result in efficiency benefits.

162. To give a sense of scale, automated processing systems within policing are used at three levels: national, local and stand-alone or small systems. The number of these systems varies

greatly across competent authorities but is generally high. For example, the Metropolitan Police Service (MPS) has approximately 600 automated processing systems, while the comparably smaller forces of Hampshire Constabulary and Thames Valley Police have approximately 45.

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

164. They have also stated that these tools would be used by constables, sergeants and administrative staff. The wage for administrative staff was taken from the Annual Survey of Hours and Earnings (ASHE) 2021 Table 14.5a (SOC code 41) and uprated to include non-wage costs of 21.8 per cent. This increased the hourly wage from £12.30 to £14.98. Hourly wages for constables and sergeants were taken from the Home Office staff costs database at £30.38 and £50.04 respectively. These were adjusted to 2021 prices using the CPIH index and final values were obtained at £31.13 and £51.28. Wages for admin are taken as the low estimate, constables as the central estimate and sergeants as high.

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

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

Table 26: MPS logging justification ongoing benefits for four automated systems, 2022.

	No. system access per year (million)	Time spent logging justification (hrs)	Hourly wage (£)	Benefit per year (£ million)	Total benefit (£ million PV)
Low	22.42	0.01	14.98	3.7	32.1
Central	22.42	0.02	31.13	15.5	133.5
High	22.42	0.03	51.28	38.3	329.8

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

Notes: Totals may not sum due to rounding.

167. This means that for the four systems in the MPS, the estimated ongoing benefits of this proposal lie in the range of **£32.1 to £329.8 million** (PV), with a central estimate of **£133.5 million** (PV) over 10 years.

168. This can be upscaled to apply for all LEAs by multiplying the number of system accesses by low, central and high values of 2, 3 and 4 respectively. The high value is taken from the consultation with the MPS where they suggested that the MPS represents a quarter of all

police officers. There were 135,301 police officers in England and Wales in 2021,[122] compared to 33,326 in the MPS (as of 28 February 2022).[123] Dividing the total number of officers by the MPS numbers, gives a value of 4.06 which provides evidence for the MPS consultation response.

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

Table 27: All LEAs logging justification ongoing benefits, No. hrs, £, £ million (PV), 2021.

	No. system access per year (million)	Time spent logging justification (hrs)	Hourly wage (£)	Benefit per year (£ million)	Total benefit (£ million PV)
Low	44.83	0.01	14.98	7.5	64.2
Central	67.25	0.02	31.13	46.5	400.5
High	89.67	0.03	51.28	153.3	1,319.3

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

Notes: Totals may not sum due to rounding.

170. Estimated ongoing benefits for all LEAs lie in the range **£64.2 to £1,319.3 million** (PV), with a central estimate of **£400.5 million (PV) over 10 years.**

Non-compliance risks

171. There is currently an exemption available to controllers at Schedule 20(14) DPA 2018 which allows for automated processing systems set up before 6 May 2016 to not have to comply with Section 62 if compliance would involve disproportionate effort. This exemption ceases to have effect on 6 May 2023.

172. LEAs have highlighted that it is technically challenging to capture logging 'justifications' in existing automated systems. If they fail to meet this requirement after the end of the exemption on 6 May 2023, they may face compliance risks.

173. This proposal should reduce the non-compliance risks associated with 'justifications' in automated system

International-Law Enforcement Alerts Platform (I-LEAP) proposal

174. To introduce a delegated power to pass secondary legislation enabling the technical implementation of new international alert sharing agreements: The International-Law Enforcement Alerts Platform (I-LEAP) will deliver real-time alert exchange with key international partners and so strengthen joint capabilities to tackle shared threats, including migrant smuggling. Delegated powers will allow swift implementation, through secondary

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

legislation, of technical aspects of new agreements with international partners. This approach provides legal and operational certainty to UK operational partners and ensures that the required international agreements have a basis in UK legislation. This will enable the UK to implement new alert-sharing arrangements with close partners.

175. The ‘do nothing’ option for the I-LEAP proposal in this IA represents the lack of delegated powers to pass secondary legislation to enable new alert-sharing agreements.

176. Costs and benefits for this proposal will be taken from the I-LEAP full business case. This business case calculated costs and benefits relative to a ‘do nothing’ option which represents not implementing I-LEAP. This means that the ‘do-nothing’ option represented in this analysis is different to the ‘do-nothing’ option in the full business case. The analysis also assumes that I-LEAP would be implemented through bilateral agreements, however, the focus is now on completing an agreement with the European Commission.

177. These differences mean that the costs and benefits taken from the full business case should be seen as an indication of scale, rather than direct estimates of the impacts of the I-LEAP proposal in this analysis.

178. The costs and benefits outlined below **will not be** included in the total NPSV or costs and benefits summary.

179. The business case contained four shortlist options, not including ‘do nothing’, however, this section will focus on Option 3, which was recommended as the preferred way forward.

180. The business case breaks benefit down into four categories:

a. Reduction in the risk of societal harm through additional opportunities to identify international offenders.

b. Reduction in the risk of societal harm through additional opportunities to identify missing and vulnerable persons.

c. Improved efficiency and effectiveness in data sharing with international partners.

d. Improve public confidence and international reputation.

181. Total benefits are estimated to lie in the range £44.2 to £114.4 million (PV), with a central estimate of £79.3 million (PV) over 10 years (2021 prices)

Direct Benefits - Non-Monetised

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

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

Introduce a 'legal professional privilege' exemption

183. In the UK GDPR there is a 'Legal Professional Privilege' exemption that covers the right of access and the right to be informed, however this exemption does not apply to data processed under Part 3. This proposal seeks to replicate that exemption in Part 3 for consistency and clarity. Controllers and processors under Part 3 must currently rely on ad hoc restrictions contained within Sections 44 (Right to be informed) and Section 45 (Right of access) themselves, which need to be evaluated and justified depending on individual circumstances, even where 'Legal Professional Privilege' would normally apply. Stakeholders have indicated that they must conduct the balancing exercise that Section 44 (Rights to be informed) and Section 45 (Right of access) require, even though the restriction will almost certainly always be applied in that context. The main issues are a lack of clarity for the data subject that 'Legal Professional Privilege' will apply, and a greater workload on controllers without any benefit to the data subject. Therefore, the effect of this inclusion would be to make it clearer when data controllers should restrict the rights of a data subject where the information at question is legally privileged.

184. This proposal may result in efficiency benefits as controllers and processors under Part 3 will no longer have to spend time evaluating and justifying ad hoc restrictions based on individual circumstances and will instead be able to refer to the legal professional privilege exemption. There will be greater efficiencies when processing legal professional privilege exemptions.

Amendments to Part 4 of the DPA 2018 - National Security Notices

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

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

Empowering the police to use new technologies like biometrics (HO)

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

Oversight Reform

188. The current oversight arrangements for the police's use of biometrics and overt surveillance are crowded and confusing. The Biometrics Commissioner (BC) covers police use of DNA and fingerprints, the Surveillance Camera Commissioner (SCC) covers all use of surveillance cameras by local authorities and the police, while the ICO covers the processing of all personal data by the public and the private sector in the UK. In 2021, the Government appointed one person as BC and SCC to reflect the emerging combination of biometrics and surveillance camera technologies, but it is now seeking to simplify further by absorbing those functions into the ICO and/or other existing bodies (for example, IPCO, HMICFRS) in order to reduce duplication and improve consistency.

189. Planned changes will reduce the overhead costs associated with the Biometrics and Surveillance Camera Commissioners, including the related workload in resourcing the offices and appointing the Commissioners. In addition, there should be some efficiency benefits for LEAs through a reduction in engagement activity with multiple oversight bodies.

Indirect Benefits - Monetised

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

Impact on UK Business Productivity and innovation

191. There is evidence that the current UK GDPR raises high compliance burdens, relative to size and turnover of SMEs.[124] This is corroborated with evidence that the average SME in the EU could expect its annual costs to increase by £2,500 to £6,000, representing 16 and 40% of current annual SME IT budgets compared to 2013 under UK GDPR.[125] Research on start-ups in Germany found that while the UK GDPR can stimulate innovation, the cumulative impact of privacy regulation reduces start-ups' access to data making certain products and technologies harder to develop, especially in the field of big data and AI. Also, data protection regulation might lead firms to abandon products or product ideas that are judged, possibly incorrectly, to be incompatible with the regulation.[126] UK firms have also reported that the current regime can be complex to interpret and apply, especially for small and medium businesses.[127] Such complexity is understood to be a barrier to compliance and lead to uncertainty, and potential over- or under-compliance (through strategy or error).[128]

192. Many of the reforms within the bill are designed to encourage firms to better harness the power of the data already available to them and to encourage more firms to use data in decision making and for efficiency gains. Some proposed measures will specifically increase data processing for specific activities, such as those in relation to R&D. In our initial analysis note we conducted a literature review that found data is a factor of production and driver of firm-level productivity, with more (or higher quality) data driving higher output through lower costs, better coordination and improved products.

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

194. There are many mechanisms by which the acquisition of data can improve and increase outputs. In essence, data-intensive analytics can be used to discover new insights which enhance decision-making and optimise processes or coordination. This includes quality improvements in existing products and services, cost reduction in delivering products and

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

services, (e.g. analytics can reduce the costs of delivery, better credit scoring can reduce the cost of delivering, lower wastage and dynamic efficiency from improved data on performance), and greater innovation in development of new products and services.[129]

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

196. Using the UKBDS findings, we are able to estimate the total number of businesses that could be impacted, however, in reality we expect that only a proportion of these businesses are likely to change their activities. We have used evidence from the UKBDS and ONS to help inform the estimates of the true proportion of firms impacted and where evidence is less readily available we have gone on to conduct sensitivity analysis which can be found in the risks and assumptions section of this IA.

Table 28: Estimated number of businesses expected to increase their data use as a result of these reforms to the nearest hundred

Reform	Upper bound number of organisations potentially affected[130]	Proportion of these organisations actually affected (assumed medium scenario)[131]	Total estimated number of businesses affected
Creating non-exhaustive list of ways businesses can use data	31,000 organisations that analyse data, don't find GDPR clear, and have been prevented from implementing a new or improved product as a result, 39% of which use data to improve marketing or sales performance[132]	25%	3,000
Simplifying rules for data processing for R&D	22,000 organisations that analyse data, adopt R&D, don't find GDPR clear, and have been prevented from implementing a new or improved product as a result	35%	7,800
Enhancing the approach to explainability and accountability for fair processing in the context of profiling in AI systems	13,000 organisations that adopt AI, don't find GDPR clear, and have been prevented from implementing a new or improved product as a result	10%	1,300

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

[130] UK Business Data Survey, 2021

[131] Not all firms would increase their data sharing as a result of these measures. Where evidence is not available we have applied informed assumptions that are tested in the sensitivity analysis section further into the document.

[132] Data sharing in the private sector - ODI/YouGov poll results - 2020-04-30

Improving use-based and risk-based standards on data minimisation techniques	80,000 organisations analyse data, are unclear on when a dataset is anonymous under GDPR and share data with other organisations	10%	8,000
Reducing and simplifying record-keeping requirements, for organisations that control or process low risk data.	19,000 organisations organisations that analyse less sensitive personal data to generate new insights or knowledge, don't find GDPR clear, and have been prevented from implementing a new or improved product as a result	25%	4,800

197. As can be seen in the table, we estimate approximately 25,000 firms may change their use of data as a result of these policies.

198. In order to estimate the impact of our specific reforms on the we rely on the significant relationships identified in three academic papers; Bahkshi et al. 2014,[133] Brynjolfsson et al. 2011[134] and Bassetti et al. 2020.[135] Bahkshi et al. find that a one-standard deviation increase in the use of online data is associated with an 8% higher level of productivity (TFP). Looking at decision making based on data and business analytics ('data driven decision making' or DDD), Brynjolfsson finds firms adopting DDD have output and productivity 5-6% higher than what would be expected, all else being equal. Bassetti et al. look at the relationship between TFP, wages and AI patents; the headline finding is that every AI patent graded contributes to a higher TFP by 3.2%.

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

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

201. Quantifying, and particularly monetising, the value of this data poses a difficult challenge. For example, defining the volume of data in terms of bytes does not reflect the quality of that data in terms of its many characteristics (such as accuracy, timeliness, and the degree to which it is processed). The value of data will vary greatly according to context and there is

[133] The analytical firm: Estimating the effect of data and online analytics on firm performance, Nesta, 2014
[134] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486
[135] Bassetti, T., Borbon Galvez, Y., Del Sorbo, M. and Pavesi, F., Artificial Intelligence – impact on total factor productivity, e-commerce and fintech, EUR 30428 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-24694-7, doi:10.2760/448034, JRC122268.

limited information on prices. Nonetheless, rather than omitting a monetised impact from our analysis, we use GVA as one potential way to capture the value added to the economy on a top-down basis. Through the mechanisms described above, we expect that data use will improve TFP, improving allocation of resources and coordination to increase firm-level output with all other inputs unchanged.

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

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

- Carrying out sensitivity analysis on all assumptions used in the modelling.
- Making this a focus area for future analysis by building capacity to monitor and evaluate the impact of data reforms on productivity. This requires observing the impact on the market over a period of time, and for this reason the department aims at conducting longitudinal studies looking at the relationship between productivity and data use (more details of this are in the monitoring and evaluation section).

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

- A proportion of potentially affected organisations would increase data use, which in total constitute a fraction of the estimated number of firms using data
- The impact of additional data use on productivity is linear: in other words, the effect of increasing data use by 10% is the same regardless of whether the organisation starts from a low or a high initial level of data use. This is a simplifying assumption to:
    - Reflect the lack of evidence in the literature indicating increasing or diminishing marginal returns.
    - Ensure we remain conservative in our analysis. For example, if we were to assume diminishing marginal returns, this would greatly increase total estimated benefits as the majority of firms in the UK are classified as micro and start from a lower level of data use than large firms.[136]

205. In order to calculate the total impact on GVA of each reform, we take the total number of firms that analyse data to gain insight and knowledge, and the proportion of these that find current guidelines hard to follow and have therefore been stopped from implementing a

[136] As observed in DCMS:UK Business Data Survey, 2021

change or a new product into business practices. We then assume on the likely increase in data use as a result of these measures. All assumptions in the model are tested in the risks and assumptions section of the IA.

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

Table 29: Estimated impact on UK productivity of each proposed reform, 2021 prices

Average annual benefit to UK productivity (GVA)	
Reform	£m
Legitimate Interests	10.2
Research Purposes	17.6
AI and Machine Learning	5.6
Data minimisation and anonymisation	36.8
Accountability Framework: Record Keeping	2.2
Total	72.5

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

208. In order to model this impact, we have had to make assumptions for policies where existing evidence is weak. More on these assumptions can be found in the sensitivity analysis section. Testing these assumptions by using a low, medium and high scenario tells us that the total GVA impact is between £18.9 million and £208.8 million.

Table 30: Estimated impact on UK productivity of each proposed reform split by scenario, 2021 prices

Impact on UK productivity (GVA) (£m)			
	Low scenario	Medium scenario	High scenario
Legitimate Interests	2.1	10.2	30.5
Research Purposes	10.0	17.6	30.2
AI and Machine Learning	2.8	5.6	8.4
Data minimisation and anonymisation	3.7	36.8	132.5
Accountability Framework: Record Keeping	0.3	2.2	7.0
Total	18.9	72.5	208.8

Increased Interoperability and Trust of Digital Identity Systems

209. More detail on the calculation of the monetised value of potential benefits of the proposed Digital Identity reforms can be found in the published Digital identity and attributes - De Minimis Assessment.[137] In this Data Protection and Digital Information Bill Impact Assessment we provide an outline of the main monetised benefits of the proposal. This analysis looks at four potential use cases and compares the benefits across 3 different scenarios.

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

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

Table 31: Total number of annual DI checks at steady state by use case

Category of checks	Total number of checks
DBS checks	7,174,588 - 9,694,574[138]
RTW checks	8,225,000
Qualification checks	1,727,250
Travel authorisation and ticketing	259,595,875
Home buying	8,882,775
Trusted financial transactions	860,772
Total	285,184,531

[137] Digital identity and attributes - De Minimis Assessment DCMS, 2021

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

212. A central, best- and worst-case scenario is modelled in which the amount of years it takes for both the first Digital Identity checks to take place and the amount of years it takes to reach a 100% uptake level varies. In this impact assessment we will look solely at the central case and the total range of estimations, however more detail can be found on the best- and worst-case scenarios in the Digital identity and attributes - De Minimis Assessment.[139]

213. The indirect benefits for the 4 use case scenarios are split down in to the following categories:

a. Employee Mobility

i. According to Deloitte analysis,[140] a fully functioning digital identity market may positively impact employee mobility by:

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

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

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

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

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

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

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

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

[139] Digital identity and attributes - De Minimis Assessment DCMS, 2021
[140] Economic analysis, Measuring the economic benefits of adopting digital identity, Deloitte, 2020, is available upon request.

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

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

b. Travel authorisation and ticketing

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

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

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

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

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

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

c. Home buying

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

      1. Setting up a savings account

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

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

1. **Improving delivery:** Digital identity checks may streamline the home buying process and offer real-time response and confirmation of the various steps required for home ownership (e.g. when applying for a mortgage)

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

d. Trusted financial transactions

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

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

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

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

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

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

214. The central estimation of the ten-year undiscounted value of the benefits unlocked by a fully realised digital identity market for the four use cases together is £5,401.96m. Whereas,

we estimate that the total value of the benefits worst- and best-case scenario may be £2,996.17m and £7,385.92m respectively.

Table 32: Indirect benefits of Digital Identity schemes: total, £, millions

	Annual value of the benefits[141]	Benefits over the 10-year appraisal period (undiscounted) (£m)		
		Central case estimate	Best case estimate	Worst case estimate
Employee mobility (including second order)	293.0	1,831.2	2,518.8	1,112.3
Travel authorisation and ticketing	296.9	2,078.5	2,375.4	1,544.0
Home buying	133.0	930.7	1,063.6	691.4
Trusted financial transactions	184.7	1,292.9	1,477.6	960.5
Total	907.6	6,133.3	7,435.5	4,308.2

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

215. This section of analysis has been provided by the Home Office.

216. The data on the volume of births and deaths shows that 613,936 births and 607,922 deaths were registered in the UK in 2020. The amount of deaths registered was 14% higher compared to 530,841 in 2019 and significantly higher than any year back to 2010, [142] and birth figures for 2019 were 640,370. The Home Office makes no official forecast of future volume or birth and death registration. For the purpose of this IA, ONS figures for births and deaths for each year between 2010 to 2019 were used to form a low, central and high assumption. Over the 10 years, the low assumption was calculated using the minimum of these values, the high scenario was calculated using the maximum and the central scenario was calculated using the average. Births and deaths were summed and rounded to give total registrations to be used in estimates. See the table below

Table 33: Volume of births, deaths, total registrations and scenario volumes, 2019

	Births	Deaths	Total Registrations
2019	640,370	530,841	1,171,211
Low	640,370	484,367	1,124,737

[141] The annual values of the benefits assume that the digital identity market has reached its steady state.
[142] https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/impactofbirthsanddeathsonukpopulationchange/2020#:~:text=In%20the%20calendar%20year%20of%202020%20there%20were%2090%2C173%20deaths,fall%20of%2029%2C489%20from%202019.

Central	695,220	512,444	1,207,664
High	729,674	541,589	1,271,263

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

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

219. Wherever employee time has been costed, a low, central and high wage per minute for both registrar and superintendent registrars have been used. The gross wage per hour was calculated using Local Registration Service (LRS) data for 2020-2021 salaries. The net annual salary was taken and the national insurance and pension were added on to get the gross salary. This was then divided by 210 days,[143] then divided by 7 hours. Table 2 presents these below. Within the IA, these figures are divided by 60 minutes, to give the per minute value for calculations

220. **Table 34:** Gross wage per hour (£/hr) for superintendent registrars and registrars, 2020/21.

	Superintendent Registrar	Registrar
Low	24.6	19.5
Central	36.4	23.9
High	49.0	30.5

Registration service

Administration of paper registers

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

[143] The average number of days worked by registrars by year across all 174 local authorities. This figure has been agreed by a sub-committee of the National Panel for Registrars.

222. The action to print the register page, put it into the register and lock the register away takes approximately two minutes,[144] within a range of 1.75 to 2.25 minutes. The cost per hour for a registrar is given in Table 2. The cost of time taken is multiplied by the number of births and deaths per year (low, central and high scenario) from the ONS. The estimated savings in salaries lie in a range of £5.4 to £12.1 million, with a central estimate of £8.0 million (PV) over 10 years in 2019 prices.

Retrieval of paper registers

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

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

224. This amounts to a savings in salaries in the range of £0.1 to £0.2 million with a central estimate of £0.1 million (PV) over 10 years in 2019 prices.

Certification process

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

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

226. This amounts to savings in salaries in a range of £6.7 to £19.5 million, with a central estimate of £12.3 million (PV) over 10 years in 2019 prices.

Home Office

Supply of manual register folders

227. Reduction of cost to Home Office regarding supply of manual register folders. The cost to GRO (who supply the register folders to the registration service) is £17.34 for each birth or

[144] Average time was identified as part of the process for developing fees by the Home Office. Time and motion studies are conducted by the National Panel for Registrars.

death register and a total of 4,562 registers were issued to the registration service in 2019/2020. The reduction in cost is estimated as:

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

228. This represents an annual saving of £79,105. This is a saving of £0.7 million (PV) over 10 years in all scenarios.

Supply of registration paper

229. Reduction of cost to Home Office regarding supply of loose leaf and water marked registration paper. Loose leaf, water marked register paper is supplied to the registration service by GRO. During 2019/2020 a total of 4,562 registers were issued by the local registration service when registering births and deaths in England and Wales. A set of paper is needed for each register per year at a cost of £1.89 per pack of 300 sheets, this will save £8.622 each year, with estimated savings of £0.1 million (PV) over 10 years, for all scenarios.

Distribution of registers, paper registers and registration paper

230. Reduction in administration cost for distributing register covers and registration paper. The GRO will not need to supply register folders and paper therefore, there should be resource savings with their delivery contract. The contract is approximately £80,000 per year. This cost saving has been taken as the high scenario, in the instance that the contract is completely cancelled, giving a per year saving of £80,000 and a benefit of £0.7 million (PV) over the 10-year period. In the central scenario a reduction in cost of £70,000 per year is assumed, a significant reduction in the annual contract cost to £10,000, which is used for other, less frequently used distribution purposes, giving £0.6 million of benefit (PV) over 10 years. In the low scenario contract savings of £50,000 are estimated per year, leaving a £30,000 per year charge, which allows for restrictions or legal issues with terminating the contract. This gives a benefit of £0.4 million (PV) over 10 years.

Table 35: Total monetised benefits of the reform, £m, 2019 prices

Total Monetised Benefits	Low scenario	Medium scenario	High scenario
Supply of manual register folders (GRO)	0.7	0.7	0.7
Supply of registration paper (GRO)	0.1	0.1	0.1
Distribution of registers and paper registers and registration paper (GRO)	0.4	0.6	0.7
Administration of paper registers (LRS)	5.4	8.0	12.1
Retrieval of paper registers (LRS)	0.1	0.1	0.2

Certification process (LRS)	6.7	12.3	19.5
Total Benefits	13.3	21.7	33.2

Indirect Benefits - Non-monetised

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

Creation of Robust and Secure Smart Data Schemes (BEIS)

232. This analysis has been taken from the Smart Data Impact Assessment 2022 published by BEIS. For a more detailed breakdown of some of the indicative sector specific costs and benefits please refer to the Smart Data Impact Assessment directly.

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

234. By accelerating the implementation of Smart Data schemes consumers would realise the benefits sooner. Customers, third party providers (TPPs) and wider society are the main groups who could see benefits from Smart Data schemes. Indicative analysis within the BEIS Impact Assessment has provided estimated benefits associated with speeding up the implementation of a telecommunications Smart Data scheme.

235. The extension of Smart Data will, in time, deliver new innovative services, stronger competition in the affected markets, and better prices and choice for consumers and small businesses, including through reduced bureaucracy. Competitive data-driven markets can reduce friction for established market players, and drive start-ups, investment, and job creation.[145]

236. Greater productivity and competition benefits enabled by personal data mobility have been estimated to increase UK GDP by £28.0 billion per annum.[146][147][148] This figure, as reported by 'Ctrl-Shift',[149] has been quantified by aggregating the estimated value of data mobility for a wide range of sectors. For this analysis we have assumed that the benefits are spread evenly across the economy and therefore we have used this estimated annual GDP uplift as a basis for these benefit calculations.

237. To provide an indicative estimate of the potential benefits, BEIS has focussed on the potential benefits associated with introducing Smart Data schemes in the telecommunications sector. In 2019, this sector accounted for around 1.8% of the total general value added in the UK.[150]From this we can assume an annual benefit of £498m per annum with the full rollout of smart data schemes, facilitating greater personal data mobility.

---

[145]BEIS: Next steps for Smart Data, 2020

[146] Ctrl-Shift (2018): "Data mobility: The personal data portability growth opportunity for the UK economy", £27.8bn based on 2017 GDP estimates. The GDP estimates have been uprated to 2021 prices. The economic estimates were developed using a GDP wide modelling approach, as such the accuracy of the impact on specific sectors is prone to significant discrepancies due to the differing use of and commercial and economic impact of personal data within each sector.

[147] This estimate was also sense checked against a McKinsey data mobility benefit figure. This highlighted that open financial data has the opportunity to impact GDP by 1-1.5% by 2030.

[148] This figure, as reported by Ctrl-Shift, has been quantified by estimating the value of data mobility for a wide range of sectors as a proportion of GDP, adjusting this for the impact of that sector and applying the adjusted impact rate to economy-wide GDP. This quantification for data mobility is anchored in the financial services sector.

[149] https://www.ctrl-shift.co.uk/

[150] ONS (May 2021): "Regional gross value added (balanced) by industry: all ITL regions". 61 was used for this purpose.

238. The extension of Smart Data will, in time, deliver new innovative services, stronger competition in the affected markets, and better prices and choice for consumers and small businesses, including through reduced bureaucracy. Competitive data-driven markets can reduce friction for established market players, and drive start-ups, investment, and job creation.[151]

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

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

240. The following section sets out some of the potential benefits that could emerge at the secondary stage, following the introduction of a sector scheme. This analysis builds on the experience of Open Banking (as the only live Smart Data scheme), and considers wider evidence from the finance, telecommunications, energy, and pension sectors.

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

242. This analysis is not fully quantified given that:

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

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

243. As well as more detailed analysis at the secondary legislation stage, BEIS would expect additional research and further consultation for specific Smart Data schemes. This should include research into and further engagement with relevant stakeholders, including data holders, TPPs, consumer and business groups, social enterprises, and charities.

244. Initial consultations have already taken place for Open Finance and Open Communications, demonstrating the work already being done towards implementing Smart Data. DCMS have also published a further consultation and consultation stage Impact Assessment for Open Communications.[152]

[151] BEIS: Next steps for Smart Data, 2020
[152] Waiting for DCMS publication to link these documents

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

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

Table 36: Indirect benefits of the creation of Smart Data Schemes by recipient

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

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

Privacy, trust and individual data rights

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

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

250. We have begun to consider the consumer-side impact of measures on privacy and levels of trust in the data regime. With a view to quantifying these impacts, we have assessed the evidence on the hypothetical value of privacy rights currently enshrined in the UK GDPR, and on the impact of trust on data sharing.

251. Current literature suggests that UK consumers have become less concerned about the use of their data. In 2018, Deloitte reported that 47% of digital consumers were "very concerned" about the use of their data but this halved to 24% in 2020.[153]Moreover, an ONS survey found 70% of adults in Great Britain considered data useful when governments use it to understand and better serve society, and 65% said data was useful when researchers or scientists used it to improve knowledge.[154]

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

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

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

[153] Deloitte (2020) Digital Consumer Trends survey

[154] DCMS (2020) The Opinions and Lifestyles Survey - Percentage of adults (16+) who agree that data (including personal data) is useful in a range of scenarios.

255. The CDEI highlights the importance that data subjects place on openness when it comes to firms processing their personal data. If this openness were to change then consumers may be less inclined to engage with a business, resulting in a decrease in available data for firms to use and a decrease in firm level productivity as a result.

Delivery of better public services

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

257. In the context of Covid-19, responsible data use has been crucial to the public response. Globally, around 75,000 scientific publications on Covid-19 were published between January and November 2020, of which more than three quarters were open access.[155] Research databases and scientific publishers removed playwalls so that the scientific community could quickly share COVID-19-related data and publications.

258. Data flows allowed labs at the forefront of the outbreak to share information and rapidly develop tests for the virus.[156] Spirometers, a device used to measure lung capacity, were issued by the NHS to patients at extreme risk from Covid-19. The device allowed patients to measure their lung capacity and share this information remotely with their doctors via an app.

259. More widely, the OECD[157] highlight that there are three ways in which the public sector can use data to generate public value;

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

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

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

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

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

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

[155] OECD (2021) notes that "the pandemic has triggered an unprecedented mobilisation of the scientific community"
[156] Deep mind (2020) Computational predictions of protein structures associated with COVID-19
[157] OECD (2019) The Path to Becoming a Data-Driven Public Sector

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

ii. Feasibility to complete extensive work involving analysis

iii. The application of new methods of data presentation

iv. The creation of algorithms to suggest appropriate solutions.

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

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

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

263. There is evidence that there remain important barriers to data use in the provision of public services, including time taken to access data and constraints in data access for commercial companies, not just data protection rules. When surveyed, members of the health data user community reported that only 25% of recent requests for data had been completely successful, and only 45% of requests for clinical trial data were successful.[158]

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

Impacts of changes to the Digital Economy Act

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

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

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

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

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

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

Table 37: Indirect benefits of the changes to the Digital Economy Act by recipient

Impacted party	Benefits
Businesses	**Reduced duplication of data entry:** Businesses will save time and therefore costs by only being required to provide information to the government once. Furthermore, this benefit will occur each time that a business applies for a new service/grant/subsidy etc as they will no longer be required to submit their information on each unique occasion. The Estonian government has set up the eesti.ee portal, where all information and requirements regarding opening up and running a company are gathered in one place. It aims to help established and continuing businesses to fulfil their information obligations and to reduce their administrative burden.[159] **Ease of access to government support:** Having a single portal for applying for business support services will allow businesses to more easily engage with the government. This could save time for businesses when attempting to apply for the services that they require. Businesses may also be able to use this route to receive financial assistance in ways that they did not know were possible. For example, the proportion of firms claiming R&D tax credits is very low, despite HMRC setting aside billions in funding.[160] Many firms don't understand if their operations qualify as innovative or are unable to complete the application due to lack of expertise.[161] **Induced investment by the private sector, driving growth and productivity** The BEIS/HMT Business Productivity Review evidence shows that many of the productivity constraints on businesses are caused by internal factors, including; weak management skills, shortcomings in business planning and reluctance to take external advice.[162] Many managers are unclear about what support is available that would benefit their business, and where to find it. It is therefore possible that with better data HMG could target marketing at these businesses to reduce the information asymmetry and induce them to invest or co-invest in improving their business processes or management skills.
Government	**Reduced duplication of data processing:** As data about businesses becomes increasingly connected across

[159] Digital Government Factsheet 2019 - Estonia
[160] AI Sector Deal
[161] Poor knowledge of government incentives is holding back the innovation economy, Business Money, 2021
[162] Business Productivity Review, 2019, BEIS

	government, data will no longer have to be collected and processed in multiple departments. This would result in efficiency benefits for HMG as civil servants who were initially involved in processing this data are able to provide support elsewhere. **Improved policy-making, allocation of resources and impact:** Better access to data and ability to turn data into useful insights helps create economic value, as these insights can be used by decision-makers to optimise the allocation of resources.[163] Research shows that firms adopting data-driven decision-making can have 5-6% higher output and productivity.[164] **Reduction of programme costs:** If BEIS has the ability to segment the business population and market services directly, this could reduce the need to fund a direct marketing company to recruit businesses to a programme. While the admin costs may rise slightly to undertake the targeting, it is likely that the total cost to taxpayers would be lower. **Reduced fraud and error:** A centralised source of information about businesses may enable increased cross-checking of details about businesses. This will result in more accurate assignment of funding and reduce the ability of businesses to submit fraudulent applications of funding. Members of the fraud prevention service, Cifas, share data with other members outside of their own organisation in order to improve fraud prevention. Cifas members prevented fraud totalling over £1.4 billion in 2018.[165] **Corporate transparency and regulation:** Better use of data held by the government, in accordance with the Data Standards Authority framework, promotes a culture of transparency, safeguarding and assurance, which builds and maintains public trust. As a result, businesses will be more willing to provide data and the government will have a more comprehensive view on business information and activity, aiding the regulation of markets.

Improved customer outcomes

270. It is expected that when consumers are better informed, through sharing their data, they will make different consumption choices. These different choices will result in benefits not captured by loyalty penalty estimates. For example, analysis of the Pensions Dashboard highlights the potential recovery of up to £19.4m of "lost" pension pots.[166] Consumers will have

[163] Connected Open Government Statistics, ONS
[164] Strength in Numbers: How Does Data-Driven Decision-making Affect Firm Performance, Erik Brynjolfsson SSRN Electronic Journal
[165] Tackling fraud in Government with data analytics Starting the conversation CO/DCMS, 2019
[166] DWP (October 2019): "Pension Schemes Bill 2019 Impact Assessment"

more information available to them to make better informed choices and engage more effectively with the market.

271. Consumers being informed does not necessarily mean they will choose the cheapest deal, but consumers may choose the deal that is best suited to them. For example, Ofcom found that 71% of people who changed their mobile phone provider in the last 12 months did not consider mobile phone strength as a factor when making this decision. Of these respondents, 20% stated this was because it did not occur to them, 9% said they did not know where to find the information, and 7% said it was too much hassle.[167] Similar non-price factors are also important to SMEs, and this type of comparable information may not be available for them without Smart Data.[168]

272. Further benefits may manifest as a result of consumers being better informed. For example, previous analysis of the energy and retail markets[169] have highlighted the effects of better-informed decisions in increasing energy efficiency and healthier choices, leading to carbon savings and improved health outcomes. Again, these benefits are expected to be sector specific, so they will likely be captured by sector schemes through ongoing evidence gathering or in future sectoral analysis.

Improved Interoperability across Health and Social Care Systems

273. Analysis in this section is based on analytical findings conducted by the Department for Health and Social Care in cooperation with DCMS.

274. Engagement with the health supplier market has begun. It is anticipated that there will be some resistance from suppliers who currently dominate the market, while others will see it as an opportunity to enter into the health and social care space. Many of these suppliers provide services across international markets.

275. Large-scale open platform implementations have been introduced in a number of countries. Some of the current global trends are provided below:

- In Estonia, various legislation has been passed to regulate the information in the health information system, responsibilities of patients, Health Care Practitioners and provide requirements for document standards.

- Norway's eHealth strategy aims to provide a seamless and secure environment to patients and HCPs to access and use data and has passed legislation to assess requests for health data.

- The European Commission has set standards for the exchange of patient health information across borders, and regulators are taking an interest in data portability and interoperability in the European General Data Protection Regulation

[167] Ofcom (August 2020) "Open Communications: Enabling people to share data with innovative services"
[168] Ofcom (August 2020) "Open Communications: Enabling people to share data with innovative services"
[169] DECC (2014): "Legislation to require energy suppliers to provide key, personal information on consumers bills in a machine-readable format" & BIS (2012): "Order making power for midata"

- In the US, the Office of the National Coordinator (ONC) for Health Information Technology made an important final ruling in March 2020. The ONC rule gives patients secure access to their data and implements interoperability requirements through open data sharing via standardised APIs, and it sets out provisions which prohibit health IT suppliers and providers from undertaking activities that constitute information blocking[170].

276. The Secretary of State for Health and Social Care is pursuing a policy of person-centred care, where information about an individual's care more closely follows that person as they move around the public and private health and adult social care system. This is the primary policy objective behind the enabling powers proposed. The secondary policy objectives are to facilitate population wide research and analysis, operational planning and promote innovation within the health and care IT supplier market.

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

278. Open platforms can also help improve interoperability and a more open market supported by separation of applications. Adopting an 'open' approach to architecture, in the technical sense, will support innovation. In fact, it will encourage a more open market and inspire vendors to adapt to a world that truly focusses on interoperability in an open, needs focussed manner.

279. Given the right security and consent from people accessing health and care services, it is indisputable that data liquidity across all care settings will benefit and empower the citizen/patient whilst providing invaluable insight to clinicians and frontline staff to improve patient care. Executed in the right way the data can flow between providers, ICSs, regions, nationally and internationally. Data sets at all levels provide the key foundation for population health management. For example, Norway introduced a new national system for sharing health information across regions and health organisations [171]. Patient accessible health records have also been rolled out nationally, which have been perceived as useful by patients and have offered a number of clinical benefits including providing patients with a better knowledge about their health condition, improved ability to manage their conditions and improved communications with those providing their care[172].

280. The future vision of health and care data architecture must be needs-focused and centred around developing person-centric and person-driven care services. Our measures seek to support this future vision.

281. Further beneficial outcomes are provided in the table below:

Table 38: Indirect benefits of DHSC policy

Outcome	What will change	Potential Outcomes

[170] Information Blocking | HealthIT.gov
[171] Electronic Health Records Norway | Accenture
[172] Patient Use and Experience with Online Access to Electronic Health Records in Norway: Results from an Online Survey - PubMed (nih.gov)

Supporting staff to safely access information when they need it and at a time and place that is convenient to them, aiding the quality of the care they provide.	● Caregivers have access to all the relevant information that they need (and have the authority to access) in order to provide care, in real time, irrespective of which system they use to access that information and which system was used to generate it. ● Staff can access, interrogate and process data in real time by anyone with the authority to access that data, irrespective of the system used by the health or adult social care provider who collated, produced or otherwise processed that data. ● Easier for staff to move across settings as there will be no new EPR to learn to use.	● Clinical outcomes, patient safety, and quality of care, patient satisfaction and sustainability. ● Improved productivity. ● Improved clinical decision making enabled by access to accurate and complete information.
Open Data Architecture	● Suppliers adopt changes that allow data to be accessed and made available according to open data standards and a common architecture. ● More control over specification and standards; interoperability will mean data can move across settings easily for patient care. ● Ability to operationally manage across the whole system. With open data it will be possible to manage waiting lists nationally, allocating patients to alternative settings.	● A standardised version of the data. ● A cleansed dataset that removes duplicated or obsolete records. ● Data that can be more easily accessed and analysed. ● Better and more clear procurement and commissioning by NHS providers, increased confidence in the products on offer. ● A more modular approach to EPRs, avoiding supplier lock-in and creating a more dynamic and responsive market. ● Innovation takes place securely and openly on top of the data, with applications able to access the data directly rather than wait for the EPR suppliers to provide access.

		● An enhanced and responsive digital market with improved commercial capabilities established.
Research and innovation	● Better data available to support the development of new treatments to improve the NHS, making data captured for care available for clinical research, and publish, as open data, aggregate metrics about NHS performance and services. ● Data can flow between care settings, and between health and care, both for direct care, and for population health, system management and research. ● IT suppliers in the system will lead the way in innovation in the software market for EPR systems, and international collaboration to help us deliver our goals.	● Integrated and prevention focussed, rather than treating disease. ● Creation of a defined minimum data set that builds on existing work by Care Quality Commission and Professional Records Standards Body. This programme will help to drive a more standardised approach to data collection so that one collection can be shared with multiple stakeholders.
Empowered citizens and patients with information and tools to support their health, care and wellbeing.	● Bringing people closer to their care records by giving them access to their own information when clinically appropriate to do so. ● People have transparency in the data that has been captured, and confidence in how their data is used by understanding the safeguards in place.	Separating data from the systems that hold it to create a network of decentralised personal data stores. People can update information once, which can then be seen across all platforms.
Help to become a greener health and care system through reduced travel, reduced reliance on buildings and paper storage.	● Data to be held in a cloud-based environment secured by the NHS/DHSC, with access to the data, controlled by an NHS/DHSC/adult social care body.	● Reduced data centre footprint. ● Accessible systems anytime and anywhere.

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

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

Subject Access Requests (SAR)

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

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

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

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

Mirror the national security exemption from part 2

287. Currently, the national security restrictions in Part 3 are not as extensive as in Part 2. The current restriction-based approach in Part 3 is also more limited than the protections provided by the Part 4 national security exemption. This creates risks when, for example, a data subject exercises their rights. Mirroring the national security exemption into Part 3 would be more consistent to protect national security, as well as assist close working between law enforcement and intelligence services.

