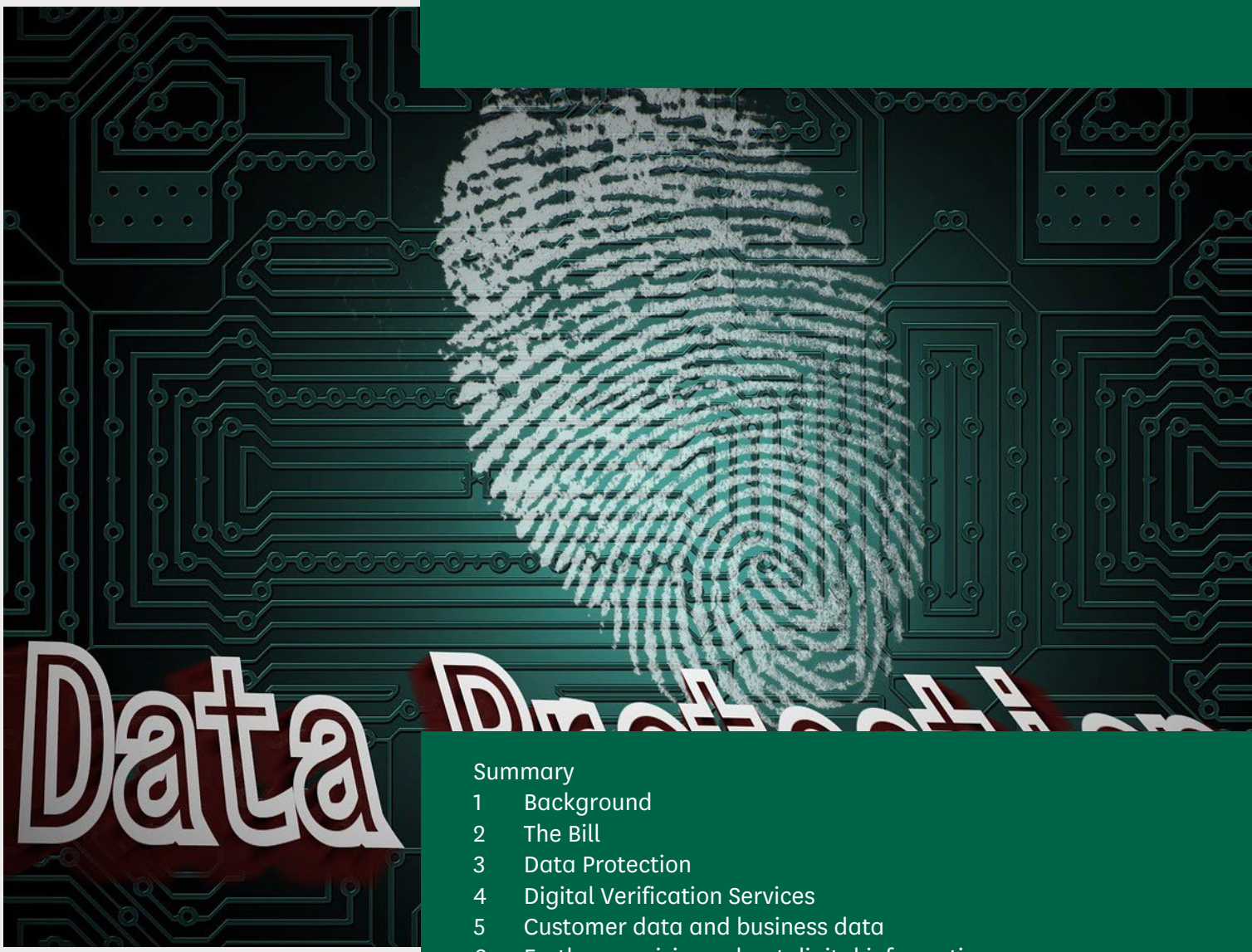
House of Commons Library

Research Briefing

By John Woodhouse

28 March 2023

Data Protection and Digital Information (No. 2) Bill



Summary

Contributing Authors
Adam Clark, Digital Verification Services;
Lorraine Conway, Privacy and electronic marketing;
Catherine Fairbairn, Register of births and deaths;
Neil Johnston, Direct marketing and democratic engagement;
Tom Powell, Health and social care

Image Credits
Data protection. Licenced under Creative Commons CC0. No copyright required.

Feedback
Every effort is made to ensure that the information contained in these publicly available briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Please note that authors are not always able to engage in discussions with members of the public who express opinions about the content of our research, although we will carefully consider and correct any factual errors.

You can read our feedback and complaints policy and our editorial policy at commonslibrary.parliament.uk. If you have general questions about the work of the House of Commons email hcenquiries@parliament.uk.

Contents

Summary

The Data Protection and Digital Information (No. 2) Bill [Bill 265 2022-23] was introduced in the House of Commons on 8 March 2023. Second reading is scheduled for 17 April 2023.

Much of the Bill is the same as the Data Protection and Digital Information Bill [Bill 143 2022-23] which was introduced in the Commons on 18 July 2022. The Bill was scheduled to have its second reading on 5 September 2022. A Library Briefing on the Bill (PDF) (31 August 2022) was published for the debate. However, in a Business Statement on 5 September 2022, the Government said that, following the election of Elizabeth Truss as Conservative Party leader, second reading would not take place. This was to allow Ministers to consider the Bill further. The Bill was withdrawn on 8 March 2023.

What would the Data Protection and Digital Information (No. 2) Bill do?

In a Written Ministerial Statement of 8 March 2023, Michelle Donelan, Secretary of State for Science, Innovation and Technology, said the new Bill followed a detailed codesign process with industry, business, privacy and consumer groups. The Bill would seize the post-Brexit opportunity to "create a new UK data rights regime tailor-made for our needs". It would reduce burdens on businesses and researchers and would boost the economy by £4.7 billion over the next decade. The Secretary of State explained that changes had been made to the original Bill that would:

- reduce compliance costs in the sector and reduce the amount of paperwork that organisations need to complete to demonstrate compliance.
- reduce burdens by enabling businesses to continue to use their existing cross-border transfer mechanisms if they are already compliant.
- give organisations greater confidence about the circumstances in which they can progress personal data without consent.
- increase public and business confidence in AI technologies.

The Bill would:

- establish a framework for the provision of digital verification services to enable digital identities to be used with the same confidence as paper documents.
- increase fines for nuisance calls and texts under the Privacy and Electronic Communications Regulations (PECR).

- update the PECR to cut down on 'user consent' pop-ups and banners.
- allow for the sharing of customer data, through smart data schemes, to provide services such as personalised market comparisons and account management.
- reform the way births and deaths are registered in England and Wales, enabling the move from a paper-based system to registration in an electronic register.
- facilitate the flow and use of personal data for law enforcement and national security purposes.
- create a clearer legal basis for political parties and elected representatives to process personal data for the purposes of democratic engagement.