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

Introduce a definition of 'consent' to Part 3 (DPA 2018 part 3)

289. Although rarely used, the ‘consent’ of a data subject is an available legal basis for processing under Part 3 of the DPA 2018. As ‘consent’ is a word used frequently in natural language and has alternative meanings within the policing context, there is a very small risk that it may be interpreted incorrectly in the absence of a clear definition. As such, the inclusion would provide data controllers under Part 3 with a clear and uniform definition of ‘consent’ they can refer to. Therefore, this proposal seeks to replicate the UK GDPR definition of consent into Part 3 as there is currently no explicit definition.

290. Introducing a clear definition may reduce the risk that the definition of consent is interpreted in a way which does not align with the definition under Article 4(11) UK GDPR.

Clarifying use of Section 76 DPA to cover larger scale transfers

291. Introducing some flexibility to Section 76 DPA 2018: Concerns the international transfer of personal data where ‘special circumstances’ are present. Currently, the conditions and restrictions imposed within the provision make it too inflexible to meet modern law enforcement needs and therefore, unnecessarily limit public safety efforts and goals. The reform clarifies how law enforcement can legitimately use S76 which enables the transfer of personal data where ‘special circumstances’ are present to give confidence to the law enforcement community to use this section to transfer larger amounts of data in the pursuit of the detection and prevention of crime.

292. Adding flexibility should give legal clarity to competent authorities when engaging in large scale transfers, therefore reducing the chance that they may face legal costs.

Reform subsequent transfer's provision

293. Under the current legislation, UK competent authorities must make it a condition of any transfer for a law enforcement purpose that data is not to be further transferred to a third country or international organisation without the authorisation of the transferring controller (or another competent authority). This reform considers introducing a targeted small exemption to allow competent authorities to provide a dispensation from the requirement in the case of an immediate and serious threat where authorisation cannot be obtained in good time. In such cases, the third country would be required to notify the relevant competent authority of the transfer as soon as practicable.

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

294. This section of analysis has been provided by the Home Office.

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

Non-quantified benefits

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

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

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

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

Increase in data use for research purposes

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

a. There will be benefits to the public associated with the increase in the use of data in commercial settings for R&D. For example, Artificial Intelligence related R&D, a data intensive activity, can add the equivalent of an additional £232bn to the UK economy, therefore highlighting the potential benefits of R&D to living standards and the economy.

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

Costs

Summary

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

1. Direct Costs
    a. Monetised
        i. One off familiarisation cost
        ii. Improved Regulatory Oversight
        iii. Enhancement of the work of the UK intelligence services and law enforcement bodies in the interest of public security
    b. Non- monetised
        i. Enhancement of the work of the UK intelligence services and law enforcement bodies in the interest of public security
        ii. Improved interoperability across health and social care systems
2. Indirect Costs
    a. Monetised
        i. Increased interoperability and trust of digital identity systems
        ii. Remove the requirement for paper birth and death registers moving to an electronic register
    b. Non-monetised
        i. Creation of robust and secure Smart Data schemes
        ii. Increased interoperability and trust of digital identity systems
        iii. Delivery of better public services
        iv. Empowerment of the police to use new technologies like biometrics
        v. Improved interoperability across health and social care systems
        vi. Costs to businesses of increased data use

Direct Costs - Monetised

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

Familiarisation Costs

Familiarisation Costs for UK Businesses

302. Other quantifiable impacts include familiarisation costs associated with the new measures. The analysis included in the initial consultation note estimated a one-off familiarisation cost of £71.1 million to £96.3 million, as businesses learn about and respond to new measures.

303. We continue to use a time-cost approach to estimate the administrative costs of reading the new legislation. This approach to familiarisation costs had been adapted from the ICO's methodology used in their Impact Assessment for the Data Sharing Code.[173] While the ICO modelled familiarisation costs for a single piece of guidance (the Code), the main difference in approach is that the familiarisation costs have been broken down by policy measure, as different measures apply to different populations of businesses. Familiarisation costs for each measure have therefore been calculated individually, and then subsequently summed together.

304. Although this methodology has not changed we have updated some of our assumptions feeding into the model using new evidence. In order to identify the relevant 'number of affected businesses' per measure, we look at an organisation's data use to determine if they are in scope of the model. We assume that familiarisation costs are borne in year one as all organisations read the new guidance, taking this direct measure of impact. We draw from an analysis commissioned by Frontier Economics which identifies the relevant population of businesses per measure.

305. The ICO assumes that one data protection officer per organisation would be required to read guidance, and estimates their hourly unit cost of this work at £26.71. As wages would vary according to size of business and small businesses are less likely to have data protection offices we now reflect this in our modelling.

306. The wage assumptions have been updated by assuming that at small and medium-sized enterprises senior officials would read the guidance rather than data protection officers.[174] The hourly unit cost of this work was estimated to be £26.85 using median hourly occupational earnings estimates from ASHE.[175] For micro-sized firms (zero employee firms) we have updated our wage assumptions by applying median annual earnings estimates of the self-employed from DWP's Family Resources Survey and estimating the hourly unit cost of this work at £11.20.[176] The self-employed wage assumption is used as a simplification to reflect the average wage of a micro-sized firm with zero employees.

307. We continue to assume that the guidance would be at a similar level of reading difficulty to the ICO's data sharing code, and therefore have used a similar Fleisch reading ease score of

[173] Data Sharing Code of Practice Impact Assessment, ICO, (2019)
[174] All wage estimates have been uplifted by non-wage labour costs using RPC guidance
[175] ONS Annual Survey of Hours and Earnings (2021)
[176] DWP Family Resources Survey (2020)

40, which corresponds to a reading speed of 75 words per minute. Assuming an average number of words per page of 500, this gives a reading speed of 9 pages per hour.

308. We have updated the estimate for the number of pages of guidance provided to businesses. We have done this following consultation with policy colleagues and by looking at the average number of pages of guidance previously prepared when changes to UK GDPR have been made. As a result, we now estimate the one-off compliance costs to be the following:

Table 39: Total one-off familiarisation cost by scenario and reform for UK businesses, 2021 prices

Total Familiarisation Cost (£m)			
Reform	Low scenario	Medium scenario	High scenario
Research Purposes	3.2	3.8	4.4
Legitimate Interests	8.1	9.5	11.0
AI and machine learning	2.6	3.0	3.5
Data minimisation and anonymisation	8.1	9.5	11.0
Accountability Framework	44.0	51.8	59.6
Privacy and Electronic Communications	5.1	6.0	6.9
Total	71.1	83.7	96.3

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

310. We have also looked into the inclusion of any long-term training costs that would have to be undertaken following the implementation of the bill. To estimate these costs, we conducted an extensive literature review into the reported costs of training UK businesses for changes to data policy. The UKBDS found that only 17% of respondents engaged in training after the publication of UK GDPR and the DPA 2018. Christensen et al. (2013)[177] also report that “the training of staff at most Small and Medium Enterprises (SME’s) will take up to one week a year for a DPO (for both new starters and refreshers for existing staff and preparing training materials) “.

311. After further investigation of the surrounding literature and the smaller magnitude of the proposed changes when compared to UK GDPR, we are assuming no additional training costs. DPOs would likely cover the changes as part of standard refresher training that would occur in both the do-minimum and do-something; on-going training is evidenced by the

[177] The Impact of the Data Protection Regulation in the E.U. by L. Christensen, A. Colciago, F. Etro and G. Rafert, 1 February 13, 2013

average UK employee undertaking 3.6 days of training per year (UK Employer Skills Survey, 2019). Any training to disseminate to colleagues within firms is already part of a DPO's responsibilities. For new DPOs, given the changes replace aspects of DPA rather than create additional responsibilities, we can assume that the time taken to become certified would remain the same. For those who train DPOs, we assume any small familiarisation costs would likely be recouped quickly through the market via the cost charged to students. The assumption also ensures reduced risk of double-counting as it is likely that the cost of SSCs implicitly capture other marginal costs from the changes.

Familiarisation Costs of enhancing the work of the UK intelligence services and law enforcement bodies in the interest of public security (HO)

312. This section of analysis has been provided by the Home Office, and is broken down by measure. Where evidence is unavailable costs have been assessed qualitatively and can be found in the relevant 'non-monetised section'.

313. Stakeholders were unable to provide comprehensive responses to data requests. This was mainly due two factors:

314. Time constraints, where there was a possibility that data could be obtained but there was not enough time to put it together.

315. The specificity of the data required, meaning that stakeholders did not record the data required for monetisation.

316. Therefore, many costs and benefits have not been monetised. In these cases, a qualitative analysis of costs and benefits was undertaken.

317. The number of competent authorities was taken from Law Enforcement Directive (LED) impact assessment for the DPA 2018. The UK Intelligence Services was then added to this. The number of organisations in scope is estimated to be between 407 and 507, with a central estimate of 457. This includes a number of private businesses between 34 and 134, with a central estimate of 84.

318. The length of guidance (2,400 words) was also taken from the LED IA as well as the average wage bracket of those affected by guidance (Higher Executive Officer) and the average number of employees expected to require training (50).

319. The appraisal period is 10 years and the discount rate used is 3.5 per cent. All monetised costs and benefits are given in 2021 prices and are assumed to be direct unless stated otherwise.

320. Implementation costs are temporary costs which are assumed to factor in only in the first year of the proposals being implemented. These will include any familiarisation costs, as well as any additional temporary burdens such as the cost of additional infrastructure.

321. Familiarisation costs are expected to apply with any change in regulation and apply to all proposals. They represent the cost of time to an organisation of employees having to read new

guidance. Below, an overall familiarisation cost will be calculated which will encompass the effects of all proposals.

322. It is assumed that the familiarisation cost applies to all competent authorities (including UK Intelligence Services) as a result of the relevant proposals being implemented, with low, central and high values representing the range of uncertainty.

323. It is estimated that there are between 407 and 507 competent authorities (including UK Intelligence Services) with a central estimate of 457. Of these, there are between 34 and 134 which are private entities, with 84 as a central estimate.

324. It is assumed that between 25 and 100 employees will have to read new guidance, with a central estimate of 50. The average wage of an employee required to read guidance is assumed to be that of a Higher Executive Officer (HEO) which is between £26.19 and £29.89, with a central estimate of £27.37 taken from the Home Office staff costs database with a price base year (PBY) of 2020/21. This was then adjusted for inflation using the CPIH index. In 2021 prices, the wages are assumed to lie between £26.84 and £30.63, with a central estimate of £28.05.

325. The high estimate of the guidance is taken from the LED IA, at 2,400 words. Low and central estimates are calculated as a proportion of the high estimate; 1,200 (50 per cent) and 1,800 (75 per cent) respectively. These proportions are used as default as the Government has not been able to obtain an estimate from stakeholders, but since these proposals are an update it is assumed that the guidance will be shorter than for the whole LED.

326. The time spent reading guidance is calculated using a readingsoft calculator, using reading speeds of 700 words per minute (wpm) for low, 400 wpm for central and 200 wpm for high. This includes extra re-read time which is based on the estimated levels of comprehension and number of words. Estimated total time spent reading guidance is in the range 0.03 to 0.3 hours, with a central estimate of 0.1 hours.

327. To calculate familiarisation costs, the total number of employees expected to read guidance was obtained by multiplying the number of competent authorities (including UK Intelligence Services) and employees per authority assumed to read guidance. This total number of employees was then multiplied by the average wage and time spent reading guidance.

328. This familiarisation cost can be split into private and public costs, by multiplying the cost by the proportion of private firms in the total cohort.

Table 40: Familiarisation Costs 2021 PBY[178]

	Total Employees			Average Wage of Employees (£ hours)			Time Spent Reading Guidance (hours)			Familiarisation Cost (£)		
	L[179]	C	H	L	C	H	L	C	H	L	C	H
Private	850	4,200	13,400	26.8	28.1	30.6	0.03	0.1	0.3	700	11,800	123,100

[178] Source: LED IA, HO Staff Costs Database, readingsoft.com

[179] Notes: Low (L), Central (C), High (H). Rounding may lead to slightly different results if calculated using values in the table.

Public	9,325	18,650	37,300	26.8	28.1	30.6	0.03	0.1	0.3	7,500	52,300	342,800
Total	10,175	22,850	50,700	26.8	28.1	30.6	0.03	0.1	0.3	8,200	64,100	465,900

329. Total familiarisation costs are estimated to lie in the range £0.01 to £0.47 million, with a central estimate of £0.06 million (2021 PBY) in year 1 only.

330. The Home Office estimates their familiarisation cost using a different methodology compared to DCMS because the organisations affected by their policies are authorities that process personal data for law enforcement and the relevant guidance has different requirements.

Improved Regulatory Oversight - ICO analysis

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

a. Strategy, Objectives and Duties

b. Governance Model and Leadership

c. Accountability and Transparency

d. Codes of Practice and Guidance

e. Complaints

f. Enforcement Powers

332. These reforms aim to move the ICO away from handling a high volume of low-level complaints and towards addressing the most serious threats to public trust and inappropriate barriers to responsible data use.

333. The proposed legislative changes are set in the wider context of increased complexity and scale of processing, which increases demand for upstream engagement and advice and the complexity of downstream enforcement and supervision. They are also set against the backdrop of ongoing work to ensure the ICO has the skills and capacity to respond to increased demand for our activities arising from the implementation of UK GDPR. This existing work is planned on the basis of retention of our current fees model and will be further supported by the proposed approach to fine retention currently being discussed with the government.

334. Working alongside the ICO we have been able to provide monetary estimates of the predicted impact of these reforms on the ICO directly. Evidence for these calculations has been gathered from internal conversations, research and consultation responses.

335. We estimate that the package of reforms will help reduce barriers to data use, however we also acknowledge that these policy changes are likely to have short run and ongoing costs to the ICO as they adapt to the new changes and legislation. In this section we have looked at

the initial costs, medium term costs and the long run recurring costs compared to a status quo scenario where these changes do not occur.

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

337. In the short run we expect there to be a period of adjustment in which systems and guidance will change. This includes the following activities:

a. Governance, administrative and legal changes to prepare for the change in the ICO's legal status represented by the move away from a Corporation Sole Model. This includes changes to all contracts, leases, agreements etc to reflect our change in legal status.

b. Systems and IT changes will need to be prepared for and put in place for 'day 1', when legislative changes come into effect. Examples include complaints, where proposals could result in different procedures for organisations to follow that will require different back-end systems and reporting processes.

c. Identifying updates to all existing ICO guidance and information to ensure it reflects the updated legislation, including where it will be necessary to resolve areas of complexity or ambiguity.

d. Training and information for staff, particularly those providing externally facing advice services to ensure all staff are able to provide up to date support and engagement from day 1.

e. Development of key new guidance products likely to be required on day 1, to maximise regulatory certainty for businesses.

f. Developing clear policies and approaches to the management of supervisory activity likely to fall across the transition to the new legislative framework, including legal advice and updated staff training and advice. I

g. Incorporating the implication of the reforms in any ongoing work with the ICO's sandbox participants and representative bodies or organisations developing codes of conducts or certification schemes, including assessing the impact on agreed project delivery dates and overall feasibility. Developing and agreeing an approach to assessing the impact on existing certification schemes.

338. We are able to estimate the potential cost savings of these reforms to the ICO using a time-cost approach and evidence gained from discussions with the ICO on resourcing, wage costs and activities. A breakdown of these estimated costs can be found in the table below, these are annual costs and are expected to be incurred in the first and second year after implementation

Table 41: Estimated 1-2-year costs to ICO of policies, 2021 prices

Reform	Impact	FTE Estimate		Annual Cost Estimate (£m)	
		Low	High	Low	High
Governance, admin and legal costs of move from Corporation Sole	Medium	6	15	0.3	0.7
Systems & IT	Small	1	5	0.0	0.2
Updates to existing guidance	Small-Medium	1	15	0.0	0.7
Staff Training & Info	Small	1	5	0.0	0.2
Key new guidance products	Medium	6	15	0.3	0.7
Supervisory policies and approaches	Small	1	5	0.0	0.2
Ongoing work with stakeholders	Small	1	5	0.0	0.2
Stage 1 Total		17	65	0.8	3.0

339. After the initial transition period we expect there to be secondary costs of setting up new processes and guidance incurred by the ICO. These include tasks that would need to be completed as soon as possible after the introduction of any new legal framework (e.g. within the first one to two years following new legislation). The intensity of the resource requirement will depend on what, if any, provisions are made about a transition period. These activities include the following:

a. The ICO regulatory action policy (RAP) will need to be updated following changes to legislation across the board and the new strategic direction given by the new objectives, powers and duties. This will include development of clear policies and approaches to using new and enhanced powers, setting up any required appeals processes or safeguards etc.

b. Guidance: There are many areas that will require new and updated guidance. This analysis assumes that most of that guidance would be delivered over the following 2-4 years once legislation is passed. However, we assume that there may be 3-4 guidance products required from day 1. This will therefore have a medium impact. If this work is more front ended, e.g., most of this to be delivered in the first year, it would have a large impact. We have set out all of the currently identified pieces of guidance separately in Annex 6.

c. Changes to the approach to auditing based on the new accountability framework. The current approach is based on a toolkit, and this will need to be changed based on the new Privacy Management Programme approach

d. Initial increase in reactive advice and support required, as organisations seek ICO input on new legislative requirements

e. Planned proactive work to support key sectors or organisations where there is likely to be the greatest change/highest risk. This would build on existing approaches but would require additional focus during the transition period.

340. The estimated annual costs of these activities are set out below:

Table 42: Estimated annual costs to ICO of policies, 2021 prices

Reform	Impact	FTE Estimate		Annual Cost Estimate (£m)	
		Low	High	Low	High
RAP	Medium	6	15	0.3	0.7
Guidance	Medium-Large	6	20	0.3	0.9
Auditing Changes	Small	1	5	0.0	0.2
Reactive advice and support	Medium	6	15	0.3	0.7
Proactive external support	Small	1	5	0.0	0.2
Stage 2 Total		20	60	0.9	2.8

341. After the initial costs outlined above we expect there to be an increase in annual costs compared to the status quo as the ICO responsibilities and structure changes. These are costs are outlined below

a. Accountability/DPIAs: Controllers will no longer be required to consult the ICO under Article 36 prior to high-risk processing where the risk cannot be mitigated; rather, this current mandatory requirement will be made optional. To encourage controllers and organisations to be more proactive in this area, prior consultation will be explicitly introduced as a mitigating factor for enforcement under Article 83. The ICO currently handles around ten prior consultation cases per year under Article 36, and it is unlikely that this reform will radically change these numbers. There is a possibility that organisations feel an additional incentive to consult the ICO; however, the threshold for prior consultation (and definition of ‘high risk’ in this context) is not being changed. For this reason, this would have a small to medium impact on ICO resources.

b. Modifications to the framework for certification schemes, and provisions that clarify that prospective certification bodies outside of the UK can be accredited to run UK-approved international transfer schemes. We understand that DCMS is considering dropping this proposal, but that approval of certification schemes could still operate through SoS’s new power to approve ATMs. Depending on volume/take-up, there is a potentially medium-large impact, due to increased demands on the ICO if we are involved in assessing the certs schemes.

c. Clarifying rules on the collection, use and retention of data for biometrics by the police through the use of codes of practice and guidance. Section 4.4, para 302. Small. Our understanding is that this will be led by the Home Office but is likely to require ICO support. If these are ICO codes and guidance the impact will be medium.

d. New ICO duty to consult with other regulators. This introduces a new set of checks and balances which will require more staff coordination. This overall will have a small impact.

e. Mandatory impact assessments when developing statutory codes and statutory guidance, will require an expansion of resources to ensure robust impact assessments which are supported with appropriate evidence.

f. Setting up expert panels for statutory codes of practice and statutory guidance: giving the Secretary of State for DCMS the power to require the ICO to set up a panel of persons with expertise when developing statutory codes of practice and statutory guidance. This builds on existing ICO work but will require some additional work to identify, recruit and provide support to relevant panels. This may be a small impact, though this will be dependent on the number of statutory codes and guidance the ICO are asked to produce.

g. Governance changes: salary for the new board. There are likely to be small ongoing net costs for additional NEDs.

Table 43: Estimated annual costs to ICO of policies, 2021 prices

Reform	Impact	FTE Estimate		Annual Cost Estimate (£m)	
		Low	High	Low	High
Accountability/DPIAs	Medium	6.0	15.0	0.3	0.7
Modifications to the framework for certification schemes	Medium-Large	6.0	20.0	0.3	0.9
Clarifying rules on the collection, use and retention of data for biometrics by the police	Small	1.0	5.0	0.1	0.2
New ICO duty to consult	Small	1.0	5.0	0.1	0.2
Mandatory IAs for statutory codes and guidance	Small	1.0	5.0	0.1	0.2
Setting up expert panels for statutory codes and guidance	Small	1.0	5.0	0.1	0.2
Governance changes	Small	1.0	5.0	0.1	0.2
Costs Total		17.0	60.0	0.8	2.8

Enhance the work of the UK intelligence services and law enforcement bodies in the interest of public security (HO)

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

Introduce the ability to actively review automated decisions

343. Currently, LEAs are required to inform a data subject as soon as reasonably practicable when a decision which produces an adverse legal effect, is made which is based solely on automated decision making (ADM). The purpose of this is to allow the data subject to then request that a human either reconsiders that decision or takes a fresh decision not based solely on ADM.

344. The police have stated that this can cause them difficulties. For example, in a scenario where automated decision making is used to match an individual to a record on a dataset, the police must then either inform the data subject that they are under investigation (thereby tipping them off that they are of interest) or, alternatively, ensure that there is human intervention in the decision (thereby removing the need to inform the data subject but running the risk that by the time the human review had been completed, it would be too late to act).

345. This proposal will provide an alternative option for LEAs to provide for a human to actively review the decision after it has been taken as soon as is reasonably practicable (or in any case within a month) thereby removing the need to notify the data subject at the time. It effectively builds in the remedy that the data subject should have had were they notified that a decision had been made based solely on automated processing. However, in order to ensure that the new power is only used when necessary, LEAs will only be able to use it if informing the data subject would engage one of the grounds set out under section 44(4) of the DPA (ie.eg. to avoid obstructing an official or legal inquiry, investigation or procedure etc.). This change ensures that the rights of data subjects who are subject to ADM continue to be protected whilst improving the ability of the police to tackle crime, ensure public safety and bring offenders to justice. It contributes to the HO priority outcomes of reducing crime and the risk of terrorism to the UK and UK interests overseas.

346. This is permissive legislation as it is assumed that LEAs will only if they expect the benefits to equal or exceed the costs. This proposal should result in a ‘no worse than zero net cost’.

347. There will be increased efficiency costs for LEAs if they decide to provide an ‘active’ human review instead of notifying the data subject. This is because it is assumed that not all data subjects are notified of human review, thus increasing the workload on policing.

348. Also, police sometimes decide not to deploy systems which use ADM because of the notification requirement as, by using it, they risk alerting potential suspects that they are under investigation thereby compromising investigations and/or police capabilities this change would better enable the use of such systems which will allow data to be processed more swiftly, thereby providing efficiency savings for LEAs.

349. Where there is a risk of compromising investigations and/or police capabilities, the MPS stated that they expect to use active human review in around 90 per cent of cases; this was taken as a central value, with 80 and 100 percent used as low and high values respectively to represent uncertainty around the central estimate. This is likely to lead to an increase in workload and a corresponding increase in costs for LEAs. This is a strong assumption given the likelihood that some form of human review would have been conducted anyway; however, it is likely that the volume of human reviews will increase as a result of this proposal.

350. The MPS also estimate that their current caseload is in the low hundreds annually. This implies a range of between 100 and 500 with an average central estimate of 300. This number of cases was then multiplied by 2, 3 and 4 respectively to give values for the whole of the UK.

These values come from the fact that the MPS employs one quarter of all UK police officers so the highest figure assumes that there will be identical utilisation of active human review throughout the UK with the low and central estimates representing lower utilisation.

351. The time taken to complete an active human review was given as between 0.5 and 1 minutes (where comparing two records to determine if they relate to the same person) and between 15 and 30 minutes (for more complex matters where, for example, there may be a number of data points to be analysed). The low estimate is taken as 1 minute, central as 15 minutes and high as 30 minutes.

352. For cases involving investigations, the review would be conducted by a police officer or police staff depending on the type of review conducted. For cases involving a series of linked pieces of intelligence, it would be performed by an intelligence analyst. Pay grades for these professions were not provided, however, an hourly pay rate was taken from the ASHE Table 15. a[180] (ASHE SOC code 3). The wage of £15.90 was then adjusted to £19.37 to reflect non-wage costs.[181]

353. The number of cases, percentage of cases for which active human review would be pursued, time taken per review and wage of employees are multiplied to give the ongoing cost.

Table 44: Active human review ongoing costs, 2021.

	No of cases	Percentage reviewed (%)	Review time (hrs)	Reviewer wage (£/hr)	Cost per year (£)	Total Cost (£ PV)
Low	160	80	0.02	19.37	50	400
Central	810	90	0.25	19.37	4,000	33,800
High	2,000	100	0.50	19.37	19,400	166,700

Source: MPS Consultation, ASHE Table 14.5a
Notes: Totals may not add due to rounding.

354. Ongoing costs lie in the range £0.00 to £0.17 million (PV), with a central estimate of £0.03 million (PV) over 10 years in 2021 prices.

International-Law Enforcement Alerts Platform (I-LEAP) proposal

355. To introduce a delegated power to pass secondary legislation enabling the technical implementation of new international alert sharing agreements: The International-Law Enforcement Alerts Platform (I-LEAP) will deliver real-time alert exchange with key international partners and so strengthen joint capabilities to tackle shared threats, including migrant smuggling. Delegated powers will allow swift implementation, through secondary legislation, of technical aspects of new agreements with international partners. This approach provides legal and operational certainty to UK operational partners and ensures that the required international agreements have a basis in UK legislation. This will enable the UK to implement new alert-sharing arrangements with close international partners.

356. The ‘do nothing’ option for the I-LEAP proposal in this IA represents the lack of delegated powers to pass secondary legislation to enable new alert-sharing agreements.

[180] Annual Survey of Hours and Earnings (ASHE) - Guide to tables - Office for National Statistics (ons.gov.uk)
[181] Statistics | Eurostat (europa.eu)

357. Costs and benefits for this proposal will be taken from the I-LEAP full business case.[182] This business case calculated costs and benefits relative to a 'do nothing' option which represents not implementing I-LEAP.

358. This means that the 'do-nothing' option represented in this analysis is different to the 'do-nothing' option in the full business case.

359. The analysis also assumes that I-LEAP would be implemented through bilateral agreements, however, the focus is now on completing an agreement with the European Commission.

360. These differences mean that the costs and benefits taken from the full business case should be seen as an indication of scale, rather than direct estimates of the impacts of the I-LEAP proposal in this analysis.

361. The costs and benefits outlined **will not be included** in the total NPSV or costs and benefits summary.

362. Capital costs include all costs related to the build of I-LEAP. These are expected to apply for the first three years and amount to a total of £29.9 million (2021 prices).

363. Resource costs represent the annual sustainment and running costs for maintaining I-LEAP. They are estimated at £23.9 million (2021 prices)

364. Total costs including risk, optimism bias and discounting amount to £61.7 million (2021 prices)

[182] Home Office Internal Estimates

Direct Costs - Non - Monetised

365. This section of analysis provides a breakdown of all non-monetised costs that UK businesses and public organisations could face as a result of this package of reforms.

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

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

Subject Access Requests (SAR)

367. A data subject can exercise their right to request what information is held about them through a SAR. Currently all SARs under Part 3 (Law Enforcement) and 4 (Intelligence Services) need to be actioned within one month. Unlike the UK GDPR, Parts 3 and 4 of the DPA 18 do not recognise and allow for a proportionate time period for dealing with particularly complex requests. The proposal is to mirror an existing UK GDPR provision within Part 3 and 4 of the DPA 18 that permits a two-month extension to a SAR time period when a request is particularly complex.

368. The UK Intelligence Services and National Crime Agency (NCA) expect that there will be little actual change regarding costs associated with processing SARS. This is because SARs will still be processed, regardless of how long it takes, so a two-month extension for complex SARs will not result in an increase in ongoing costs.

369. It is assumed that this response from the UK Intelligence Services and NCA is representative of all competent authorities

Introduce a power to allow bodies representing Part 3 controllers and processors to produce 'Codes of Conduct'

370. In the UK GDPR codes of conduct can be produced by representative bodies (for example, trade associations) to clarify the application of data protection laws in particular sectors, which are then approved by the ICO. There is no equivalent power under Part 3 DPA 2018 and stakeholders have indicated that this could be a useful tool to future-proof their data use. This proposal aims to expand it to the law enforcement sector enabling similarly representative bodies to create codes of conduct for Part 3 under the purview of the ICO.

371. This is permissive legislation, as it proposes to give bodies representing LEAs the ability to produce codes of conduct but does not mandate it. These bodies should only engage in this activity if they deem the costs greater than or equal to the benefits. It is assumed that this proposal will result in a 'no worse than zero net cost' to LEAs.

372. There will be higher efficiency costs imposed on the ICO if representative bodies decide to take advantage of newly granted powers as the ICO will have to approve any new codes of conduct.

373. There will be an additional cost to LEAs of representative bodies introducing codes of conduct as this will require their employees to familiarise themselves with new data protection rules.

374. There will be increased efficiency costs associated with the drafting of codes of conduct for the representative bodies who decide to undertake this.

375. There is also nothing to stop an organisation from voluntarily adopting a code issued by another body which may reduce the overall set-up costs of this proposal.

376. This may, however, lead to a ‘free-rider’ problem where organisations have reduced incentives to expend resources to create their own code of conduct if they believe other bodies will do so for them. This may provide a disincentive to be a ‘first mover’ in creating a code of conduct.

377. The ICO will also have to approve new codes of conduct which will create an additional efficiency cost as ICO employees will have to dedicate their time to approval processes. This cost will depend on the number of representative bodies who decide to introduce codes of conduct.

378. Representative bodies who decide to introduce codes of conduct will be expected to put in place monitoring processes to ensure that the new rules are followed. The time spent by employees on doing this will be an additional cost.

379. Monitoring will have to take place on an ongoing basis and more employee time will have to be spent on this. This will result in greater efficiency costs.

Amendments to Part 4 of the DPA 2018 - National Security Notices

380. Currently, policing and the intelligence services are governed by different data protection regimes which present challenges to joint operational working.

381. UK Intelligence Services believe that this proposal will lead to more dynamic working practices with police, such as the option to share databases. It should also lead to improved confidence in sharing data.

382. There will be additional administration requirements on data controllers which will increase costs. This will be limited by the fact that this proposal will only take effect in very limited circumstances.

Improved Interoperability across Health and Social Care Systems

383. The proposals outlined are for enabling powers only and it is therefore not possible to robustly quantify what, if any, burden may be imposed on suppliers or providers at this point. This means that the full impacts cannot be accurately appraised at this stage because of significant uncertainty regarding the timing of any use of the powers and the content of any commencement regulations and/or further regulations or exemptions.

384. It is therefore also not possible to provide an Equivalent Annual Net Direct Cost to Business (EANDCB) at this stage. However, where possible, this impact assessment qualitatively assesses the impacts of these measures and provides an indication of the likely scale of impact. A full and robust assessment of the impacts, including an EANDCB will be produced as part of commencement regulations and/or regulations (secondary legislation stage) once the details of how the powers will be used are finalised.

385. We have provided an indication of the likely scale of impacts on these businesses in line with RPC guidance. Evidence at this stage is limited and therefore indicative, work is continuing on the refinement of these estimates and this will be presented in more detail at the commencement regulations and/or regulations stage. It is important to note that any additional costs to businesses will be minimised when exercising these powers through phasing in the new standards over a proposed period of 5 -10 years.

386. To provide an indication of the impact on businesses, the two central enabling aspects of the proposal have been separated:

i) A power for the Secretary of State for Health and Social Care to prepare and publish standards for IT products and services used in the health and adult social care sector in England and will require the suppliers of the products to comply with these standards.

ii) A power to establish and operate a voluntary accreditation scheme (accreditation of products and services). IT suppliers can opt-in to the scheme by demonstrating that their products or services meet or exceed the standards required to be compliant (i.e. demonstrate that their products/services are of a ‘superior’ quality, where open data architecture is concerned)

387. The potential direct costs of the first part of the reforms are outlined in the table below:

Table 45: Direct costs of the proposal

Stakeholder group	Anticipated cost	Cost type
IT suppliers	We anticipate that there will be reconfiguration costs for some suppliers who seek to modify their products and services so that they can meet the new standards to supply products and services to health and social care commissioners and providers.	Cost to business (Direct)

388. Through taking a phased approach to implementation, we plan to minimise additional costs to suppliers and there may also be some exemptions for particular types of suppliers, products and/or services.

389. Currently the NHS spends about £27 billion every year on goods and services. There are approximately 193[183] accredited/assured suppliers of sector specific IT-related products and services to the health and care system. As an example, 8 of these supply enterprise-wide EPRs to acute, community and mental health hospitals. The majority of these firms are large and well-established - 5 out of 8 of the accredited EPR suppliers listed are large firms with over 250 employees.[184]

390. The cost of reconfiguration to each of the IT suppliers is highly uncertain at this stage and will depend on the details of the standards set, the type of supplier (as not all suppliers will provide IT products or services that are scope), and the size of the supplier.

391. Costs are likely to be incurred in the following areas (all of which relate to updating systems and processes in line with open data standards):

a. The completion of frameworks

b. Introduction of new or updating existing IT software and equipment

c. Increase in staff employment

d. Increase in staff training

e. Additional risk assessments and audits

392. Evidence from the Health and Social Care Bill suggests that these costs usually scale with size with small businesses facing less of a reporting burden. The overall scale of these costs will depend on the size of the supplier, the infrastructure and frameworks already in place. Further analysis of the characteristics of these firms will take place at the commencement regulations and/or regulations stage.

393. As at this stage, we will use examples from other markets that have undergone similar regulatory changes to establish and estimate the potential scale of these costs to IT suppliers.

394. Firstly, using evidence from the midata impact assessment analysis, [185] which assesses the cost implications of its similar (though more limited) proposal for increasing data mobility. This policy is aimed at correcting the information asymmetry between consumers and businesses where firms collect data about their customers' transactions but do not make it easily available to them. This information asymmetry also exists in the health and social care IT sector. Health and social care providers have difficulty accessing data as it is held across multiple systems with different architecture. Furthermore, IT suppliers are often entitled to charge additional fees for proprietary solutions to overcome technical barriers to providers appropriately accessing and sharing information held within such systems.

395. Similarly, to the healthcare IT sector, data shared between businesses and consumers in other sectors is often not provided to a common standard that makes comparison easy. It was

[183] NHS (including acute, community and mental health hospitals) - 176 IT-related accredited suppliers - Source: https://www.england.nhs.uk/hssf/supplier-lists/ ; Adult Social Care - Digital Social Care Records only - 8 assured suppliers - Source: Assured Supplier List - Digital Social Care. NHS Primary Care - 10 (however 1 supplier has been captured in the other NHS figures) - Source: Internal NHS figures for GPIT Futures Programme. This is not an exhaustive list figure for suppliers of IT products and services to all parts of the health and adult social care system in England (e.g. dentistry and optometry), nor does it include all types of IT products and services supplied to the health and adult social care system in England.

[184] Where a reliable estimate for the number of employees could not be found for the UK subsidiary - the figure for the parent company was used instead.

[185] https://www.legislation.gov.uk/ukia/2013/1048/pdfs/ukia_20131048_en.pdf

argued in the midata Impact Assessment that the private sector could, in principle, provide a standard, however without government intervention this may not happen, which is also the case in the healthcare IT supplier market. The preferred option outlined in the midata Impact Assessment is therefore, to give order making power for the Secretary of State to compel suppliers of goods and services to supply to the consumer, at their request, their transaction data in a machine-readable format.

396. As part of the midata proposal, businesses are therefore expected to make investments in their IT infrastructure to ensure that data is stored in an electronic and machine-readable format. This includes:

a. Designing a user interface

b. Investment in IT hardware to present information in a secure manner

c. The installing, commissioning and testing of the facilities system

d. Ongoing/administration costs to business for making data available to customers, such as updates to internal IT strategies and maintenance costs of the infrastructure.

This is in line with the change's IT suppliers are expected to undertake as part of these proposals in this IA. Given these business actions relate to comparable changes to comparable IT systems, they provide an indication of the scale of impact. For these reasons, the unit costs are likely to be similar for the IT suppliers in scope.

397. Although the number of businesses impacted by the midata proposals is on a much larger scale than those currently operating in the healthcare IT sector we assume the reconfiguration costs for firms will be similar due to the nature of the changes to supplier's infrastructure needed and the similarities between policies. However, we intend to determine estimates of reconfiguration costs through a subsequent IA.

398. Evidence on the potential costs of the midata policy was collated through business surveys, engagement and roundtables, on the implementation and ongoing costs of proposed data mobility initiatives. The markets considered were retail, personal current accounts, energy and mobile contracts. All of these markets have attributes similar to that of the healthcare IT sector, in that data sharing in a standardised way and format was lacking.

399. In aggregate, the total equivalised annualised cost to business for implementation and ongoing compliance were estimated to range from £1.3 million for energy, up to £1.9 million for mobile contracts[186] (2012 prices). Where businesses already collect the data in the relevant form the additional costs will be low. However, costs were higher in cases where more changes are needed to be made to IT infrastructure.

400. These estimates were derived assuming that data is provided on a one-off basis within the midata proposals of 40-day response times for data portability, with the analysis highlighting that instant access would substantially increase the cost. For the healthcare IT supplier market, we assume that the majority of the costs relate to reconfiguration of products or services that will then be supplied to health and social care providers. We also assume there

[186] These are 2012 prices and whilst they provide an indication of the scale of impact they are likely to differ from the costs associated complying with the open data architecture measure, given inherent differences in the markets/industries concerned, and the time that has elapsed since the 2012 analysis was undertaken.

will be no ongoing costs relating to requests for data to be shared from supplier to provider. Instead the sharing of data would be between providers within the health and social care system, which we also assume would be multiple and instant. We assume that this would not incur a 'cost-per transaction' given that the systems holding the data would be designed in a way to facilitate such ongoing access.

401. In line with the midata Impact Assessment it is assumed that 15% of firms in scope of the proposal would already have the correct architecture in place and would not face any initial reconfiguration costs. We assume that this would also be the case in this IT supplier market where some IT suppliers may already have the necessary capabilities, though the exact number will be established through research at the secondary stage. The midata assessment estimated that 210,200 UK businesses were in scope and that 16 of the largest businesses would deal with over 100 million data requests in total. In the healthcare IT supplier market, around 193[187] businesses are in scope and would, due to the nature of the proposed changes, be dealing with less direct data requests than those in the midata example.

402. The impact assessment accompanying the DWP Pensions Dashboard primary legislation can also be used as an example to help estimate the scale of the impacts of these reforms on IT suppliers.[188] The Pensions Dashboard measure seeks to enable citizens to securely access their pensions information online, to support better planning and preparation for retirement. It aims to do this by introducing legislation to compel pension providers to make certain data available to members via dashboards. Primary legislation is used to introduce necessary powers to set out the conditions of a qualifying dashboard service.

403. Although healthcare IT suppliers are not required to supply their data for a specific dashboard they will be required to use common architecture so that data can be accessed as easily by care providers. In both cases, businesses are therefore expected to carry out actions such as dedicating time to familiarise themselves with the legislation, investment in IT infrastructure so that data is accurate, cleansed where necessary, digitised, calculated and in an appropriate format, and ongoing maintenance and updates to ensure standards are maintained. Given these actions relate to comparable changes to those in the healthcare IT system, we believe they provide an indication of the likely scale of impact and that unit costs are unlikely to be significantly different for IT suppliers as part of these proposals. We therefore believe this policy also provides a useful example of the potential scale of the costs to suppliers of employing standardised data architecture.

404. DWP's analysis considers understanding, implementation and ongoing costs (relating to providing data, annual regulatory compliance and governance), segmented by the size of provider and contingent on the scope of data to be included in the initiative. These are outlined below:

    a. Familiarisation costs: There will be costs for the pensions industry to familiarise with new requirements. Illustrative costs are provided for familiarisation costs (£2m in year 1 only).

[187] Based on accredited and/or assured suppliers to certain parts of the health and adult social care sector only. This figure does not represent all suppliers of IT products and services to all parts of the health and adult social care sector.
[188] https://publications.parliament.uk/pa/bills/lbill/2019-2019/0005/20005-IA-Summary-of-Impacts.pdf

b. Implementation costs: We expect material costs for pension schemes and providers to invest in new software/IT architecture to be able to provide data to the dashboard(s).

c. Ongoing costs: To provide data, ongoing governance, and regulatory compliance on an annual basis.

d. One-off implementation costs and ongoing costs are estimated under three scenarios with different data requirements and coverage to highlight the potential range of impacts. Estimated one-off implementation costs range from £200m to £580m over 10 years and ongoing costs range from £245m to £1.48bn over 10 years.

405. Whilst the Pensions Dashboard will require firms to adhere to legislation similar to that being proposed in this IA, there are thousands of pension suppliers, compared to the tens of IT suppliers in this market, meaning the costs are likely lower than those presented above. It is also likely that, for these Open Data Architecture proposals, some of the costs to IT suppliers may have already been factored into their development budgets, and therefore are not brought about solely due to the legislation and would be incurred anyway.

406. Based on the two comparable smart data initiatives, direct costs to business of changing systems to meet the required standards are expected to be within the estimated ranges of the midata and the Pensions Dashboard examples. The intention is to take a phased approach to implementation of the standards to minimise costs to businesses. Subsequent impact assessments supporting secondary legislation will provide a robust assessment of the impacts of this measure.

407. There may be some exemptions for particular types of suppliers, products and/or services however, until the exemptions have been finalised, it is not possible to give a comprehensive assessment on the scale of impact of this aspect of the measure on businesses.

408. Throughout this assessment we assume that there will be 100% compliance with the proposed legislation, that is to say that all IT suppliers will where necessary make the required changes to systems. However, when the commencement regulations and/or regulations are implemented, we acknowledge - as with all regulations - some suppliers may receive fines for not meeting the standards set. Details on the size of fines and the process of enforcement is as yet undetermined and will be set out in subsequent secondary legislation supported by future impact assessments.

409. There may be enforcement costs associated with non-compliance. The potential cost to in-scope businesses of receiving fines or penalties for non-compliance is excluded from the business impact target under administrative exclusion G for the current parliament. This is because we do not have any evidence there would be any meaningful level of non-compliance and therefore, consider the assumption of 100% compliance to be reasonable in this case. To provide an indication of the likely scale of impact, while the details of fines are currently unknown, the size of these fines are likely to correlate to the scale of non-compliance and size of business. Evidence from the Information Commissioner's Office average levied fine following the introduction of GDPR was £143,000 in 2018/19. [189]

410. There is the potential that firms could either be unable or unwilling to meet the minimum standards of compliance to remain in the market. Where this is the case we would expect

[189] https://www.rpc.co.uk/press-and-media/average-ico-fine-jumps-14-percent-in-a-year-in-the-wake-of-gdpr/

these firms to exit the market. This could be due to the size and costs of the changes needed to be made to IT infrastructure and processes. In the long run however, we would expect an increase in market competition and innovation.

Indirect Costs - Monetised

411. This section of analysis provides a breakdown of all indirect monetised costs that UK businesses and public organisations could face as a result of this package of reforms, specifically the creation of robust and secure smart data schemes and the Increased Interoperability and Trust of Digital Identity Systems.

Increased Interoperability and Trust of Digital Identity Systems

412. More detail on the calculation of the monetised costs of the proposed Digital Identity reforms can be found in the published Digital identity and attributes - De Minimis Assessment.[190] In this Data Protection and Digital Information Bill Impact Assessment we provide an outline of costs of the proposal. This analysis looks at the same four potential use cases measured in the benefits section.

413. All costs to business are indirect because the legislation only allows public sector organisations the option to open their data for private sector use. It does not mandate anything for private sectors companies to do, not even when it comes to familiarisation. As a result of the legislation being permissive, these estimated costs are not included in the NPSV or EANDCB of the bill.

414. More detail on the calculation of the monetised value of potential costs of the proposed Digital Identity reforms can be found in the published Digital identity and attributes - De Minimis Assessment.[191] In this Data Protection and Digital Information Bill Impact Assessment we provide an outline of the main monetised costs of the proposal. This analysis looks at the same four potential use cases measured in the benefits section;

a. Employee mobility
b. Travel authorisation and ticketing
c. Home buying
d. Trusted financial transactions

and compares the benefits across the 3 different scenarios (central, best and worst case) and both the costs to both private and public sector organisations.

415. DCMS carried out a stakeholder engagement exercise to attempt to define the indirect costs[192] businesses may face compliance with the legislation, both for digital identity as a whole and in relation to the four specific use cases. We engaged with a variety of sectors. Multiple responses came from organisations that currently operate within the digital identity sector, such as identity service providers, or relying parties that would use the digital identification system. Other responses came from various different sectors. The organisations that took part ranged from micro to large businesses. The engagement enabled us to make some qualitative and quantitative assumptions of what costs businesses may face to familiarise and adapt to the digital identity legislation.

416. The quantitative estimations were then used to model the costs under the three scenarios. Due to the early stage of the legislative planning, it was difficult to precisely estimate what

[190] Digital identity and attributes - De Minimis Assessment DCMS, 2021
[191] Digital identity and attributes - De Minimis Assessment DCMS, 2021
[192] All costs to business are indirect because the legislation only allows public sector organisations the option to open their data for private sector use. It does not mandate anything for private sectors companies to do, not even when it comes to familiarisation.

costs businesses are expected to incur. Nevertheless, we expect these costs to be rather small especially for digital identity providers already established in the market as they believe they are expected to undertake limited development work to adapt to the legislation.

417. We assume that only UK medium and large businesses face the costs to adapt to digital identity because their incentive from the potential cost savings allowed by digital identity are expected to outweigh the costs to adapt to the new technology 30. Therefore, the estimated costs per business were multiplied by the number of medium-large UK businesses to estimate what the costs may be for all businesses as a whole.

418. We assume that the size of the total per check fees costs follows the estimated trend of the digital identity market towards the steady state. This is because we expect the number of digital identity checks carried out in the UK to be proportional to the size of the market.

419. Focusing solely on one-off costs to private sector businesses of the proposed changes to digital identity schemes across all use cases, include:

a. **One-off familiarisation costs for businesses:** the costs businesses expect to face to familiarise with the potential digital identity legislation based on the estimations provided by the stakeholder engagement exercise

b. **One-off organisational change costs for businesses:** Organisational change costs consider the costs businesses face to adapt the structure of the organisation, both in terms of how it functions and the staff employed. Examples include the cost to implement a digital identity solution, the cost to hire new staff, or the costs to purchase or change technology platforms.

c. **One-off connection fee for service providers:** We assume that organisations wishing to perform checks against government-controlled data may have to pay a one-off fee upfront

d. **Certification fee for service providers:** We expect service providers to pay a certification fee to be certified against some given standards.

e. **Annual membership fee for service providers:** We expect certified service providers to pay the governance function an annual membership fee.

420. As well as one off familiarisation costs, we assume that UK businesses wishing to make digital identity checks against government-held databases may have to pay an annual fee in order to carry out each check Therefore the annual cost of per check fees for businesses have been estimated for each use case. We calculate this annual cost as the annual total expected number of checks times the expected price per check which varies depending on the type of identity check.

421. The estimated cost of these checks will vary depending on the type of check, the scenario (time taken for adoption for each use case) and the estimate of the total number of checks for each type of request. More information on these assumptions can be found in table 19 of the Digital identity and attributes - De Minimis Assessment.[193] The total estimated costs for each use case are in the table below alongside the total one-off costs.

[193] Digital identity and attributes - De Minimis Assessment DCMS, 2021

422. The estimated total costs include the estimated total cost of the per check fee for all four use cases, one-off familiarisation costs, one-off organisational change costs for the relying parties and one-off total connection fees and membership fees for service providers. The central estimate of the undiscounted costs to UK private sector organisations is £1,449.8m over the 10-year appraisal period. We estimate that the lower and upper bound of the total undiscounted costs all medium and large businesses together may face over the appraisal period are £822.6m and £2,631.6m respectively.

Table 46: Estimated total costs of Digital Identity reforms by scenario and cost, 2021 prices

£, millions	Central estimate		Best estimate		Worst estimate	
	Annual estimated costs, £, millions	Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)	Annual estimated costs, £, millions	Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)	Annual estimated costs, £, millions	Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)
Employee mobility: per check fee costs	4.9	31.5	3.0	21.9	9.8	46.2
Travel authorisation and ticketing: per-check fee costs	64.9	454.3	38.9	311.5	129.8	675.0
Home buying: per-check fee costs	2.2	15.5	1.3	10.7	4.4	23.1
Trusted financial transactions: per-check fee costs	0.2	1.5	0.1	1.0	0.4	2.2
One-off familiarisation costs		227.7		113.9		455.4
One-off organisational change costs		710.2		355.1		1,420.4
One-off connection fees cost for service providers		0.6		0.4		0.7
Certification fees cost for service		3.5		3.6		3.4

providers						
Annual membership fee for service providers	0.6	5.0	0.5	4.6	0.6	5.1
Total, £, millions		1,449.8		822.6		2,631.6

423. A breakdown of the monetised costs for public sector organisations can be found in the Digital identity and attributes - De Minimis Assessment. DCMS engaged with three public bodies to try and estimate the costs[194] public organisations may pay to adapt to the potential digital identity legislation and thus allow the digital identity market to fully develop. For instance, we gathered some information on the potential costs public sector bodies may face to understand the legislation or make the organisational changes required to allow the private sector to check the databases they hold. We expect public sector organisations to face some rather significant costs to adapt to the legislation, especially to allow the private sector to make checks against the Government-held datasets.

424. We define the worst case estimate as the scenario based on the assumptions that lead to the highest expected costs. We predict high costs for all public sector bodies in a high digital identity uptake scenario where more Departments invest resources to familiarise and adapt to the digital identity system. In order for digital identity to fully develop a high uptake across public sector bodies is required. Therefore, the worst-case cost estimate is not necessarily unwelcomed.

425. For the worst-case scenario, we have assumed that all departments that may hold significant identity or eligibility data, 9 in total,[195] will face these costs. For the central and best-case scenario, we have assumed that only Home Office, DVLA, DWP, HMRC, and DfE[196] in line with the four digital identity use cases analysed.

426. Based on our assumptions we estimate that, on average, public sector bodies may face a one-off cost of £43,637.0 to ensure that members of the policy teams familiarise with the legislation. However, these are rough estimates based on a small sample size so should be considered indicative only.

427. Total one-off estimated familiarisation costs for public sector organisations can be seen in the table below:

Table 47: One-off public sector familiarisation costs, 2021 prices

	Estimated one-off familiarisation costs per Department, £	Number of Government Departments	Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)

[194] All costs to Government bodies are indirect because the legislation only allows public sector organisations the option to open their data for private sector use. It does not mandate anything for public sector organisations to do.
[195] The 9 Departments are: Home Office, DWP, HMRC, DVLA, DfE, HM Land Registry, DHSC, Companies' house, and MoJ.
[196] These are the Departments that are required to open their databases in order for digital identity checks to be carried out in the four use cases.

Central case estimate	43,637.0	5.0	0.2
Best case estimate	43,637.0	5.0	0.2
Worst case estimate	43,637.0	9.0	0.4

428. Additional indirect costs estimated for public sector firms also include:

a. **The cost to allow private sector access to Government-held datasets for public sector organisations:** we expect Government Departments to face costs both to allow the private sector to make checks against their data and to maintain the system in place. The costs estimated in the analysis are baseline and in practice will be subject to iteration. Further examples of these costs can be found on page 41 of the Digital identity and attributes - De Minimis Assessment DCMS, 2021. [197]

b. **Cost to set up and run a governance function:** The digital identity market may function in a trusted and interoperable way conditional on the fact that there is an effective governance function overseeing the market. For instance, we expect the governance function to ensure trust in the market by checking that the members of the Trust Framework meet the required standards. Therefore, we assume that without functioning governance the benefits of a fully functioning digital identity market may not be realised.

429. We estimate that, based on our assumptions, the costs public sector bodies may face over the appraisal period to fully realise the digital identity market may range from £149.87m to £505.28m. The central case estimate for the estimated public sector costs is £149.87m.

Table 48: Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)

	Estimated costs over the 10-year appraisal period, £, millions, (undiscounted)		
	Central case estimate	Best case estimate	Worst case estimate
One-off familiarisation costs	0.2	0.2	0.4
Organisational change costs	138.5	138.5	498.7
Governance function funding costs	11.1	35.6	6.2
Total, £, millions	149.9	174.4	505.3

430. The central estimate of the undiscounted costs to UK private and public sector organisations is £1456.2m over the 10-year appraisal period. We estimate that the lower and

[197] More information on how this is calculated can be found in the Digital identity and attributes - De Minimis Assessment DCMS, 2021

upper bounds of the total undiscounted costs all organisations together may face over the appraisal period are £853.8m and £2632.0m respectively.[198]

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

431. This section of analysis has been provided by the Home Office. Data on the volume of births and deaths and the scenarios used in the modelling can be found in table 31. Gross wage of superintendent registrars and registrars can also be found in table 32.

Set up Costs

IT set up costs

432. The Home Office will update RON functionality to accommodate a move to the electronic register for births, still births and deaths. This cost is estimated at £71,000 based on the requirements identified which are similar to recent changes to the IT system for other services. Based on the uncertainty surrounding this figure and the fact it is an IT cost, optimism bias has been applied (0%, 25%, 50% for the low, central and high scenarios). The low estimate is about £0.07 million, the central estimate is about £0.09 million and the high estimate is £0.1 million.

Set up cost to registration service (Closure of open registers)

433. There will be a cost to the registration service of closing the current birth and death registers in year 1 only. Each of the 782 registrars of births and deaths for England and Wales holds an open birth and an open death register. This means that a total of 1,564 registers (taken from secure stock records held by GRO) will need to be closed. A low, central and high length of time taken is estimated at 4, 5 and 6 minutes. The gross wage per hour is outlined in baseline volumes (see Table 2), for a registrar. The estimated cost is in the range of £2,100 to £4,800, with a central value of £3,100 in year 1 only.

Home Office set up cost

434. Changes to processes are minimal therefore face-to-face training for the registration service will not be required. The Home Office will issue new guidance for registration officers together with instructions for the closing of current birth and death registers. The cost of providing written guidance is minimal and is included within business as usual costs so has not been included for the purpose of this IA.

Ongoing Costs

435. The current process in which the superintendent registrar checks and certifies all birth and death entries will be replaced by a quality assurance check of the records. For the purpose of this IA it has been assumed superintendent registrars will complete a quality check of 20 percent of all births and deaths registered by registrars. This check is likely to take less time than the old certification process which involved the superintendent registrar retrieving the register from a locked safe and then cross-referencing all parts of the register entry to be sure that the information from the register has been correctly keyed into the electronic RON system. This new quality check will take approximately one minute of a superintendent registrar's time

[198] More information on how this is calculated can be found in the Digital identity and attributes - De Minimis Assessment DCMS, 2021

for each birth, still birth or death registration. 0.75 minutes are taken as a low scenario, and 1.25 as a high scenario. This is calculated as: time (hours) taken to check entries x cost per hour of superintendent registrar time (see baseline volumes) x number of births and deaths per year. This gives costs in the range of £0.8 to £1.7 million, with a central estimate of £1.2 million (PV) over 10 years.

Table 49: Summary of impacts, (£ million, 10-year present value), 2018/19.

Costs (£ million, PV)	Low	Central	High
IT (one off costs) (GRO)	0.1	0.1	0.1
Closure of open registers (LRS)	0.0	0.0	0.0
Superintendent checks (LRS)	0.8	1.2	1.7
Total	**0.8**	**1.3**	**1.8**

Indirect Costs - Non-Monetised

436. Where indirect costs to businesses and the public sector cannot be monetised due to a lack of historical evidence we have provided an in-depth qualitative analysis alongside other government departments.

Creation of robust and secure Smart Data schemes

437. This analysis was led by BEIS as part of the published Smart Data Impact Assessment. For a more detailed breakdown of these costs and benefits please refer directly to the Smart Data Impact Assessment.

438. Minimal direct costs would be incurred from the primary legislation; instead, direct costs would occur when the Smart Data powers are put into practice via secondary regulations. Our analysis focuses on the indirect implications of bringing forward the costs of implementing the schemes and additional years of costs when the schemes are operational. Within the Impact Assessment indicative estimates, based on Open banking costs, have been produced for the indirect costs of expediting the implementation of a telecommunications Smart Data scheme.

439. When Smart Data schemes are introduced via secondary regulations, there will be costs incurred to operationalise the schemes successfully, and to ensure adequate regulatory oversight. These costs will initially fall on the sector regulator, or any other administrator, who will be named in the secondary regulations as responsible for specific roles. Resources to cover the costs incurred by regulators and scheme administrators will not come from central government, and instead they will be recouped from industry via charges or using the sector regulators existing levy raising mechanisms.

440. The costs incurred from Smart Data can therefore be separated into two categories:

a. Costs incurred by regulators and scheme administrators which are then recouped from industry via charges and levies (referred to in this IA as ‘implementation costs’);

b. Costs incurred directly by data holders and TPPs to participate in the Smart Data scheme

441. As discussed throughout this IA, due to several uncertainties, it is not possible to isolate or predict the costs of potential future Smart Data schemes. The full impacts of future smart data schemes would be detailed and analysed when these specific schemes are introduced in secondary legislation.

442. However, to give an indication of the costs that could arise from further data sharing schemes, and the impacts that there could be as a result of expediting their implementation, the costs of Open Banking have been used as the basis for estimating the associated costs for other smart data schemes in the BEIS Impact Assessment. We would expect the ‘implementation costs’ for future schemes to be lower than those incurred by Open Banking as a result of technical differences between schemes, and learnings from Open Banking.[199]

443. For a more detailed breakdown of these indicative costs please refer directly to the BEIS Smart Data Impact Assessment.

[199] Ofcom (July 2021): “Statement: Update on Open Communications: Enabling people to share data with innovative services”

444. As stated above, we do not expect any direct costs from the delivery of primary legislation alone. The following table sets out some of the potential costs that could emerge at the secondary stage, following the introduction of a sector scheme. This analysis builds on the experience of Open Banking (as the only live Smart Data scheme), and considers wider evidence from the finance, telecommunications, energy, and pension sectors.

445. Various groups could see costs from the introduction of Smart Data. These include regulators/other scheme administrators, data holders and data recipients (TPPs).

446. Further discussion and evidence on the costs of Smart Data can be found in the Impact Assessment.

Table 50: Summary of non-monetised costs of Smart Data regimes

Regulators/Other scheme administrators	Data holders	Data recipients – third party providers
Regulation and enforcement of Smart Data schemes.	• Initial implementation of Smart Data scheme. • Familiarising employees with regulations. • Upgrading or improving technical and system infrastructure • Ongoing costs to comply with regulations.	• Familiarising employees with regulations. • TPPs face the cost of accreditation, to be authorised to handle and use customer data. • Setting up and running technical infrastructure e.g. APIs and customer interface.

NOTE: Smart Data schemes are intended to be self-financing and should not require funding from existing government funds. TPPs will not be mandated to participate in a Smart Data scheme, therefore any costs that they incur will be at their own discretion.

Increased Interoperability and Trust of Digital Identity Systems

447. More detail on the calculation of the non-monetised costs of the proposed Digital Identity reforms can be found in the published Digital identity and attributes - De Minimis Assessment.[200] In this Data Protection and Digital Information Bill Impact Assessment we provide an outline of costs of the proposal. This analysis looks at the same four potential use cases measured in the benefits section.

a. Employee mobility

i. We expect businesses to face some costs to adapt their organisation in order to carry out real-time digital verification for DBS, RTW and employability checks. For instance, businesses may be required to set in place a platform which determines the requirements based on nationality and work location. Consequently, new hires may be invited to complete a self-service right to work check and may be able to provide the necessary attributes through a digital identity service to complete the checks. We expect businesses wishing to use digital ID checks to carry out these checks to have

[200] Digital identity and attributes - De Minimis Assessment DCMS, 2021

to pay for the required platform. The payment will most likely be on a subscription basis but were unable to estimate these ongoing costs at this early stage.

b. Travel authorisation and ticketing

   i. Verifying passport data when booking a flight and reducing in-journey ID verification

      1. We expect businesses to shoulder costs to use digital identity to reduce in-journey ID verification. For instance, businesses may need to integrate a remote identity verification solution through a platform that passengers may use to submit their passport details for real-time verification. We expect businesses to outsource the required platform and pay it on a subscription basis, therefore creating an ongoing cost for the business. However, we are unable to estimate what these costs may add up to at this early stage.

   ii. Costs to align with industry initiatives on passenger identification (e.g. ICAO's OneID)

      1. We also expect businesses to take actions to align with industry initiatives on passenger identification to streamline the journey of passengers by creating an interoperable system between airports, airlines and governments. We are currently unable to estimate what these costs may add up to.

c. Home buying

   i. Cost to extended ID verification to witnesses

      1. We assume businesses may have to take actions to extend remote ID verification to witnesses to facilitate identity proof throughout the home buying process, where necessary. Currently, the real estate market relies significantly on witness proofing, which in turn may require the identity verification of the involved witnesses. Unless the steps taken to digitise the identity verification system of the home buyers is extended to witnesses, the market will be unable to fully function digitally and the benefits of using digital identity will not be maximised. We are unable to predict such costs at this early stage.

      2. It is also possible that the requirements for witnessing certain deeds may change in future. In particular the use of Qualified Electronic Signatures, in conjunction with the digital identity trust framework, is something which can be explored further as a means of replacing existing requirements for witnessing.

   ii. Reducing friction in the home value chain

      1. We assume that businesses may have to adapt the ID checking process required throughout the entire house buying process to the digital identity verification system. We believe that these steps are essential in order to use digital identity across the multiple identity verification process required throughout the home buying process. Unless all identification steps are digitised, the real estate market will not be able to fully function using digital identity.

      2. Businesses are expected to face costs to create and maintain the system for any potential platform required to remove the friction in the home value chain.

Businesses may incur costs to adapt to closing contracts digitally. However, due to the level of uncertainty we are unable to estimate these costs.

d. Trusted financial transactions

   i. Businesses may pay to adapt their organisation in order to digitally prove the identity of customers throughout financial transactions. Businesses may either outsource or build and maintain the platform in-house. However, we are currently unable to estimate what these costs may add up to.

448. A breakdown of the non-monetised impact on the **public sector** can be found in more detail in the Digital identity and attributes - De Minimis Assessment.[201]

Delivery of better public services

Impacts of changes to the Digital Economy Act - CDDO

449. The below section is based on analysis by the Central, Digital and Data Office.

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

451. As there are few examples of where this data has been shared between departments previously, this means that the evidence base for the analysis of costs is currently limited. As a result, we are only able to provide a qualitative assessment of the impacts of this primary legislation reform.

452. There will be little or no direct costs of the extension of data sharing powers. The impacts will be experienced when public authorities utilise these powers to share data in order to support government services for businesses.

453. The table below provides high level quantitative analysis of the potential costs of the reform for both private businesses and the public sector. More analysis will be provided at a secondary legislation stage when data sharing powers are enacted.

Table 51: Summary table of costs of changes to the DEA 2017 by recipient

	Costs
Businesses	**One-off administration costs:** There may be a one-time sign up process for businesses, implying a small administrative cost in order to complete this process.
Government	**Policy-related costs of data sharing:** There will be a cost associated with creating the legal framework that is required in order for data sharing to occur between departments. This process requires the support of policy advisors and analysts, an element of which may be ongoing. **Technical costs enabling data sharing:**

[201] Digital identity and attributes - De Minimis Assessment DCMS, 2021

	Once the legal framework for data sharing is in place, there will be a cost associated with the overhauling of legacy systems. Data technicians would be required to create the cross-government data sharing mechanism. An element of this cost will be ongoing in order to maintain and improve data sharing infrastructure.

Empowering the police to use new technologies like biometrics (HO)

454. This section is based on Home Office analysis. Where evidence is unavailable costs have been assessed qualitatively.

Oversight Reform

455. This proposal seeks to substantially simplify the oversight framework for the police use of biometrics and overt surveillance. Feedback from the consultation and analysis undertaken by the Home Office highlighted the duplication between the remit of the ICO and the SCC. As the ICO already covers the statutory remit of the SCC. The proposed changes will not add to the ICO's list of statutory duties. There is also significant overlap between the ancillary functions of the SCC and current activities undertaken by the ICO into surveillance systems. However, there are certain projects that the SCC has led on, such as the third-party certification for surveillance camera systems, which, if taken forward by the ICO, could potentially increase the ICO's workload in this area, but it is assessed that any additional costs would be minimal.

456. The Home Office intends to transfer the casework functions of the Biometrics Commissioner to the Investigatory Powers Commissioner (IPCO), which will result in some increased costs to the IPCO to manage these processes. It is expected that any change would be cost neutral as resources would be transferred from the Biometrics Commissioner's Office to IPCO.

Improved Interoperability across Health and Social Care Systems

457. The proposals outlined are for enabling powers only and it is therefore not possible to robustly quantify what, if any, burden may be imposed on suppliers or providers at this point. This means that the full impacts cannot be accurately appraised at this stage because of significant uncertainty regarding the timing of any use of the powers and the content of any commencement regulations and/or further regulations or exemptions.

458. It is therefore also not possible to provide an Equivalent Annual Net Direct Cost to Business (EANDCB) at this stage. However, where possible, this impact assessment qualitatively assesses the impacts of these measures and provides an indication of the likely scale of impact. A full and robust assessment of the impacts, including an EANDCB will be produced as part of commencement regulations and/or regulations (secondary legislation stage) once the details of how the powers will be used are finalised.

459. We have provided an indication of the likely scale of impacts on these businesses in line with RPC guidance. Evidence at this stage is limited and therefore indicative, work is continuing on the refinement of these estimates and this will be presented in more detail at the commencement regulations and/or regulations stage. It is important to note that any additional

costs to businesses will be minimised when exercising these powers through phasing in the new standards over a proposed period of 5 -10 years.

460. To provide an indication of the impact on businesses, the two central enabling aspects of the proposal have been separated:

iii) A power for the Secretary of State for Health and Social Care to prepare and publish standards for IT products and services used in the health and adult social care sector in England and will require the suppliers of the products to comply with these standards.

iv) A power to establish and operate a voluntary accreditation scheme (accreditation of products and services). IT suppliers can opt-in to the scheme by demonstrating that their products or services meet or exceed the standards required to be compliant (i.e. demonstrate that their products/services are of a 'superior' quality, where open data architecture is concerned).

Table 52: Indirect costs of the proposal

Stakeholder group	Anticipated cost	Cost type
IT suppliers	We anticipate that there will be costs associated with undertaking the accreditation process to enable suppliers to demonstrate their products and services meet or exceed the required standard. There may also be subsequent costs associated with further developing their products to meet new or more advanced requirements for accreditation.	Indirect
Health and social care commissioners/providers	As the powers will require health and social care commissioners and providers to procure compliant IT products and services, we anticipate that there may be administrative costs associated with revisiting existing contract arrangements and/or switching suppliers should any of their procured products or services be noncompliant. These impacts are likely to vary between provider sizes and types.	Cost to government
	There may also be changes to how data needs to be processed by health and social care commissioners and providers to conform with the new standards, alongside upskilling staff to use new systems or new functionalities within existing systems. This may bring about costs where staff time is concerned.	Cost to government

461. The aim of the accreditation scheme is for IT suppliers to the health and adult social care sector to demonstrate that specific, compliant products and services that they offer meet or exceed what is required to achieve compliance i.e. that their products or services are of a 'superior' quality. The scheme will be voluntary and suppliers of non-accredited products and

services will still be able to supply said products or services to the health and adult social care sector. The primary intention of the voluntary accreditation scheme is not to assess compliance, and participation is not a requirement to operate in the market (once determined, further details about the accreditation scheme will be provided in a subsequent IA).

462. Voluntary accreditation shows that a supplier's product or service goes above and beyond in terms of open data architecture and is not specifically the only way of demonstrating compliance with minimum standards. For example, non-accredited firms could still meet the standards set and easily demonstrate this without accreditation. Additionally, while the health and social care sector will only be able to procure compliant products and services (those that meet minimum standards), it certainly isn't the case that suppliers with accreditation would necessarily be looked on more favourably (resulting in a de facto requirement). There are a number of factors that will influence purchasing decisions such as price, quality, experience with the supplier, reliability, ability to deliver to timescales and others. Accreditation is simply one way for suppliers to demonstrate a particular competence in open data architecture. For this reason, the impacts are considered indirect and do not amount to a de facto requirement on suppliers.

463. On this basis, this assessment expects businesses already supplying the sector (approximately 193[202] businesses) to incur the following additional costs, if they wish to undergo accreditation:

a. The additional administrative burden of demonstrating their product or service meets or exceeds the required standard of compliance in order to receive accreditation (indirect cost).

464. Suppliers will only opt-in to the voluntary accreditation model if they expect the costs of their product or service becoming accredited to be exceeded by the commercial benefits to the supplier. It has not been possible at this stage to quantify the indirect cost of demonstrating a superior level of compliance (for accreditation purposes) or the potential commercial benefits. However, the process of accreditation will be designed to minimise burdens on businesses and therefore any costs are expected to be minimal.

465. In addition to the administrative burden associated with voluntarily demonstrating a superior level of compliance, any new suppliers across the appraisal period (those not currently supplying to the sector) may also face costs associated with ensuring that their products and services meet new and updated standards - these are expected to be in line with compliance estimates above (see costs from midata). Similarly, new entrants will only decide to supply to the sector and opt-in to the accreditation scheme if the benefits of doing so exceed the cost of complying with standards and the administrative burden of demonstrating compliance for accreditation purposes.

[202]Based on accredited and/or assured suppliers to certain parts of the health and adult social care sector only. This figure does not represent all suppliers of IT products and services to all parts of the health and adult social care sector.

Indirect costs to businesses of increased data use

466. Many of the reforms within the bill are designed to encourage firms to better harness the power of the data already available to them and to encourage more firms to use data in decision making and for efficiency gains. Some proposed measures will specifically increase data processing for specific activities, such as those in relation to R&D, record keeping and processing bases.

467. Using the sources and methodology listed in the 'Indirect benefits - Monetised' section of this report we highlight that greater data use will lead to greater firm level productivity. It is important to consider that for the reforms we anticipate this to be the case for, that there may also be indirect costs associated with directing more resources towards data use.

468. We predict that the reduction in the burden for firms no longer having to keep records for low risk processing activities will encourage further data use. This will take the form of firms that currently lack incentive to now use data due to the current burden, deciding to now use it, and also firms that now have extra resource spend expanding their data use capabilities.Though these firms will face costs in setting up data processing systems, we expect these quantitative costs to fall in scope of our familiarisation cost estimates. There may also be indirect costs and benefits to businesses of increasing their data use, for example, extra time spent by staff exploring the data costs to businesses of establishing and extending legal frameworks, and the potential additional employment of data specialists. These costs are difficult to quantify as they depend on the initial level of data use within the firm and also whether the infrastructure is already in place.

Wider impacts

Summary

469. This section of analysis provides an outline of the wider impacts of the proposed package of reforms that do not fall into the cost or benefit categories. These include analysis carried out by DCMS and other government departments and focus on factors such as the impact on competition, equalities, national security and law enforcement and any environmental impacts.

Impact on Competition

470. There are reforms within this proposed package that are considered as pro-competitive as defined by the CMA.[203] For example some proposals are designed to remove the barriers of data use for UK businesses and public sector organisations and as a result increase its use more widely. As a result of this increase, we expect the number of private firms using data as an asset to increase, helping to render them more competitive. Whilst this is the case for the majority of reforms there are some included in the bill where it is difficult to determine whether the same applies.

471. In digital markets there is increasing concern that access to data is a huge barrier to entry and this leads to concentrated benefits for the small number of businesses with data access, highlighted in CMA's Online platforms and digital advertising interim report. It is believed that relying on pure market mechanisms for increased data sharing/access is unlikely to lead to

[203] Competition impact assessment, CMA, 2015

sufficient solutions for these problems. Similarly, ineffective competition was the motivation for the CMA's Retail Banking Market Investigation Order and the Government's price cap in retail energy.[204] Government intervention is necessary to address this market failure, as discussed in the Furman Review.[205] The measures included in this bill are designed to promote competition and data sharing to overcome this market failure.

472. Looking more closely at the example of Smart Data. Strong competition drives innovation, high quality, and low prices. Innovative services can help consumers and businesses make better informed decisions in increasingly complex markets. We have seen this emerge in Open Banking[206] since the introduction of Smart Data. However, if the innovative third parties cannot access data, this limits innovation, and customers will miss out on new and improved products and services. This may also mean customers are not able to meaningfully participate in the market as a rational actor.

473. Similarly, in the health sector, there are a number of markets that are dominated by a small number of large suppliers, with high switching costs alongside high barriers to market entry, which are currently not competitive. The Electronic Patient Record (EPR) vendor markets for primary, community and mental health are highly segmented with similar levels of market concentration in each of the relevant segments, and the General Practice EPR market is a duopoly. Therefore, a mixture of interventions to set stronger regulations and promote competition for the market are required to incentivise suppliers to follow standards, improve service, reduce costs and innovate. Although this legislation is currently enabling, we expect the secondary legislation to deliver these market outcomes. However, we also acknowledge that there may be a period after implementation where market competition falls as firms adjust to the new legislation. More analysis on these impacts will be carried out at the secondary legislation stage and will include mitigations for policies that may initially negatively impact competition levels within the market.

Impact on Equalities

474. Prior to the publication of the 'Data: A New Direction consultation' DCMS completed analysis of whether any of the proposals in the consultation paper engage the Public Sector Equality Duty (PSED) under the section 149 of the Equality Act 2010. That duty requires Ministers to have due regard to the following objectives when developing new proposals:

a. Eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the Equality Act 2010;

b. Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;

c. Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

475. In light of responses to the consultation we have updated our PSED analysis. The consultation exercise was especially informative in relation to the following areas:

[204] CMA (February 2017): "Retail Banking Market Investigation Order 2017" & BEIS (July 2019): "Victory for consumers as cap on energy tariffs to become law"
[205] Jason Furman & Digital Competition Expert Panel (March 2019): "Unlocking digital competition"
[206] See 'Open Banking use cases' box above.

a. **Subject access requests -** Our pre-consultation analysis considered whether the re-introduction of a nominal fee for Subject Access Requests (SARs) could harm or disadvantage individuals who make these requests, and this was highlighted in a small percentage of consultation responses as having a potential impact on individuals with protected characteristics, particularly age and disability. The government will not re-introduce a nominal fee for subject access requests and will not proceed with introducing a cost ceiling. The government also considered whether introducing a similar safeguard in the Data Protection Act 2018 as the one provided under Section 16 of the Freedom of Information Act (for public bodies) to help data subjects by providing advice and assistance is necessary. The government deems the current duty to facilitate data subject rights under Article 12(2) UK GDPR and Section 52(6) of the DPA 2018 to be sufficient. Potential revised guidance from the ICO would further mitigate any impact on groups with protected characteristics. The government is satisfied that proposals in this area will not disproportionately impact groups with protected characteristics.

b. **Legitimate interests -** Our pre-consultation analysis noted the potential indirect impacts of the legitimate interests' proposals on groups with protected characteristics. This was supported by consultees who warned that removal of the requirement to take individuals' rights and interests into account in a wide range of situations when processing personal data could disadvantage children or vulnerable groups in society who are less able to complain to the regulator if their personal data has been misused. Having considered consultation responses, the government is minded to pursue the proposal only in respect of a narrow range of processing activities where there are clear public interest reasons for the processing to occur. This could include, for example, processing that is necessary for crime prevention or safeguarding. Removal of the balancing test and associated compliance paperwork in these situations could encourage organisations to make the authorities aware of individuals who are at risk without delay. This could have direct benefits for children and other groups with protected characteristics. Even if the balancing test were removed in these scenarios, data controllers would continue to be required to comply with data protection principles (for example, on lawfulness, fairness and transparency), which would further reduce the risks of any adverse impact on groups with protected characteristics.

c. **Cookie proposals -** Some respondents raised concerns about websites processing increased volumes of personal data without consent, especially if it relates to children or people with disabilities or mental health issues. Concerns were raised by some respondents about the importance of not undermining the Age Appropriate Design Code (AADC) standards, notably the need for a high level of transparency when children's data is being collected. The proposals that the government will take forward (i.e. permitting audience measurement and some other non-intrusive cookies without consent), will be carefully designed with safeguards to protect the rights of individuals, such as limiting any information that is processed for audience measurement purposes to aggregate statistical information and not using the data for more intrusive purposes. A move from an opt-in to an opt-out consent model for websites would only take place once Ministers are content that users have access to technology that supports them to effectively manage their preferences on how their data is processed.

d. **Extending the soft opt-in to non-commercial organisations (such as political parties and charities) -** Our pre-consultation analysis recognised that this proposal would mean that some people will receive direct marketing material that they would not have received previously. Some groups in society (e.g. older people, people with mental health issues) may be more concerned than others by emails, messages, texts from people they do not know well. To mitigate the risks identified here, the government will design this proposal so that non-commercial organisations are subject to exactly the same rules as commercial organisations in terms of respecting a person's right to opt out and making it easy for them to do so.

e. **ICO complaints -** Concerns were raised by some respondents that requiring data subjects to complain to the relevant controller before complaining to the ICO would create a barrier between data subjects and the ICO, and prevent data subjects being able to exercise their rights to complain or seek redress. To mitigate these risks, we will combine this proposal with appropriate safeguards. As such, the data subject will be able to escalate their complaint to the ICO if they have not received an adequate response after a set time period, or if the data controller has not provided the data subject with contact details to raise a complaint, for example. We will also retain current statutory accountability mechanisms to ensure that the ICO does not use its discretion to not respond to complaints too freely. Article 78 of UK GDPR confers the right of judicial remedy where the supervisory authority 'does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint' and this will be maintained.

f. **AI proposals -** In our pre-consultation analysis we considered how our proposal on creating a new condition for processing of sensitive personal data for bias monitoring and correction in relation to AI systems would impact the public sector equality duty under section 149(1) Equality Act 2010. This proposal is likely to lead to an increase of processing of sensitive personal data on individuals with protected characteristics. The purpose of this proposal is to support organisations to monitor harmful bias and eliminate discriminatory outcomes, so any detrimental impact is considered justifiable on this basis. Furthermore, the more representative the data that an AI system is trained on, the more the system will reflect a broader cross-section of the population. This in itself is likely to mitigate bias and resulting discrimination, on an individual with protected characteristics. Similar considerations were involved in a closely related proposal for processing of personal data for bias monitoring and correction in a list of legitimate interests for which organisations would not be required to take individuals' rights and interests into account when relying on the "legitimate interests" ground to process personal data. The government is continuing to assess the merits of this related proposal as part of the proposed reforms to legitimate interests outlined in sub-paragraph (b) above.

g. **Future-proofing article 22 -** Consultation responses raised concerns over safeguards for automated decision-making, and particularly that removing the right to human review could have a disproportionately negative impact on people with protected characteristics, for example on the basis of their sex or race. A frequently cited example of this was the 2020 A-Level results algorithm, which respondents felt discriminated unfairly against pupils. Though precautions were taken to prevent bias based on protected characteristics, the profiles of those attending different schools inevitably led

to outcomes being different based on their protected characteristics, including race and sex. In this example, there was uncertainty over the appeal mechanisms pupils could access. Our proposals retain human review as currently required under Article 22 but will ensure that a data subject has access to clearer safeguards for any significant decision made without meaningful human involvement, potentially to include a justification of how a decision is reached which may enable a data subject to more easily identify how protected characteristics have been factored into a decision.

h. **Removal of prescriptive requirements to complete Data Protection Impact Assessments (DPIAs) -** our pre-consultation analysis considered whether this proposal could mean that potential disproportionately detrimental effects of the processing for individuals with protected characteristics is not identified. However, organisations will still be required to consider risk through implementation of their risk-based privacy management programme and therefore this in itself is likely to mitigate the potential risk of protected characteristics not being identified.

476. Overall, our analysis is still that the government does not consider that any negative impact of our proposals for individuals with protection characteristics are disproportionate.

Impact on Individuals

ICO Taxonomy of Harms

477. The reforms within the bill are designed to minimise the harms related to imperfect data protection. Harms can result when individuals or groups are prevented or impeded from asserting their information rights (e.g. a lack of transparency around how data is processed or inability to hold a public body accountable). Quantifying data protection and information rights harm is difficult therefore the ICO produced a non-exhaustive and non-hierarchical taxonomy with illustrative examples of harms.[207]

478. The ICO's taxonomy of harms uses the risk management distinctions between causes, events and consequences to focus on harmful consequences. The cause is a factor that alone or in combination gives rise to risk, for example poor data security. The event is an occurrence with some probability of occurring such as a data breach. The consequence is the outcome of the event that leads to a negative impact, for example financial loss which is also the harm. The harm to an individual can vary in degree and type, and harms can include:

a. Physical harm: physical injury or other harms to physical health

b. Material harm: harms that are more easily monetised such as financial harms; or

c. Non-material harm: fewer tangible harms such as distress.