The governance structure and powers of the Information Commissioner's Office (ICO, the data protection regulator) would also be reformed and transferred to a new body, the Information Commission.

Where would the Bill take effect?

Data protection is a reserved matter. The Bill's changes to the Data Protection Act 2018 and the UK General Data Protection Regulation would extend to the whole of the UK, apart from one provision relating to the Information Commission's seal, which does not extend to Scotland.

Other provisions in the Bill would require legislative consent motions from the devolved administrations – eg in relation to smart data. Annex A to the Explanatory Notes (PDF) gives detailed information on the Bill's territorial extent and application.

Reaction to the Bill

John Edwards, the Information Commissioner, has welcomed the re-introduction of the Bill and "its ambition to enable organisations to grow and innovate whilst maintaining high standards of data protection rights".

However, the Open Rights Group, an organisation campaigning on surveillance, privacy, and free speech, has claimed that the Bill would, among other things, weaken data subjects' rights, water down accountability requirements, and reduce the independence of the ICO.

Big Brother Watch, a civil liberties campaign group, claims the Bill would "tear up" privacy rights protecting the public from automated-decision making in high-risk areas.

TechUK, the trade association for technology, believes the Bill "would help boost innovation while upholding privacy rights and EU adequacy".

The Investing and Savings Alliance, a not-for-profit membership organisation, has welcomed the Bill's provisions on smart data schemes.

Some commentators have noted that the Bill might put at risk the European Union's June 2021 adequacy decisions on the UK. These allow personal data to flow freely between the EU/EEA and the UK.

More on the Bill

The Government has published the following material on the Bill:

- Explanatory Notes (PDF).
- Impact Assessments.
- Memorandum from the Department for Science, Innovation and Technology to the Delegated Powers and Regulatory Reform Committee (PDF).
- European Convention on Human Rights Memorandum (PDF).
- British Businesses to Save Billions Under New UK Version of GDPR, Department for Science, Innovation and Technology press release, 8 March 2023

1 Background

1.1 The UK's data protection framework

Part 2 of the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) govern the general processing of personal data in the UK. The UK GDPR is the retained version of the EU General Data Protection Regulation (PDF)[1] which came into force on 25 May 2018.[2]

There are separate regimes for law enforcement processing (Part 3 of the 2018 Act) and for intelligence services processing (Part 4 of the 2018 Act).

The Information Commissioner's Office (ICO) oversees and enforces data protection law in the UK. Its functions and powers are set out in Parts 5 and 6 of the 2018 Act.

Further background on the bill that became the 2018 Act is available in the Library Briefings:

- Data Protection Bill [HL] 2017-19 (PDF) (1 March 2018).
- Data Protection Bill [HL] 2017-19: Committee Stage Report (PDF) (13 April 2018).

General processing of personal data

Part 2 of the 2018 Act supplements the UK GDPR and applies to the general processing of personal data. It sets out the responsibilities of:

- data controllers - the persons or bodies that determine the purposes and means of processing of personal data; and
- data processors - those who process personal data on behalf of a controller.

The legislation also details the rights of "data subjects" (the people whose data is being processed). These include a right of access, a right to get data

1 Regulation 2016/679 EU (accessed 13 March 2023)

2 The EU GDPR was incorporated into UK law at the end of the EU Transition Period under section 3 of the European Union (Withdrawal) Act 2018 and modified by the Data Protection, Privacy and Electronic Communication (Amendments etc) (EU Exit) Regulations 2019 under the power in section 8 EUWA 2018 to create the UK GDPR.

corrected, and a right to object to how personal data is being used. The ICO website gives further detail on the rights of data subjects.[3]

Under the UK GDPR, personal data can only be processed if there is a lawful basis for doing so. There are six bases:

- Consent – an individual has given clear consent for their personal data to be processed for a specific purpose.
- Contract - processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering a contract.
- Legal obligation – processing is necessary for compliance with a legal obligation to which a data controller is subject.
- Vital interests - processing is necessary to protect someone's life.
- Public task – processing is necessary for the performance of a task carried out in the public interest or for official functions and the task or function has a clear basis in law.
- Legitimate interests - the processing is necessary for a data controller's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Personal data must be processed in accordance with seven principles, including purpose limitation, data minimisation, and accuracy.

There are additional protections for special category data – personal data that reveals, for example, a person's racial origin, political opinions, health data, or sexual orientation. To process special category data, there must be a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. One of the conditions is explicit consent. There are nine others including health/social care and substantial public interest. The latter two must have a basis in law.

Further detail on the above is available in ICO guidance on the UK GDPR (PDF)(October 2022).

Law enforcement processing

Part 3 of the 2018 Act transposed the provisions of the Law Enforcement Directive[4] into UK law. It sets out a separate regime for authorities with law enforcement functions when they are processing personal data for law

[3] ICO website, For the public (accessed 13 March 2023)

[4] Directive 2016/680/EU (accessed 13 March 2023)

enforcement purposes. Further detail is available in ICO guidance on law enforcement processing (PDF)(October 2022).

Intelligence services processing

Part 4 of the 2018 Act sets out a separate regime for the processing of personal data by the intelligence services. Further detail is available in ICO guidance on intelligence services processing (PDF)(October 2022).

1.2 National Data Strategy (September 2020)

In September 2020, the then Department for Digital, Culture, Media and Sport (DCMS)[5] published a National Data Strategy.[6] Oliver Dowden, then Secretary of State, said the Strategy aimed to place the UK "at the heart of the data revolution", would "harness the power of digital technology to drive our recovery from coronavirus" and:

- boost growth and productivity.
- create new businesses and jobs.
- improve public services.
- position the UK at the forefront of the next wave of innovation.[7]

Oliver Dowden explained that the Strategy set out the Government's "ambitions and global-facing vision for maximising the benefits of the effective and trusted use of data". The Strategy proposed five "priority missions":

1. unlocking the value of data across the economy.
2. securing a pro-growth and trusted data regime.
3. transforming government's use of data to drive efficiency and improve public services.
4. ensuring the security and resilience of our data infrastructure.
5. championing the international flow of data.[8]

There was a twelve-week consultation on the Strategy. This sought views on, among other things:

---

5 Responsibility for data protection law has now passed from DCMS to the Department for Science, Innovation & Technology (DSIT)

6 DCMS, National Data Strategy [online], updated 9 December 2020 (accessed 13 March 2023)

7 DCMS, National Data Strategy, Written Ministerial Statement (HCWS442), 9 September 2020

8 As above

- how the UK's data protection framework could remain fit for purpose.
- how the UK could improve on international transfer mechanisms, while ensuring that the personal data of UK citizens was appropriately safeguarded.