479. The harms may fall into more than one category and can arise from actual damage or intangible harm.[208]

480. There may also be wider societal harms. For example, damage to the economy is described as a harm that has a negative impact on the economy that is significant at local, regional or national level, or for a specific sector and may involve a misuse of personal data

[207] Regulatory Policy Methodology Framework, ICO 2021
[208] Draft journalism code impact assessment, ICO, 2021

leading to an unfair competitive advantage.[209] The reforms aim to mitigate data protection harms by ensuring key safeguards and high standards of data protection are maintained. Approaches to quantifying the value of data protection harms are still being investigated.

Artificial Intelligence Ethics

481. The ethical implications of using AI technologies have been considered within the proposed reforms. AI ethics is a set of values, principles and techniques that employ widely accepted standards of right and wrong to guide moral conduct in the development and use of AI technologies.[210]

482. AI ethics are a response to the harms an individual or society may face due to the misuse, poor design or unintended negative consequences caused by AI. The ethics are intended to support the production of ethical, fair and safe AI applications. The potential harms caused by AI systems include.[211]

a. Bias and Discrimination: AI systems can reproduce, reinforce and amplify patterns of inequality that exist in society.

b. Denial of Individual Autonomy, Recourse and Rights: When AI systems produce decisions or predictions, there is no directly accountable party responsible for the outcome.

c. Non-transparent, Unexplainable or Unjustifiable Outcomes: AI systems operate using models that are difficult to explain and this lack of explainability may be problematic when the results are considered discriminatory or unfair.

d. Invasions of Privacy: Threats to privacy are posed by AI systems both as a result of their design and development processes, and as a result of their deployment.

e. Isolation and Disintegration of Social Connection: In the future, excessive automation may reduce the need for human-to-human interaction.

f. Unreliable, Unsafe or Poor-Quality Outcomes: Unreliable, unsafe or poor-quality outcomes can do direct damage to the wellbeing of individuals and the public's welfare.

483. The reforms targeted at AI and Machine Learning in this bill include the future proofing of Article 22 and the enhancement of the approach to explainability and accountability for fair processing in the context of profiling. Article 22 is drafted to give a data subject a right not to be subject to a decision made by solely automated processes which has a legal or similarly significant effect, however there is a lack of clarity in practice over how this right is invoked, what constitutes a significant effect, as well as which decisions can truly be said to be made by ‘solely’ automated processes. This ambiguity means that Article 22 is rarely applied or considered in the way it was intended to be.

484. Automated decision-making (ADM) and profiling are being used more and more frequently by organisations to streamline their processes. These automated processes often rely on AI technologies and as such are a key part of the government’s wider approach to the development and deployment of AI systems. These proposals are pivotal in addressing the

---

[209] Regulatory Policy Methodology Framework, ICO, 2021

[210] Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute

[211] Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute

risks of harm in AI-powered automated decision-making and in deciding the data protection controls required to build and maintain trust in their application.

Increased Interoperability and Trust of Digital Identity Systems

485. More detail on the wider impacts of this proposed reform can be found in the Digital identity and attributes - De Minimis Assessment.[212] Here we provide a summary of the wider impacts of the preferred reform.

486. Although a digital identity market already exists, it is not developed to its full potential and it presents some key flaws which may exclude minorities or those with protected characteristics. For example:

d. When setting up a digital identity, individuals have highlighted that the process usually requires a sequencing of tasks which are considered difficult for people that are, for instance, digitally excluded or neuro-diverse.[213]

e. The digital identity system can be rather rigid, therefore excluding people whose circumstances differ from the expected social structure, such as those wishing to manage two bank accounts at the same bank from one mobile phone.[214]

487. The digital identity legislation, by promoting the growth of the digital identity market in an inclusive way, provides the opportunity to use a digital alternative, giving to excluded individuals an easier option for proving their identity or eligibility. For example, those who cannot afford a passport may instead opt for a digital identity product based on their data or a 'vouch'.[215]

488. Inclusion is explicitly mentioned in the UK digital identity and attributes trust framework. Although signing up to the Trust Framework is not compulsory, organisations will need to be certified against it to prove that their products or services meet the UK Government requirements for checking government-held records of identity-related data. The Framework aims at improving inclusivity by:

a. Stating that all identity service providers should ensure no one is excluded due to their 'protected characteristics'". There are exemptions to this, for instance restricting the availability of a product or service to an individual due to their age (e.g. businesses cannot sell alcohol to underage individuals).

b. Giving examples of ways organisations can increase inclusivity. For instance, when choosing a system for facial recognition, digital identity and attribute providers should ensure that the chosen system is built in an inclusive way. A system which was tested with a small sample of white men risks excluding users of other genders and ethnicities, therefore excluding minorities or those with protected characteristics from being able to use the service.

[212] Digital identity and attributes - De Minimis Assessment DCMS, 2021
[213] Digital Identity: Ground-up Perspectives Report Summary
[214] Digital Identity: Ground-up Perspectives Report Summary
[215] A vouch is a declaration from someone that knows the user which can be used as evidence for identity proof.

c. Requesting both public and private sector organisations to meet appropriate accessibility standards. For instance, those that operate in Wales offer products and services available in Welsh.

d. Requiring organisations that sign up to the framework to submit an annual inclusion report.

Environmental Impacts

Primary legislation to extend the Digital Economy Act to benefit businesses

489. There may be less printed documentation required as a result of business data being accessible across the government, providing an environmental benefit

Increased Interoperability and Trust of Digital Identity Systems

490. We expect that the legislation, by fostering the uptake of digital identity checks, will have a positive effect on the environment. This is because less trips will be required during the identity verification process and to allow the individuals to obtain the required physical identities. Furthermore, a greater uptake of digital IDs may lead to less people choosing traditional IDs over digital alternatives which in turn may lead to a lower quantity of IDs produced and disposed every year. This could be beneficial to the environment. However, despite the fact that digital identity should benefit the environment, these benefits are expected to be very small and possibly insignificant. For instance, the total number of trips related to identity verifications carried out every year, although substantial, is not large enough to significantly impact the environment

National Security Impacts

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

491. These wider impacts have been provided by the Home Office.

492. The following proposals are expected to contribute to the Home Office priority outcomes of reducing crime and risk of terrorism to the UK and interests overseas:

a. Mirroring the national security exemption from Part 2 is expected to increase cooperation between LEAs and the UK Intelligence Services, particularly relating to CT.

b. Introducing the ability to actively review automated decisions is expected to lead to more effective use of automated systems to identify persons of interest, particularly in border settings, and reduce the risk of tipping them off, therefore increasing the chance that they will be stopped and apprehended.

c. By improving cooperation across data boundaries, it is expected that UK Intelligence Services and LEAs will be able to conduct more effective investigations, increasing the probability that they are successful and contributing to a reduction in crime.

d. The I-LEAP proposal should increase the opportunities to identify international persons of interest through its alert system, increasing the chance that a terrorism or serious crime incident is avoided.

493. The following proposal is expected to help future proof the data protection regime:

e. Introducing ‘codes of conduct’.

494. The following proposals are expected to increase clarity around data protection rules:

f. Introducing a definition of ‘consent’.

g. Reforms to the oversight framework for biometrics and overt surveillance.

Mirror the national security exemption from part 2

495. Currently, the national security restriction in Part 3 is not as extensive as in Part 2. The current restriction-based approach is more limited than the protections provided by the Part 4 national security exemption. This creates risks when for example, a data subject exercises their rights. Mirroring the national security exemption into Part 3 would assist close working between law enforcement and intelligence services and provide greater legal certainty for international transfers concerning national security.

496. When collaborating under joint investigations, each data controller is subject to different standards. Part 3 contains fewer national security protections which may lead to disclosures by LEAs which may undermine the intelligence services and expose operational risks. This is a barrier to co-operation.

497. By providing a national exemption to Part 3 of the DPA 2018, this proposal may lead to more effective CT investigations thus contributing to the Home Office priority outcomes of reducing crime and risk of terrorism to the UK and UK interests overseas.

Introduce a power to allow bodies representing Part 3 controllers and processors to produce ‘Codes of Conduct’

498. In the UK GDPR codes of conduct can be produced by representative bodies (for example, trade associations) to clarify the application of data protection laws in particular sectors, which are then approved by the ICO. There is no equivalent power under Part 3 DPA 2018 and stakeholders have indicated that this could be a useful tool to future-proof their data use. This proposal aims to expand it to the law enforcement sector enabling similarly representative bodies to create codes of conduct for Part 3 under the purview of the ICO.

499. The LEAs will be able to adapt data protection standards to suit their needs which will help future-proof data use.

Introduce the ability to actively review automated decisions

500. Currently, LEAs are required to inform data subjects as soon as reasonably practicable when a decision which produces an adverse legal effect is made which is based solely on automated decision making. The purpose of this is to allow the data subject to then request that a human either reconsiders that decision or takes a fresh decision not based solely on automated decision making.

501. Automated decision making (ADM) is the process whereby a decision, which affects a data subject, is made wholly by automated means without any human involvement.

502. The police have stated that this can cause them difficulties. For example, where ADM is used to match an individual to a watchlist, the police must then either inform the data subject that they are under investigation (thereby tipping them off that they are of interest) or, alternatively, ensure that the decision is reviewed by a human (thereby removing the need to inform the data subject but running the risk the individual may have moved beyond their reach before any action can be taken).

503. This proposal will provide an alternative option for LEAs to provide for a human to actively review the decision after it has been taken as soon as is reasonably practicable thereby removing the need to notify the data subject at the time. However, in order to ensure that the new power is only used where necessary, LEAs will only be able to use it if informing the data subject is necessary for one of the restrictions set out under section 44(4) of the DPA (e.g. to avoid obstructing an official or legal inquiry, investigation or procedure etc.) This change will ensure that the rights of data subjects who are subject to ADM continue to be protected whilst improving the ability of the police to tackle crime, ensure public safety and bring offenders to justice. It contributes to the Home Office priority outcomes of reducing crime and the risk of terrorism to the UK and UK interests overseas.

Clarifying use of Section 76 DPA to cover larger scale transfers

504. Introducing some flexibility to Section 76 DPA 2018: This section concerns the international transfer of personal data where ‘special circumstances’ are present. Currently, the conditions and restrictions imposed within the provision make it too inflexible to meet modern law enforcement needs and therefore, unnecessarily limit public safety efforts and goals. The reform clarifies how law enforcement can legitimately use s.76 which enables the transfer of personal data where ‘special circumstances’ are present to give confidence to the law enforcement community to use this section to transfer larger amounts of data in the pursuit of the detection and prevention of crime.

505. If this proposal leads to more frequent large-scale transfers on the basis of national security or serious and organised crime, it may lead to more effective investigations, thus contributing to the Home Office priority outcomes of reducing crime and risk of terrorism to the UK and UK interests overseas.

Amendments to Part 4 of the DPA 2018 - National Security Notices

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

507. UK Intelligence Services believe that this proposal will lead to more dynamic working practices with police colleagues, such as the option to share databases. It should also lead to improved confidence in sharing data.

508. This may result in more effective investigations and a higher probability that they are successful, thus contributing to the Home Office priority outcomes of reducing crime and risk of terrorism to the UK and UK interests overseas.

International-Law Enforcement Alerts Platform (I-LEAP) proposal

509. To introduce a delegated power to pass secondary legislation enabling the technical implementation of new international alert sharing agreements: The International-Law Enforcement Alerts Platform (I-LEAP) will deliver real-time alert exchange with key international partners and so strengthen joint capabilities to tackle shared threats, including migrant smuggling. Delegated powers will allow swift implementation, through secondary legislation, of technical aspects of new agreements with international partners. This approach provides legal and operational certainty to UK operational partners and ensures that the required international agreements have a basis in UK legislation. This will enable the UK to implement new alert-sharing arrangements with close international partners.

510. Additional opportunities to identify international subjects of interest may lead to increased pressure on the Criminal Justice System (CJS).

511. There are also significant non-monetised benefits:

- Reduced risk of harm to UK society through reciprocal data sharing.
- Reduction in the risk of minor, medium and major terrorism incident.
- Reduced risk of harm to UK society through the deterrence of international criminality.
- Reduced reputational risk and higher societal confidence in national security and public safety.
- Improved international standing.
- Increased effectiveness for UK front line officers in identifying persons of interest due to enhancements to Interpol.
- Reduced risk of harm to UK society through capability to extradite international criminals.
- More successful prosecutions.

Impact on small and micro businesses

512. The proposed set of reforms are expected to have an impact on small and micro businesses. The percentage of small and micro businesses that collect personal data is 71% and 68%, respectively.[216] Larger businesses tend to have greater levels of data use than micro businesses. On average larger firms are more productive than smaller firms, particularly in manufacturing. This typically reflects the increasing returns to scale through capital-intensive production.[217] Small and micro businesses that process data are less likely to analyse data to generate insight and knowledge when compared to large businesses.[218] This suggests that there are potentially more productivity gains available to small and micro businesses through increased data use than their larger counterparts. There is evidence that larger businesses that handle digitised data are more likely to transfer data internationally than smaller businesses.[219] Around 25% of micro businesses in the UK that do not transfer data consider a lack of resources as a barrier to sharing data internationally and are more likely to cite this as a barrier than medium-sized businesses.[220]

513. The reforms aim to provide small and micro businesses with the opportunity to increase their data use to boost innovation and facilitate international trade. Participation in international trade activities is one of the key characteristics of high productivity in firms and enabling more firms to trade might assist in boosting their productivity.[221] The proposed reforms are designed to encourage small and micro businesses to use data more effectively in their decision making and therefore boost productivity. Small and micro businesses are expected to see proportionally higher reductions in compliance costs than larger businesses as a result of the reforms. The reforms are expected to reduce the barriers to sharing data internationally that small and micro businesses face and therefore increase their international trade.

514. The proposed set of reforms are not expected to place a disproportionate burden on small and micro businesses. We expect small and micro businesses to benefit proportionally more from the reforms than larger firms because they are more likely to have lower levels of data use prior to the reforms.

515. In this section we have analysed the estimated impacts of the reforms on small and micro businesses. Where evidence is available we have done this for all monetised costs and benefits. Many of the reforms in the preferred package are aimed at improving data use in the public sector so do not fall into the scope for this section. We have focused on providing a breakdown of the compliance cost savings, productivity benefits, familiarisation costs, digital identity schemes and smart data initiatives.

---

[216] UK Business Data Survey (2021)
[217] Productivity in SMEs and large firms, OECD (2021)
[218] 69% of large businesses that process data analyse data to generate insight or knowledge compared to 39% and 32% for small and micro businesses, respectively
[219] UK Business Data Survey (2021)
[220] UK Business Data Survey (2021)
[221] Research findings do confirm a clear, strong link between international trade and productivity, although the direction of the relationship remains unclear, i.e. do more productive firms end up trading internationally, or does international trade help in boosting firm productivity. For more information see https://www.ons.gov.uk/economy/economicoutputandproductivity/productivitymeasures/articles/uktradeingoodsandproductivitynewfindings/2018-07-06

516. Where sector data is available we have also included sectoral breakdowns of the monetised impacts of the proposed package. We also explore any impacts that may vary due to geographical factors.

Small and Micro Business Impacts

Summary of changes since June 2022 publication

517. The addition of the extra five policy reforms has resulted in greater savings for micro and small businesses particularly. The addition of the record keeping reform will result in small and micro businesses facing an increase in familiarisation costs of approximately £18.9 million as they get to grips with the new legislation. We estimate that these costs will be outweighed by the fact that those micro and small businesses that process low-risk data will save approximately £20 million more a year in compliance cost savings than without this additional policy. The clarification to both the legitimate interests and automated decision making legislation are also estimated to bring further savings for firms of all sizes but particularly small and micro firms as more of them are likely to be impacted.

Compliance Cost Savings

518. We predict that the reforms will have a direct benefit on small and micro businesses. As discussed in the direct benefits section, the reforms are expected to change compliance requirements and lower the compliance burden on businesses. Small and micro businesses are expected to achieve greater overall compliance cost savings than larger businesses. There are assumed to be a higher number of micro and small businesses in scope of the reforms and therefore more are expected to benefit from compliance cost savings.

519. The table below shows the compliance cost savings by organisation size. For micro businesses the compliance cost savings are estimated to be £51.8 million, while for small businesses the compliance cost savings are estimated to be £37.3 million. Together this is greater than the total benefit for large firms (£39.0 million). This is explained by the fact that large businesses spend more of their resources dealing with Subject Access Requests, than smaller businesses who invest more into research and development in order to expand.

Table 53: Annual Compliance Cost Savings by organisation size, 2021 prices

Compliance cost by firm size (£m) (medium scenario)					
Reform	Micro (0 to 9)	Small (10 to 49)	Medium-sized (50 to 249)	Large (250+)	Total
Legitimate Interests	1.6	2.8	0.1	0.0	4.5
AI and Machine Learning	1.9	0.6	0.0	0.0	2.6
Research Purposes	3.1	5.25	0.2	0.1	8.7
Accountability Framework: Record Keeping	29.4	9.1	0.2	0.0	38.7

Privacy and electronic communications and the use of personal data for the purposes of democratic engagement	9.7	5.9	0.2	0.1	15.8
Subject Access Requests	5.7	13.7	0.8	38.8	59.1
Total	51.4	37.3	1.6	39.0	129.3

Productivity Benefits

520. The preferred package of reforms is designed to encourage firms to better harness the power of data already available to them and to encourage more firms to use data in decision making and for efficiency gains. As mentioned above, the impact of additional data use on productivity is assumed to be linear for all firms that analyse data, therefore we expect that small and micro businesses will achieve the same increase in productivity as larger firms. As there is a greater share of large firms the total impact for large firms will be greater than that of small and micro, however this is down to the distribution of the total number of firms.

Table 54: Estimated change to UK GVA split by business size, 2021 prices

Impact on UK Productivity (GVA)(£m)					
Reform	Micro (0 to 9)	Small (10 to 49)	Medium-sized (50 to 249)	Large (250+)	Total
Legitimate Interests	1.5	0.3	1.0	7.4	10.2
AI and Machine Learning	2.5	0.2	0.6	2.3	5.6
Research Purposes	3.7	0.6	1.8	11.5	17.6
Data minimisation and anonymisation	0.8	2.7	4.2	29.1	36.8
Accountability Framework: Record Keeping	1.2	0.1	0.3	0.7	2.2
Total	9.7	4.0	7.9	51.0	72.5

Familiarisation Costs

521. We adapted the assumptions of our methodology to reflect the cost of familiarisation on small and micro businesses. This analysis assumes that a micro-sized firm has zero employees and a small firm has between 1 and 49 employees. Small and micro businesses are estimated to face greater familiarisation costs than medium-sized and large businesses because we assume that a higher number of small and micro businesses are in scope of the reforms. We updated the wage assumptions of our time-cost approach by assuming that at small businesses senior officials would read the guidance rather than data protection officers, and estimated the hourly unit cost of this work at £26.85 using occupational estimates from the Annual Survey of Hours and Earnings (ASHE).[222] For micro-sized firms we have adapted our

[222] ONS Annual Survey of Hours and Earnings (2021)

wage assumptions by applying median annual earnings estimates of the self-employed from DWP's Family Resources Survey and estimating the hourly unit cost of this work at £11.20.[223] We do not expect the reforms to disproportionately impact small and micro businesses.

522. The table below shows the familiarisation cost estimates split by business size. For micro businesses this is estimated to be between £40.4 million and £54.6 million, while for small businesses this is estimated to be between £29.9 and £40.4 million. We expect the familiarisation costs for all activities including data use for research and development and data anonymisation to be higher for small and micro businesses compared to large firms as their wage costs are likely to be higher compared to larger firms with dedicated resources and systems in place. At a business level, the familiarisations costs are expected to cost around £6.22 per micro business and £14.92 per small business.

Table 55: Familiarisation costs split by business size, 2021 prices

Familiarisation cost by firm size (£m) (medium scenario)					
Subheading	Micro (0)	Small (1 to 49)	Medium-sized (50 to 249)	Large (250+)	Total (£m)
Research Purposes	1.9 - 2.5	1.3 - 1.8	0.0 - 0.0	0.0	3.2 - 4.4
Legitimate Interests	4.7 - 6.3	3.3 - 4.5	0.0 - 0.1	0.0 - 0.0	8.1 - 11.0
AI and Machine Learning	1.4 - 1.9	1.1 - 1.5	0.0 - 0.0	0.0	2.6 - 3.5
Data minimisation and anonymisation	4.7 - 6.3	3.3 - 4.5	0.1 - 0.1	0.0 - 0.0	8.1 - 11.0
Accountability Framework: Record Keeping	24.8 - 33.6	18.7 - 25.3	0.4 - 0.6	0.1-0.1	44.0 - 59.6
Privacy and Electronic Communication	2.9 - 4.0	2.1 - 2.9	0.1 - 0.1	0.0 - 0.0	5.1 - 6.9
Total	40.4 - 54.6	29.9 - 40.4	0.7 - 1.0	0.2-0.2	71.1 - 96.3

Powers for Digital Identity and Attributes Initiatives

[223] DWP Family Resources Survey (2020)

523. Analysis in this section is based on Digital Identity and Attributes Initiatives De Minimis Assessment.[224] Here we provide a summary of the impact on small and micro businesses of the proposed reforms.

a. Relying parties.[225]

i. The legislation is expected to not significantly impact small and micro businesses as we assume that small-micro relying parties will be significantly less likely than bigger ones to adopt digital identity because their expected benefits are less likely to outweigh the costs. For instance, businesses are considered small-micro if they employ less than 50 staff members. Therefore, we assume they are less likely to be interested in digital RTW checks as their gains from digital checks will not be significant compared to the cost of familiarising and adapting to digital identity.

ii. According to ONS data, the average turnover of small micro businesses in 2020 was £606,501. We estimated that the one-off familiarisation costs plus the one-off organisational change costs for a business wishing to adopt digital identity may add up to £17,657.5. Therefore, these estimated costs add up to roughly 2.9% of the average revenue of a small-micro business in 2020. Whereas, the equivalent calculation for medium-large businesses adds up to 0.08%. This suggests that the estimated costs of adapting to the legislation may create a greater burden for small-micro businesses relative to larger ones. However, this legislation is not designed to substitute traditional identification checking. Therefore, we expect small and micro relying parties that may experience a significant burden to adopt digital identity to continue to only use traditional identification systems. Therefore, overall, we do not believe that small-micro businesses will be disproportionately affected by the legislation in a significant way.

b. Service providers:[226]

i. Small-micro identity and attribute service providers have a greater risk of being disproportionately impacted by the legislation. We expect these businesses to face familiarisation costs and organisational. These costs may generate a greater burden for small micro firms relative to medium-large businesses. However, we do not believe this disproportionate impact will be significant as small and micro identity and attribute service providers are already established in the market so we expect that their costs to understand and adapt to the legislation to be minimal.

524. The legislation aims at providing the right legislator environment to promote the adoption of digital identity. Therefore, we expect the small-micro providers to experience a growth in demand on the back of the legislation. We believe that the resulting increase in revenue will cover some, if not all, the costs businesses may experience due to the legislation.

---

[224] Digital Identity and Attributes De Minimis Assessment (2021)

[225] We define relying parties as organisations that get (or 'consume') digital identity products or services.

[226] This assessment defines service providers as organisations that prove and verify users' identities and/or attributes. They might not need to do all parts of the identity checking process. They can specialise in designing and building components that can be used during a specific part of the process.

Regulatory Powers for Smart Data

525. Analysis in the section is based on the Regulatory Powers for Smart Data Impact Assessment produced by BEIS.[227] Here we provide a summary of the potential impact on small and micro businesses. The impacts on Small and Micro firms (SMFs) have been considered for the main Smart Data schemes currently in scope: Finance (including Pensions and insurance) and Telecommunications and should be treated as indicative.

526. The specific thresholds for mandatory participation will be decided for individual schemes to reflect differing market structures and will be set out in secondary regulations. We expect Smart Data to be mandatory for medium/large, incumbent data holders in scope of the regulations, with smaller data holders and TPPs choosing to participate on a voluntary basis. We would therefore expect SMFs to participate where they see the benefits to exceed the costs for their business.

527. In terms of **cost savings**, Frontier Economics conducted analysis into the benefits of Smart Data to small and micro businesses and TPPs.[228] A full methodology explanation and set of assumptions can be found in their research note.[229] This work indicates the potential benefits over 5 years across banking, finance, energy and communications. For TPPs, the estimates focus on potential productivity gains and growth in the number of TPPs. For SMF users of Smart Data, the estimates focus on potential cost savings. These are a direct benefit of the Smart Data initiatives.

528. Alternatively looking at **costs**, BEIS conducted a survey to collect evidence on the costs of Open Banking. Focusing on the costs currently faced by organisations with less than 49 employees can provide an illustration of the costs faced by Small and Micro firms (SMFs) to participate in a mandated data sharing scheme. We found that the majority of small and micro firms faced implementation costs below £200,000. This ranged from £5,000 to £200,000. No SMFs estimated their total one-off implementation costs to be above £2m. The majority of SMFs estimated their annual ongoing costs to be below £75,000 per annum. From those who provided firm estimates, this ranged from £50,000 down to £10,000 per annum. No SMFs estimated ongoing costs to be above £200,000. More detail on this survey can be found in 'Primary Legislation Costs'.

Improved Interoperability across Health and Social Care Systems

529. DCMS has worked alongside the Department for Health and Social Care to ensure that all policy risks and impacts of the proposed reform to increase interoperability across health and social care systems are included in this impact assessment.

530. The introduction of new enabling powers for the Secretary of State to prepare and publish standards for IT products and services used in the health and adult social care sector in England and the requirement of firms to comply with these standards, may impact smaller suppliers differently compared to larger suppliers. There are currently a limited number of IT suppliers who have adopted an open architecture approach as their standard for products and services supplied to the health and adult social care system despite the existence of published interoperability information standards that some health providers had to have regard to. It

[227] Regulatory Powers for Smart Data Impact Assessment, BEIS (2022)
[228] *Will reference when published*
[229] *Will reference when published*

follows that there is often no suitable alternative product on the market that meets all of a health or social care provider's needs that they can switch to, creating vendor lock-in, and providers have limited leverage to require their suppliers to undertake costly reconfigurations that are perceived to benefit the provider's organisation alone. By putting in place a common set of standards we encourage a more modular approach to EPRs, avoiding supplier lock-in and creating a more dynamic and responsive market and opening up the marketplace to smaller suppliers.

531. There is a risk of compliance costs having a disproportionate impact on smaller and newer suppliers. For example, in the health sector in particular, the IT supplier market is already dominated by a small group of large suppliers. There are approximately 193[230] accredited/assured suppliers of sector specific IT-related products and services to the health and care system. As an example, 8 of these supply enterprise-wide EPRs to acute, community and mental health hospitals. The majority of these firms are large and well-established - 5 out of 8 of the accredited EPR suppliers listed are large firms with over 250 employees.[231]

532. Increased competition is not a new risk arising as a direct result of the proposed measures, however, requiring all IT suppliers of products and services to the health and care sector (regardless of their size) to comply with a set of standards in order to operate within the market may place smaller and newer suppliers at a competitive disadvantage. They already have a smaller share of the market and the standards could bring about additional compliance costs. Larger suppliers may already be in the process of meeting the new standards or in a position to meet them with greater speed due to greater resource, and therefore maintain or increase their market share.

533. To mitigate this, we intend to develop the standards themselves and the implementation of the measures in consultation with varying supplier types. We will also consider any further exemptions that can be applied if these powers were exercised. Regulations will set out the procedure for preparing and publishing information standards and this is intended to ensure that the new standards set are reasonable and achievable.

Enhance the work of the UK intelligence services and law enforcement bodies in the interest of public security (HO)

534. The proposals are not expected to have a significant economic impact on small and micro-businesses. The vast majority of the proposals and impacts are targeted at LEAs and the UK Intelligence Services. There are some private businesses who are also competent authorities, however, they are unlikely to face the more resource intensive costs and benefits of the proposals such as the logging 'justification' and ADM proposals as these concern LEAs. Of these private businesses there may be a small number of small and micro-businesses but

[230] NHS (including acute, community and mental health hospitals) - 176 IT-related accredited suppliers - Source: https://www.england.nhs.uk/hssf/supplier-lists/ ; Adult Social Care - Digital Social Care Records only - 8 assured suppliers - Source: Assured Supplier List - Digital Social Care. NHS Primary Care - 10 (however 1 supplier has been captured in the other NHS figures) - Source: Internal NHS figures for GPIT Futures Programme. This is not an exhaustive list figure for suppliers of IT products and services to all parts of the health and adult social care system in England (e.g. dentistry and optometry), nor does it include all types of IT products and services supplied to the health and adult social care system in England.

[231] Where a reliable estimate for the number of employees could not be found for the UK subsidiary - the figure for the parent company was used instead.

they are expected to face significantly smaller impacts compared to LEAs and the UK Intelligence Services.

Impact on Medium businesses

535. As well as small and micro businesses the package of reforms will also have direct and indirect impacts on medium sized businesses. [232] 99% of medium sized businesses handle some form of digitised data according to the UK Business Data Survey and 80% handle personal data, which is more than both small and micro businesses. [233]

536. Similarly to small and micro businesses, the package of reforms is not designed to put a disproportionate burden on medium businesses. We expect medium sized businesses to benefit proportionally more from the reforms than larger firms because they are more likely to have lower levels of data use prior to the reforms.

537. In this section we have analysed the estimated impacts of the reforms on medium sized businesses. Where evidence is available we have done this for all monetised costs and benefits. Many of the reforms in the preferred package are aimed at improving data use in the public sector so do not fall into the scope for this section. We have focused on providing a breakdown of the compliance cost savings, productivity benefits and and familiarisation costs.

Compliance Cost Savings

538. We predict that the reforms will have a direct benefit for medium sized businesses. The reforms are expected to change compliance requirements and lower the compliance burden on businesses. Medium-sized businesses are expected to achieve the smallest overall benefit of £1.6 million annually, as seen in table 52. This is because there is a smaller proportion of medium sized businesses in scope of these reforms compared to small and micro businesses. Medium businesses also tend to receive less SARS than large businesses meaning they are likely to save less from the reforms aimed at SARs.

Productivity Benefits

539. The preferred package of reforms is designed to encourage more firms to use data in decision making that result in efficiency gains and increased productivity. As with small and micro businesses, the impact of additional data use on productivity for medium sized businesses is assumed to be linear. We estimate that medium sized firms will benefit from an annual increase in productivity of £7.6m, this is in line with the proportion of medium sized businesses estimated to increase their data use because of the reforms.

Familiarisation Costs

540. We adapted the assumptions of our methodology to reflect the cost of familiarisation on medium sized business. This analysis assumes that a medium sized business has 50 to 249 employees. As seen in table 54 small and micro businesses are estimated to face greater familiarisation costs than medium-sized and large businesses because we assume that a higher number of small and micro businesses are in scope of the reforms.

541. We updated the wage assumptions of our time-cost approach by assuming that for small and Medium Sized Enterprises senior officials would read the guidance rather than data protection officers, and estimated the hourly unit cost of this work at £26.85 using occupational

[232] Businesses with 50 to 249 employees, as per previous BEIS definitions

[233] https://www.gov.uk/government/statistics/uk-business-data-survey-2021/uk-business-data-survey-2021-summary-report

estimates from the Annual Survey of Hours and Earnings (ASHE).[234] Using this assumption we estimate that the total familiarisation costs for medium-sized businesses will be between £0.7 and £1.0 million.

[234] ONS Annual Survey of Hours and Earnings (2021)

Sectoral Impacts

542. The reforms aim to increase responsible data use across all sectors of the economy. Better use of data can help organisations of every kind succeed. As of 2020, the two sectors most likely to say they share personal data with other organisations were Finance and Insurance (59%) and Real Estate (39%).[235]

543. We expect the reforms to have distributional impacts on different sectors as a result of differing levels of data use between sectors. The compliance cost savings estimates are broken down by sector and different assumptions are made on the number of businesses per sector that are in scope of the reforms based on results from the UK Business Data Survey.

Compliance Cost Savings

544. The table below shows the total compliance cost savings estimates by sector. The sector estimated to benefit the most from compliance cost savings is the Professional/Scientific/Technical sector with savings of £18.0 million, this can be explained by the fact that many of these reforms are focused on removing barriers to data use for research purposes and artificial intelligence which are most prolific in this sector. The Mining, Energy and Water sector is estimated to save the least at £1.3 million as we predict this sector to be one of the least impacted by the AI and research measures. The Finance and Insurance sector is estimated to save £3.7 million with £2.4 million of this being saved in response to the changes in SAR regulations.

Table 56: Compliance cost savings by sector, 2021 prices

	Total Compliance Cost Saving (£m)						
Sector	Legitimate Interests	AI and Machine Learning	Research Purposes	Accountability Framework: Record Keeping	Privacy and electronic communications	Subject Access Requests	Total
Agriculture, Forestry and Fishing	0.1	0.1	0.3	1.1	0.5	1.5	3.5
Manufacturing	0.3	0.1	0.5	1.8	0.8	8.4	11.9
Mining, Energy, Water	0.0	0.0	0.1	0.2	0.1	0.9	1.3
Construction	0.6	0.4	1.2	6.4	2.5	2.8	14.0
Wholesale and Retail, Repair of Vehicles	0.6	0.3	1.2	3.8	1.8	8.8	16.5
Transport and Storage	0.2	0.1	0.4	2.2	0.8	2.6	6.3
Hotel/Catering	0.3	0.1	0.6	1.3	0.7	4.7	7.8
Information and Communication	0.3	0.2	0.5	2.4	1.0	3.1	7.5
Finance and Insurance	0.1	0.0	0.2	0.7	0.3	2.4	3.7
Real Estate	0.1	0.1	0.2	0.9	0.4	1.3	3.1
Professional/Scientific/Technical	0.7	0.4	1.2	5.9	2.4	7.4	18.0
Administrative and Support Service	0.4	0.2	0.8	3.2	1.3	6.8	12.7

[235] UK Business Data Survey (2021)

Education	0.1	0.1	0.3	2.1	0.7	0.6	4.0
Human, Health and Social Work	0.2	0.2	0.5	2.4	0.9	4.6	8.8
Arts, Entertainment and Recreation	0.2	0.1	0.3	1.9	0.7	2.1	5.3
Other Service Activities	0.3	0.2	0.5	2.4	0.9	1.1	5.3
Total	4.5	2.5	8.7	38.7	15.8	59.1	129.3

Familiarisation Costs

545. We expect to see distributional familiarisation costs across different sectors of the economy as a result of the reforms. The estimated familiarisation costs differ between sectors based on the business data use results from the UK Business Data Survey. This defines the number of businesses per sector that are impacted by the reforms.

546. The table below shows the familiarisation cost estimates broken down by sector. Similarly, to compliance cost savings the sector with highest estimated familiarisation costs is Professional/Scientific/Technical as this has a high level of data use and the sector with the lowest estimated familiarisation cost is Mining, Energy and Water which in comparison has a lower level of data-use so is to be expected.

547. Findings from the UK Business Data Survey, 2021[236] state that businesses in the Finance and Insurance sector were more likely to share personal data than other sectors, however, we do not expect the Finance and Insurance sector to be disproportionately impacted as data suggests that 90% of businesses in this sector already have privacy frameworks in place and are 'very confident' in their staff's proficiency in handling personal data. Businesses in this sector are also more likely to employ someone leading on data protection compliance when compared to the Construction or Wholesale and Retail sector. Approximately 98% of firms in the Finance and Insurance sector also expressed confidence in understanding and complying with data subjects' rights under GDPR and DPA 2018 and are more likely to be aware of the ICO and their guidance already in place. As a result, we expect that this sector will face lower costs when familiarising themselves with these policy changes than other sectors which may not already have frameworks in place.

Table 57: Familiarisation costs by sector, 2021 prices

Total Familiarisation Costs (£m)							
Sector	Legitimate Interests	AI and Machine Learning	Research Purposes	Data Minimisation and anonymisation	Accountability Framework: Record Keeping	Privacy and Electronic Communications	Total
Agriculture, Forestry and Fishing	0.2	0.1	0.1	0.2	1.3	0.1	2.0
Mining, Energy, Water	0.1	0.0	0.0	0.1	0.3	0.0	0.5

[236] DCMS: UK Business Data Survey, 2021

Manufacturing	0.4	0.2	0.2	0.4	2.6	0.3	4.1
Construction	1.1	0.5	0.3	1.1	8.1	0.5	11.6
Wholesale and Retail, Repair of Vehicles	0.7	0.3	0.2	0.7	5.8	0.6	8.3
Transport and Storage	0.2	0.1	0.1	0.2	2.4	0.3	3.3
Hotel/Catering	0.3	0.1	0.1	0.3	2.4	0.2	3.4
Information and Communication	1.1	0.2	0.6	1.1	3.1	0.6	6.7
Finance and Insurance	0.3	0.1	0.2	0.3	1.1	0.2	2.2
Real Estate	0.2	0.1	0.1	0.2	1.5	0.2	2.3
Professional/Scientific/Technical	1.8	0.5	0.8	1.8	7.9	1.0	13.8
Administrative and Support Service	0.8	0.3	0.4	0.8	4.4	0.6	7.3
Education	0.5	0.1	0.2	0.5	2.4	0.4	4.1
Human, Health and Social Work	0.8	0.2	0.4	0.8	3.2	0.6	6.0
Arts, Entertainment and Recreation	0.5	0.1	0.2	0.5	2.2	0.2	3.7
Other Service Activities	0.4	0.2	0.1	0.4	2.9	0.3	4.3
Total Cost	9.5	3.0	3.8	9.5	51.8	6.0	83.7

Geographical Impact

548. Based on our research and evidence we do not expect the reforms aimed at UK private sector organisations to have disproportionate geographical impacts. We expect the reforms to impact all parts of the UK and have distributional impacts. Results from the UK Business Data Survey show no evidence of disproportionate impacts on Northern Ireland compared to the rest of the UK.

549. Police officers in the Metropolitan Police Service (MPS) make up one quarter of all total police officers in England and Wages and so the impacts of proposals concerning LEAs will be larger in London compared to the rest of the UK.

A summary of the potential trade implications of measure

Summary

550. Cross-border data transfers are a key facilitator of international trade, particularly for digitised services. Transfers underpin business transactions and financial flows. They also help streamline supply chain management and allow business to scale and trade globally. [237]

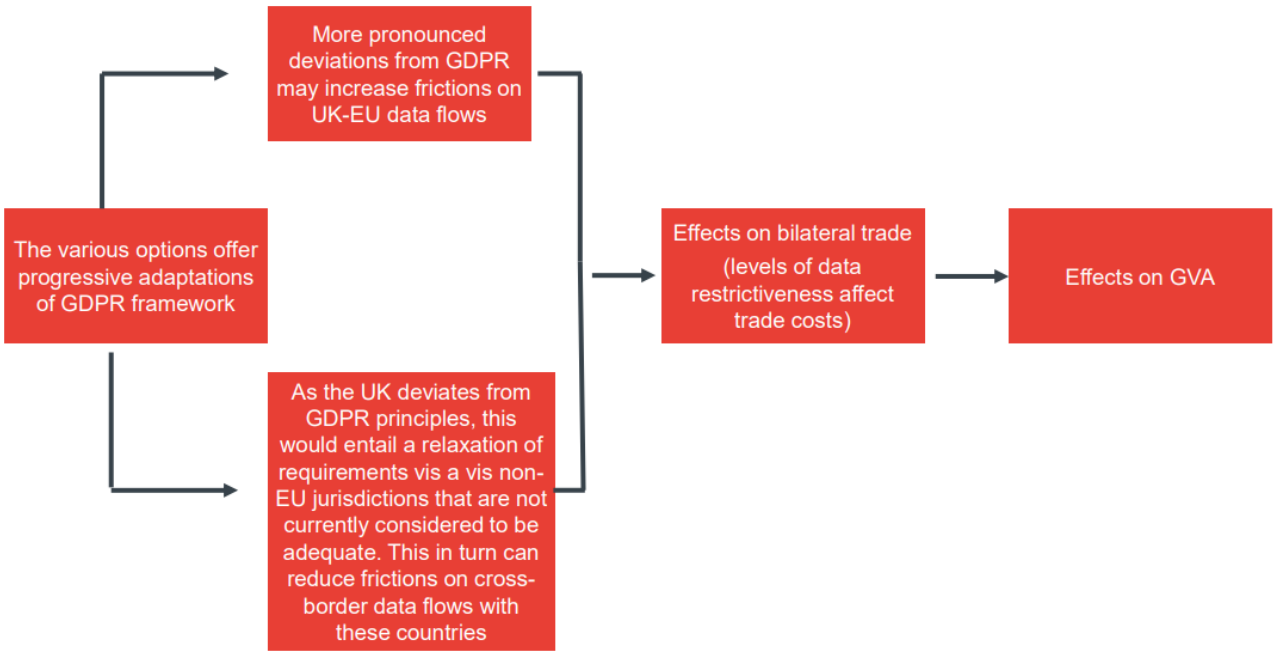
551. DCMS analysis of ONS data shows that the UK exported £234 billion in digitally/remotely delivered services (74% of total UK services exports) and imported £124 billion services via remote trade (57% of UK services imports) in 2019.[238] This section aims to provide a novel look at the potential of data reform to enable more trade between countries. The analysis however includes several important caveats, outlined below, which means that the results should be treated as merely indicative of the range and scale, rather than a granular and detailed account of the impacts. **For this reason, none of these results are included in the summary EANDCB and NPV**. Instead this section provides a transparent exposition of all of the research the department has undertaken and gathered as part of this analysis, with an aim to assist in further developing our understanding of this topic and help drive research - while also contributing into defining our monitoring and evaluation framework that will hopefully help us refine our estimations in the future.