Government response to the consultation (May 2021)

The Government published its response to the consultation in May 2021.[9] This noted that respondents "generally welcomed" the Government framing data as a strategic asset to be used for economic and social benefit. They also "broadly agreed" that data use should be "embraced as an opportunity to drive productivity and innovation across the economy, fuel scientific research, revolutionise the public sector and create a fairer and more prosperous society for all".[10] However, respondents also drew attention to challenges around the incorrect or inappropriate use of data, digital inclusion and connectivity, and the need for all citizens to have the appropriate skills to operate and thrive in a data-driven economy.[11]

On "Mission 2" of the Strategy - securing a pro-growth and trusted data regime – the "vast majority" of respondents supported a regime that "maintains high data protection standards and encourages data sharing, without creating unnecessary barriers to responsible data use or sharing".[12]

Achieving data adequacy was consistently referenced as being of high importance to UK organisations. Data adequacy decisions, discussed in section 3.7 of this briefing, enable personal data to be freely transferred between the UK and other countries. In June 2021, the European Commission adopted decisions on the UK's adequacy under the EU GDPR and Law Enforcement Directive so that most personal data could flow from the EU and the EEA.[13]

Respondents to the consultation also stressed the importance of ensuring that the UK's data protection framework could easily adapt to technological advances and changes in the data landscape. Two potential areas of risk were identified:

- businesses had invested heavily in the UK's data protection regime and any substantive reform would incur costs.

---

9 DCMS, Government response to the consultation on the National Data Strategy [online], 18 May 2021 (accessed 13 March 2023); DCMS, Government response to the public consultation on the National Data Strategy and the Data Sharing Code of Practice, Written Ministerial Statement (HCWS37), 18 May 2021

10 DCMS, Government response to the consultation on the National Data Strategy [online], 18 May 2021

11 As above, Executive summary

12 DCMS, Government response to the consultation on the National Data Strategy [online], 18 May 2021, Annex B

13 EU adopts 'adequacy' decisions allowing data to continue flowing freely to the UK, DCMS press release [online], 28 June 2021 (accessed 13 March 2023)

- data reform could risk weakening UK data protection standards, at the expense of citizens' rights. These respondents tended to call for more proactive enforcement of the current framework by the ICO.[14]

On "Mission 5" of the Strategy – championing the international flow of data – "many respondents" agreed that the UK should work internationally to reduce unnecessary barriers to cross-border data flows. However, many also argued that the UK should seek to embody the global 'gold standard' for data protection. There was support for maintaining EU data adequacy as an "essential priority". A "significant number" of respondents also recommended that the UK explore alternative transfer mechanisms to adequacy arrangements, such as standard contractual clauses (SCCS) and binding corporate rules (BCRs).[15]

Annex B to the Government's response set out a full summary of findings from the consultation.

1.3 DCMS consultation on a "new direction for data" (September 2021)

On 10 September 2021, the DCMS launched a consultation on reforming the UK's data protection regime.[16] In a Written Ministerial Statement, Sir John Whittingdale, then Minister of State for Media and Data, explained that the Government had the "freedom to create a bold new data regime outside of the EU".[17] He referred to "Mission 2" of the National Data Strategy and said the Government wanted to create a "more pro-growth and trusted regime for personal data protection".

Sir John Whittingdale noted that any data protection regime required "active interpretation and pragmatic application to new and emerging technologies". However, over three years after its introduction in 2018, there was "persistent uncertainty" about how to apply the current framework, with aspects of it being "unnecessarily complex or vague". This risked "barriers to responsible data access, use and sharing". According to the Minister, the reforms outlined in the consultation would:

- Strengthen our position as a science superpower, by simplifying data use by researchers and developers of AI and other cutting edge technologies.

- Build on the unprecedented and life-saving collaboration between the public and private sectors in using data responsibly to tackle the Covid-19 pandemic.

14 DCMS, Government response to the consultation on the National Data Strategy [online], 18 May 2021, Annex B

15 As above

16 DCMS, Data: a new direction (PDF), 10 September 2021 (accessed 13 March 2023)

17 DCMS, Data: a new direction, Written Ministerial Statement (HCWS276), 10 September 2021

- Secure the UK's status as a global hub for the free and responsible flow of personal data, complementing our ambitious agenda for new trade deals and data adequacy agreements with some of the world's fastest growing economies.

- Reinforce the responsibility of businesses to keep personal information safe and encourage investment in effective compliance activities that reflect how they operate and their users' expectations.

- Ensure that the Information Commissioner's Office remains a world-leading regulator, empowered to ensure people can use data responsibly to achieve economic and social goals.

The UK would "maintain its high standards of data protection, while taking a pragmatic and risk-based approach". Sir John Whittingdale said the proposed reforms would have "clear benefits" for citizens and businesses including:

- introducing more flexibility in how organisations embed privacy management in their processes alongside greater transparency about how their users' data is protected and clearer procedures for handling complaints.

- taking action to tackle nuisance calls which can disproportionately affect the most vulnerable.

- exploring whether the ICO should have powers to impose higher fines and carry out audits of companies which broke direct marketing rules.

- clarifying how businesses could innovate responsibly with personal data.

- requiring the ICO to recognise and account for how its regulatory activity could impact on competition and innovation.[18]

An Analysis of expected impact (PDF) was also published.[19] The consultation closed on 19 November 2021.

DCMS response to the consultation (June 2022)

The DCMS published its response to the consultation on 17 June 2022.[20] Annex A to the response lists the consultation's proposals and the Government's next steps on each. Annex B lists the organisations that responded to the consultation. Julia Lopez, then Minister for Media, Data and Digital Infrastructure, summarised the Government's response in a Written Ministerial Statement of 20 June 2022. This explained that the Government

18 DCMS, Data: a new direction, Written Ministerial Statement (HCWS276), 10 September 2021

19 DCMS, Data: a new direction - analysis of expected impact (PDF)[online], Undated (September 2021?) (accessed 13 March 2023)

20 DCMS, Data: a new direction - government response to consultation [online], 17 June 2022 (accessed 13 March 2023)

would "create a new, flexible, independent regime under which the value of data can truly be maximised".[21] This would involve, among other things:

- clarifying data protection rules regarding research so that scientists would have the confidence to use data responsibly and effectively, leading to "greater data-driven innovations".
- removing some of the "most prescriptive but unnecessary rules" in the UK GDPR to reduce burdens on businesses.
- removing "inappropriate barriers" to the flow of UK personal data overseas to support trade and scientific collaboration as well as national security and law enforcement cooperation.
- better enforcement of data protection and privacy breaches.
- taking firmer action against nuisance callers and making it easier to stop this behaviour.
- making it easier for public bodies to share data, making public healthcare, law enforcement and Government services more effective.
- modernising the governance framework of the ICO and making it more accountable to the public and Parliament.
- creating a clearer legal basis for political parties and elected representatives to process personal data for the purposes of democratic engagement.[22]

21 DCMS, "Data: a new direction" consultation: Government Response, HCWS120, 20 June 2022

22 As above

2 The Bill

The Data Protection and Digital Information (No. 2) Bill [Bill 265 2022-23] was introduced in the House of Commons on 8 March 2023.

The following supporting material is available:

- Explanatory Notes (PDF).
- Impact Assessments.
- Memorandum from the Department for Science, Innovation and Technology to the Delegated Powers and Regulatory Reform Committee (PDF).
- European Convention on Human Rights Memorandum (PDF).
- Data Protection and Digital Information (No. 2) Bill, House of Commons Written Ministerial Statement (HCWS617), 8 March 2023
- British Businesses to Save Billions Under New UK Version of GDPR, Department for Science, Innovation and Technology press release, 8 March 2023

Much of the Bill is the same as the Data Protection and Digital Information Bill [Bill 143 2022-23] which was introduced in the Commons on 18 July 2022. The Bill was scheduled to have its second reading on 5 September 2022. A Library Briefing on the Bill (PDF) (31 August 2022) was published for the debate. However, in a Business Statement on 5 September 2022, the Government said that, following the election of Elizabeth Truss as Conservative Party leader, second reading would not take place. This was to allow Ministers to consider the Bill further. The Bill was withdrawn on 8 March 2023.

What are the policy objectives of the Data Protection and Digital Information (No. 2) Bill?

An Impact Assessment on the Bill has not yet been published. However, the Impact Assessment (IA) (PDF) on the withdrawn Bill claimed that data was a "strategic asset and its responsible use should be seen as a huge opportunity to embrace".[23] The IA said the complexity of the current data protection framework meant that firms, public sector organisations and consumers

[23] Impact Assessment on the Data Protection and Digital Information Bill (PDF)[online], July 2022, p1. The July 2022 IA has been republished to accompany the No. 2 Bill until a fully revised IA is available (accessed 13 March 2023)

could not take full advantage of the benefits that could be available to them through the effective use of data and data sharing. The Government would therefore intervene "to allow for the realisation of all benefits derived from more effective data use". The IA said the Bill's provisions would deliver a data protection regime that would:

- 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.
- make it easier for public bodies to share vital data, improving public service delivery.[24]

What would the Bill do?

In a Written Ministerial Statement of 8 March 2023, Michelle Donelan, Secretary of State for Science, Innovation and Technology, said the new Bill followed a detailed codesign process with industry, business, privacy and consumer groups.[25] The Bill would seize the post-Brexit opportunity to "create a new UK data rights regime tailor-made for our needs". It would reduce burdens on businesses and researchers and would boost the economy by £4.7 billion over the next decade. The Bill would:

- establish a framework for the provision of digital verification services to enable digital identities to be used with the same confidence as paper documents.
- increase fines for nuisance calls and texts under the Privacy and Electronic Communications Regulations (PECR).
- update the PECR to cut down on 'user consent' pop-ups and banners.
- allow for the sharing of customer data, through smart data schemes, to provide services such as personalised market comparisons and account management.

[24] As above, p1

[25] Data Protection and Digital Information (No. 2) Bill, House of Commons Written Ministerial Statement (HCWS617), 8 March 2023

- reform the way births and deaths are registered in England and Wales, enabling the move from a paper-based system to registration in an electronic register.
- facilitate the flow and use of personal data for law enforcement and national security purposes.
- create a clearer legal basis for political parties and elected representatives to process personal data for the purposes of democratic engagement.

The governance structure and powers of the Information Commissioner's Office (ICO, the data protection regulator) would also be reformed and transferred to a new body, the Information Commission.

How does the Bill differ from the withdrawn Bill?

In the Written Ministerial Statement of 8 March 2023, Michelle Donelan explained that changes had been made to the original Bill that would:

- reduce compliance costs in the sector and reduce the amount of paperwork that organisations need to complete to demonstrate compliance.
- reduce burdens by enabling businesses to continue to use their existing cross-border transfer mechanisms if they are already compliant.
- give organisations greater confidence about the circumstances in which they can progress personal data without consent.
- increase public and business confidence in AI technologies.

Structure of the Bill

The Bill has six parts and thirteen schedules:

- **Part 1** would make changes to the UK's data protection regime.
- **Part 2** would regulate the provision of digital verification services through the creation of a trust framework, a register of providers, an information sharing gateway, and a trust mark.
- **Part 3** would allow data sharing to support the delivery of public services which benefit businesses or "undertakings" (eg those carrying on trade whether for profit or not for profit and bodies established for charitable purposes).
- **Part 4** would, among other things, increase fines for nuisance calls and texts under the PECR. It would introduce a new opt-out model for cookies to reduce the need for users to click through consent banners on every website they visit. Part 4 would also:

- update the way births and deaths are registered, moving from a paper-based system to an electronic register used by officials.
- make it easier for elected representatives to process general personal data where necessary for the purposes of democratic engagement activities.

Part 5 would abolish the Information Commissioner's Office and transfer its functions to an Information Commission. Part 5 would also make changes to the regulation and oversight of biometrics, CCTV, and the National DNA Database.

Part 6 contains final and procedural provisions relating to consequential amendments, powers for making regulations, interpretation, and the Bill's commencement.

Territorial extent

Data protection is a reserved matter. The Bill's reforms to the Data Protection Act 2018 and the UK GDPR would extend to the whole of the UK, apart from one provision relating to the Information Commission's seal, which does not extend to Scotland.

Other provisions in the Bill would require legislative consent motions from the devolved administrations – eg in relation to smart data. Annex A to the Explanatory Notes gives detailed information on the Bill's territorial extent and application.[26]

[26] DSIT, Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF)[online], March 2023, Annex A (accessed 13 March 2023)

3 Data Protection

Part 1 of the Bill would make changes to the Data Protection Act 2018 (the 2018 Act) and the UK General Data Protection Regulation (UK GDPR). The IA on the withdrawn Bill said this was necessary because the current regime could be "complex to interpret and apply, especially for small and medium businesses". This could lead to uncertainty and hinder compliance.[27] Much of Part 1 is highly technical. This section gives an overview of some of its main elements, together with comment from stakeholders. For a clause-by-clause overview, the reader should consult the Explanatory Notes to the Bill.[28]

3.1 Amended definition of personal data

Background

Section 3(2) of the 2018 Act defines personal data as "any information relating to an identified or identifiable living individual". The 2018 Act does not apply to non-personal or anonymous data. Under section(3(3), an "identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to:

> (a)an identifier such as a name, an identification number, location data or an online identifier, or
>
> (b)one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

The Bill

Clause 1 of the Bill would amend the definition of personal data to provide greater clarity about which type of data would be in scope of the legislation.[29] **Clause 1(1)** would amend section 3(3) of the 2018 Act to confirm that a living individual may be identifiable either directly or indirectly.