552. Cross-country analysis indicates that both data policies on domestic use and the cross-border movement of data are likely to have an effect on productivity. Ferracane et al. 2018 found that countries with stricter data policies have a negative and significant impact on the performance of downstream firms in sectors reliant on electronic data. This adverse effect is stronger for countries with strong technology networks, for service firms, and holds for several robustness checks.[239] Cross-border digital trade has grown rapidly in recent years, as new digital products and business models have been delivered globally by improvements in technology and communication. This changes the nature and compositions of trade, as well as its overall value. In total, the value of UK data-enabled exports grew from £185.8 billion in 2008 to £295.8 billion in 2018 (51% of total exports), representing 59% growth.[240]

553. Policies that make substantial changes to the UK GDPR framework may lead to EU-UK frictions, and a decrease in requirements with non-EU jurisdictions. As a result, both the data flows and trade between these three groups of countries are likely to change. This will cause a change to production patterns and ultimately productivity, measured by GVA. This theoretical framework is presented in the diagram below.

Figure 3: Theory of change following a change to UK GDPR legislation

[237] DCMS (2021), International data transfers: building trust, delivering growth and firing up innovation
[238] DCMS internal analysis on the world total of UK services exports, based on 2019 ONS published statistics, in sectors defined as data-enabled by UNCTAD (United Nations Conference on Trade and Development).
[239] European Centre for International Political Economy (2020) Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?
[240]DCMS calculations: The primary approach used by DCMS is to estimate the UK's data-enabled service exports and imports. DCMS uses ONS trade data and UN classification of 'digitally deliverable services', to aggregate services trade in certain digitally deliverable industries. This provides an estimate of potentially data-enabled services trade.



554. The proposed measures in the Data Protection and Digital Information Bill are designed to boost data use and reduce barriers to data flows. This in turn is expected to increase data-dependent trade, along with higher data sharing and flows with international trading partners.[241] At a high-level, the theory of change for the proposed measures (seen in Figure 4) is that general improvements in flexibility for data transfers and reduced services trade restrictiveness are associated with an increase in trade. Moving to a system which allows personal data to be transferred more flexibly via data bridge or Alternative Transfer Mechanisms (ATM's) is expected to lower transaction costs and increase cross-border data flows.

Figure 4: Theory of change following a change to GDPR legislation

555. Estimating changes in trade and onward productivity benefits is fundamentally challenging. Data economics is a nascent field and assessing the impact of policy reform is still under development both in academia and the industry. This is even more so the case when looking at the impacts of data policy on trade. To illustrate this point, the EC's impact assessment for implementing GDPR did not evaluate impacts on trade, making the quantification of some of the impacts of reforming data policy novel in their approach.

556. The analysis uses a 'bottom-up' approach developed by DCMS using business-level data. Limited direct impacts of a data bridge or Adequacy can be straightforward to model, businesses no longer face the need for alternative transfer mechanisms to transfer personal

[241] Ferracane, M., van der Marel, E., Do Data Policy Restrictions Inhibit Trade in Services? (2018)

data saving time and legal costs. At the same time, the reduction in non-tariff barriers likely represents an opportunity for additional indirect impacts for increased trade beyond the value of reduced compliance costs and direct loss of export revenue when costs are imposed. This method likely underestimates the impact as a result.

557. The **results of this analysis are therefore indicative** and for the purposes of transparency and **do not** form part of our overall estimates for the total cost and benefits of the package of reforms. Scenario analysis and sensitivity testing is also employed to capture uncertainty with the approach in the following sections of the Impact Assessment.

Rest-of-world data bridge modelling approach

558. UK data reform will support the UK's ambition to encourage greater flows of data internationally. This is consistent with international commitments in areas such as trade and the Free Flow of Data with Trust framework. These commitments involve supporting the free flow of data and moving away from more protectionist approaches.

559. We have developed an approach that assesses the number of businesses that rely on data to trade, and estimates the potential impact of the following reforms on business costs and trade:

a. Underpinning the UK's future approach to regulations establishing a data bridge with principles of risk-assessment and proportionality[242]

b. Relaxing the requirement to review data bridge regulations every 4 years

c. A new power for the Secretary of State to formally recognise new ATMs

d. Changes to the standard and approach to alternative transfer mechanisms. (Art 46)

560. Businesses currently face costs to trade with countries we do not have a bridge with when that trade involves sending personal data. As a result, when businesses choose to trade or not they face compliance costs in the form of implementing International Data Transfer Agreements (IDTAs) or Standard Contractual Clauses (SCCs)[243]; if these costs outweigh potential profits from trade, businesses may choose not to trade. It should be noted that this approach takes a focused look at direct changes in compliance costs for businesses once the UK has a data bridge with those countries. The potential of the reforms would remove the cost of implementing IDTAs in contracts with business partners in those countries. The estimates provided are the **annual, maximum, theoretically-realisable benefit once the UK has established a data bridge with all non-red-rated, non-adequate, RoW countries.** It is not necessarily the case that the UK will establish a data bridge with all possible countries, instead the UK is undertaking a prioritisation exercise to identify countries that are most likely to receive one. The UK government has prioritised a number of countries for initial assessments of data bridge regulations ; Australia, Colombia, Dubai International Financial Centre, Republic

[242] Replacing adequacy, 'data bridge' is the term now used by the UK government to describe the mechanism for the trusted flow of data from the UK to another country without restrictions.
[243] From 21 March 2022, the ICO's IDTA took effect as a replacement for the EU SCCs. For the purposes of this analysis, the old SCCs and the IDTAs are treated as equivalent in terms of how they function and how much they cost to implement. DCMS is currently undertaking an evaluation of the change to verify this assumption. To maintain the language of the previously published DPDI Bill IA and the published RoW Adequacy Umbrella IA, SCCs are used below throughout.

of Korea, Singapore and the United States of America. Longer term priority partners are: Brazil, India, Indonesia, and Kenya.

561. Individual businesses' SCC costs were estimated using DCMS survey data in which businesses estimated the time required to put SCCs in place. It was assumed that these estimates equate to one full time administrator working for the length of time given by the respondent. ONS Annual Survey of Hours and Earnings[244] published statistics on average salary by profession were used to calculate the resultant cost. Per RPC guidance, a non-wage uplift of 22% is applied.[245] These costs are shown below:

Table 58: Average cost of SCC's according to business size, 2021 prices

Number of employees	Average SCC cost to businesses (over 5 years)
Micro (0 - 9)	£7,015
Small (10 - 49)	£13,176
Medium (50 - 249)	£15,128
Large (250+)	£20,618

562. These are the one-off costs incurred by a business as it becomes compliant to exchange data internationally, and are assumed to hold until the beginning of a new five-year contract cycle.

563. These cost assumptions reflect the average over all UK businesses in each size category. The cost for the 'micro' category in the *Transfer Tools Survey* is the weighted mean of the 0 and 1-9 categories, weighted by the business population in each category. The large category includes a relatively small number of very large businesses that will incur considerably higher costs.

564. The main reason the cost increases by business size is that larger businesses generally have more contracts with a greater number of foreign business partners that involve the exchange of personal data. Therefore, the total amount of work required to implement SCCs to cover all their international relationships is greater. The relationship is not linear by employee size with a large increase between costs to sole traders and micro businesses being observed, reflecting the evidence that small and micro firms might be proportionally more affected by compliance costs than larger firms.

565. Analysts in BEIS, DIT and HMT, and a data protection lawyer in BEIS were consulted to obtain a view on how reasonable these SCC cost estimates are. The general consensus was that they were likely to underestimate the real cost, although it was agreed that it was better to remain on the conservative side in order to avoid overestimating the total impact estimated by the model. Therefore, these inputs have been widely agreed upon for use in modelling the cost implications of SCCs.

566. The first direct benefit of a data bridge is the removal of the cost of implementing SCCs, in contracts with business partners in that country. Businesses currently trading with those

[244] Employee earnings in the UK Statistical bulletins, ONS
[245] RPC guidance on implementation costs, 2019

countries no longer face the compliance costs of setting up SCCs. The top-down estimate of the total, global cost (excluding the EU) of this comprises the following steps:

567. Take the total number of UK businesses by size category from ONS Business Population Estimates 2020.[246] The size categories used are commonly-used:

Micro (0 to 9)
Small (10 to 49)
Medium-sized (50 to 249)
Large (250+)

568. The *International Transfer Tools Survey*, conducted in October 2020, provided the percentage of UK businesses that send data to the Rest of World, by the same size categories.

569. The product of categories 1 and 2 gives us the number of UK businesses that send data to the RoW.

570. The *UK Business Impacts Model* (described below in the EU Adequacy loss section) has been regularly used and updated since 2018 to estimate the cost to individual businesses from implementing SCCs. This was originally used to estimate the cost to businesses of the UK leaving the EU without an Adequacy decision. We assume it costs a UK business the same to implement SCCs to enable transfers of personal data to the RoW as it does those to the EU. This is a reasonable assumption as the work would generally be carried out by the same people in either case.

571. The Business Impacts Model assumed that all relevant businesses would be required to incur this cost upon the UK leaving the EU. However, since the contractual relationships that include SCCs with the RoW already exist, the average five-year contract refresh cycle assumption is used here in order to spread the benefit. Therefore, the SCC cost estimates are divided by five to obtain a per-year value.

572. Multiplying category 3 and 4 together gives us the total cost by size category to businesses of implementing SCCs with respect to transfers of personal data to non-EU countries.

573. Taking the total over the size categories gives us the final estimate of **around £360m for the current**, **annual SCC cost**.

Table 59: Total annual SCC cost, 2021 prices

	Micro (0 to 9)	Small (10 to 49)	Medium (50 to 249)	Large (250+)	Total (rounded)
Population	5,724,700	211,845	36,140	7,835	6m
% send data to RoW	4%	6%	16%	31%	4%
Num. send data to RoW	209,185	13,391	5,901	2,448	230k
SCC assumption per year (incl. non-wage cost uplift)	1,403	2,635	3,026	4,124	
SCC cost per year / £m	£294m	£35m	£18m	£10m	£360m

[246] Business population estimates (2020), BEIS

574. For **small and micro-businesses**, although a relatively small proportion send data to the RoW, because they make up by far the majority of UK businesses the majority of the estimated SCC cost applies to them, at **£330m**.

Top-down - Suppressed Exports

575. Additional export activity will be enabled if other countries' data protection standards are determined as adequate. SCC costs will be removed and no longer act as a non-tariff barrier. The EU Exit modelling work mentioned below, in addition to the SCC cost, also estimates the value of exports that would be lost as a result of the cost of SCCs becoming necessary to receive personal data from the EU in order to export services there. The value of these exports as a proportion of the current total can be used as a 'suppression factor', i.e. the proportion by which exports to the EU would be suppressed by the cost of SCCs acting as a barrier to trade.

576. To estimate the additional export activity, the inverse of this suppression factor is applied to the value of current data-dependent RoW exports, on the assumption that trade is already suppressed in the same manner. Therefore, the following formula is applied to the export value. This formula 'inflates' the current export value back up to 100% from its presumably suppressed value, and takes the difference between that and the suppressed value.

$$d\frac{1}{1-s} - d$$

where:

- Data-dependent RoW exports,[247] £220bn * 14% = £30bn
- The data-dependency value of 14% is taken from the *UK Business Data Survey*
- Suppression factor, *s* = 0.0030 (high=0.005; low=0.0026)

577. Here, data-dependent RoW exports excludes countries that already have a data bridge and those given a red rating during the gate-keeping process mentioned earlier in this document. Two of the most common reasons for exclusion is that a country has little or no data protection legislation and/or there are security or privacy concerns.

578. This gives a value of around **£90m (with a sensitivity range of £80m-£160m based on low and high suppression factor estimates) per year in suppressed export revenue** that is assumed would be enabled if all non-red-rated, non-EU and those that do not currently have a data bridge were given a data bridge by the UK.

579. This estimate makes two important assumptions:

a. That the effect of SCC costs on exports to the RoW is currently the same as that on exports to the EU would have been had we not received an Adequacy decision from the EU. That the effect is symmetrical. The EU Exit analysis modelled the need to receive data from the EU in order to export to the EU. The suppressed trade calculation here applies the same methodology to exports to the RoW that depend on sending data to

[247] Services from UK trade in services: service type by partner country, non-seasonally adjusted (2022) and goods from UK Overseas Trade in Goods Statistics Summary of 2021 Trade in Goods (2020).

the RoW. This assumption is necessary because we currently lack the analysis to differentiate between the two directions.

580. It is not possible to produce a suppressed export revenue figure specifically for small and micro-businesses. Whilst we know from ONS data that around £15.6bn of exports to the RoW is attributable to these businesses,[248] it is not possible to remove those with a data bridge and red-rated countries from this value and so any figure produced would be a considerable overestimate (for all business sizes, adding in red-rated countries adds around £60m to the £90m estimate).

Impact on firms on changes to Article 27 representatives

581. The main function of Article 27 representatives is currently to facilitate effective and prompt communication between controllers and processors caught by the extraterritorial scope of UK GDPR - Article 3(2), who have no establishment or presence in the UK and UK data subjects and the ICO.

582. Controllers and processors within scope of Article 3(2) could potentially be more difficult to contact for UK data subjects and the ICO, than those controllers and processors who are either based or have establishments in the UK and the existence of an Article 27 UK based representative may help mitigate this.

583. There is limited information and data on the benefits of having an Article 27 representative as it is a relatively new and untested requirement and also one that applies exclusively to businesses and organisations outside of the UK which makes gathering evidence very challenging. It is therefore difficult to ascertain precisely how successful the Article 27 representative is at facilitating effective communication.

584. Whilst evidence is limited on the costs and benefits of Article 27 representation, since the initial version of the Impact Assessment was published we have conducted a market review and worked alongside representative service providers to gain a greater understanding of the prices and services offered.

585. Market wide, the cost of an Article 27 representative differs depending on the revenue of the company, the number of data subjects the company has, and the type of service offered. As of February 2023 firms such as Versafe[249] prices range from $2,700 for a small firm with less than $25 million annual sales to $12,000 for firms with sales between $100 and $500 million a year. Data rep[250] on the other hand offer services to small companies with less than 1000 data subjects for between $161 and $269 a year, and for companies with up to a million data subjects $5,000-$6,000 a year. Services offered by Prighter[251] also vary depending on the size of the business but fall between €19 a month for start up businesses and €480 a month for large businesses.

586. In line with our initial estimates provided in the June 2022 Impact Assessment costs of Article 27 representatives increase with the size of the firm, however, the variety in packages and services offered for these prices make them difficult to compare.

---

[248] UK services trade by business characteristics: 2016 to 2018 (2020), ONS, figure 2.
[249] https://verasafe.com/privacy-solutions/gdpr-article-27-representative-program/
[250] https://www.datarep.com/shop/?wcmlc=GBP
[251] https://prighter.com/product/gdpr-rep/

587. There is also currently no available evidence that suggests the true level of compliance with Article 27 under the UK-GDPR, and in reality, this may be very low. Therefore, we are unable to provide quantitative estimates of the impacts of removing the requirement for a representative.

588. It should also be borne in mind that the Data Protection Act 2018 requires that organisations outside the UK, that receive UK personal data, implement Article 27 representatives in the UK and it is not possible with currently available data to estimate this cost.

589. Although reliable quantitative data is unavailable, we have provided a qualitative overview of some of the potential benefits and costs associated with the reform, and will factor in this evidence gap into our Monitoring and Evaluation framework.

590. The removal of Article 27 costs may be economically beneficial to firms with representatives outside of the UK that are already caught by Article 3 and are already easy to contact, as this will remove an administrative burden from them. Any cost associated with appointing a UK representative can be considered a compliance burden for businesses and a potential barrier to trade. By removing the mandatory obligation to appoint a representative, this financial burden will ease, especially for medium and small sized enterprises with lower revenue, that choose to no longer use one.

591. There may also be potential efficiency gains to be made from the removal for UK firms as there are other articles in the UK GDPR which already mandate effective communication between the ICO, UK data subjects and controllers and processors caught by Article 3(2).

592. By removing Article 27 there is also scope that this will reduce the requirements on businesses that trade internationally and as a result, reduce the potential for conflict with trade commitments on e.g. local presence, market access and different treatment for different companies/investors.

593. These potential benefits to firms must be balanced against the fact that there may also be costs to businesses, such as a decrease in methods of communication with the ICO, and the risk to EU Adequacy of making changes to the UK GDPR that could impact the effectiveness of data transfers.

594. Having an Article 27 representative can also bring benefits to a firm, though these are often difficult to monetise. For example in The International Association of Privacy Professionals Response to the DPDI bill,[252] potential benefits are highlighted and include facilitating easier communication between data subjects and firms, offering specific skills and knowledge to help overseas companies understand UK privacy laws and also additional tools that may form part of a package that offer solutions to dealing with data subject requests, data breaches or legal services. These benefits can help firms keep costs low, ensure compliance with privacy laws and result in time saving efficiencies in the long run.

595. By offering firms a choice over whether to appoint an Article 27 representative, we are enabling them to make a decision, based on their own organisational circumstances, on the relative costs and benefits of representatives. This should also make the representative market

[252] https://iapp.org/news/a/the-value-of-a-u-k-representative-a-response-to-the-dpdi-bill/

more competitive, at the expense of those providers "who offer little more than a postbox service". [253]

Impacts of ensuring businesses are able to continue to seamlessly use their pre-Bill existing transfer mechanisms

596. This reform provides for additional transitional arrangements in the Bill for a wider set of current alternative transfer mechanisms (ATMs). Similar to the approach taken for pre-commencement adequacy regulations and pre-commencement standard data protection clauses, this reform introduces transitional provisions for pre-Bill appropriate safeguards in Article 46 UK GDPR, Schedule 21 (paragraph 9) DPA 2018, and Section 75, Part 3, 2018 Data Protection Act currently in operation which meet the required level of protection under the existing framework.

597. The UK's standard data protection clauses, the International Data Transfer Agreement and Addendum to the EU Standard Contractual Clauses, are already captured by transitional provisions in the Bill. These are the most widely-used alternative transfer mechanism. Currently, the Bill outlines at a high-level, provisions for an ATMs data protection test (which has been supplemented by the ICO's recently issued Transfer Risk Assessment [TRA] tool). Without these transitional provisions, this data protection test would result in businesses who use less well-used alternative transfer mechanisms incurring familiarisation costs. Businesses would have to check whether the new data protection test is met and potentially seek reapproval by the ICO for some ATMs, even when they meet the required level of protection under the UK's current framework. This would mean a UK data exporter would incur familiarisation costs before they can continue to transfer personal data using the mechanism. The TRA Tool has recently been published in November 2022 and the ICO published an IDTA and TRA (IDTA Toolkit) impact assessment in December 2022 which sets out some of the relevant familiarisation costs. In summary, these additional transitional provisions capturing a wider set of alternative transfer mechanisms mean the familiarisation costs that would have been incurred as a result of the original Bill text can be mitigated against.

598. The reform introducing additional transitional provisions acts to mitigate an issue that has been identified since the submission of the original IA. As a result, compared to the do-nothing scenario, no major additional costs or savings are incurred to those businesses using the transfer mechanisms in scope of this reform. Costs capturing potential familiarisation and compliance costs for those mechanisms not captured in the previous transitional provisions should have been calculated at that time but were not. Qualitatively we acknowledge there may be very small costs for checks required by those responsible for data protection to check in with any guidance to make people aware of which pre-Bill Mechanisms will remain valid

Risks of changes to the EU/UK Adequacy agreement

599. EU Adequacy decisions are adopted through a unilateral, autonomous EU process controlled and managed by the European Commission. It is for the EU to decide how it monitors and reviews them.

600. As the Commission itself has made clear, a third country is not required to have exactly the same rules as the EU in order to be considered adequate. They must be considered to provide

[253] https://iapp.org/news/a/the-value-of-a-u-k-representative-a-response-to-the-dpdi-bill/

an ‘essentially equivalent’ level of protection for data subjects. The UK continues to move forward with our ambitious, pro-growth data agenda while maintaining our high standards of data protection.

601. The UK’s position is that the proposals within the Bill are consistent with maintaining EU adequacy. That said, it is the Government’s responsibility to model a range of scenarios, including those we consider unlikely, as part of our sensitivity analysis. Therefore, we have included an analysis that estimates the impact in the event of a loss of adequacy through a full and immediate revocation of the decision by the EU on the day the bill is introduced to Parliament. This is a scenario the Government considers highly unlikely, and this analysis does not attempt to assign probabilities to the scenario.

602. As there is uncertainty in both the likelihood and timing of any potential decision, the impact is not included in the net present value or other measures in the summary for the IA as a whole. The analysis also only considers the commercial impact of a full and immediate revocation of the GDPR adequacy decision. It does not consider scenarios relating to an amendment or partial suspension of GDPR adequacy and does not consider wider impacts on the provision of public services. The analysis does not include the LED adequacy decision. The impacts have been uprated and discounted as if the decision was made presently. The impacts are presented for the purposes of transparency.

603. It is important to note here that adequacy decisions are distinct from financial services equivalence decisions. Currently, the EU only has one, time-limited, financial services equivalence decision in place for the UK (the UK has granted the EEA 28 equivalence decisions; the UK’s decisions are not time-limited). Data adequacy is not linked to these financial services equivalence decisions, so a loss of adequacy would not directly impact them. In the event adequacy decisions were withdrawn, financial services firms carrying out personal data transfers may need to use alternative transfer mechanisms to transfer personal data.

604. The model assumes that in the absence of adequate arrangements, UK businesses that trade personal data would have to use EU SCCs as an alternative transfer mechanism (because in the absence of adequacy EU organisations would only be able to send personal data to the UK if an alternative legal basis under EU GDPR were available). These legal requirements and associated implementation costs would act as non-tariff barriers to trade. The assumption is that businesses whose export revenue from trade with the EU exceeds the cost of implementing EU SCCs would accept the cost impact and continue to operate, while for the rest they will cease to trade with the EU. EU organisations would also incur costs, but these have not been included in the analysis. The overall cost would be captured by total lost export revenue and the total cost of implementing EU SCCs.

605. As a result, there is a trade-off between the two impacts, as more businesses incur SCC costs, less export revenue is lost. The model analyses across all goods and services sectors. However, it should be noted that the goods proportion of the result is constant across the scenarios (£200m in lost revenue and £40m in SCC costs) and has not been updated since the initial pre-consultation analysis due to data availability. The analysis was previously carried out by HMRC in a commission from DCMS; we were not given continued access to the underlying HMRC customs data required to update this estimate.

606. The model previously estimated that the direct financial impact on UK businesses would be around £1.4 billion over five years, the estimated period in which compliance and SCCs would

fully feed through to affected organisations. This comprised around £1 billion in reduced trading revenue and £420 million in increased compliance (SCC) costs. The services methodology has now been reviewed and improved upon in line with evidence accumulated between consultation and this final stage assessment.

607. The changes extend beyond the previous parameters used and affect key parts of the methodology, rendering it difficult and erroneous to compare previous results (expressed over a 5-year horizon), with the new results (expressed over a 10-year horizon). Namely, our updated assumptions over compliance rates, following RPC best practice to assume 100% compliance from year 1, means the update is conservative when calculating lost export revenue over a 10-year period as costs are incurred annually. It is instead likely there would be a lead-in period for business compliance meaning lost export revenue would be smaller in nearer years, an approach reflected in our previous methodology.

608. We have adapted some of the previous assumptions such as:

- Assuming a 100% compliance rate to reflect that all UK businesses comply with all data compliance requirements. It is likely an unrealistic, but analytically conservative assumption as some businesses will fail to comply with the regulations in practice (and therefore will continue to trade without additional costs). We have sensitivity tested this parameter with compliance between 80-100%.

- A share of UK businesses that trade with the EU already have SCCs in place, reflecting DCMS' past effort to encourage their use due to the risk in the event of a no-deal EU Exit. We estimate it to be14%, based on results from the UKBDS. The figures vary drastically by business size (from 9% for sole traders to 47% for large businesses). 14% is potentially an overestimate due to the two questions in the UKBDS that ask about SCCs being independent from one another.[254] Not all businesses that have SCCs in place necessarily use them with respect to EU trade, if they also share data with the RoW.

- Not all costs are borne by UK businesses and that a percentage of the costs will fall on EU businesses,[255] especially where firms hold market power. Again, the figures vary by business size (from 25% for sole traders to 50% for large businesses). This represents the fact that legal expertise from the EU side is also needed when putting SCCs in place meaning some of the cost is passed onto EU businesses. The amount of this legal cost which is passed on increases with business size, representing the power of larger businesses to pass on costs to EU partners and implicitly reflects their market power.

- We have updated the investment horizon that the business considers when making its decision whether to continue trading or not. Previously we assumed firms only considered a single-years export profits, we now assume a five-year horizon. If the cost of implementing SCCs is greater than five years' worth of export profit then firms will cease trading. The previous assumption did not reflect the evidence since collected through stakeholder engagement, and while the exact time horizon will depend on the business planning of each firm, a five-year

[254] These 2 questions include 'do you trade with the EU?' and 'do you have SCCs in place?'
[255] The Cost of Data in Adequacy (2020), New Economics Foundation

horizon is a more realistic representation. We have also updated the assumed profit margin on exports.[256]

- The latest profitability of UK company's data shows a 14.6% average profit margin over the last 5 years for service sector businesses. A 5 percentage point downwards adjustment for risk aversion is made resulting in an assumption of 9.4%.

- Sensitivity analysis has been conducted around all of the parameters to account for the uncertainty and confidence associated with each. A Monte Carlo simulation has also been undertaken (see Annex 4) to explore how the uncertainty of parameters interact with each other. Discussion of how parameters differ by scenario is in the Risks and Sensitivities section below.

609. The results of the updated modelling estimate an economic impact of £410m (range of £190-£460m) in one-off SCC costs and an annual cost of £240m (range of £210m and £420m) in lost export revenue. Once appraised over a 10-year period, the estimated NPV (2019 prices, 2020 present value) of EU Adequacy is £2 billion (range of £1.6 and £3.4 billion).

610. Trade impacts may be higher when considering supply chain impacts as this analysis focuses on direct UK-EU exports only. However, unfortunately at this time supply chain data is limited.

611. Including these costs in the calculation of the total NPV for the bill is not appropriate due to uncertainty in both likelihood of the loss of EU adequacy occurring and the timing of which it is lost. It is also important to note that all trade effects would likely take place over the medium/long term and trying to include them in a clear 10-year horizon (NPV calculation) is fundamentally not robust.

612. The table below presents a scenario in which EU adequacy is completely revoked. This is the NPV of the Data Protection and Digital Information Bill if adequacy were to be lost in the first year after the implementation of the bill. This has only been presented for indicative 'worst case scenario' purposes and should not be interpreted as the final NPV of the package of the reforms, or as even a potential scenario based on the Government's engagement with its international partners.

Table 60: NPV of the bill when EU adequacy is revoked

Net Benefit (Present Value (PV)) (£m)					
Low:	-2,140.1	High:	7,416.7	Best Estimate:	2,684.8

613. Additionally, the table below adds the potential benefit of data bridge regulations to all possible rest-of-world countries. This is again not a potential scenario but it is also provided for illustrative reasons and to provide a more comprehensive picture of all the potential effects that the government has considered. As above, an annual benefit of up to £360m in SCC benefits with a range of export revenue benefits (£80m, £90m and £160m) was calculated. Similar to the impacts of the loss of EU adequacy, the timings of individual data bridge regulations are

[256] Profitability of UK companies – rates of return and revisions the data used is focused on non-financial corporations. Whilst not lining up directly to the business types of focus in our analysis, we take a downwards adjustment for risk aversion. Similarly, the exclusion of financial sector corporations likely has a downwards impact on the average as it is likely the financial sector has high profit margins. The parameter is also adjusted as part of sensitivity analysis below.

uncertain and the benefits identified are if all countries are awarded data bridge regulations. Presently, only a number of countries have been announced to be taken forward for assessment. As a result, assigning the benefits in the first year of the NPV calculation is unrealistic. The below should not be interpreted as the final NPV of the package of reforms.

Table 61: NPV of the bill when EU adequacy is revoked but adequacy to all other countries is considered

Net Benefit (Present Value (PV)) (£m)					
Low:	974.8	High:	11,097.9	Best Estimate:	5,870.5

Risks and assumptions

Introduction

614. We have ensured that the analysis carried out in this Impact Assessment is detailed and robust. Where numerical evidence is not yet available we have provided a qualitative assessment of the costs and benefits of the preferred option. This analysis is detailed and thorough however some of it relied on assumptions that are open to debate. We have therefore ensured that we have carried our sufficient sensitivity analysis and testing to make sure that we accounted for these potential risks. In this section we provide a breakdown of the key risks identified and the sensitivity analysis carried out. We also provide an overview of the policy risks related to the set of reforms.

Policy Risks and Assumptions

Parliamentary opposition

615. There may be targeted opposition on specific elements of the Bill by Parliamentarians, supported by pressure from the NGOs. In particular, we expect there to be some opposition to the introduction of a Secretary of State approval process for ICO statutory codes of practice, and the removal of the requirements for controllers and processors to appoint Data Protection Officers in certain circumstances, complete Data Protection Impact Assessments in relation to specific processing activities and consult the ICO on any high risks identified. Some might argue that these measures could result in a reduction of protection for individuals, including in relation to sensitive healthcare data or data relating to children. We also expect some opposition related to the perception that the reform package could lead to the loss of the UK's global standing (as a result of ICO reforms), and the revocation of EU Data Adequacy decisions for the UK. This concern has already been raised by a Parliamentary Trade Committee.

616. The ICO are supportive of the reforms in the Bill and have indicated this position publicly, but will likely publicly oppose if there are any new measures during passage that they believe infringe on their independence. We have worked closely with the Information Commissioner on these reforms.

617. We undertook a significant amount of engagement during the consultation period and will work with strategic stakeholders in advance of the launch who may wish to publicly support

this work, for example, Tech UK is already developing case studies to demonstrate the benefits of our data reform.

618. In relation to the criticisms around the removal of DPO, DPIAs etc. we will highlight the measures with which they will be replaced. Organisations will still have to carry out risk assessments and appoint suitably experienced individuals responsible for compliance when their processing activities are likely to result in a high risk to individuals, but they will not be obliged to comply with prescriptive compliance rules currently required by the UK GDPR.

Devolved Administrations (DA) handling

619. We are aware that we will require legislative consent motions (LCM) for three measures in the reform package - the Digital Identity measure, the CDDO measure focusing on the Digital Economy Act s35, and the Smart Data measure.

620. DCMS will continue to work with the Devolved Administrations throughout passage to ensure we receive consent on our LCMs.

Improved Interoperability across Health and Social Care Systems

621. DCMS has worked alongside the Department for Health and Social Care to ensure that all policy risks of the proposed reform to increase interoperability across health and social care systems are included in this impact assessment.

622. Through clinical and non-clinical use case analysis, it is anticipated that the introduction of information standards compliance will be staggered and aligned to resolving interoperability challenges in line with the highest priority patient and citizen pathways. This limit (and signposts) the impact of changes required to be made by suppliers.

623. <u>The risk of IT suppliers leaving the market:</u> Digitisation of healthcare is a global trend and many suppliers are facing very high demand for their services, leading to significant backlogs for new installations. Many of the biggest suppliers are global (Cerner, Epic) however there are no global standards around interoperability. This means that suppliers can prioritise investing in standard configurations for other, larger markets, such as the US and not in bespoke products to meet the proposed health and care IT standards. Our proposals therefore risk IT suppliers leaving the market due to an increased burden to deliver a product or service that is compliant in England, the rest of the UK and/or other nations. To mitigate this, we intend to consider international best practice concerning interoperability and engage with the health and care IT supplier market to ensure both of these inform the contents of our IT standards.

624. <u>The risk of increased cost of IT products/services:</u> There is a risk that despite an increase in competition, prices increase because the increased cost of compliance outweighs the downward pressure on prices resulting from the increased competition. To mitigate this, we intend to develop the standards themselves and implementation of the measures in consultation with varying supplier types.

625. <u>The risk of provider non-compliance due to the inherent differences in the health and social care provider market:</u> Whilst the health care provider market is largely composed of NHS organisations, the providers in the adult social care market (although commissioned by local authorities) are largely independent, autonomous enterprises. There is already a pronounced level of fragility in the adult social care provider market. The proposed measures, if not

implemented with the inherent market differences in view, could be met with non-compliance, due to the costs associated with re-procuring from an accredited list of IT suppliers, and place an additional burden on care providers. To mitigate this risk, we intend to develop the implementation plan with stakeholder input to ensure that the plan is appropriate for the target market. There will also be funding provisions included in our measures as mentioned.

626. The value for money of any measures implemented using the powers established in the measures set out in this Impact Assessment will be assessed according to such developments, in advance of commencement regulations and/or regulations. Such regulations would also be reviewed constantly once in place, to understand and allow mitigation of any such risks.

Reform of the Accountability Framework

627. This policy instruction proposes to introduce a new accountability framework which would reinforce and expand on two of the core accountability obligations under Chapter IV of the UK GDPR, Articles 24 and 25, by introducing a requirement on controllers to implement a privacy management programme. The proposed framework aims to emphasise and establish more greatly the principles at the core of accountability, such as organisational responsibility, risk management, transparency, training and awareness of staff, and continuous monitoring, evaluation and improvement of data privacy management. As a result of the new framework a number of existing requirements will be removed.

628. To ensure organisations take a holistic and organisation-wide approach to accountability, there will be a requirement on controllers to implement a privacy management programme which should be tailored to the processing activities of the controller and be based on the controller having considered the volume and sensitivity of the personal data they are processing.

629. In order for a privacy management programme, and organisational accountability more widely, to be genuinely effective, all employees must be actively engaged in data protection to some extent, and this will be achieved through the requirement on controllers to ensure that staff understand the organisation's data protection policies and processes and proportionate training is provided where relevant. Organisations will have the flexibility to do this flexibly and suited to their own needs - for example, some may need their staff to be educated in data protection generally, and for those who handle personal data directly, they will need additional training specifically tailored to their roles. Therefore, the new framework will ensure adequate and appropriate training is conducted to give staff the knowledge and understanding they need to protect and handle data lawfully and in line with organisational expectations in their day-to-day roles, but without prescribing in legislation how this should be achieved.

630. There is a risk that the new framework is seen as a lowering of standards but the new requirements should strengthen the core principles of accountability by giving greater effect to the need for controllers to establish a holistic, robust and risk-based approach to data protection management which is embedded within the organisation. We expect the new requirements to result in the following improved outcomes in relation to the protection of personal data within organisations: better leadership, oversight and governance, greater transparency, more tailored, flexible and risk-based policies and processes, improved training and awareness, and ongoing monitoring and auditing.

631. There is a risk that many controllers will continue to comply with the current framework and may not implement a privacy management programme, resulting in a deadweight loss. However, given that we expect an explicit requirement on the face of legislation for controllers to implement a privacy management programme, we expect all controllers to implement this and failure to do so would result in an infringement of the law, and therefore the ICO would have the discretion to investigate and take relevant action, if necessary. Controllers may wish to incorporate their current policies and processes into their privacy management programme as long as all of the obligations under the new requirements are met.

Analytical risks and Assumptions

632. The analysis presented in this impact assessment is proportionate and detailed. Where costs and benefits have been able to be monetised, this has been carried out using certified and robust data sources. Where assumptions have had to be made due to a lack of available evidence we have highlighted these and carried out sensitivity analysis to test them where possible.

633. When carrying out the sensitivity analysis we have taken a proportionate approach, in occasions where the assumptions are minor we have flexed these by an arbitrary 15% as suggested in HMT's Green Book, in the case of modelling various scenarios surrounding EU Adequacy we have conducted Monte Carlo simulations to test multiple assumptions. We have also tested the total benefits, costs and NPV using Monte Carlo simulations. These assumptions and results are highlighted below.

Direct Benefits - Compliance Costs

634. Compliance cost savings have been calculated using both assumptions and evidence. The table below outlines the assumptions that are relevant to all measures that are expected to impact compliance costs for UK businesses. The rest of this section goes through the assumptions specific to each proposed reform.

Table 62: Assumptions used in modelling and RAG rating of confidence in assumptions

Assumption	Description	Source	RAG Rating
Number of businesses affected	Assumed the number of businesses affected by each measure	UK Business Data Survey	
Key compliance requirements and activities	Assumed the activities that would incur a compliance cost e.g. seeking legal advice, consumer complaints handling etc.	Frontier Economics and Data Protection and Digital Information Bill Consultation	

635. As outlined in the direct benefit section of this Impact Assessment, the package of reforms is expected to impact UK firms costs of compliance. As well as modelling our core scenario highlighted in the analysis, we have applied sensitivity analysis to our assumptions to build both a low and high scenario. Firstly, looking at the estimated annual compliance cost saving from creating a limited non-exhaustive list of legitimate interests for which businesses can use

personal data. The assumptions feeding into this estimation are below along with the low and high scenario values tested for each.

Table 63: Breakdown of assumptions for the legitimate interest's reform

Measure: Legitimate Interests[257]			
	Low scenario	Medium Scenario	High scenario
Effect: Need to seek legal advice to clarify regulation			
How much data use is affected by clarification under this measure	10%	25%	40%
% reduction in legal advice required to clarify the legislation in these cases	10%	25%	40%
% of these businesses that seek legal advice in a year	35%	50%	65%
Effect: Reduction in customer complaints about data use			
% data use affected	10%	25%	40%
% reduction in complaints	10%	25%	40%

636. We estimate that firms that analyse data and firms that use data for activities included on the list of 'recognised legitimate interests' (i.e. improving marketing or sales performance) will see a reduction in their compliance costs.

637. Applying these assumptions in our modelling provides us with an estimated cost saving of between £0.6 million and £14.8 million with the central estimate being £4.5 million.

638. It is also important to acknowledge the risks of the impacts to privacy and trust of these reforms. The scale of these impacts is dependent on the number and willingness of firms to change their approach from relying on an alternative basis to that of 'Legitimate Interests'. Although the legitimate interest basis is flexible and applicable across a wide array of situations, there may be unmeasured costs and risks for businesses changing from a consent only approach to a different basis that requires use of a balancing test.

639. The CDEI highlights the importance that data subjects place on openness when it comes to firms processing their personal data.[258] If this openness were to change then consumers may be less inclined to engage with a business, resulting in a decrease in available data for firms to use and a decrease in firm level productivity as a result.

640. Looking at the estimated compliance cost savings for UK businesses that use data for research and development purposes, assumptions have been made where data is lacking or research suggests a varied level of impact. By testing the assumptions feeding into the model we are able to provide a range of potential monetary impact. The assumptions and their ranges are in the table below.

Table 64: Breakdown of assumptions for the research purposes reform

[257] More information and detail on this reform can be found in the direct benefits - monetised section of this Impact Assessment
[258] Public attitudes to data and AI: Tracker survey, CDEI 2022

Measure: Research Purposes			
	Low scenario	Medium Scenario	High scenario
Effect: Need to seek legal advice to clarify regulation			
How much of data usage is affected by clarification under this measure	20%	35%	50%
% reduction in legal advice required in these cases	10%	25%	40%
% of these businesses that seek legal advice in a year	35%	50%	65%
Effect: Reduction in customer complaints about data use			
% of complaints in firms that have R&D member of staff - related to R&D	5%	10%	25%
% data uses affected	10%	25%	40%
% reduction in complaints	10%	25%	40%

641. We estimate the cost saved for these firms to fall between £1.4 million and £26.9 million depending on the % of legal advice required, number of complaints that relate to research and development and the % reduction estimated in these complaints as well as the other factors listed above. Our best estimate predicts a total cost saving of £8.7 million for firms using data for research purposes.