Clause 1(2) would add a new section 3A to the 2018 Act. New section 3A (1)-(3) sets out two cases in which information being processed by a controller or processor would count as information relating to an identifiable individual:

27 Impact Assessment on the Data Protection and Digital Information Bill (PDF)[online], p10
28 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF)[online]
29 As above, para 101

1. where the controller or processor can themselves identify a living individual from the information they are processing by reasonable means.

2. where the controller or processor knows, or ought reasonably to know, that another person is likely to obtain the information because of the processing and could identify a living individual by reasonable means.

New section 3A (4) is new to the Bill. It would clarify that "obtaining information as a result of the processing" - as referenced in subsection 3A(3)(a) – would also include information obtained because of inaction by the controller or processor (eg because of their failure to put in place appropriate measures to prevent, or reduce the risk of, hacking).[30]

Under new section 3A (5) and (6), "by reasonable means" would include any means that a person would be likely to use, taking account of, among other things:

- the time, effort, and cost to identify an individual from the information.

- the technology and other resources available.

3.2 Legitimate interests

Background

Under the UK GDPR, processing for "legitimate interests" is one of the six lawful bases for processing personal data. It is more flexible than the other bases and can, in principle, apply to any type of processing for any reasonable purpose.[31] When relying on legitimate interests as a lawful basis, organisations must carry out a "balancing test" to show that the processing is necessary and to document how their interests outweigh the rights of data subjects.[32] In its September 2021 consultation on data reform, the DCMS said this balancing test could cause uncertainly for organisations who viewed it as more complicated and risky than the other lawful bases.[33]

The DCMS' June 2022 response to the consultation said it would create a limited number of carefully defined processing activities for which organisations could use personal data without applying the balancing test.[34]

30 As above, para 105
31 ICO, What is the 'legitimate interests' basis? [online] (accessed 13 March 2023)
32 As above
33 DCMS, Data: a new direction (PDF) [online], 10 September 2021, para 58
34 DCMS, Data: a new direction - government response to consultation [online], 17 June 2022

Further detail on legitimate interests and the balancing test is available in ICO guidance.

The Bill

Clause 5(2)(b) would create a new lawful ground for processing personal data by inserting new Article 6(1)(ea) into the UK GDPR. This would provide that processing would be lawful where it was necessary for a recognised legitimate interest.

Clause 5(4) would insert new paragraphs into Article 6 of the UK GDPR. New Article 6(5) would define processing necessary for a recognised legitimate interest for the purposes of new Article 6(1)(ea) as processing that met a condition in new Annex 1 to the UK GDPR.[35] Under new Articles 6(6) to (8), the Secretary of State could make regulations to amend the recognised legitimate interest activities in Annex 1. Before laying regulations, the Secretary of State would need to consider the effects of any changes on the interests and fundamental rights and freedoms of data subjects, particularly children. The regulations would be subject to the affirmative procedure.

New Article 6(9) is new to the Bill. It gives illustrative non-exhaustive examples of activities that could constitute legitimate interests for the purposes of Article 6(1)(f) of the UK GDPR:

> (a) processing that is necessary for the purposes of direct marketing,
>
> (b) intra-group transmission of personal data (whether relating to clients, employees or other individuals) where that is necessary for internal administrative purposes, and
>
> (c) processing that is necessary for the purposes of ensuring the security of network and information systems.

The processing of personal data for these activities would have to be necessary and the data controller would be required to make sure that its interests in processing the data without consent were not outweighed by the individual's rights and interests.[36]

The recognised legitimate interests set out in New Annex 1 to the UK GDPR would include, among other things, processing for the purposes of:

- safeguarding national security, protecting public security or for defence purposes.
- responding to an emergency as defined in the Civil Contingencies Act 2004.

35 Inserted by clause 5(7) and Schedule 1

36 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF)[online], para 129

- detecting, investigating or preventing crime or apprehending or prosecuting offenders.
- safeguarding a child or vulnerable adult who is over 18 and considered to be at risk.
- democratic engagement. This relates to data subjects aged 14 years, reflecting the variations in voting age where, in Scotland (for example), a person can register to vote at the age of 14 as an attainer.

Comment

The Open Rights Group has criticised the creation of additional legitimate grounds for processing personal data and new exemptions from the purpose limitation principle. The Group said there would be no meaningful parliamentary scrutiny in this area and "little regard" for the impact on people's rights.[37]

3.3 Subject access requests

Background

Article 15 of the UK GDPR gives data subjects a "right of access" – also known as subject access - to find out:

- what personal information an organisation holds on them.
- how they are using it.
- who they are sharing it with.
- where they got the data from.

An organisation can refuse to comply with a request if they consider it "manifestly unfounded or excessive". These terms are not defined, but the ICO has said that a request can be considered manifestly unfounded or excessive if:

- it has been made with no real purpose except to cause an organisation harassment or disruption.

[37] The Data Discrimination Bill attacks our data protection rights, Open Rights Group blog, 7 March 2023 (accessed 13 March 2023). The blog includes a link to an open letter (PDF) to the Secretary of State for Science, Innovation and Technology.

- the person making the request has no genuine intention of accessing their information (eg they may offer to withdraw their request in return for some kind of benefit, such as a payment from the organisation).

- it overlaps with a similar request the organisation is still addressing.[38]

In most circumstances, there is no charge for a request (under the Data Protection Act 1998, now repealed, there was a £10 fee). However, an organisation can charge a "reasonable fee" to cover their administrative costs if they consider a request to be manifestly unfounded or excessive.

Subject access requests must normally be responded to within one month, with the possibility of a two-month extension.

The ICO website gives further detail on what the right means for data subjects. There is also ICO guidance on what organisations must do to comply with the right.

In its September 2021 consultation on data reform, the DCMS said some organisations found processing subject access requests time-consuming, taking up significant levels of resource.[39] In addition, some organisations believed the threshold of "manifestly unfounded" made it difficult for them to "navigate" instances in which it would be appropriate to enquire about the purpose of the request, or to provide sufficient grounds for a refusal to comply with a request.[40]

The DCMS' June 2022 response to the consultation said it would change the threshold for refusing or charging a reasonable fee for a subject access request from "manifestly unfounded or excessive" to "vexatious or excessive", to bring it in line with the grounds for refusing a freedom of information (FOI) request.[41]

The Bill

Clause 7(3) would insert new Article 12A into the UK GDPR. This would amend the threshold for charging a reasonable fee or refusing a subject access request from "manifestly unfounded or excessive" to "vexatious or excessive". The new threshold would apply to all requests under Articles 15 to 22 and 34 of the UK GDPR.