642. Reforms aimed at the use of data in AI and Machine Learning are designed to save businesses compliance costs. Our estimations of the monetary value of these savings rely on the following assumptions that we test below using a low medium and high scenario.

Table 65: Breakdown of assumptions for the AI and Machine Learning reform

Measure: AI and Machine Learning			
	Low scenario	Medium Scenario	High scenario
Effect: Need to seek legal advice to clarify regulation on data for AI			
How much of data usage is affected by clarification under this measure	5%	20%	35%
% reduction in legal advice required in these cases	10%	25%	40%
Effect: Reduction in customer complaints about data use			
% of complaints in firms that use data on AI - related to AI	5%	10%	25%
% data uses affected	10%	25%	40%
% reduction in complaints	10%	25%	40%

643. Changing these assumptions provides an estimate of compliance cost savings for UK businesses of between £0.3 million and £7.3 million with a central estimate of £2.5 million.

644. There will also be wider impacts to both firms and data subjects because of this reform. For example, the CDEI report on data use for Automated Decision Making highlights data subjects' opinions on the use of ADM. Using a polling approach, the report found that in October 2020 awareness of the use of ADMs to make decisions for the public was at 62% and of those 23% disagreed with the principle. The report also found that this level of awareness and trust differs

across sectors, with 54-57% of people being aware of the use of ADM in Financial Services but only 29-30% by local authorities.

645. This highlights the potential impact this policy may have on data subject levels of trust in ADMs. By clarifying the circumstances in which safeguards apply to significant decisions about individuals on the basis of profiling, there is likely to be an increase in data subjects' awareness of the personal data being used in ADM, and the safeguards available to them.

646. The increased awareness of personal data being used in ADM by data subjects could lead to an increase in trust in the use of ADM, resulting in an increase in use and an increase in benefits such as, quicker and more consistent decisions for individuals, particularly in cases where a very large volume of data needs to be analysed and decisions made very quickly. Conversely, there may be a risk that this increased awareness could also increase the proportion of the public that disagree with the principle. We will attempt to measure this impact going forward and include it in the Final Impact Assessment.

647. The record keeping reform is designed to reduce the burden on businesses keeping records of their data usage, storage and processing. This reform ensures this exemption will now be based on risk rather than business size or frequency of data processing. Organisations will not have to keep records unless the processing is likely to result in a high risk to the rights and freedoms of individuals. This aligns with the threshold for carrying out a data protection impact assessment, as currently defined by the ICO.

648. The reform also seeks to expand on current Article 35(4) and Article 35(5) such that it applies across to clause 14 senior responsible individuals and clause 15 duty to keep records. This will provide greater flexibility and clarity in guidance on what constitutes high risk processing and will help firms identify which of their data processing activities fall into which category.

649. This policy is designed to reduce the burden on businesses of keeping records of their data usage, storage and processing. This reform ensures this exemption will now be based on risk rather than business size or frequency of data

650. As a result of this reduction in burden, firms will spend less time and money on ensuring they are compliant with the current guidelines and paying for legal advice. We estimate that 2.3 million businesses in the UK process 'less sensitive' personal data. Using data from the 2021 UKBDS and internal assumptions, we estimate that 6.2% of these businesses seek legal advice annually to establish record keeping requirements, resulting in an aggregate £66m cost to businesses. We expect the clarifications to reduce the scope for seeking legal advice for low risk activities, assuming a 25% reduction and applying this to only half of all data usage taking place in these companies. These assumptions remain conservative as we do not expect all firms that currently seek legal advice to change their behaviour, and that some of their activities might still be "high risk" activities. We also test these assumptions using scenario analysis.

651. As well as removing the need for certain businesses to pay for legal advice, firms will also have to spend less demonstrating their compliance. Of the 2.3m businesses processing less sensitive data we assume all of these businesses face this demonstration cost. We estimate this cost to be approximately £50 per business, and we assume that 25% of this cost will be

saved. Once again we remain conservative as we make the assumption that there will still be a cost for demonstration of compliance.

652. We estimate the total compliance saving to be between £13.8 million and £71.0 million a year, with a central estimate of £38.7 million a year in 2021 prices.

Table 66: Breakdown of assumptions for the Record Keeping reform

Measure: Accountability Framework : Record Keeping			
Assumption	Low scenario	Medium Scenario	High scenario
How much of data usage is affected by clarification under this measure (i.e. how much of low risk data will no longer be within scope of legislation)	35%	50%	65%
% reduction in legal advice required in these cases	10%	25%	40%
% of these businesses that seek legal advice in a year	35%	50%	65%
Share of demonstrating compliance saved as a result of measure	10%	25%	40%

653. Whilst we hypothesise that a reduction in record keeping for low risk activities will provide benefits to businesses it is also important to note that the scale of these are dependent on certain factors.

654. It is up to firms to understand the definition of high risk processing and determine whether this change in record keeping is applicable to them. The PMP clauses will expand on current Article 35(4) so that the list of processing operations produced by the ICO also apply across to clause 14 senior responsible individual and clause 15 duty to keep records.

655. In reality, it is possible that some firms are not compliant with current guidelines and do not ensure that the correct information is held.The UKBDS found that 82% of businesses that handle digitised personal data said they either tended to or strongly agreed that they understand the requirements under GDPR and DPA 2018. If some firms do not understand the requirements and are currently not keeping the correct level of records then the introduction of this policy will result in no further compliance savings benefit for the firm.

656. There are also potential knock-on secondary impacts on data subjects' privacy and confidence if this is the case and firms are not storing the appropriate level of detail. For example, London Economics highlights that data subjects appreciate the existence of regulation and fines for when companies misuse data. They also value transparency about how their data is dealt with and control over how it is used. This is in agreement with the CDEI's Public Attitudes to Data Tracker which found that Data security was seen as the greatest risk of data use and respondents expressed anxieties about the security of personal data and the trustworthiness or capabilities of organisations to protect it. If this confidence is lost then data subjects will be less willing to share their data with businesses resulting in a reduction in data use and firm level productivity.

657. Alternatively, it may be the case that some businesses will continue to keep these records regardless of now being exempt, to ensure this level of trust is maintained with data subjects. For example, London Economics found that the reputational costs of data sharing are the

highest reported cost by organisations that share data with each other. If firms choose to try and avoid this reputational cost and continue to demonstrate a high level of record keeping regardless of the risk level there will be no decrease in compliance activities and therefore legal and demonstrative costs. However, the firm may see an increase in trust amongst its data subjects leading to an increase in consumer confidence and loyalty. This impact would be dependent on the privacy preferences of the firms data subjects and the transparency of the firms data processing activities.

658. The estimated compliance cost savings with regards to the privacy and electronic communications policies depend on an assumption made on the proportion of businesses that will no longer need to offer opt-in/opt-out services. This assumption is tested using the values in the table below.

Table 67: Breakdown of assumptions for the PECR reform

Measure: Privacy and Electronic Communication			
	Low scenario	Medium Scenario	High scenario
Effect: Activities required to obtain consent for data processing			
Proportion of businesses that will no longer need to offer opt-in/out	15%	30%	45%

659. These assumptions provide an estimated cost saving of between £7.9 million and £23.7 million with a central estimate of £13.9 million.

660. In the table below the assumptions regarding policies designed to reform the Subject Access Requests process are tested. This includes modelling a low and a high scenario for the share of SARs that are received from third parties and the predicted reduction in these as a result of the policies. As well as this we scale down the average number of SARs received by UK businesses as the source of this figure was calculated for only large firms, we expect small and micro firms to deal with less SARs so we adjust the number accordingly.

Table 68: Breakdown of assumptions for the SARs reform

Measure: Subject Access Requests			
	Low scenario	Medium Scenario	High scenario
Effect: Activities required to obtain consent for data processing			
Scale down factor to account for the fact that EC survey only included organisations employing 20+ people	10%	25%	40%
Share of SARs from third party	10%	25%	40%
Reduction in SARs from third party	10%	25%	40%

661. As a result, we estimate the cost savings to be between £9.3 million and £153.0 million with a medium estimate of £59.1 million.

662. The total estimated compliance cost savings for UK businesses for each measure are in the table below. We estimate compliance cost savings to fall between £33.3 and £299.6 million annually.

Table 69: Breakdown of total compliance costs saved by reform and scenario, 2021 prices

Total compliance cost saving	Cost by firm size (£m)		
Reform	Low Scenario	Medium Scenario	High Scenario
Legitimate Interests	0.6	4.5	14.8
AI and Machine Learning	0.3	2.5	7.3
Research Purposes	1.4	8.7	26.9
Accountability Framework: Record Keeping	13.8	38.7	71.0
Privacy and electronic communications and the use of personal data for the purposes of democratic engagement	7.9	15.8	23.7
Subject Access Requests	9.3	59.1	153.0
Total	**33.3**	**129.3**	**296.6**

Indirect Benefits - Productivity Impacts

663. Productivity impacts have been calculated using both robust sources of evidence as well as modelling assumptions; the table below outlines the assumptions that are relevant to all measures that are expected to impact UK business productivity. The rest of this section goes through the assumptions specific to each proposed reform.

Table 70: Assumptions used in modelling and RAG rating of confidence in assumptions

Assumption	Description	Source	RAG Rating
Number of businesses affected	Assumed the number of businesses affected by each measure	UK Business Data Survey	
Proportion of organisations affected	The number of organisations that will be more productive	Estimate	

664. In this modelling we make informed assumptions on the proportion of firms that would increase their data use because of these reforms. We have tested these assumptions by carrying out sensitivity analysis around these percentages and creating a low scenario where the actual number of businesses increasing data use is less than assumed (10%) and a high scenario where the opposite is the case (50%). We also tested the assumption of the proportion of firms that would increase AI use due to the reforms in the bill, presenting a low scenario (5%) and a high scenario (15%). A list of all assumption per measure for each scenario can be found in the table below:

Table 71: Breakdown of assumptions when modelling the impacts on UK GVA and productivity

	Low	Medium	High scenario

	scenario	scenario	
Legitimate Interests			
Scaling factor to account for the fact that not all firms would increase data use based on this measure	10.0%	25.0%	50.0%
Scaling factor on the productivity impact as measures will only affect data use	5.0%	10.0%	15.0%
Research Purposes			
Scaling factor to account for the fact that not all firms would increase data use based on this measure	20.0%	35.0%	60.0%
Scaled proportion of total business that could increase their data use with clearer guidance	0.04%	0.10%	0.2%
AI and Machine Learning			
Scaling factor to account for the fact that not all firms would increase AI use based on this measure	5.0%	10.0%	15.0%
Data minimisation and anonymisation			
Proportion of businesses for which improving standards would lead to additional sharing	5.0%	10.0%	15.0%
Scaling factor on the productivity impact as measures will only affect data use	5.0%	10.0%	15.0%
Accounting for the fact that this is about data shared across organisations rather than all data	10.0%	25.0%	40.0%
Accountability Framework: Record Keeping			
Scaling factor to account for the fact that not all firms would increase data use based on this measure	10.0%	25.0%	40.0%
Scaling factor on the productivity impact as measures will only affect data use	5.0%	10.0%	15.0%
Relationship between average impact on productivity and low risk/low intensity data and general data use	35.0%	50.0%	65.0%

665. The results suggest a range in the scale of benefits of between £18.9m and £208.8m. A breakdown of this impact by reform can be found below:

Table 72: Breakdown of total impacts on UK GVA by measure and scenario, in 2021 prices

Total Increase in GVA (£m)			
	Low scenario	Medium scenario	High scenario
Legitimate Interests	2.0	10.2	30.6
Research Purposes	10.1	17.6	30.2
AI and Machine Learning	2.8	5.6	8.4
Data minimisation and anonymisation	3.7	36.8	132.5
Accountability Framework: Record Keeping	0.3	2.2	7.0
Total	**18.9**	**72.5**	**208.8**

Direct Costs - Familiarisation costs to UK businesses (private sector)

666. Familiarisation costs have been calculated using a variety of assumptions and evidence sources; the table below outlines the assumptions that are relevant to all measures that are

expected to inflict familiarisation costs on UK businesses. The rest of this section goes through the assumptions specific to each proposed reform.

Table 73: Assumptions used in modelling and RAG rating of confidence in assumptions

Assumption	Description	Source	RAG Rating
Number of pages of guidance	Assumed 5 pages of guidance per measure	DCMS policy teams	
Wage Estimates	Assumed the wage of the employee reading the guidance per measure	Annual Survey of Hours and Earnings and ICO/DCMS (2020) Impact Assessment for the Age Appropriate Design Code	
Number of businesses affected per measure	Assumed the number of businesses affected by each measure	UK Business Data Survey	
Hours Required	Assumed the reading speed of the employee reading the guidance	ICO/DCMS (2020) Impact Assessment for the Age Appropriate Design Code	

667. When calculating the expected familiarisation costs for UK businesses of the proposed package of reforms we test the assumptions that feed into the modelling.

668. We continue to use a time-cost approach to estimate the administrative costs of reading the new legislation. Although this methodology has not changed we have updated some of our assumptions feeding into the model using new evidence. In order to identify the relevant 'number of affected businesses' per measure, we look at an organisation's data use to determine if they are in scope of the model.

669. We have updated our wage assumptions by assuming that at small and medium-sized enterprises senior officials would read the guidance rather than data protection officers, and estimated the hourly unit cost of this work at £26.85 using occupational estimates from the Annual Survey of Hours and Earnings (ASHE).[259] This analysis assumes that a micro-sized firm has zero employees. For micro-sized firms we have updated our wage assumptions by applying median annual earnings estimates of the self-employed from DWP's Family Resources Survey and estimating the hourly unit cost of this work at £11.20.[260]

670. We continue to assume that the guidance would be at a similar level of reading difficulty to the ICO's data sharing code, and therefore have used a similar Fleisch reading ease score of 40, which corresponds to a reading speed of 75 words per minute.

Table 74: Breakdown of total impacts on Familiarisation costs for UK businesses by measure and scenario, in 2021 prices

[259] ONS Annual Survey of Hours and Earnings (2021)
[260] DWP Family Resources Survey (2020)

Total Familiarisation costs (£m)			
Reform	Low scenario	Medium scenario	High scenario
Research Purposes	3.2	3.8	4.4
Legitimate Interests	8.1	9.5	11.0
AI and machine learning	2.6	3.0	3.5
Data minimisation and anonymisation	8.1	9.5	11.0
Reform of the Accountability Framework	44.0	51.8	59.6
Privacy and Electronic Communication	5.1	6.0	6.9
Total	**71.1**	**83.7**	**96.3**

Digital Identity

671. This section of analysis highlights the assumptions and sensitivity analysis undertaken in the Powers for Digital identity and Attributes Initiatives De Minimis Assessment produced by DCMS.[261] The following table outlines how this analysis has been classified into a low, medium and high scenario. More detail on this can be found in the full Impact Assessment.

Table 75: Breakdown of all risks and assumptions included when modelling the impact of the Digital Identity measures

Assumptions			
CENTRAL ESTIMATE SCENARIO	**LOW ESTIMATE SCENARIO**	**HIGH ESTIMATE SCENARIO**	**RISK ASSESSMENT**
Wage estimation			
Wage data used in both the cost and benefit estimate has been inflated by 22% to adjust for overhead costs, according to RPC guidance.			No sensitivity analysis has been undertaken.
Estimated cost values			
The values used to calculate the estimated costs have been gathered from an engagement exercise with stakeholders.			There is a risk that the data collected may not be very representative. We have set different scenarios to attempt to mitigate this risk
Averages of the inputs gathered throughout the engagement exercise were used to estimate the potential average cost of each task for a business.			
The cost estimations provided by the engagement exercise are in 2021 value.			
Wage per hour has been calculated by dividing the gross annual wage by the number of			No sensitivity analysis has

[261] Powers for Digital Identity and Attributes Initiatives De Minimis Assessment, DCMS (2021)

weeks in a year (52) by the ONS' 2019 average number of working hours in a week. We took the 2019 value as the 2020 value has been significantly affected by Covid 19 and would not have been representative of the usual working patterns.			been undertaken.
Costs over the 10-year appraisal period are undiscounted.			
Number of businesses			
We assume that only medium and large UK businesses will take up digital identity as their benefits will significantly outweigh the transition costs. Data regarding the Number of UK medium and large businesses was collected from the ONS data release: UK "BUSINESS: ACTIVITY, SIZE AND LOCATION - 2020", table 3.			No sensitivity analysis has been undertaken.
Familiarisation costs			
The values from the engagement exercise have been used to calculate the central estimate of the potential average familiarisation costs per business.	We reduced the central estimate by 50%. This is a standard assumption.	We inflated the central estimate by 100%. This is a standard assumption.	There is a risk that the data collected may not be very representative. We have set different scenarios to attempt to mitigate this risk.
For each task the estimated costs have been calculated as: average resources required (employees and time) * average wage per hour (including 22% overhead costs)			
We estimated the familiarisation costs per businesses and multiplied the value by the 2020 number of UK medium and large businesses.			
The familiarisation costs are one-off costs.			
We assume all businesses face familiarisation costs in year one independently of the use case.			
Organisational change costs			
The values from the engagement exercise have been used to calculate the central estimate of the potential average organisational costs per business.	We reduced the central estimate by 50%. This is a standard assumption.	We inflated the central estimate by 100%. This is a standard assumption.	There is a risk that the data collected may not be very representative. We have set different scenarios to attempt to mitigate this risk.
We estimated the organisational costs per business and multiplied the value by the 2020 number of UK medium and large businesses.			
Due to the limited number of responses and the presence of outliers we have used the median number of hours gathered from the engagement exercise to calculate the expected costs per business.			
The organisational change costs are one-off costs.			
For each task the estimated costs have been calculated as: average resources required (employees and time) * average wage per hour (including 22% overhead costs)			
We estimated the familiarisation costs per businesses and multiplied the value by the 2020 number of UK medium and large businesses.			

Businesses in the sector related to each of the use cases face the organisational change costs the year that the digital ID checks take place for the first time. (E.g. real estate businesses face the organisational change costs when the checks related to the home buying process begin). If businesses are affected by multiple use cases they face the organisational change costs only once.			
All medium and large UK businesses face organisational change costs to adapt to carrying employee mobility checks digitally.			
One-off connection fee			
We assume that the one-off connection fee may be £5650. This value has been estimated by a research project carried out by the private sector on behalf of DCMS.	We assume that the one-off connection fee may be £3900. This value has been estimated by a research project carried out by the private sector on behalf of DCMS.	We assume that the one-off connection fee may be £7400. This value has been estimated by a research project carried out by the private sector on behalf of DCMS.	We set different connection fee costs in each scenario to attempt to mitigate the risk of under or overestimating the connection fee costs.
The number of identity providers that may pay the connection fee has been estimated by the private sector on behalf of DCMS. This number (100) does not vary across scenarios.			No sensitivity analysis has been undertaken.
Linear trend over time of the digital identity market towards the steady state			
We assume that the digital identity uptake grows over time following a linear trend. For instance, in the central scenario we assume that only 15% of the total potential number of checks and expected benefits estimated by Deloitte takes place in year 1. In the central scenario 100% of digital identity uptake is reached by year 7 of the appraisal period.	The trend in the best-case scenarios is 33% higher than the central scenario.	The trend in the worst-case scenarios is 33% lower than in the central scenario.	There is a risk that the estimated trend lines may be incorrect. We have set three different scenarios to attempt to mitigate this risk.
The trend has been estimated through conversations with the policy team based on their knowledge of the digital identity sector.			
Cost per check			
We assume that the per-check fee may be 10p. The assumption has been set in agreement with the policy team based on their market knowledge.	We assume that the per-check fee may be 5p. The assumption has been set in agreement with the policy team based on their market knowledge.	We assume that the per-check fee is 50p. The estimate comes from the Home Office Passport Pilot Scheme.	There is a risk that these costs may not be true to reality. To mitigate this risk, we have taken one of the cost scenarios from the Home Office Passport Pilot Scheme and we have set three different scenarios.

Number of checks			
The annual number of checks (assuming the steady state market level) for each use case has been estimated by a research project carried out by Deloitte. The values are constant across scenarios.			There is a risk that the full number of annual checks estimated by Deloitte may not be realised as soon as checks begin. To mitigate this risk, we have multiplied the annual volume of checks by the estimated trendline.
The number of digital ID checks grows over time following the estimated trendline. The trendline varies depending on the scenario.			
Total annual cost of per check fees			
We calculate this estimate by multiplying the estimated annual number of checks (adjusted to the trend) by the estimated per check fee.			No sensitivity analysis has been undertaken.
Year the costs and benefits take place			
The assumptions regarding the year the digital ID checks may begin for each use case and scenario are based on information provided by the policy team based on their knowledge of the sector.			There is a risk that these assumptions may be incorrect. To mitigate this risk, we have set different years in each of the three scenarios.
The years assumed in the best and worst scenarios are variations of what is estimated in the central scenario.			
Scenarios			
In the central scenario we assume that the checks that rely only on passport data may start taking place from year 2 onwards. Whereas, it may take 3 years for those that rely on passport data and guidance being updated. Lastly, it may take 5 years for the checks that rely on datasets other than passport data.	In the best-case scenario, we assume early uptake, low costs and high benefits.	In the worst-case scenario, we assume later uptake, high costs and low benefits.	There is a risk that these assumptions may be incorrect. To mitigate this risk, we have set different years in each of the three scenarios.
Benefits			
The estimated benefits over the 10-year appraisal period have not been discounted.			
The values used in the Deloitte methodology to calculate the benefits have been modified to align with the cost estimations. Estimated wage values have been inflated by 22% to account for overhead costs and monetary values have been inflated to 2021			

prices. Where the year was unclear we assumed the values were in 2020 prices.	
First order indirect benefits	
The estimated annual economic value for the UK of carrying out digital ID checks has been by Deloitte.	No sensitivity analysis has been undertaken.
The estimated values assume that the steady state level of the market is reached. Therefore, we adjusted the estimated values of the benefits by the estimated digital identity market trend over time.	
We split the total value of the benefits by the value we expect private citizens to experience and the value we expect businesses to experience.	
Second order indirect benefits	
We assume that one proportion of the value of benefits related to faster employee mobility for people on short notice periods begins to take place when digital DBS checks are realised, the second part when digital RWT checks begin to take place and the remaining value when digital qualification checks begin to happen. Each percentage is proportional to the annual number of checks estimated for DBS, RWT and qualification checks.	No sensitivity analysis has been undertaken.
The assumption above is set for productivity improvement as well.	
The total value of the indirect benefits related to reduced fraudulent applications arises when digital qualification checks begin to take place as we assume the current costs are related to hiring workers with false credentials.	
Non-monetised costs to businesses: Costs to private sector businesses	
We expect businesses to have to pay to adapt their way they carry out ID verification to digital identity. For instance, by setting up a platform to perform digital ID checks.	No sensitivity analysis has been undertaken as we were unable to monetise these costs.
Non-monetised costs to businesses: Costs to join the Trust Framework	
Although being signed up to the trust framework will not be compulsory to operate in the market, we assume that private-sector access of government-held databases is only granted to the businesses signed up to the trust framework. Therefore, businesses will have to sign up to it in order to effectively operate in the market.	No sensitivity analysis has been undertaken as we were unable to monetise these costs.
Cost for public sector bodies	
We assume that public sector bodies face familiarisation costs, costs to digitise any IDs in paper-only form (e.g. birth certificates before a certain year), costs to allow private sector access to their databases and costs to set up and run the governance function. All costs except digitisation costs have been included in the net benefits calculations.	No sensitivity analysis has been undertaken.
In the central and best scenarios, we assume that 4 Departments adapt to digital identity. Whereas, in the most pessimistic scenario we assume all 43 ministerial and non-ministerial departments adapt to digital identity.	Sensitivity analysis has been undertaken by varying the number of Departments across

	scenarios.
Net benefits	
The net benefits have been discounted so they are presented in NPV.	

Creation of Robust and Secure Smart Data Schemes (BEIS)

672. This section is based on analysis by BEIS for the Regulatory Powers for Smart Data Impact Assessment.[262] This covers the analytical risks of the proposed preferred option.

673. The primary risks associated with the introduction of new Smart Data powers are:

a. The powers are not used to introduce schemes and no acceleration benefits are realised;

b. Inconsistent implementation and design of secondary regulations limits the potential for coordination, efficiencies, and interoperability

674. BEIS has engaged extensively with relevant stakeholders to mitigate these risks. For example, the Smart Data working group was established to bring together government departments and regulators with the aim to:

a. support the development and delivery of smart data infrastructure and standards for the benefit of consumers, particularly vulnerable consumers

b. where appropriate encourage commonality or consistency of approach across Smart Data initiatives to enable interoperability and cross-sector innovations

c. improve efficiency by reducing duplication across smart data initiatives and re-using assets or resources from prior smart-data initiatives

d. BEIS will continue to drive cooperation and coordination across sectors in future. We intend to build on the work undertaken by the Smart Data Working Group, to develop an active ecosystem for Smart Data and support greater collaboration and coordination. As part of this we will look to identify a variety of use cases, find ways to encourage greater cross-sector data sharing, and support wider sectors to explore future Smart Data schemes.

e. To identify and mitigate against any risks or unintended consequences, any secondary regulations using the Smart Data powers will go through the affirmative procedure to ensure there is robust legislative scrutiny of the measures. As part of this, a proportionate Impact Assessment and relevant Post Implementation Review requirements would need to be produced.

Reduced competition

675. There is a risk that Smart Data may unintentionally harm competition. For example:

[262] Regulatory Powers for Smart Data Impact Assessment, BEIS (2022)

a. ***Too strenuous compliance obligations for data holders or third parties***, leading to increased barriers to entry and reduced competition. A consultation prior to secondary legislation will help minimise this risk.

b. ***Data mobility provides dominant incumbent data holders with more market power***. Emerging research[263] suggests that increased data mobility could lead to customers becoming increasingly attracted to their existing, dominant providers who can utilise product/performance data from other providers to their advantage. However, Open Banking has been recognised by the CMA as a key step towards unlocking competition in retail banking and the evolution of the UK's fast-growing fintech sector.[264] This is evidenced in the continued growth of the Open Banking ecosystem.[265] Smart Data schemes can minimise these effects (for example by providing exemptions for smaller providers) and existing competition law should mitigate the potential for excessive market power.

c. ***Damaged incentives to differentiate on privacy and security*** if the government mandates interoperability, which is a key source of competition in markets such as digital platforms.[266] Using the tiering of standards, for instance based on risk factors or the nature of the data involved, or specific exemptions could mitigate this by ensuring proportionate approaches are used.

d. ***Lock-in to a suboptimal standard specified by the government***. This risk constraining industry from innovating beyond the standards which could improve Smart Data schemes. To minimise this risk, broad stakeholder engagement will be required when designing future schemes.

Reduced data holder incentives

676. If data holders have to share their collected data with Third Party Providers (TPPs), they may be less likely to recover the cost of data collection in the first place as any competitive advantage may be lost. This could present a free rider problem, where TPPs benefit from data collection without contributing to its provision. This risk is minimised by the fact that the majority of data in-scope of Smart Data is personal and product data, which will have been collected regardless of intervention. This risk is further minimised by the UK GDPR's data minimisation principle.

Poor security

677. Smart Data is expected to benefit consumer data security by creating strong standards and displacing less secure practices such as screen scraping. However, if security considerations behind the standards are weak, this could risk decreased security of customer data, including leakage of data.

678. In addition, increasing the use of digital services and enabling new intermediaries could present new opportunities for security risks as data is more readily transferred from one place to another. However, accreditation requirements, that would likely include security

[263] BoE (December 2019): "Platform competition and incumbency advantage under heterogeneous switching cost — exploring the impact of data portability" paper, & Stratechery (May '18): "The Bill Gates line" article
[264] CMA (November 2021): "Update on Open Banking"
[265] Number of TPPs entering Open Banking has grown by 80% in just under 2 years, 134 TPPs (2019) and 245 TPPs (December 2020).
[266] FT (October 2017): "Privacy is a competitive advantage" article, among other examples such as Signal, DuckDuckGo etc.

requirements, would help ensure that participants in the Smart Data ecosystem have adequate security and are trustworthy. Accreditation requirements are also expected to aid consumers, reducing the need for time spent understanding which agents are legitimate and which are not.

Lack of uptake of Smart Data schemes

679. The benefits of Smart Data would be reduced, yet the majority of costs would still be incurred, if there is a lack of uptake of Smart Data schemes. This may be because of a lack of trust in the ecosystem, a perception that there is no benefit of Smart Data enabled services, or a lack of awareness these services exist. A recent business survey into identifying the features of ethical and trustworthy Smart Data schemes by the Centre for Data Ethics and Innovation (CDEI) and BEIS found that appetite for new schemes was low.[267]

680. However, over recent years we have seen exponential growth in Open Banking users. The pandemic has also been a catalyst for a step- change in digital skills for some participants, as internet access across the UK increased from 89% in March 2020 to 94% in March 2021.[268] Furthermore, 83% of internet users used online banking,[269] up from 51% in 2019,[270] much of which is likely facilitated by Open Banking and APIs.

Lack of demand for Smart Data services

681. Related to low user uptake is the assumption that Smart Data will enable products that customers will want to use and an ecosystem TPPs want to join.

682. Evidence from banking shows the wide-ranging innovations offered by TPPs and high user demand for these services. There are several other examples in the energy sector:

a. The collective switching energy trial[271] featured a simplified switching process, similar to potential Smart Data use case, and found a “substantial impact on switching among customers who have not switched energy tariff for many years and can be delivered at scale”.

b. Ofgem user research on midata[272] tested a functional prototype of a price comparison website. Participants were less concerned about sharing their energy data than their financial data, but were generally comfortable with sharing data when it is clear what they are consenting to. A key takeaway from this research is that clear communication and messaging is required to drive adoption, particularly around consent.

c. Previous midata[273] IA contains surveys showing demand for a better system for consumers to be informed by their own data. For example, 43% strongly agreed and a further 47% were in favour of wanting easy access to personal data. Further research from Ofcom highlights that 40% of surveyed internet users were not aware of any of the ways in which online companies collect their personal information.[274]

[267] *Will add evidence and reference for research when published*
[268] Ofcom (April 2021): “Adults' media use and attitudes report 2020/21”
[269] Ofcom (April 2021): “Adults' media use and attitudes report 2020/21”
[270] Ofcom (May 2019): “Online Nation 2019 report”
[271] Ofgem (August 2018): “Eight times as many people get a better deal in Ofgem’s collective switch trial” Press Release
[272] Ofgem (October 2020): “midata Discovery and Proof of Concept User Research Findings”
[273] Referenced in the BIS (2012): “Order making power for midata”
[274] Ofcom (April 2021): “Adults' media use and attitudes report 2020/21”

Changing prices for consumers

683. It is unclear how incumbent data holders will amend their pricing strategy in response to Smart Data schemes. Costs could potentially be passed onto customers, an uncertainty which Ofcom noted but stated they see no immediate competition concerns arising from Open Communications.[275]

Misuse of customer data

684. As a result of increased data sharing, there is a potential for an increase in the misuse of customer data. This could include potential risks such as an increase in 'nuisance' calls and contact, or unwelcome selling-on data.

685. However, standards and security requirements would ensure that customer data can only be used for purposes as specifically requested by the consumer. There is a potential for agents to sell on customer data, but it would be at the customer's discretion whether they consent for their data to be used for these purposes.

National Security and Law Enforcement

686. This section of analysis has been provided by the Home Office. This covers the analytical risks of the proposed reforms to data use for National Security reasons.

687. Time constraints and a lack of data meant that it was not possible to monetise most costs and benefits.

688. Stakeholders were unable to provide the relevant information under the strict time constraints required by the analysis, although they responded as best they could with qualitative and some quantitative evidence. For certain proposals the data required to monetise costs and benefits simply could not be obtained as they were too specific and were not recorded.

689. Although the analysis conducted is limited, it effectively conveys the degree of uncertainty about the economic costs and benefits of these proposals, and this should be considered.

690. This analysis is also in line with previous impact assessments conducted for the DPA 2018, where data difficulties posed significant problems for monetisation of costs and benefits.

691. There are significant analytical risks given that a mostly qualitative analysis was performed resulting in a narrative based assessment.

692. A lack of data means that most costs and benefits were not monetised, and therefore the scale of the potential costs and benefits of the relevant proposals cannot be clearly demonstrated.

693. There has been an attempt to provide an idea of scale, however the information is still limited, and significant uncertainty remains.

694. There is a risk that for the proposal to remove the need to log the 'justification' for consultation / disclosing data disclosure, the number of system accesses is not constant over

[275] Ofcom (August 2020) "Open Communications: Enabling people to share data with innovative services"

the appraisal period. This could lead to a reduction or increase in benefits depending on the number of times automated systems are accessed.

695. There is also the risk that after accessing a system, LEA employees perform tasks which require further logging which would increase the scale of benefits.

696. Upscaling the benefits of this proposal to the MPS so that monetised benefits are obtained for all LEAs is risky as there is no data to suggest how utilisation compares among other LEAs. This means that the values obtained should be viewed with caution.

697. Costs and benefits for the I-LEAP proposal are taken from the full business case which assumed a slightly different 'do nothing' option and relied on multiple bilateral agreements as opposed to the current strategy of obtaining an agreement with the European Commission. This means that these costs and benefits should be viewed as indicative and have not been included in the NPSV.

Impact to international trade

698. HMG accepts that reforms need to comply with the UK's international legal obligations. The reforms proposed are in line with international practice. We are working with DIT legal and policy to understand whether the changes would affect our compliance with FTA measures. If any impacts are identified through this analysis, they will be in due course reflected in the present impact assessment.

Impact of changes to EU Adequacy

699. An outline of the modelling assumptions used to estimate the impacts of EU adequacy can be found in the table below.

Table 76: Assumptions used in modelling and RAG rating of confidence in assumptions

Assumption	Description	Source	RAG Rating
Investment Horizon	Assumed a five-year investment horizon when firms decide whether or not to continue trading with the EU	Estimate	
Compliance Rate	The percentage of businesses that will comply with the regulations.	Estimate	
Profit Margin	The profit margin firms would need to continue trading with the EU	Profitability of UK Companies Data	
SCCs in place	The percentage of businesses that have SCC's in place	UK Business Data Survey	
SCC Cost Rollover	The percentage of SCC costs likely to be rolled over to EU businesses	New Economic Foundation Report	
SCC Cost	The cost to firms of producing SCCs	Estimate	

700. The table above describes analysis of the potential value of EU Adequacy. As outlined, several parameters were adjusted to capture uncertainty around business decision-making,

such as the profit margin, the investment horizon as well as adjustments to SCC costs such as compliance, the number that already have SCCs in place and the proportion of costs borne by the UK business. When parameters vary by business size, the minimum and maximum of the range is used to account for uncertainty in that parameter. The three tables below outline how the parameters vary.

Table 77: EU Adequacy Parameters Sensitivity

	Best Estimate	Low	High
Profit Margin	9.6%	4.6%	14.6%
Investment Horizon (years)	5.0	2.0	10.0
SCC Compliance Rate	100.0%	100.0%	80.0%

Table 78: UK-EU SCC Cost Rollover (Borne by UK Firms)

Business Size	Best Estimate	Low	High
0	75.0%	75.0%	50.0%
1 - 9	75.0%	75.0%	50.0%
10 - 49	65.0%	75.0%	50.0%
50 - 249	60.0%	75.0%	50.0%
250 +	50.0%	75.0%	50.0%

Table 79: Percentage of UK Firms that have SCCs in place

Business Size	Best Estimate	Low	High
0	9.0%	9.0%	47.0%
1 - 9	20.0%	9.0%	47.0%
10 - 49	25.0%	9.0%	47.0%
50 - 249	31.0%	9.0%	47.0%
250 +	47.0%	9.0%	47.0%

701. The results of the updated modelling estimate an economic impact of between £190 and £460 million in one-off SCC costs and an annual cost of between £210 and £420 million in lost export revenue. Once appraised over a 10-year period, the estimated NPV of value of EU Adequacy is between £2 and £4 billion.

Impacts of ensuring businesses are able to continue to seamlessly use their pre-Bill existing transfer mechanisms

702. This reform provides for additional transitional arrangements in the Bill for a wider set of current alternative transfer mechanisms (ATMs). Similar to the approach taken for pre-commencement adequacy regulations and pre-commencement standard data protection clauses, this reform introduces transitional provisions for pre-Bill appropriate safeguards in Article 46 UK GDPR, Schedule 21 (paragraph 9) DPA 2018, and Section 75, Part 3, 2018 Data Protection Act currently in operation which meet the required level of protection under the existing framework.

703. We estimate that this reform will have a net zero impact, allowing businesses to continue to use their pre-bill mechanisms. It is important to note that this impact is dependent on additional transitional provisions for currently unapproved EU BCRs. In absence of these, initial estimates suggest there will potentially be between 29 and 39 companies still awaiting approval by Royal Assent incurring a potential compliance cost of between £2.9 and £14.7 million. Policy teams are working to ensure these costs are not incurred, and this will be assessed further in the Royal Assent impact assessment.

Sensitivity of final results

704. There are a significant number of assumptions made across the models used in our cost-benefit analysis. To be transparent on the potential range of uncertainty, we have undertaken a Monte-Carlo analysis varying the final results. The final results include the total costs, total benefits and net benefits. DCMS analysts have used Monte-Carlo analysis to present probabilistic results that allow us to see the likelihood of each outcome.

705. The table below shows the summary statistics for the Monte-Carlo analysis showing the mean, standard deviation, minimum and maximum for each of our results of interest. The analysis was run 50,000 times picking a random selection of each of the parameters. The costs and benefits are in present value over a 10-year appraisal period.

706. The table below shows a relatively large range of results. The net benefit of the preferred reforms varies between £2911.5m and £8063.3m with a mean of £5490.4m. The graphs below show the distribution of the final results including net benefit, total cost and total benefits. The net benefit graph shows a relatively uniform distribution, while the total cost graph shows a maximum value of £2418.8m and a minimum value of £946.9m with a mean of £1612.6m. The total benefits graph shows a mean of £7102.9m with a minimum value of £4820.7m and £9642.9m.