Data controllers would be able to charge a reasonable fee for or refuse requests that they considered "vexatious", as well as "excessive". The

38 ICO website, What to expect after making a subject access request (accessed 13 March 2023)

39 DCMS, Data: a new direction (PDF) [online], 10 September 2021, para 186; See also DCMS, Data: a new direction - government response to consultation [online], 17 June 2022, chapter 2.3

40 DCMS, Data: a new direction (PDF) [online], 10 September 2021, para 186; See also DCMS, Data: a new direction - government response to consultation [online], 17 June 2022, chapter 2.3

41 DCMS, Data: a new direction - government response to consultation [online], 17 June 2022, chapter 2.3. For an overview of freedom of information law, see the Library Briefing, Freedom of information requests (PDF) (accessed 13 March 2023)

Explanatory Notes state the revised threshold would capture a clearer set of requests which a controller could charge a reasonable fee for or refuse to act on. Where a controller charges for a request, section 12 of the 2018 Act allows the Secretary of State, through secondary legislation, to place limits on the fees.[42]

In determining whether a request was vexatious or excessive, the following would have to be considered:

- the nature of the request.
- the relationship between the data subject and the controller.
- the resources available to the controller.
- the extent to which the request repeats a previous request made by the data subject to the controller.
- how long ago any previous request was made.
- whether the request overlaps with other requests made by the data subject to the controller.

Examples of requests that could be considered vexatious could include requests that were:

- intended to cause distress.
- not made in good faith.
- an abuse of process.

Clause 8(3) would amend references to time periods across the legislation on the right of access to refer to the "applicable time period" and sets out what the period would be in different circumstances. In general, subject access requests would have to be replied to within one month of being received. The provision for a controller to extend the standard response period by a further two months would be retained – ie where the nature of a request was complex, or the process an organisation had to follow to respond was complex.

Comment

The Open Rights Group has criticised the "lowering [of] the threshold for organisations to refuse a subject access request".[43]

---

42 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 146

43 The Data Discrimination Bill attacks our data protection rights, Open Rights Group blog, 7 March 2023 (accessed 13 March 2023).

In a Law Gazette article on the withdrawn Bill, Ariane Adam and Tatiana Kazim of the Public Law Project also claimed the Bill would make it more difficult for people to access their personal data. They argued that bringing the grounds for refusing subject access requests in line with those for refusing FOI requests involved a "false and meaningless" comparison:

> ...This reasoning ignores the unique position of data subjects. Anyone can make a request under the Freedom of Information regime. But subject access requests are different. They are requests people make in relation to their own personal data. The Freedom of Information regime in this context is a false and meaningless comparison, and the effect will be to restrict individuals' data rights.[44]

3.4 Automated decision-making

Background

In its September 2021 consultation on data reform, the DCMS noted that, when used responsibly, data-driven artificial intelligence (AI) systems had the potential to bring "incredible benefits to our lives".[45] The consultation focused on the interplay of AI technologies with the UK's data protection regime. It explored how reforms could help organisations build or deploy AI systems responsibly, and to innovate with care, while ensuring that risks were managed, and data subjects' rights respected.[46]

Article 22 of the UK GDPR provides safeguards around the use of automated individual decision-making. The consultation considered Article 22 of the UK GDPR (Automated individual decision-making) in the context of AI. It sought to explore whether there was scope for providing more certainty on how and when the Article's safeguards would apply in practice.[47]

Under Article 22, organisations cannot make decisions based solely on automated processing if the decision affects the legal rights (or other equally important matters) of data subjects unless the decision is:

- necessary for the purposes of a contract between the data subject and an organisation.
- authorised by law eg to prevent fraud or tax evasion.
- based on the data subject's explicit consent.[48]

---

44 Adam A and Kazim T, Data: the wrong direction, Law Gazette [online], 23 June 2022 (accessed 13 March 2023)

45 DCMS, Data: a new direction (PDF) [online], 10 September 2021, para 63

46 As above, section 1.5

47 As above, para 97

48 ICO website, Your rights relating to decisions being made about you without human involvement (accessed 13 March 2023)

Article 22 gives data subjects the right:

- not to be subject to a decision that is based solely on automated processing if the decision affected their legal rights or other equally important matters eg automatic refusal of an online credit application, and e-recruiting practices without human intervention.
- to understand the reasons behind decisions made about them by automated processing and the possible consequences of the decisions.
- to object to profiling in certain situations, including for direct marketing.[49]

Further information on Article 22 is available in ICO guidance.[50]

In its June 2022 response to the consultation , the DCMS said it was considering how to amend Article 22 to clarify the circumstances in which it would apply. It wanted to align proposals in this area with a broader approach to governing AI-powered automated decision-making that would be set out in a white paper on AI governance. The Government wanted its reforms to cast Article 22 as a right to specific safeguards, rather than as a general prohibition on solely automated decision-making. The reforms would enable the deployment of AI-powered automated decision-making, providing scope for innovation with appropriate safeguards in place.[51]

The Bill

Clause 11 would substitute Article 22 of the UK GDPR with new Articles 22A-D so that automated decision-making would not be restricted to the three circumstances as at present.

A decision would be based solely on automated processing if there was "no meaningful human involvement in the taking of the decision".[52] A decision would be a "significant decision" in relation to a data subject if it:

- produced a legal effect for the data subject, or
- had similarly significant effect for the data subject.[53]

Article 22A(2) is new to the Bill. This would require controllers to consider, among other things, the extent to which a decision had been taken based on

49 As above

50 ICO, Rights related to automated decision making including profiling [online] (accessed 13 March 2023)

51 DCMS, Data: a new direction - government response to consultation [online], 17 June 2022, chapter 1.5

52 Article 22A(1)(a)

53 Article 22A(1)(b)(i) and (ii)

profiling when establishing whether or not human involvement had been meaningful.[54]

A significant decision involving special category personal data could not be taken based solely on automated processing unless one of two conditions was met:

1. the data subject had given explicit consent.
2. the decision was required or authorised by law. The decision would also have to be in the substantial public interest.[55]

Safeguards for when a significant decision had been taken through solely automated processing would include:

- notifying the data subject after such a decision had been taken.
- enabling the data subject to make representations about the decision.
- enabling the data subject to obtain human intervention on the part of the controller in relation to such a decision.
- enabling the data subject to contest such a decision.[56]

The Secretary of State would have the power, through regulations, to amend what would constitute a significant decision that produced an effect on a data subject that was similarly significant to a legal one.[57] The Explanatory Notes state this would ensure the scope of Article 22A could be amended to, for example, keep pace with the rapid advancement and adoption of technologies related to automated decision-making, as well as changing societal expectations of what constituted a significant decision in a privacy context.[58]

The Secretary of State would also be able, through regulations, to amend the safeguards for decisions taken through solely automated processing.[59] The regulations would be subject to the affirmative procedure.