Table 80: NPV Monte-Carlo Summary Statistics

Results	N	Mean	St. Dev.	Min	Max
Net Benefit	50000	5501.3	703.1	2935.2	8065.7
Total Cost	50000	1612.6	223.5	946.9	2418.8
Total Benefits	50000	7113.9	666.	4841.1	9647.1

Chart 1: Net Benefit (£m), Final Results Monte Carlo Analysis (50,000 simulations)

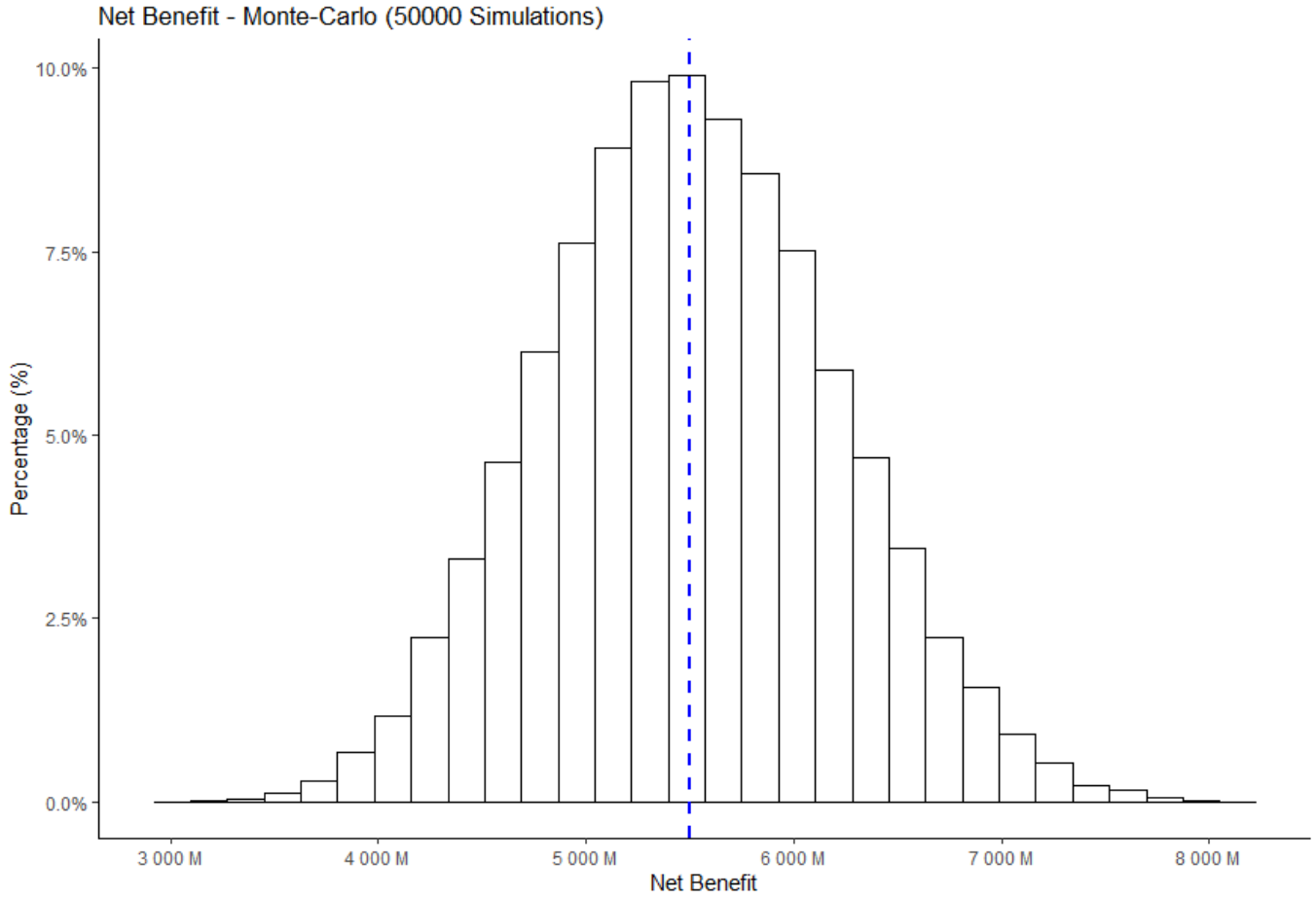


Chart 2: Total Cost, Final Results Monte Carlo Analysis (50,000 simulations)

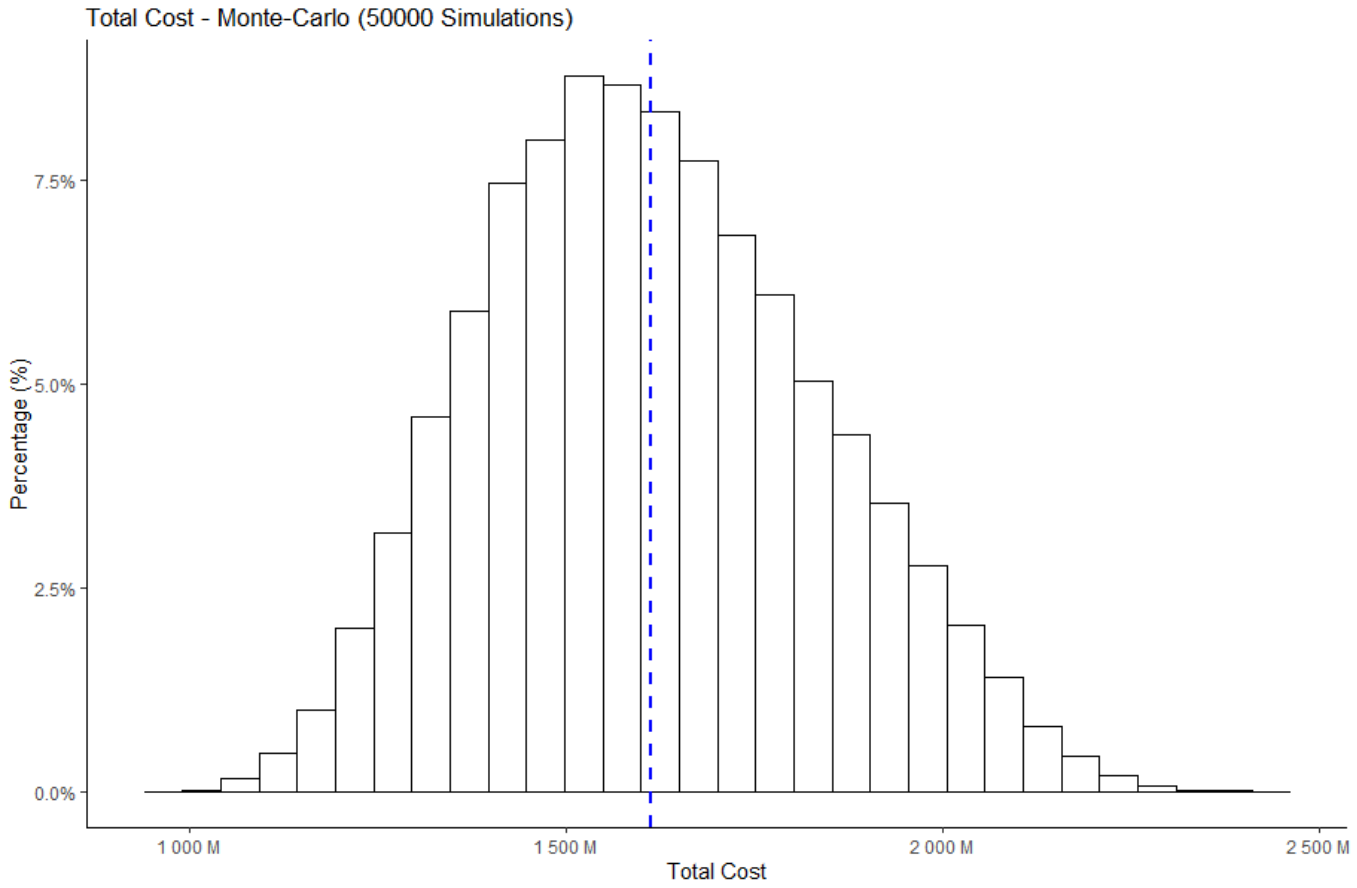
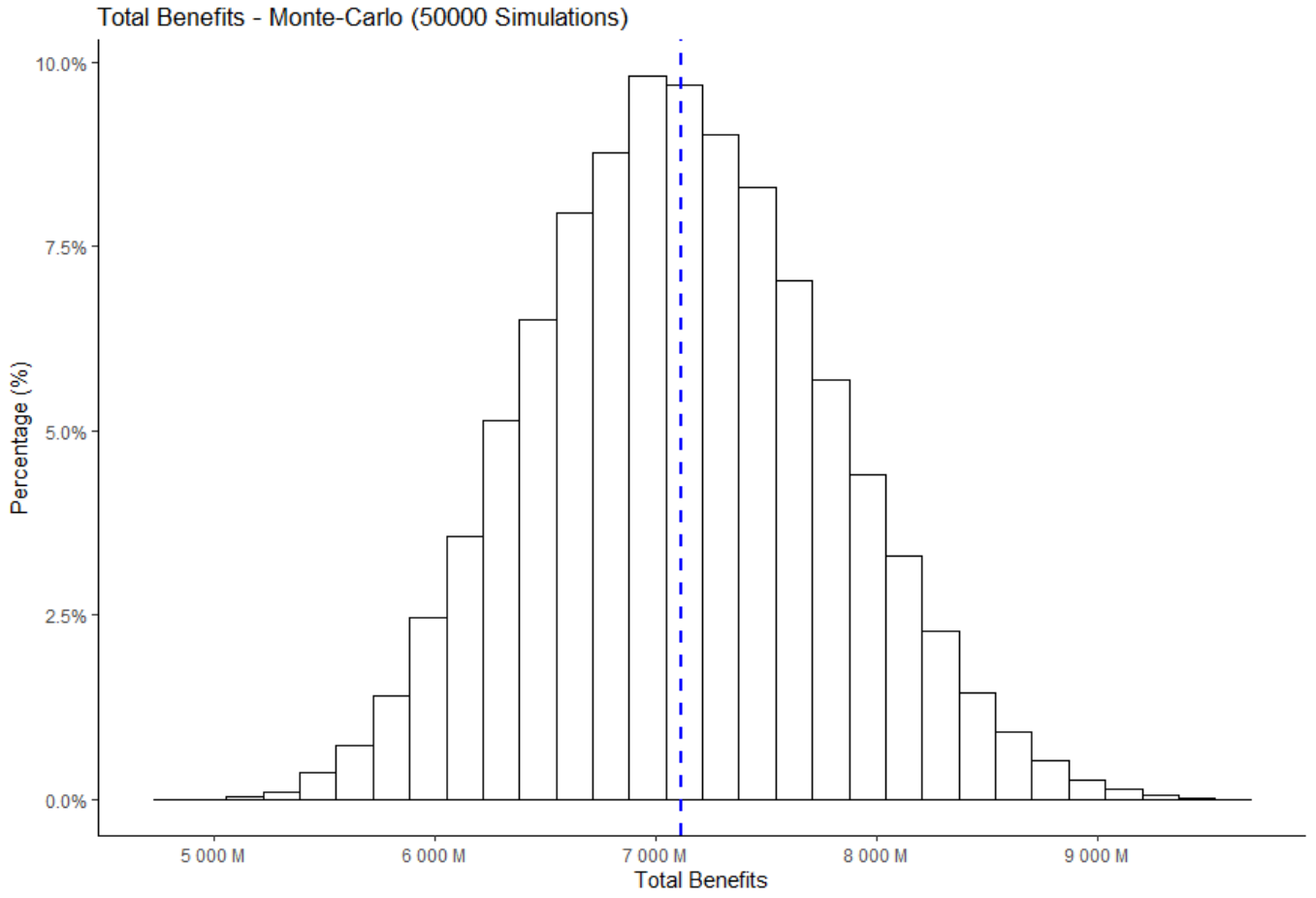


Chart 3: Total Benefits, Final Results Monte Carlo Analysis (50,000 simulations)



Monitoring and Evaluation

707. Evaluation is essential in evidence-based policy making. It helps policy officials understand impact, and therefore make better decisions. DCMS needs effective evaluation practice to credibly demonstrate the impact of its efforts, make better decisions and promote and defend its value, and the value of its network of Arms' Length Bodies (ALBs).[276] In 2021 The National Data Strategy Monitoring and Evaluation Plan[277] was published, this was designed to ensure that we are driving progress in the world of data, and that the strategy remains fit for purpose in the coming years.

708. The Data Protection and Digital Information Bill plays an important role in the delivery of the National Data Strategy and its second pillar, Mission Two: Securing a pro-growth and trusted data regime. As outlined in the strategy the first step in the monitoring and evaluation of this area was to conduct the consultation analysis in preparation for the bill. This gave us an overview of the current data landscape and the market failures currently facing UK businesses and public sector organisations. Now that the consultation has been completed we have identified further evidence gaps that will need to be monitored going forward, including the cost of compliance activities, how they vary by firm and the time spent by businesses familiarising themselves with the legislation. Through the process of putting the Impact Assessment together we have also identified key metrics that can be tracked and measured going forward that will be able to gauge the success of the proposed measures.

709. Given the scale of intervention, there is a legal requirement to perform a Post Implementation Review (PIR),[278] within 5 years of the implementation of the bill. This will include having to carry out two types of proportionate evaluations including;

a. Process evaluations: to check how things are happening and how changes are being made to improve implementation of future reforms

b. Impact evaluations: to assess the scale of effects caused by the planned changes, compared to initial ambition of the measure

710. Given that these are legislative changes that apply to all businesses, from the point of implementation, we will be basing our assessment around a Theory Based Evaluation.[279] Therefore the basis of both the impact and process evaluation comes from the Theory of Change presented earlier in the assessment.

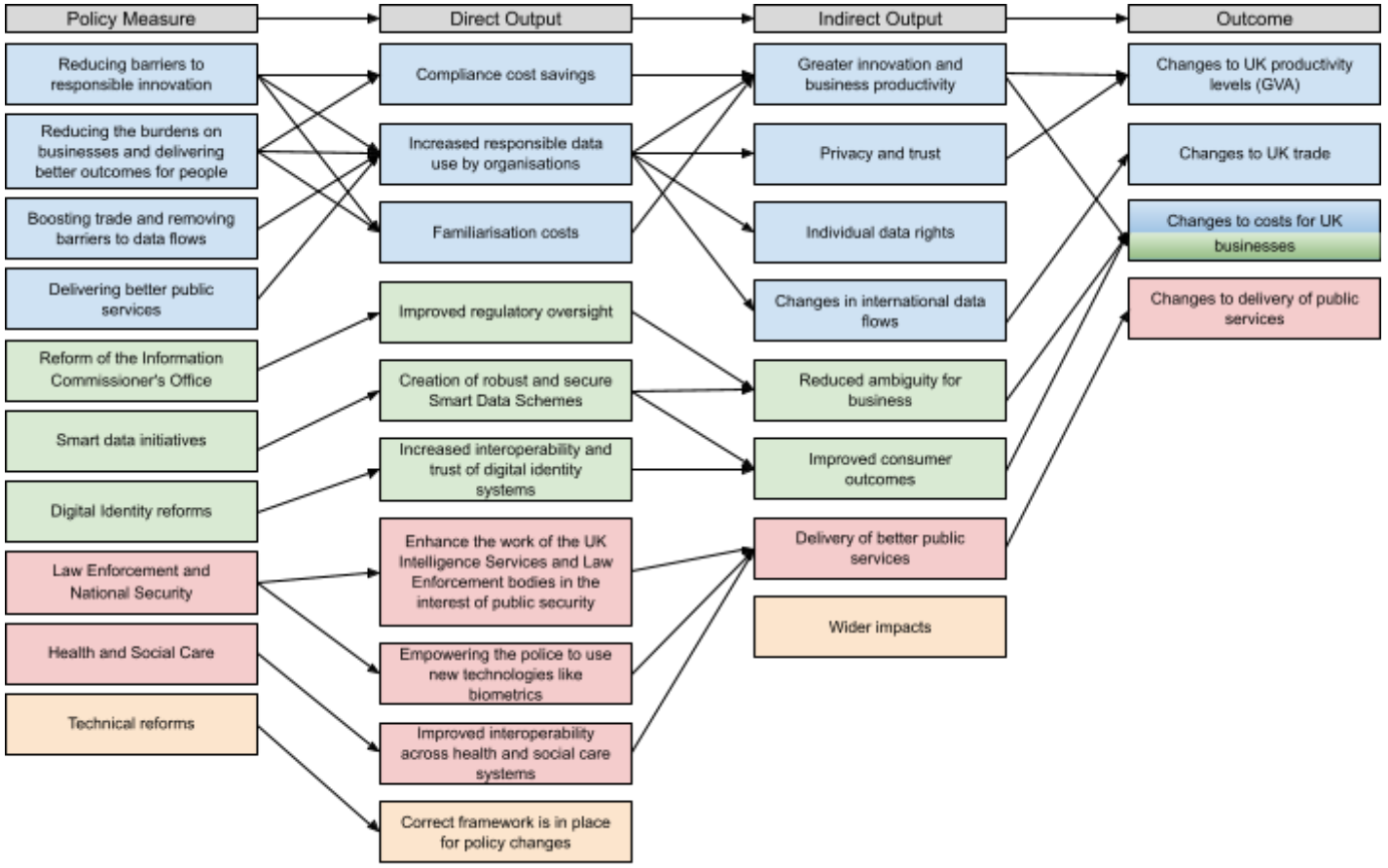
[276] The DCMS Evaluation Strategy, 2021, Central Analysis Team, DCMS

[277] DCMS: Data Policy, National Data Strategy Monitoring and Evaluation Plan, 2021

[278] https://www.gov.uk/government/publications/business-regulation-producing-post-implementation-reviews/producing-post-implementation-reviews-principles-of-best-practice

[279] If there were reforms stratified by size of business (for example, a rule only applying to businesses which employ more than 250 people) one option is to commission bespoke evaluator studies which use a difference in difference approach (that is, looking at companies just above or below the cut-off point specifically to assess a difference in changes over time)

Figure 5: Theory of change for the preferred option



711. The theory of change outlined the expected long-term outcomes and impacts of the preferred package of reforms. These included the following impacts:

a. An increase in data use amongst businesses

b. An increase in familiarisation costs

c. An increase in consumer privacy and trust

d. Changes to international data flows and UK trade

e. Improved regulatory oversight

f. Lower compliance costs for UK businesses

g. Increase in UK business productivity

h. Introduction and take up of smart data schemes

i. Competition in data markets

j. Introduction and take up of digital identity schemes

k. Improvement in public services

   i. Increase in data sharing across Government departments (CDDO)

ii. Increase in data use and sharing for National Security and Law Enforcement purposes including the use of biometric tech

iii. Increase in interoperability across health and care systems

712. The table below details the proposed methodologies and resources required in order to accurately and efficiently measure the success of the proposed policies within the Data Protection and Digital Information Bill.

Table 81: Long run impacts of the package of reforms and how these will be monitored and evaluated

Long Run Impact	How this will be monitored and evaluated
An increase in data use amongst businesses	DCMS annual UK Business Data Survey asks businesses whether they use data, what type of data (personal or non-personal), if they receive or share data and with whom. After this bill is passed we will be able to compare figures from before implementation to those afterwards to track the trajectory of data use, and we will attempt to infer how much of this change can be attributed to these reforms. Many of the reforms are targeted at increasing data use in fields such as research, AI and Machine learning. Using data from a variety of sources including DCMS surveys, the office of AI[280] and McKinsey[281] alongside UKBDS results and new and ongoing consultations with private sector firms, we will be able to track changes and attempt to ascertain the impact of our reforms specifically. For changes to SARs pricing, there are existing data collections on this, so we will be able to estimate cost changes as a result of legislative changes with no extra data collection
Increase in familiarisation costs	The UK Business data survey will continue to report on familiarisation activities of UK firms. The process evaluation will also be used to ascertain the impact of our reforms on familiarisation costs.
Increase in consumer trust and privacy	Consumer trust and privacy will be monitored through use of surveys such as the CDEI tracker survey[282] and the ICO trust and confidence survey.[283] It can also be evaluated through the collection of data on the number of customer complaints and breaches of data from the ICO and number of SARs requested.
Changes to international data flows and UK trade	DCMS has an existing measure of data enabled trade using a variety of publicly available data sets, and this will continue to be refined, updated and recorded following the implementation of the bill. DCMS will also attempt to develop methodologies to measure the impact on trade of changes in data policy e.g. by developing its own econometric modelling approach, where relevant.
Impact of changes to data bridge regulations	SCC Compliance rate - This will be monitored as part of the UK Business Data Survey going forward.

280 https://www.gov.uk/government/publications/ai-activity-in-uk-businesses/ai-activity-in-uk-businesses-executive-summary

281 https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2021

282 https://www.gov.uk/government/publications/public-attitudes-to-data-and-ai-tracker-survey

283 https://www.gov.uk/government/publications/public-attitudes-to-data-and-ai-tracker-survey

Improved regulatory oversight	Changes to ICO functions will be measured using a time cost approach in which ICO will report to DCMS any additional costs and benefits of changes to their organisational structure. In terms of ICO performance this will be measured by the existing KPIs in place at the ICO.
Lower compliance costs for UK businesses	Estimated compliance costs for UK businesses will be measured using the UK Business data survey. This includes the number of full-time equivalent members of staff employed whose primary role is to undertake activities related to complying with UK data protection laws (or time spent a month for sole traders), and the activities undertaken in the last 12 months', which can be used to produce estimates of costs. The average cost of compliance activities is also taken from a variety of published academic sources. The consultation was also instrumental in providing evidence of these activities. Going forward we will track the changes in these estimations using future iterations of the UK Business Data survey and compare them to pre-implementation costs.
Increase in UK business productivity	The relationship between productivity levels and data use is a relatively new area of research. Academic literature is limited and the definition of data use and productivity varies across much of it. As a result of this DCMS is looking to monitor this relationship going forward by carrying out its own longitudinal study across sectors on the relationship between data use and firm level productivity. This will allow us to track the changes in productivity that are due to an increase in data use or availability as a result of the bill.
Introduction and take up of smart data schemes	The monitoring and evaluation plan have been provided by BEIS in the section below. As this bill covers the primary and enabling legislation an evaluation which is based on the underlying theory of change for the measure will be undertaken.
Competition in data markets	As the bill is designed to decrease the barriers to data use for UK firms and public sector organisations, we expect the market to become more competitive. DCMS will work with CMA on a programme to define and measure the competitiveness of data markets
Introduction and take up of digital identity schemes	As this is primary and enabling legislation, costs and benefits will vary by sector and use case. The monitoring and evaluation of each should be specific to each reform accordingly. However, there are metrics that can be used to monitor and evaluate the impact of the enabling legislation; these include the number of organisations certified, the number of checks made in total, the number of people signed up to the trust framework and the growth in numbers of service providers. Going forward these will be monitored by DCMS.
Increase in data sharing across departments	This is primary and enabling legislation, costs and benefits will be specific to each use case. The monitoring and evaluation of the primary legislation will use internal data from the Digital Cabinet Office. A centralised source of information should also result in a more accurate assignment of funding across government and reduce incidences of fraud which will be measured also by the Cabinet Office.
Increase in data use in National Security and Law Enforcement including use of biometric tech	The impact of the new arrangements will be monitored through existing stakeholder forums. Engagement with impacted groups takes place on a regular basis to consider the impact on these communities and their operations. Assessment of the new arrangements will be extended to these forums and any suggested amendments will also be considered

	through these channels. Any arising issues will continue to be flagged through internal data protection practitioner networks and escalated through data policy working groups, and boards, if required. This reflects existing structures that are in place to manage data protection related matters.
Increase in interoperability across health and care systems	This piece of legislation is primary and enables detailed monitoring and evaluation plans to follow with secondary legislation. In order to measure the impact of the primary legislation, key statistics such as the number of cases of non-compliance and the cost and number of times new IT equipment is procured will be monitored. Furthermore, we expect the legislation will lead to a decrease in waiting times, efficiency benefits of the removal of duplicated data entries and an increase in research and innovation, all of which will be monitored through DHSC metrics.

713. Many of the impacts will rely on new data sources that we will need to capture to fill current existing evidence gaps. In the risks and assumptions section of this Impact Assessment we highlight the modelling assumptions that have been made due to a lack of existing evidence. There this is the case DCMS will ensure that there is a strategy for recording these going forward. The table below summarises these assumptions and the proposed ways forward in terms of their monitoring and evaluation:

Table 82: Evidence gaps and proposed monitoring and evaluation approach

Long Run Impact	Evidence gap	Proposed Monitoring and Evaluation
Lower compliance costs for UK businesses	How much data use is affected by clarification of when businesses need to seek legal advice under the proposed policy changes	This will be monitored as part of the UK Business Data Survey going forward, using the number of businesses 'prevented from using or sharing data due to legal restrictions' or because 'they were unsure if it was permitted under the data protection laws'
	% reduction in legal advice required to clarify legislation	This will be monitored as part of the UK Business Data Survey going forward, using the 'proportion of businesses who sought legal advice' as a metric and tracking this over time.
	% of businesses that seek legal advice in a year	This will be monitored as part of the UK Business Data Survey going forward, using the 'proportion of businesses who sought legal advice' as a metric.
	% reduction in complaints around data use	This will be monitored using complaints data from the ICO
	% of complaints in firms that have R&D member of staff - related to R&D	This will be monitored at an industry level using industry wide statistics of firms that report partaking in R&D and the average number of complaints in these sectors
	% reduction in legal advice required in cases where businesses are using	The number of businesses that require legal advice will be monitored as part of

	data for AI	the UK Business Data Survey going forward. The share of these businesses that are using data for AI is currently taken from McKinsey's AI in the UK: Prospects and Challenges report.[284] We will continue to monitor this share using data from the Office of AI.
	Proportion of businesses that will no longer need to offer opt-in/out services	This will be monitored as part of the UK Business Data Survey going forward, using the '% of businesses who said they have introduced opt-in consent mechanisms in the last 12 months' metric.
	Scale down factor to account for the fact that EC survey only included organisations employing 20+ people	The number of SAR's received by small and medium firms will be monitored going forward by the ICO.
	Share of SARs from third parties	The number of SARs received from third parties is recorded by the ICO, DCMS will work with the ICO to monitor these figures following the implementation of the bill.
Increase in UK business productivity	The number of firms that would increase data use because of these measures	Further DCMS work to identify the link between data use and productivity is being developed
	% of firms that would not increase AI use based on the AI measures in the bill	Further DCMS work to identify the link between data use and productivity is being developed. For AI measures we will also work with the Office of AI.[285]
	Proportion of businesses for which improving standards would lead to additional sharing	Further DCMS work to identify the link between data use and productivity is being developed
	Accounting for the fact that this is about data shared across organisations rather than all data	Further DCMS work to identify the link between data use and productivity is being developed
Increase in Familiarisation costs	Wage assumptions of those responsible for familiarising themselves with new legislation - across firms of different sizes	This will be monitored as part of the UK Business Data Survey going forward.

714. We acknowledge that this Monitoring and Evaluation strategy relies on the use of the UK Business Data Survey, if changes are made to the running of this survey we will ensure to fill any evidence gaps and gain access to the information and data necessary by using either existing DCMS resources for evaluation, or run a competitive tender for new primary data collection, and synthesis of existing secondary data sources, to be done by an independent

[284] Artificial intelligence in the United Kingdom: Prospects and challenges - McKinsey 2019
[285] https://www.gov.uk/government/publications/ai-activity-in-uk-businesses/ai-activity-in-uk-businesses-executive-summary

research agency. This will ensure that the evaluation happens, and ensures its analytical rigour and independence.

715. We can design this so that primary research on the process evaluation (how it is implemented) is, to start with, on a regular (e.g. monthly/ bi-monthly, for 6 months) reporting basis so that monitoring can occur. In the event of e.g. unclear guidance to businesses, rapid corrective action could be taken. Similarly, the impact evaluation should, where possible, look to report on an annual basis to DCMS, even if the final PIR only needs to report in 3-5 years.

716. DCMS will lead the monitoring and evaluation of all policies included in this bill. Where policies are being followed up with secondary legislation by different departments, M&E plans will be developed and led by the departments directly. An outline of the policies this includes can be seen in the table below and more information on these can be found in the sections below:

Table 83: All reform areas that will need secondary legislation Monitoring and Evaluation plans

Policies that will require secondary legislation Monitoring and Evaluation	Leading Government Department
AI and Machine Learning	DCMS
Privacy and electronic communications and the use of personal data for the purposes of democratic engagement	DCMS
Changes to Digital Economy Act 2017	CDDO
Digital Identity	DCMS
Smart Data proposals	Sector specific
DHSC Open Data Architecture	DHSC
Public Safety and National Security (Home Office)	Home Office

Smart Data proposals (BEIS) - Monitoring and Evaluation

717. To monitor and evaluate the impact of the smart data primary legislation, an evaluation which is based on the underlying theory of change for the measure will be undertaken. The impact of the legislation will be assessed against the key objectives of the legislation:

a. Reduction in regulatory duplication: This should be measured by the number of Smart Data schemes using the primary legislation

b. Acceleration of schemes: The length of time taken for BEIS to develop primary legislation could be taken as a proxy for the amount of time saved for relevant sectors, assuming sectors would have independently sought primary legislation otherwise.

c. Cross-sector coordination: This could be measured by the number of TPPs operating successfully across multiple sectors, or the marginal costs to TPPs entering a second scheme, compared to the counterfactual.

718. Across all these objectives, and in evaluating the quality of Smart Data schemes, a key challenge is establishing a robust counterfactual for what would have occurred in the absence of primary legislation. There is no plausible way to separate what extent of the scheme's outcomes are a result of the coordinating work of Smart Data and what are the results of the scheme itself.

719. The counterfactual will vary by scheme and should reflect the sector specific circumstances. While Open Banking could be used as an example, it is not underpinned by this primary legislation, and it is expected that learnings from Open Banking can help accelerate the implementation of other Smart Data schemes. Examples of schemes where the counterfactual is likely no scheme emerging:

720. Open Finance - In the Open Finance consultation response, FCA said that a legislative framework would be needed for Open Finance to develop fully. In this consultation response, respondents also pointed out that coverage for existing initiatives for Open Finance-type arrangements will inevitably be partial, limiting the potential benefits.

721. Open Comms – Without government intervention, DCMS do not think industry would take forward the development of a voluntary scheme in the foreseeable future, that affords consumers easy access to, and the sharing of their data. Intervention is required to ensure that relevant data sets and types are in open formats, and to standards which would allow effective use by third-party providers. In the Open Communications consultation response, Ofcom said that they did not envisage that industry would introduce customer data mobility voluntarily

722. Additionally, Smart Data forms a critical part of the government's National Data Strategy, Mission One: Unlocking the value of data across the economy. A monitoring and evaluation framework have been published to evaluate the effectiveness of the five missions in delivering their objectives. As part of this work, DCMS has also undertaken a call for evidence to identify high-level 'indicators' to assess opportunities and track success, including indicators for data use in organisations and productivity.

723. Whether the Smart Data powers are used to introduce new schemes will be an indicator of the success of this legislation.

Enhance the Work of the UK Intelligence Services and Law Enforcement Bodies in the Interest of Public Security (Home Office) - Monitoring and Evaluation

724. The impact of the new arrangements will be monitored through existing stakeholder forums. Engagement with impacted groups takes place on a regular basis to consider the impact on these communities and their operations. Assessment of the new arrangements will be extended to these forums and any suggested amendments will also be considered through these channels. Any arising issues will continue to be flagged through internal data protection practitioner networks and escalated through data policy working groups, and boards, if required. This reflects existing structures that are in place to manage data protection related matters.

Annex

1. List of all recommended policies
2. More detailed rationale for intervention in the health and care sectors
3. Summary of preferred option with description of implementation plan of DHSC measure
4. EU Adequacy Monte-Carlo Analysis
5. List of ICO guidance updates
6. Gravity trade modelling

1.Full list of policies in preferred package of reforms

Table 84: All policy reforms included in the preferred package and whether they will be followed by secondary legislation.

Reform subheading	Reform summary	Reform Heading	Will this policy be followed up with secondary legislation? (Y/N)
Removing barriers to responsible innovation	Research Purposes	Consolidating research provisions into a single chapter Creating a statutory definition of scientific research	N
		Incorporating broad consent for scientific research into legislation	N
		Extending the “disproportionate effort” exemption on information provision requirements for further processing for research purposes of personal data collected directly from the data subject	N
		Extending the exemptions from the regime when conducting scientific research to include when that research is carried out in a commercial setting.	
	Further Processing	Clarifying how personal data can be further processed for research purposes Clarifying that further processing for an incompatible purpose may be lawful when based on a law that safeguards an important public interest or when the data subject has re-consented	N
	Legitimate Interests	Creating a limited list of legitimate interests for businesses to process personal data without applying the balancing test	N
		Clarifying activities that fall under legitimate interests, by listing activities such as direct marketing or ensuring network and information security.	N
	AI and Machine Learning	Future proofing Article 22 Enhancing the approach to explainability and accountability for fair processing in the context of AI Clarifying the circumstances in which safeguards apply to significant decisions that are taken about individuals on the basis of profiling.	Y
	Data minimisation and anonymisation	Adopting the recital 26 test for anonymisation into legislation	N
Reducing burdens on businesses and delivering ~~better outcomes for people~~	Reform of the Accountability Framework	Introduce a more flexible accountability framework, underpinned by “privacy management programmes” Reducing and simplifying record-keeping requirements, for organisations that control or process low risk data.	N

	Subject Access Requests	To amend the threshold for responding to a SAR from ‘manifestly unfounded’ to ‘vexatious’	N
	Privacy and electronic communications and the use of personal data for the purposes of democratic engagement	To remove the consent requirement for analytics cookies and similar technologies (governed by Regulation 6 of PECR) and treat them in a similar way as "strictly necessary" cookies. These measures may be superseded by an ‘opt out model’ in relation to placement of cookies on websites when technological advancements mean that people can set their preferences once using browser-based solutions or automated consent-management tools.	N
		Empowering ICO to take action against organisations for the number of unsolicited direct marketing calls 'sent' as well as calls 'received' and connected.	N
		Introducing a 'duty to report' on communication service providers to report suspicious traffic transiting their networks.	N
		Empowering ICO to impose assessment notices on companies suspected of PECR breaches	N
		Requiring websites to respect preferences set by individuals through their browser. The Bill would set out the main principle, but we may need regulations to set out further detail about how the provision would work (e.g. including what technologies are in scope).	Y
		Increasing fines under PECR to GDPR levels	N
Boosting trade and removing barriers to data flows	Data Bridge	Underpinning the UK’s future approach to data bridge regulations with principles of risk-assessment and proportionality	N
		Relaxing the requirement to review data bridge regulations every 4 years	N
	Article 27 representatives	Remove the requirement for controllers in adequate countries to have representatives in the UK (art. 27)	N
	Alternative Transfer Mechanisms	Power for SoS to formally recognise new ATMs	N
		Changes to the standard approach to alternative transfer mechanisms. (Art 46) Ensuring businesses are able to continue to use their pre-Bill existing transfer mechanisms without a requirement for further checks and avoiding additional costs.	N
Delivering better public services	Public Interest	Clarifying that private organisations & individuals asked to carry out an activity on behalf of a public body may rely on that body’s lawful ground for processing the personal data under Art 6(1)(e)	N
	Digital Economy Act 2017 (CDDO)	To extend powers under section 35 of the Digital Economy Act 2017 aimed at improving public service delivery to business undertakings, beyond the current scope of solely individuals and households	Y
Reform of the Information ~~Commissioner's Office~~	Strategy, Objectives and Duties	ICO's Objectives and Duties	N
		Statement of Strategic Priorities	N

	Governance Model and Leadership	Remove the Information Commissioner corporate sole structure. Introduce a Board structure with Chair/CEO.	N
		Remove the requirement for Parliament to agree to a change to the IC salary.	N
	Accountability and Transparency	Accountability and Transparency - require publication of key documents	N
		Codes and Guidance - ICO required to undertake and publish an Impact Assessment and consult with a panel of experts when developing statutory codes of practice and statutory guidance, unless exempt	N
		Codes and Guidance - SoS approval process for ICO statutory codes of practice and statutory guidance, unless exempt	N
	Complaints	Complaints - Introducing criteria in legislation by which the ICO can decide not to investigate a data protection complaint	N
		Complaints - organisations required to have a complaint handling process	N
	Enforcement Powers	Enforcement - power to commission technical reports	N
		Enforcement - power to compel witnesses to attend interview	N
		Enforcement - notice of intent extension	N
		Enforcement - without attending premises clarification	N
Technical Reforms	• Text stating that other primary legislation is to be treated as being subject to the data protection legislation unless express provision is made to the contrary.		N
	• Enabling statutory codes requested by the SoS under this section to have the same legal effect as those issued under sections 121 - 124 of DPA		
	• In the event that DCMS Ministers decide to ratify the Council of Europe Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (also known as C108+), outdated references to the original Convention 'C108', in ten articles of the Data Protection Act 2018, will need to be changed to C108+		
	• Amending section 128 of the Data Protection Act 2018 (DPA 2018) to make sure that any new ICO codes of practice required by regulations made by the Secretary of State have the same legal effect and status as existing ICO codes issued under the DPA 2018 (the data-sharing and age-appropriate design codes are examples of existing codes).		
	• Update the definition of "direct marketing" in PECR so that it is drawn from the DPA 2018, rather than the DPA 1998. Most of the DPA 1998 was repealed when the 2018 Act came into force, so this should make the legislation easier to navigate.		

	• Clarifying the anonymisation process by creating a test for identifiability		
	• Omitting Article 27 from UK GDPR which removes the requirement for controllers and processors caught by Article 3(2) to appoint a representative		
	• Privacy Management Programme - An amendment to ensure consistency in language between Clause 18 18(2)(b) and Clause 18(5)(b).		
	• Research - consequential provisions - Disapply the provisions of new Chapter 8A UK GDPR (inserted by Cl 22) in relation to unstructured manual data held by FOI Public Authorities.		
	• Codes of practice as to the processing of personal data - This amends section 205(2) of the Data Protection Act 2018 so as to disapply the provision about periods of time in Article 3 of Regulation (EEC, Euratom) No. 1182/71 which would otherwise apply for the purposes of section 120H(3) and (4) of that Act (inserted by clause 28 of the Bill).		
	• Enforcement: Remove duplicative reference to a 'report' in this clause		
	• Annual report on regulatory action - A minor amendment to clause 38 to clarify the definition of "enforcement powers" in new section 161A(6) so that it does not include section 142 to 159 DPA as applied by the EITSET and PEC Regs and section 20(2) of the Interpretation Act does not apply here.		
	• Consequential amendments of The Electronic Identification and Trust Services for Electronic Transactions Regulations (EITSET Regulations) - An amendment to change the words modified, as well as the modification in this clause		
	• Statutory Override - Clarification of the scope and intended effect of s183A .		
	• UK GDPR Regulations - An amendment to add "made under this Regulation or another enactment that are" in order to ensure consistency with other clauses		
	• Information disclosed by the Revenue and Customs - making equivalent provision for Welsh and Scottish revenue authorities		
	Clause 62 establishes the primary power to establish Smart data schemes with a focus on customer data, including data sharing and action initiation by an authorised person or TPP. Further details are included around the associated regulations in Clause 63.	Clause 62 amendment - This amendment makes clear that the power under clause 62(3) is available in relation to all persons authorised to receive customer data, whether or not they have received such data. Clause 63 amendment - This amends clause 63(3) so that it reflects more clearly the fact that regulations under clause 62 may enable a customer to authorise a person to receive customer data and to do other things, in particular as described in clause 62(2)(b) and (3).	

	Subsection 62 (3) is likely the focus of any amendment, although we are awaiting further legal advice.		
	● Clause 63 outlines provisions that regulations relating to customer data may, among other things, contain. ● A change to the wording in clause 63(3) to reflect the fact that the intention is that regulations may require a person who is an "authorised person" (as defined in clause 62(1)(b)) to be further authorised in order to eg. exercise a customer's rights in relation to a data holder.		
	● Smart Data regulations- Deletion of redundant subsection (5) of clause 74. Subsection (5) of clause 74, which makes provision about regulations under Part 3 of the Bill, is unnecessary because equivalent provision about regulations under the Bill is made in clause 107(4).		
	● Definitions in Democratic Engagement clause- definitions for “communication”, “public electronic communications service” and “call” to be made clear.		
	● Co-operation between supervisory authority and overseas authorities -This inserts a consequential amendment of the heading of Article 18 of the eIDAS Regulation (cooperation with EU authorities).		
	● Transfer of functions etc to the Information Commission - Adding the gloss so that "information Commissioner" and "Information Commission" are read as the same		
	● Purpose limitation: processing to be treated as compatible with original purpose - To remove the exception from various provisions for journalistic, academic, artistic and literary purposes in sch 2 para 26 in light of the change to Art 36(1).		
	● Subject access requests - In clause 7(3), new Art 12A(1) (page 9, line 10) refers to “Articles 15 to 22 or 34”. Clause 11 removes Article 22 and replaces it with new Articles 22A to 22D.The amendment would ensure that article 22 should be consequently amended by Schedule 3.		
	● Transfers of Personal Data to Third Countries - Transfers Approved by Regulations: Monitoring - Subsection 74B(7)(a) was removed and we believe that the connector "and" after this subsection should be also removed. In current drafting it is not determined and it looks like "and" should be kept and followed by subsection 74B(7)(b) which was preserved.		
	● Transfers of personal data to third countries etc: consequential and transitional provision - This amends section 205(2) of the Data Protection Act 2018 in consequence of the repeal of section 189(9) of that Act by paragraph 19 of Schedule 7 to the Bill.		
	● ICO Complaints - An amendment to ensure consistency between s.187(1)(a) and (2)(a)		
	● ICO Complaints - The amendment is consequential to the repeal of Art 77 UK GDPR by batch Comp-ICO		

	Privacy and electronic communications: Commissioner's enforcement powers ● The modifications in the new Schedule 1 to the PEC Regulations inserted by Schedule 10 to the Bill do not take account of the changes made by clause 13 of the Bill. In particular - ○ paragraph 3(d) modifies s.142 DPA 2018 by omitting subsections (9) and (10). Subsection (9) is repealed by clause 13(3)(a); ○ paragraph 4(1) modifies s.143 DPA 2018 by omitting subsections (1) and (9). Subsection (9) is repealed by clause 13(3)(b); ○ paragraph 24 modifies s.181 DPA 2018 by omitting the definition of "representative", as well as the definition of "certification provider". The definition of "representative" in s.181 DPA 2018 is to be repealed by clause 13(3)(c) of the Bill. ● Clause 13 is to come into force 2 months after Royal Assent (see clause 111(3)(b)) and the expectation is that Schedule 10 would come into force at that time or afterwards, ie. by the time it operates, the definition of "representative" will have been removed. ● The modifications listed above should be changed to take account of the changes made by clause 13(3).		
	● ICO Governance - An amendment to ensure consistency between paragraphs 8(1) and 9(6) in reference to the Commission		
OGD / Other DCMS teams' batches	Digital Identity	eIDAS/trust services	Y
		Data checking gateway	
		Trust framework accreditation and certification	
		Trust framework governance	
		Validity of digital identity	
		Mutual recognition of digital identities	
		Mutual recognition of trust services	
	Smart Data (BEIS)	Smart Data: Introduction of primary legislation, creating new "regulation-making" powers to enable Smart Data schemes to be introduced in any given sector.[286]	Y
	DHSC - Data Architecture	Create primary legislation for a new power for the Secretary of State for Health and Social Care to direct suppliers/suppliers to adopt an open data architecture approach through the use of ISNs. [287]	Y
	Public Safety and National Security (Home Office):	Subject Access Requests (SAR) (DPA 2018 part 3/4)	N

[286] This is the preferred option in the Smart Data initiatives Impact Assessment 2022 published by BEIS
[287] This is the preferred option in the DHSC proposed reforms

	Subject Access Requests		
	Public Safety and National Security (Home Office): Part 4	Amendments to Part 4 of the DPA 2018 - National Security Notices	N
	Public Safety and National Security (Home Office): Law Enforcement Data Reform Proposal	Mirror the national security exemption from Part 2 (DPA 2018 part 3)	N
		Introduce a 'Legal Professional Privilege' Exemption (DPA 2018 part 3)	N
		Introduce a definition of 'consent' to Part 3 (DPA 2018 part 3)	N
		Introduce a power to allow bodies representing Part 3 controllers and processors to produce 'Codes of Conduct' (DPA 2018 part 3)	N
		Remove the need to log the 'justification' for consulting/disclosing data disclosure	N
		Introduce the ability to actively review automated decisions (DPA 2018 part 3)	N
	Public Safety and National Security (Home Office): International Transfers	Clarifying use of Section 76 DPA to cover larger scale transfers (International Transfers)	N
		Reform subsequent transfer's provision (Section 78 DPA)	N
	Public Safety and National Security (Home Office): Biometrics	Oversight Reform (Biometrics and Overt Surveillance) (ICO)	N
	Public Safety and National Security (Home Office): I-LEAP	Introduce delegated power to pass secondary legislation enabling the technical implementation of new international alert sharing agreements	Y
	Public Safety and National Security (Home Office): Birth and Deaths	Remove the requirement for paper birth and death registers moving to an electronic register	N

2. More detailed rationale for intervention in the Health and Social Care sector

DHSC open data architecture measures are seeking through the DCMS Data Protection and Digital Information Bill to introduce new enabling powers for the Secretary of State to prepare and publish standards for IT products and services used in the health and adult social care sector in England and will require the suppliers of the products to comply with these standards.

The case for reducing burdens on businesses and delivering better outcomes for people

1. Suppliers of health care products and services do not own or control the data they hold, but the different system designs can act as a barrier to accessing it across health and social care, both for direct care and wider purposes, with no formal central outline of how suppliers should be acting. In addition, there are many unconnected legacy systems and platforms used by health and care staff, resulting in data being held in silos within individual digital public and or patient health record systems, where it is not widely accessible and can't be shared easily, providing a technical barrier to direct care, as well as operational planning, research and innovation.

2. Creating a central set of standards will ensure there is clarity for the supplier market on what they will need to provide for in their products and services; both for existing and new suppliers. It will also ensure that over time, all [legacy] systems are upgraded to allow for easier interoperability around a common set of standards, rather than requiring bespoke solutions from system to system.

3. The future success of integrated care is contingent on freeing this data to share it efficiently and effectively, first and foremost to enable patient centred care ensuring data more closely follows individuals through the health and care system. Health and care information technology systems will need to adopt changes that allow data to be accessed and made available according to open standards and a common architecture to enable this future vision.

4. In doing so, this will create the ability to share a person's care data across and between health and care professionals to provide optimal and safe care; timely data to run and operate health and care services in local areas; and provide the necessary data for local places to manage population health and reduce health inequalities. This will, for example, avoid delays in diagnosis, prevent tests from being repeated unnecessarily, and get people the treatment and care that they need.

5. People need to be able to have easy access to and share appropriate levels of their information with their care teams such as medications, procedures, test results and care plans so that they can become partners in their care. By ensuring that systems are interoperable, we will improve patient experiences by providing access to patients and carers to all appropriate clinical records, transactional data and events (like booking an appointment) relating to them, where clinically safe to do so.

6. One key example that the Secretary of State has in mind in this regard is to require information technology systems to support the inclusion of an individual's unique NHS

Number (or a similar consistent identifier) as the primary identifier in all records relating to a particular person.

7. This includes, in particular, for information technology services or products to enable users to:

    a. search system records for the correct NHS Number using the prescribed national service (currently Person Demographics Service2);

    b. record the NHS Number, including validating and verifying the NHS number;

    c. store the NHS Number and its validation/verification status within the products or services; and

    d. share the NHS Number in correspondence and on printed patient wristbands, via interoperability interfaces.

The case for boosting trade and reducing barriers to data flows

8. Suppliers provide information technology that supports an individual's care in a number of ways. They may supply standalone products that are purchased by the health or adult social care provider with no further involvement of the supplier, products that are sold to the provider but with an ongoing support service provided by the supplier, or they may purely supply a service.

9. It is considered that existing suppliers of information technology are not uniformly providing products and services that incorporate or enable interoperability so that data can easily be shared in real time between organisations that use different systems.

10. Interoperability is the ability of two or more systems either to allow information held in one system to be transmitted to and accepted by another or to allow different systems to write into and read from the same data, in both cases allowing each system to perform tasks using that data without additional intervention of an operator. At present information often has to be manually shared and entered into multiple systems, giving rise to duplicate records, increased likelihood of error or missing information, repeated testing and delay in diagnosis and treatment, as well as creating a data burden on front line clinicians. A study found that 'delayed transfers of care' cost the Manchester University Foundation Trust an estimated £20 million per year and that one causal factor of this is that social care practitioners do not have easy access to patient information needed to complete social care assessments[288]. Furthermore, arguably improving data transfer accuracy and speed within clinical pathways and beyond clinical settings into mental and community care will contribute to a reduction in clinical negligence due to data inaccuracy. Total payments relating to NHS Resolution's clinical schemes (not including administrative costs) stood at £2,209.3 million in 2020/21[289].

11. Technical barriers to interoperability exist because there are multiple different suppliers of information technology in the health and adult social care sector, providing products and services tailored to the differing needs of different types of organisations

[288]https://digital.nhs.uk/services/social-care-programme/demonstrators-programme-2019-21-case-studies/reducing-delays-to-discharging-patients-in-greater-manchester

[289]]https://lordslibrary.parliament.uk/negligence-in-the-nhs-liability-costs/

(respectively referred to in this para as suppliers and recipients). Therefore, interoperability has not been a priority either from a supplier or recipient perspective. Instead, recipients have been focussed on their own individual requirements whilst suppliers have had wide discretion as regards the technical specifications needed to meet these requirements (in relation to design and construction of products and services). This means information is often locked within an individual, purpose-built system, creating a technical barrier to accessing and processing of information by another system.

12. These “siloed” systems also result in a barrier to new market entrants, both due to the technological expertise required and, in some sectors, such as general practice, due to the market already being dominated by one or two suppliers. This has led to a limited choice of suppliers and information technology systems, and a lack of power from individual providers, or central government, to set specific standards for these suppliers to meet. Also, the process and time involved in changing suppliers and/or systems itself acts as a deterrent or barrier to change e.g. because of concerns over transition issues or potential system “down time”. There is therefore a limited incentive for suppliers to develop products and services which enable interoperability.

13. Additionally, whilst there are a number of suppliers in the health market in particular, the acute market is dominated by a small number of large suppliers, with high switching costs alongside high barriers to market entry - it is clearly not competitive. For example, almost half of all EPRs supplied to the acute, ambulatory, community and mental health settings are supplied by 4 suppliers. In the acute setting alone, only 2 suppliers provide over one third of EPRs.

14. It is clear that EPR vendor markets for primary, community and mental health are highly segmented with similar levels of market concentration in each of the relevant segments, and the General Practice EPR market is a duopoly. A mixture of interventions to set stronger regulations and promote competition for the market are required to incentivise suppliers to follow standards, improve service, reduce costs and innovate.

15. Products and services built on principles of a unified system architecture, open data standards and interoperability developed within the industry can support information access with aid system providers and suppliers, whilst giving clarity to new market entrants. This will allow for all prescribed information collected or produced by a provider and entered into their information technology system to be made available on demand in a form and manner specified.

16. Our measures intend to remove barriers to data flows, providing the technical ability to share a person’s care data across and between health and care professionals to provide optimal and safe care; timely data to run and operate health and care services in local areas; and the necessary data for local places to manage population health and reduce health inequalities.

The case for delivering better public services

17. An Electronic Patient Record (EPR) system is a secure environment that enables access to digital records detailing a patient’s health history, care provided, prescribed medications and test results to support the management of their care. EPRs give

clinical and operational teams the real-time information they need to deliver safer, faster, high quality care as well as to manage organisational operations, such as moving patients to the most appropriate expertise or clinics with shortest waiting lists. Only when universal high quality EPR coverage is achieved can the build of comprehensive Shared Care Records and Patient Health Records be met as set out in DHSC Data Saves Lives: reshaping health and care data strategy.

18. We currently face a number of challenges in achieving universal high quality EPRs:

    a. There is huge variation in digital maturity of NHS organisations. Some NHS organisations have world-class digital maturity with state-of-the-art EPRs that clinicians' rate highly, but 15% do not have EPRs at all, 62% have medium capabilities and 23% have a high level of maturity. We must bring organisations with lower capability up and ensure that they adhere to a set of shared principles from the outset, whilst helping those who are the most digitally mature progress further.

    b. NHS organisations have vastly varying skills to deliver digital transformation at the scale required by an EPR implementation. A number of NHS organisations may not have the skills and information to get the best product or deal or make the best use of NHS purchasing power. There is also variation in the capability of EPR products, with the predominant EPRs used in the mental health and community trusts failing to keep pace with the NHS's changing requirements. A shared set of standards here to build towards would be beneficial.

    c. To enable joined up care, it is not enough for all organisations to have EPRs. These systems need to interoperate in real time - with data flowing to Shared Care Records and Patient Health Records - so patients can get safe, high quality care no matter what setting they attend.

    d. There is substantial variation in how EPR suppliers store data and none of them make it easy to extract or share this data making direct care, population health management, innovation and research all much harder. Open data standards would address this.

    e. Only 24% of suppliers report having solutions that cover more than one care setting (covering acute, ambulance, community, mental health, mental health and community) making interoperability critical to achieve joined up health and care.

19. Good quality data (i.e. comprehensive, real-time, consistently recorded and shareable data) is crucial to delivering safe and effective patient care, driving productivity, matching resources to need, and supporting innovation and research. DHSC ambition, set out in the Data Saves lives: reshaping health and social care with data strategy,[290] is to develop the health data infrastructure in a way that enables the delivery of these benefits at reasonable cost, improving the delivery of public services.

20. Furthermore, the Secretary of State for Health and Social Care announced a commitment for 90% of all NHS trusts to have EPRs in place by 2023 (with the

[290] https://www.gov.uk/government/publications/data-saves-lives-reshaping-health-and-social-care-with-data-draft/data-saves-lives-reshaping-health-and-social-care-with-data-draft#bringing-people-closer-to-their-data

remaining 10% to make progress towards implementing them) and for all social care providers to adopt digital social care records[291]. Further, 80% of social care providers are expected to adopt digital records for social care by March 2024 (currently 40% of social care providers are paper based). The Secretary of State also announced £150 million to drive greater adoption of technology and achieve widespread digitisation across adult social care in England, as part of a 10-year plan to reform the sector[292].

21. Levelling up all NHS organisations and social care providers to a baseline level of EPRs and social care records is a fundamental step to ensuring that patient records are available when and where they are needed. This requires a step change in the pace and scale of delivery, and the provisions covered by this proposal are fundamental to harnessing the potential of widespread EPR and digital social care record use to improve patient care and health outcomes.

[291] Typical digital social care record contract values within adult social care are £3,000 per annum for a 25-bed care provider - Internal NHS England figures

[292] https://www.gov.uk/government/speeches/health-and-social-care-secretary-sajid-javid-speech-at-care-england-2022-conference

3. Summary of preferred option with description of implementation plan of Health and Social Care measure

DHSC open data architecture measures are seeking through the DCMS Data Protection and Digital Information Bill to introduce new enabling powers for the Secretary of State to prepare and publish standards for IT products and services used in the health and adult social care sector in England and will require the suppliers of the products to comply with these standards.

1. The preferred solution is to prepare and publish standards that apply to the products and services provided by suppliers, in order to ensure that those products and services enable and support data to be accessed, interrogated and processed in real time by anyone with the basis to appropriately access that data, irrespective of the system used by the health or adult social care provider who collated, produced or otherwise processed that data.

2. The NHS Transformation Directorate is already progressing the design and development of an open data architecture approach. The standards will require products and services to be based on principles of a unified system architecture, open standards and interoperability developed within the industry, that allow for all prescribed information collected or produced by a provider and entered into their information technology system to be made available on demand, and in a form and manner specified by the Secretary of State. It is expected that the standards will facilitate a staged process over a 5-10-year time frame towards this goal, with technical specifications evolving over time as technology changes and improves.

3. A pathway towards a unified architecture, open standards and full interoperability in the future requires effective engagement with the supplier market. DHSC has already commenced engagement through initial communication with suppliers to inform them of future plans with relation to architecture, standards and interoperability. In addition, a number of TechUK events were held in 2021 around this subject, with more planned for the future. Although engagement is critical for the success of the open data architecture project, it cannot be enough on its own without legislative tools. The standards and accreditation scheme will tie in with efforts to achieve wider interoperability, including working with the Global Digital Health Partnership to facilitate and promote the use of open standards for greater international interoperability with respect to health data.

4. DHSC will be examining existing contracts between suppliers of information technology and providers of health and adult social care, to identify any change in law provisions that may be used to mandate current suppliers to meet new standards for interoperability and open ways of working. They will also be seeking to ensure that the standard contract terms for future contracts require suppliers to comply with standards imposed under the proposed legislation even after the contract has been agreed and/or for the supplier or its products or services to be accredited.

5. The Secretary of State for Health and Social Care will continue to seek adoption of procurement frameworks enabling providers of health and adult social care to be confident that the products and services set out in the framework will meet the standards and are accredited under the new legislation. The Digitising Social Care

Programme and GP IT Futures has developed a Dynamic Purchasing System that assures suppliers of digital social care records software, and provides a mechanism to ensure they meet required interoperability standards.

6. With regards to enforcement, an example approach is provided below, although the details of implementation would be determined at the commencement regulations and/or regulations stage, to take account of the details of the regulations and costs of compliance at that time:

    a. The Secretary of State for Health and Social Care would be designated as responsible for enforcing the standards, and an appropriate body will be identified to manage and administer enforcement of the regulations including regular compliance checking.

    b. Non-compliance to the standards would result in a formal written warning and an agreed timeframe for the IT supplier to the health and social care system to bring their product or service into compliance.

    c. If non-compliance persists without an agreement in place or an exemption agreed, the IT suppliers may be subject to a financial penalty, however the exact details of this are to be determined.

7. Given that this is an enabling power with further detail expected to be outlined in commencement regulations and/or regulations and guidance, we do not yet have a specific date at which this would come into effect.

4. EU Adequacy Monte-Carlo Analysis

725. There are a significant number of assumptions in the EU Adequacy model that we have varying degrees of confidence in. To be transparent on the potential range of uncertainty, we have undertaken Monte-Carlo analysis which varies the assumptions in the model providing an indication of the potential range of results. Only services export results can be adjusted. The goods result is constant across the scenarios (£200m in lost revenue and £40m in SCC costs) and has not been updated since the initial analysis was undertaken. Table 78 shows the summary statistics for the Monte-Carlo analysis showing the mean, standard deviation, minimum and maximum for each of our results of interest. The analysis was run 50,000 times picking a random selection of each of the parameters including for those parameters which vary by business size. These are: profit margins, investment horizon, SCC compliance, the proportion of firms that already have SCCs in place and the proportion of costs borne by the UK firm.

Table 85: Summary Statistics EU Adequacy Monte Carlo Analysis Results

Statistic	N	Mean	St. Dev.	Min	Max
Business that cease trading	50,000	5,043	933	2,817	9,601
Business that continue trading	50,000	95,062	933	90,503	97,287
Annual Lost Export Revenue	50,000	£240m	£17m	£211m	£378m
SCC Costs	50,000	£352m	£29	£240m	£458m

726. The number of businesses that cease trading varies between 2817 and 9601 with a mean of 5043. The three graphs below show the distribution of our main costs (including goods). SCC costs are more uniform in distribution with a mean of £352m with a minimum of £240m and maximum of £458m. Annual export revenue lost has a left-skew with a mean of £240m with a minimum of £211m and maximum of £378m, the result indicates the non-linearity of the two main assumptions for the export decision, investment horizon and profit margin for businesses interact, as both approach their minimum values, results become larger than the mean but this is unlikely.

727. These results have a lower maximum when compared to the simpler scenario analysis described above. Similarly, whilst the mean of lost export revenue is similar, SCC costs mean is lower £352m compared to the £410m central estimate. These divergent results show the unlikelihood of getting all parameters at their absolute minimum or maximum (even when parameters are chosen a large number of times). Even in scenarios where Export Revenue loss is high, where profit margins and investment horizons are low, it does not necessarily mean that SCC costs are similarly high as other assumptions such as the compliance rate, the number of businesses that have SCCs and costs borne by UK firms all vary. The Monte-Carlo analysis was proportionate and took simple draws from triangular distributions based on the minimum, maximum and mean of each. In reality, it is likely certain parameters are highly correlated with each other for example profit margins and investment horizons which both reflect business risk aversion and decision-making.

Chart 4: Export Revenue Lost, EU Adequacy - Monte-Carlo Analysis (50,000 runs)

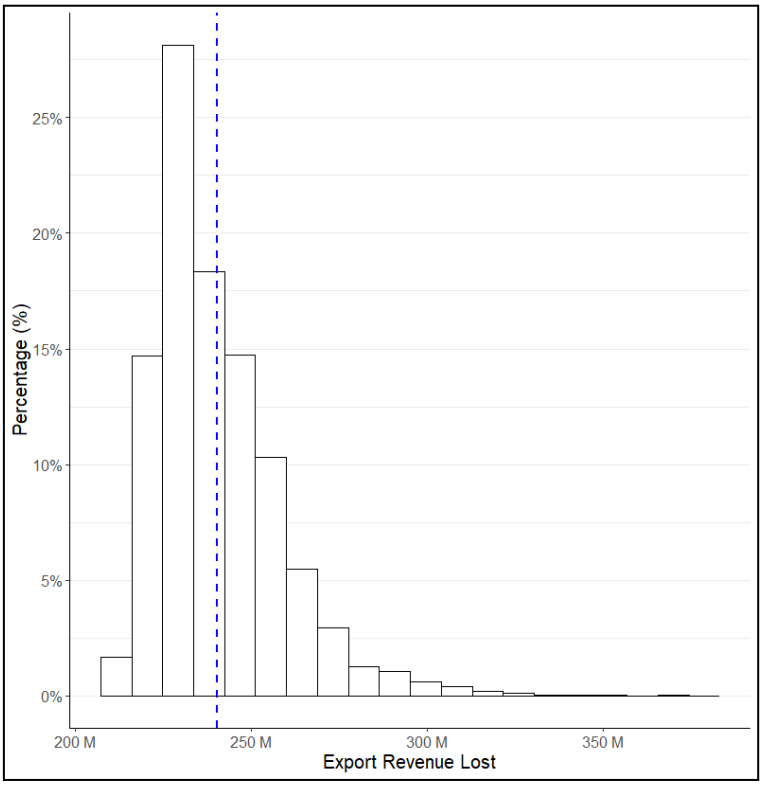
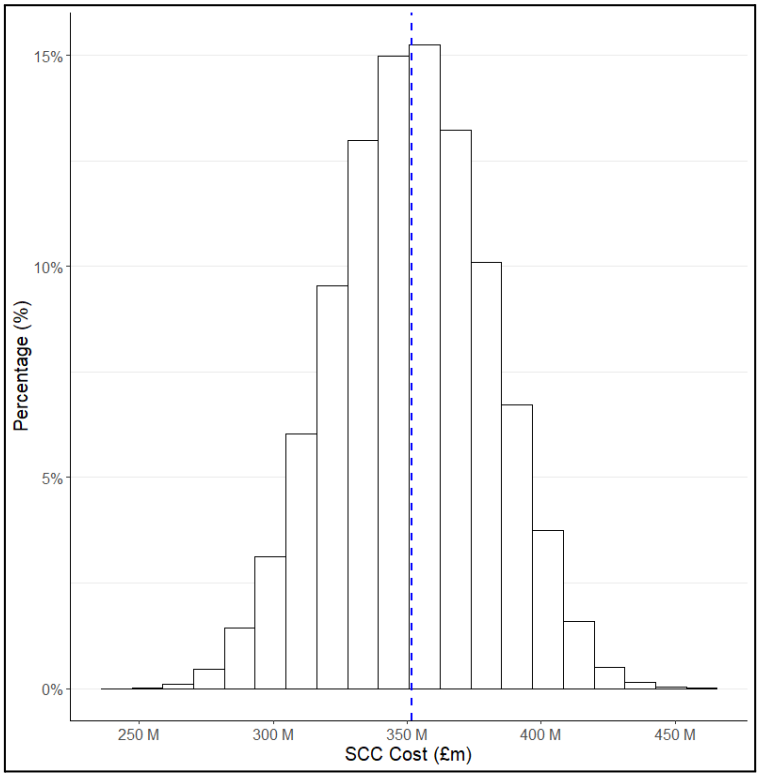


Chart 5: SCC Cost (£m), EU Adequacy Monte-Carlo Analysis (50,000 runs)



5. Guidance proposals for the ICO

Guidance Proposals

There are currently approximately 20 areas where we have identified the need for either significant revisions to or production of new guidance by the ICO.

Guidance which has been set out as needed in the consultation includes:

Chapter 1

- Guidance on schedule 1 processing conditions for AI and machine learning – section 1.5, para 91.

Chapter 2

- New guidance on updated approach to accountability, section 2.3, paras 150, and 182. This section also includes separate proposals for:
    - The ICO set out a list of processing that it considers to be high risk and new guidance on privacy impact assessments and high-risk processing, section 2.3, para 168.
- New guidance on analytics cookies, section 2.4, para 201.
- New code of practice on SARs: not explicitly referenced in the consultation response but we understand the government is minded to mandate the creation of a code on SARs which would need to include content on the interpretation of the vexatious and excessive thresholds as a basis for refusing to comply.

Chapter 3

- Changes to the international transfers framework to be supported by the ICO through practical guidance on determining risks, section 3.3 para 259.
- International transfers: proposal to allow organisations to create or identify their own alternative transfer mechanisms in addition to those listed in Article 46 of the UK GDPR. Guidance is likely to be required from the ICO and could impact on our ability to enforce infringements in these transfers, section 3.3 para 263.

Chapter 4

- Clarifying rules on the collection, use and retention of data for biometrics by the police, through the use of codes of practice and guidance. Section 4.4, para 302.

Guidance identified by the ICO as likely to be needed, but not included in the consultation:

Chapter 1

- Research and re-use of data, reviewing all guidance for consistency with legislative changes.
- Anonymisation: guidance on new provisions.
- ICO guidance on legitimate interests, section 1.4. Need to update guidance to reflect legislative changes and address questions about LIAs for activities not on list and handling of related queries by ICO. Requires, policy, legal, and economic input.

Chapter 2:

- PECR - duty to report: ICO will need to develop guidance on how the duty should be implemented by CSPs.
- PECR – cookies: new guidance based on changes to cookies permitted without consent etc.

6. Gravity trade modelling annex

STRI modelling

1. At consultation stage we outlined a potential modelling approach which included estimating the impact of these policy changes on the OECD's Services Trade Restrictiveness Index (STRI)[293] which sets out a series of sector-specific restrictions to services trade which forms a parameter in an economic gravity model to estimate the impact on trade.[294]

2. DCMS has since then expanded its gravity modelling capabilities and developed its own in-house approach with the help and expertise of other government departments. We have used the Department for International Trade (DIT) Services Trade Model as the basis for our modelling approach[295]. This ensures greater cross-government consistency in our approach.

3. STRIs are used to assess how restrictive, or open and closed to international trade and economic competition, a jurisdiction is to foreign services providers. Barriers to services trade are defined in terms of restrictions to foreign entry, movement of people, discriminatory measures, barriers to competition, and regulatory transparency. STRIs are calculated by the OECD using a scorecard approach; each restriction carries a weight and if in place is added to the score. STRIs are calculated by the OECD for 22 sectors across all OECD countries.[296] The overall modelling approach is to simulate the impact on trade of turning the data specific restrictions 'on' or 'off'. The proposed package of reforms involves restrictions being turned on or off by the UK, EU+ and other trade partners.

Model specifications

4. Full detail of the underlying model's methodology and specification is published in DIT's Services trade modelling working paper. The model works in several stages[297]. Firstly, a standard gravity model is estimated for each sector with controls such as physical and cultural distance, GDP and tax regimes. Fixed effects are also employed to control for unobserved heterogeneity.[298] The key parameter being the sensitivity of trade flows within a sector to the OECD's STRI. As a result, the model captures only countries with STRIs.[299] The second is an estimate of how changes to trade costs in a given country affect trade costs for the rest of the world.

5. The final stage is the general equilibrium simulation exercise[300]. By feeding the scenario back into the structural model estimated in the first stage, directly affected flows adjust in accordance with the sensitivity of trade flows to the STRI but also have an impact on third

---

[293] Services trade in the global economy, OECD

[294] The gravity model of international trade states that the volume of trade between two countries is proportional to their economic mass and a measure of their relative trade frictions. The gravity model has been commonly used in international trade analysis for several decades due to its intuitive appeal.

[295] Services trade modelling, DIT Analysis Working Paper

[296] ibid.

[297] ibid and for further detail on the methodology underpinning the model please see An Advanced Guide to Trade Policy Analysis: The Structural Gravity Model. WTO iLibrary.

[298] By using importer-year and exporter-year fixed effects the model controls for all importer and exporter specific characteristics.

[299]

[300] ibid and for further detail on the methodology underpinning the model please see An Advanced Guide to Trade Policy Analysis: The Structural Gravity Model. WTO iLibrary

countries. These effects feed back into the initial relationship. The results do not account for cross-sector impacts or the reallocation of factors of production. 80% confidence intervals are used to account for uncertainty in the STRI parameter.

6. To model the potential impact of the reforms, we need to appropriately model the STRI position both in the baseline, and as a result of implementing new measures. Currently the UK has among the most liberal data trade regimes worldwide, with the OECD setting only 1 out of 5 data-sector relevant STRIs in place with its international trade partners - including the EU, with which it also has a data bridge.[301]

7. We have identified the reforms most likely to impact trade through changing data restrictions. These are;

    a. Underpinning the UK's future approach to data bridge regulations with principles of risk-assessment and proportionality,

    b. Relaxing the requirement to review data bridge regulations every 4 years

    c. A new power for SoS to formally recognise new ATMs and,

    d. Changes to the standard and approach to alternative transfer mechanisms. (Art 46)

8. The most relevant STRI measures are 1.20.3 (cross-border transfer of personal data is possible to countries with substantially similar privacy protection laws) and 1.20.2 (cross-border transfer of personal data is possible when certain private sector safeguards are in place) respectively. As the OECD already defines 1.20.2 being available in the UK, the only available measure for modelling changes is 1.20.3. Therefore, turning this off between the UK and a priority country is used to represent data bridge regulations. For testing reciprocation, both 1.20.2 and 1.20.3 are relevant as some partner countries do not have alternative transfer mechanisms in place.

9. Whilst these measures do closely relate to the policies, this lack of specificity indicates a limitation of the STRI in measuring policy changes. How data bridge regulations and alternative transfer mechanisms work in practice differs by country. As above, this indicates how results may overestimate the impacts.

Table 86: Reforms that will impact trade

Reforms	Most relevant STRI measure
● Underpinning the UK's future approach to data bridge regulations with principles of risk-assessment and proportionality ● Relaxing the requirement to review data bridge decisions every 4 years ● A new power for SoS to formally recognise new ATMs and,	● 1.20.2: Cross-border transfer of personal data is possible when certain private sector safeguards are in place ● 1.20.3: Cross-border transfer of personal data is possible to countries with substantially similar privacy protection laws

[301] Replacing adequacy, 'data bridge' is the term now used by the UK government to describe the mechanism for the trusted flow of data from the UK to another country without restrictions.

• Changes to the standard and approach to alternative transfer mechanisms. (Art 46).	

10. Given the uncertainty as to the point at which trading partners might make changes, we have set out 'medium', 'high', 'low' and 'high with EU adequacy loss' scenarios to illustrate impacts under a range of different combinations of responses:

    a. A **Medium** scenario which assumes that the UK, moving unilaterally, will become less restrictive with all priority countries as a result of these reforms but all else will stay the same.

    b. A **High** scenario which assumes that the countries that are within the UK's priority list for data bridge regulations will become less restrictive in response to the UK becoming less restrictive with them as a result of these reforms. This scenario assumes that countries with which the UK already has a data bridge will stay the same. This scenario is optimistic in that data bridge regulations are unilateral and reciprocation is not assumed. 1.20.2 is also switched off, where possible[302], as the two measures are modelled together. The need for private sector safeguards between the country and the UK is assumed to be overruled by having a data bridge.

    c. A **Low** scenario, where we assume the UK still becomes less restrictive with priority countries as in the medium scenario, but that the EU+ bloc becomes slightly more restrictive in response to the implementation of these reforms. This reflects the framework outlined in the summary that a decrease in requirements with 3rd countries might be accompanied with more friction in UK-EU trade.

    d. A **High with EU Adequacy Loss** scenario which assumes the same as the 'High' scenario but that the EU bloc also becomes slightly more restrictive in response to the wider set of reforms.

11. For the purposes of modelling responses, the countries considered are placed into three groups:

    - EU+EEA. These are countries the UK already has a data bridge with and they may impose additional restrictions with respect to the UK, in response to a deviation from UK GDPR.

    - 'Priority countries',[303] that the UK has identified as key countries for future partnerships. These countries may further liberalise with respect to the UK, in response to deviations from UK GDPR. This group comprises[304] Australia, Brazil, India, Indonesia, South Korea and the United States.

    - Other countries where a STRI parameter exists but are not priority countries or in the EU+. These are affected by the general equilibrium impacts but are not directly

[302] India and Indonesia have 1.20.2 ON in the do-minimum. All other priority countries have this measure off already.
[303] UK approach to international data transfers (2021), DCMS
[304] Dubai International Finance Centre, Colombia, Singapore and Kenya are also in the 'priority' group. However, owing to lack of STRI or trade data they have not been modelled.

affected by the policy changes. This group includes: Canada, China, Israel, Mexico and Malaysia amongst others.

Table 87: Summary table of all modelling scenarios

Scenarios	UK Policy	Changes to UK STRI	Partner Policy	Changes to Partner STRI
Baseline	As is	As is	As is	As is
High	UK becomes less restrictive with priority countries	1.20.3 OFF for priority countries	Priority countries become less restrictive	1.20.3 OFF and 1.20.2 OFF for Priority countries
High with EU adequacy loss			Same as above EU+countries becomes more restrictive	1.20.3 OFF and 1.20.2 OFF for Priority countries 1.20.3 ON for EU+
Medium			No changes	No changes
Low			EU+ countries becomes more restrictive All other countries remain the same	1.20.3 ON for EU+

Caveats

12. The policy changes have been made on the set of priority countries before final assessments and decisions have been made. For each individual country, a full technical assessment will be undertaken before a decision to establish a data bridge is made. Prioritising countries for assessment are not a guarantee to receiving a positive decision. Additional countries may be announced as being assessed in the future. The full group of non-priority countries represents 22% of UK services exports. Whilst it is unlikely that the UK will establish a data bridge with all of these countries, the benefits identified in this Annex will be underestimated at least to some degree, as more countries than the initial priority list are assessed and data bridges are established.

13. The high scenarios test full reciprocation from priority countries. Although establishing a data bridge is likely to increase the likelihood of a priority country reciprocating, it is not assumed. It is likely some level of reciprocation will occur but the benefits to trade in these scenarios may be overestimated.

14. The model covers only certain sectors.[305] As above, cross-sector effects are not captured. Similarly, the model captures a subset of countries although it captures about 76% of UK services trade and 2/3s of global services trade.

15. How a data bridge operates on a bilateral basis may mean the 1.20.3 measure and its assigned weight may not be specific enough.[306] Whilst the OECD assigns differential weights for each country, bilateral-specific STRIs are not used i.e. how a data bridge functionally works between two countries may be different for another. For example, sector-specific restrictions may still be in place or some compliance activities may still be required, for example with the United States, UK companies may need to verify that the business they are sending personal data to has signed up to a certification scheme. Similarly, risk aversion of businesses may mean even with regulations, alternative transfer mechanisms are still widely used as an additional form of protection when transferring data.

16. How data and trade interact is a nascent field. The understanding of how data as an input into production due to its intangible and non-rivalrous nature affects trade requires more research in the future.

17. DCMS will continue to develop its methodologies to better understand the relationships and drivers of data-dependent trade and work with X-HMG colleagues to develop methodologies.

Results

18. Below is a break-down of the results, which represent the medium-term impact on UK exports and imports from the first set of priority countries for a data bridge.[307] In reality, decisions will be made over several years.

19. For full detail of the underlying model, please refer to DIT's published Services Trade Modelling paper[308]. Results are presented on a country grouping level and for a subsection of sectors. It should be noted that the model does not account for cross-sectoral impacts and so results should be caveated that they do not cover whole-economy effects.

Table 88: Overall Results (£m), 2021 prices

	Medium	High	Low	High with EU Adequacy Loss
Total UK Exports	597.7	1062.3	-294.1	175.4
Total UK Imports	590.0	624.0	-339.0	-304.8

20. The overall results show an increase in both exports and imports in the medium and high scenarios. The size of the impact for exports and imports is broadly similar in the medium

[305] It does not cover Manufacturing, Maintenance and Repair, Intellectual Property, Personal, Cultural and Recreational and Government sectors. These omitted sectors represent about 12% of UK services exports.
[306] The effect of the STRI on trade may vary by country pair. Due to a lack of degrees of freedom, however, the model cannot estimate country- or pair-specific STRI coefficients. The estimated STRI parameter of interest represents the average effect of the STRI across countries.
[307] For this model medium-term means results post adjustment for third-party effects.
[308] DIT Services trade modelling working paper

scenario. Both exports and imports are estimated to fall by similar magnitudes in the low scenario. Reciprocation of a data bridge decision has a large impact on exports but not imports. The effect of reciprocation leads to a net-positive impact on exports in the “high with EU adequacy loss” scenario.

21. The results are further split out by sector and country grouping below.

Table 89: UK Exports Impact by Sector (£m), 2021 prices

	Medium	High	Low	High with EU Adequacy Loss
Transport	54.3	98.6	-92.8	-48.1
Construction	0.1	9.6	-4.5	5.1
Insurance	76.3	150.7	101.4	176.3
Financial Services	299.7	348.7	58.4	107.7
Telecoms, Computer, and Information	52.6	192.2	-386.3	-244.2
Other Business Services	114.6	261.1	7.1	154.3
Distribution	0.0	1.5	22.6	24.2
Total	**597.7**	**1062.3**	**-294.1**	**175.4**

22. For UK exports, the largest affected sectors are Financial Services and Other Business Services. At the aggregate, the medium scenario sees an increase of £597.7m compared to the baseline. Scenarios testing reciprocation by priority countries show an increase in the impact to £1,062.3m compared to the baseline.

23. Each of the medium and high scenarios have been tested for what happens when EU adequacy is lost as a result of the wider set of reforms. In the most pessimistic scenario, UK exports would fall by £294.1m relative to the baseline driven by the ‘Telecoms, Computer and Information’, ‘Transport’ and ‘Construction’ sectors. All other sectors still see an increase in exports. In the scenario with reciprocation but EU adequacy loss, the net impact is net-positive with an increase of £175.4m. ‘Telecoms, Computer, and Information’ and ‘Transport’ sectors still see a fall in exports in this scenario.

Table 90: UK Exports Impact by Country Grouping (£m), 2021 prices

	Medium	High	Low	High with EU Adequacy Loss

Priority	323.9	825.8	921.1	1427.9
EU+	207.5	178.4	-1450.3	-1479.4
Other	66.2	58.2	235.1	226.8
Total	**597.7**	**1062.3**	**-294.1**	**175.4**

24. The above results break-down the results by country grouping showing the changes in exports in each scenario. Across the scenarios, priority countries see an increase in exports. The increase in exports for the priority countries is higher following the loss of EU adequacy than the direct impact of awarding adequacy due to the general equilibrium effects. Exports to other countries also increase due to trade creation. The general equilibrium effects consider the relative size of the EU+ group and their trading relationships with the UK and all other countries. A proportion of the UK's exports to the EU+ are diverted to priority and other countries partly reduce the negative impacts of the loss of EU adequacy.

Table 91: UK Imports Impacts by Sector (£m), 2021 prices

	Medium	**High**	**Low**	**High with EU Adequacy Loss**
Transport	20.8	32.9	-68.8	-56.6
Construction	20.4	20.4	-74.8	-74.8
Insurance	8.3	9.1	-15.5	-14.7
Financial Services	87.8	91.2	1.6	4.9
Telecoms, Computer, and Information	197.8	199.8	24.0	26.1
Other Business Services	205.6	221.4	-81.9	-66.0
Distribution	49.3	49.3	-123.6	-123.6
Total	**590.0**	**624.0**	**-339.0**	**-304.8**

25. In the medium and high scenarios imports increase by £590.0m and £624.0m respectively relative to the baseline, with reciprocation having a limited effect on imports. Similarly, when testing the impact of the loss of EU adequacy leads to a decrease in UK imports £304.8m to £339.0m across the two scenarios compared to the baseline.

26. The largest affected sectors depend on the scenario. For the medium and high scenarios, 'Telecoms, Computer, and Information' and 'Other Business Services' are the largest affected sectors. In scenarios that account for EU adequacy loss, 'Distribution' is the most affected sector with 'Construction', 'Other Business Services' and 'Transport' all negatively impacted.

Table 92: UK Imports Impacts by Country Grouping (£m), 2021 prices

	Medium	High	Low	High with EU Adequacy Loss
Priority	727.7	743.0	451.7	467.1
EU+	-113.2	-97.0	-702.5	-686.2
Other	-24.5	-22.0	-88.2	-85.7
Total	**590.0**	**624.0**	**-339.0**	**-304.8**

27. When looking at the imports results by country grouping, the results show that in the medium and high scenarios imports increase relative to the baseline by £727.7m and £743.0m respectively for priority countries. In these scenarios, imports from the EU+ fall by £97.0m to £113.2m and in all other countries by £22.0m to £24.5m compared to the baseline. The result differs from the exports results where EU+ and other exports also increase in these scenarios.

28. In the EU Adequacy loss scenarios, priority country imports still increase by £451.7m to £467.1m but fall by about £300m compared to the scenarios without EU adequacy loss. EU+ imports fall by £686.2m to £702.5m and other countries imports fall by around £88.2m to £85.7m relative to the baseline.

29. Imports divert from EU+ and other countries even in positive scenarios. The additional restrictions placed by the EU+ in the EU adequacy loss scenarios further reduce imports in the EU+ and other groupings but also negatively impact the increase in imports for priority countries.

Sensitivity Testing

30. To account for uncertainty in the STRI parameter, including the specificity for each bilateral country and business' behavioural reaction to policy changes, the 80% confidence interval is used. Due to the sector-specific STRI parameters, the range of impact depends on the sector of interest.

31. For changes to UK exports, the results show a range of £228.8m to £907.8m in the medium and £439.9m to £1634.8m in the high scenarios respectively. When testing the impact of EU adequacy loss, the results show a range of -£218.5m to -£341.5m in the low and -£6.0m to £396.6m in the high with EU adequacy loss scenarios respectively.

32. For changes to UK imports, the results show a range of £249.3m to £967.9m in the medium and £263.7m to £1020.0m in the high scenarios respectively. When testing the impact of EU adequacy loss, the results show a range of -£137.4m to -£536.8m in the low and -£123.0m to -£484.1m in the high with EU adequacy loss scenarios respectively.

33. As with the central results, the results do not account for cross-sector impacts or the reallocation of factors of production.