Clause 11(3) would amend equivalent provisions on automated decision making in Part 3 (law enforcement processing) of the 2018 Act.

54 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 174
55 Article 22B(1), (2), and (3)
56 Article 22C(1) and (2)
57 Article D(1) and (2)
58 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 178
59 Article 22D(3) and (4)

Comment

When discussing the withdrawn Bill, TechUK, the trade association for technology, supported the Government's decision to amend Article 22 in ways which, it claims, would retain the Article's core principles:

> This will empower organisations to implement automated decision-making in more low-risk scenarios such as personalising services for a user, while setting clear safeguards for decisions with legal or similarly significant effects, such as mortgage approvals. In such cases, individuals will have the ability to contest and seek human intervention on these decisions. This data right will be crucial in the context of AI-driven decision-making, where individuals must be able to alert businesses to any possible biases in their systems.[60]

However, Ariane Adam and Tatiana Kazim of the Public Law Project have worried that Article 22 would be "water[ed] down".[61]

3.5 Scientific research

Background

Consultation on data reform

As explained in the DCMS' September 2021 consultation on data reform, the UK GDPR provides specific allowances for processing personal data for research purposes (ie archiving purposes in the public interest, scientific or historical research and statistical purposes). These are designed to make it easier for researchers to:

> a. Re-use personal datasets for different research projects, subject to safeguards such as techniques that make it less easy to identify individuals from data sets (generically known as pseudonymisation techniques)
>
> b. Retain personal datasets, and maintain their integrity and utility.[62]

In the context of research, the UK GDPR and the 2018 Act provide additional safeguards for data subjects' rights. For example:

> a. Article 89(1) UK GDPR, which provides that processing for research purposes shall be subject to appropriate safeguards, including technological and organisational techniques which may include pseudonymisation

60 Dhiman D et al, One final push needed to reap the full benefits of reform to the UK's data laws, techUK News [online], 4 August 2022 (accessed 13 March 2023); See also, Julian David, TechUK CEO, quoted in: British Businesses to Save Billions Under New UK Version of GDPR, Department for Science, Innovation and Technology press release, 8 March 2023

61 Adam A and Kazim T, Data: the wrong direction, Law Gazette [online], 23 June 2022

62 DCMS, Data: a new direction (PDF), 10 September 2021, p12

b. Section 19 Data Protection Act 2018, which provides that processing for research purposes will not meet the criteria in Article 89(1) of the UK GDPR if it is carried out for making decisions about data subjects (unless for approved medical research) or it is likely to cause substantial damage or distress to a data subject.[63]

The consultation noted that relevant provisions were "dispersed" across the legislation and some issues (eg the definition of scientific research) were dealt with in the recitals to the UK GDPR rather than its Articles. This, according to the Government, created "interpretative ambiguity" which made it difficult to "realise the full benefits" of the system.[64] The Government therefore wanted to consolidate and bring together the research-specific provisions. This would involve, among other things:

- incorporating a clearer definition of "scientific research" into the legislation.[65]
- clarifying that data subjects would be allowed to give their consent to broader areas of scientific research when it was not possible to fully identify the purpose of personal data processing at the time of data collection.[66]
- clarifying when personal data could be re-used (further processed) when based on a law that safeguarded an important public interest.[67]

Response to the consultation

In its June 2022 response to the consultation, the Government said most respondents agreed with consolidating and bringing together research-specific provisions and with creating a statutory definition for scientific research.[68] The Government would also proceed with its plans to:

- incorporate broad consent for scientific research into legislation.
- clarify that further processing for an incompatible purpose could be lawful when based on a law that safeguarded an important public interest or when the data subject had re-consented.
- clarifying when further processing could occur when the original lawful ground was consent.

63 As above, p12
64 As above, p12
65 As above, pp13-4
66 As above, pp16-7
67 As above, pp18-20
68 DCMS, Data: a new direction - government response to consultation [online], 17 June 2022, chapter 1.2

- extending the "disproportionate effort" exemption on information provision requirements for further processing for research purposes of personal data collected directly from the data subject.[69]

The response gives further detail on each of the above areas.[70]

The Bill

Clauses 2, 3, 9, 22, and 23 would simplify the use of personal data for research purposes.

Meaning of research and statistical purposes

Clause 2 would amend Article 4 of the UK GDPR. Under new Article 4(3), references to the processing of personal data for the purposes of scientific research (including references to processing for "scientific research purposes") would mean "references to processing for the purposes of any research that can reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity". This definition is different to that set out in the withdrawn Bill.

New Article 4(4)(a) gives examples of the types of scientific research that could fall under the definition:

> 4. Such references— (a) include processing for the purposes of technological development or demonstration, fundamental research or applied research, so far as those activities can reasonably be described as scientific, but (b) only include processing for the purposes of a study in the area of public health that can reasonably be described as scientific where the study is conducted in the public interest.

New Article 4(4)(b) clarifies that research into public health only falls under the definition of scientific research if it is in the public interest.

New paragraph 5 to Article 4 clarifies that processing for genealogical research is to be considered as processing for historical research under the UK GDPR.

Clause 2 also inserts a definition of what constitute processing for "statistical purposes" under the UK GDPR – ie processing for statistical surveys or for the production of statistical results where:

> (a) the information that results from the processing is aggregate data that is not personal data, and
>
> (b) neither that information, nor the personal data processed, is used in support of measures or decisions with respect to a particular individual.[71]

69 As above, chapters 1.2 to 1.3

70 As above

71 Clause 2(6)

Consent for processing for the purposes of scientific research

Clause 3 would amend Article 4 of the UK GDPR to clarify a way for a data controller, processing for scientific research purposes, to obtain consent to an area of scientific research where it was not possible to identify fully the purposes for which the personal data was to be processed at the time of collection. Under **clause 3(3)**, consent would be obtained where, among other things:

- at the time the consent was sought, it was not possible to identify fully the purposes for which the personal data was to be processed.
- seeking consent in relation to the area of scientific research was consistent with generally recognised ethical standards relevant to the area of research.
- so far as the intended purposes of the processing allowed, the data subject was given the opportunity to consent only to processing for part of the research.

Information to be provided to data subjects

Under Article 13(3) of the UK GDPR, when a data controller intends to further process personal data for a separate purpose than that for which it was originally collected, they must provide additional information to the data subject – eg information on the other purpose.[72]

Clause 9(1) would amend Article 13 to create an exemption from Article 13(3) for research purposes where there would be a disproportionate effort to provide the required information to data subjects and where the research was in line with the safeguards for research.

Article 14(5)(b) of the UK GDPR creates a disproportionate effort or impossibility exemption for all processing where the data was not collected directly from data subjects. It also sets out research as an example of when the exemption may be used.

Clause 9(2) would remove Article 14(5)(b) and insert two new paragraphs at the end of Article 14. Paragraph 6 would replicate the non-exhaustive list of examples of disproportionate effort being inserted into Article 13 through clause 9(1). The Explanatory Notes state that this does not materially affect how the current exemption in Article 14 operates but would make it clearer that the exemption would apply to all processing activities.[73]

Safeguards for processing for research purposes

Clause 22 would add a new Chapter 8A to the UK GDPR. This would consist of four new articles combining the existing safeguards, set out in Article 89 of

---

[72] The further information that the controller may be required to provide to the data subject is listed in Article 13(2).

[73] Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 166

the UK GDPR and section 19 of the 2018 Act, for data processing for archiving in the public interest, scientific, historic and statistical research purposes. Clause 22(1) would add new Article 84A to the UK GDPR outlining the categories of data processing that would fall within the scope of this chapter (ie processing for scientific or historical research, archiving in the public interest and statistical purposes) and would create a new acronym, 'RAS purposes' to refer to these purposes.[74]

Clauses 22(2) and (3) would add new Articles 84B and 84C to the UK GDPR. These would set out the additional safeguards required for processing personal data for RAS purposes:

- the processing must not cause substantial damage or substantial distress to the data subject.
- the processing must include technical and organisational measures to respect the principle of data minimisation.
- the processing must not be carried out for the purposes of measures or decisions with respect to a particular data subject unless it was for approved medical research.

Clause 23 would make consequential amendments to the UK GDPR and the 2018 Act.

Comment

TechUK has welcomed the Bill's provisions on research, claiming they would "remove barriers to responsible innovation".[75]

3.6 Obligations of data controllers and processors

Background

The UK GDPR imposes obligations on data controllers and processors. These include:

- appointing a data protection officer.
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests.

74 As above, para 241

75 Dhiman D et al, One final push needed to reap the full benefits of reform to the UK's data laws, techUK News [online], 4 August 2022; See also, Julian David, TechUK CEO, quoted in: British Businesses to Save Billions Under New UK Version of GDPR, Department for Science, Innovation and Technology press release, 8 March 2023

- maintaining documentation of processing activities.[76]

Data protection officers

Articles 37 to 39 of the UK GDPR cover data protection officers (DPOs). Organisations are required to appoint a DPO if they are a public authority, or if certain types of processing activities are carried out. The DPO must:

- inform and advise the organisation of their obligations under data protection law and monitor compliance.
- provide advice regarding data protection impact assessments.
- act as a point of contact with the ICO.

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. They can be an existing employee or externally appointed.

Data protection impact assessment

Article 35 of the UK GDPR requires organisations to undertake a data protection impact assessment (DPIA) for processing that is likely to result in a high risk to individuals. A DPIA must:

- describe the nature, scope, context, and purposes of the processing.
- assess necessity, proportionality, and compliance measures.
- identify and assess risks to individuals.
- identify any additional measures to mitigate those risks.[77]

Prior consultation with the Information Commissioner's Office

If an organisation identifies a high risk that cannot be mitigated, it must consult the ICO before starting the processing.[78] Where the ICO decides that the intended processing would infringe data protection law, it can provide written advice to the organisation and may, depending on the circumstances, use its enforcement powers against the organisation.[79]

Record keeping

Article 30 of the UK GDPR requires organisations to keep a record of their processing activities. This must include:

---

76 ICO, Guide to the UK GDPR – accountability and governance [online], October 2022 (accessed 13 March 2023)

77 As above

78 Article 36(1) to (3) of the UK GDPR

79 DCMS, Data: a new direction (PDF), 10 September 2021, p59

- the name and contact details of the organisation.
- the purposes of the organisation's data processing.
- a description of the categories of individuals and categories of personal data.
- the categories of recipients of personal data.
- details of transfers to third countries, including documenting the transfer mechanism safeguards in place.
- retention schedules.
- a description of the organisation's technical and organisational security measures.[80]

ICO guidance gives further detail on DPOs, DPIAs, record keeping and the further obligations of data controllers and processors.[81]

Data reform consultation

In its September 2020 consultation on data reform, the DCMS said that while accountability was "fundamental", the current legislative framework could generate a "significant and disproportionate administrative burden", particularly on SMEs and organisations that carried out low risk processing. The Government wanted to implement a more flexible and risk-based accountability framework based on privacy management programmes.[82] This would involve, among other things, removing the requirements for organisations to:

- designate a DPO.[83]
- to undertake a data protection impact assessment, so organisations could adopt different approaches to identify and minimise data protection risks that better reflected their specific circumstances.[84]
- keep records as required under Article 30. There would be new requirements to keep certain records, but organisations would have more flexibility about how to do this – ie in a way that reflected the volume and sensitivity of the personal information they handled, and the type of data processing they carried out.[85]

80 ICO, Guide to the UK GDPR – accountability and governance [online], October 2022
81 As above
82 DCMS, Data: a new direction (PDF), 10 September 2021, p54
83 As above, pp57-8
84 As above, pp58-9
85 As above, p60

- consult with the ICO in advance of processing personal data in cases that might involve high risk processing.[86]

Response to the consultation

In its June 2022 response to the consultation, the Government said the majority of respondents disagreed that the current framework should feature fewer prescriptive requirements and be more risk-based, as many considered the current legislation to be sufficiently flexible and risk-based.[87] However, when looking at responses from organisations only, the majority of respondents agreed that the framework should be more flexible and risk-based.[88] On the Government's specific proposals, most respondents disagreed with:

- the proposal to remove the requirement to designate a DPO. However, the Government said its proposed new requirement to appoint a senior responsible individual would shift the emphasis to ensure that data protection was established at a senior level to "embed an organisation-wide culture of data protection". The Government would therefore proceed with its proposal to remove the requirement to designate a DPO.

- the proposal to remove the requirement to undertake DPIAs. In its response, the Government said that, under the new privacy management programme, organisations would still be required to identify and manage risks, but they would be granted greater flexibility as to how to meet those requirements. It would therefore proceed with removing the requirement to undertake DPIAs.

- the proposal to remove the requirement to maintain a record of processing activities. The Government said it would proceed with the proposal because privacy management programmes would still require organisations to document the purposes of processing, but in a more tailored way.[89]

Most respondents agreed that organisations would be more likely to approach the ICO before commencing high-risk processing activities on a voluntary basis, if this was considered as a mitigating factor during any future investigation or enforcement action. The Government said it would proceed with removing the mandatory requirement for organisations to consult the ICO before high-risk processing.[90]

---

86 As above, p59. The Government's proposals are set out in further detail on pp53-69 of its consultation document.

87 DCMS, Data: a new direction - government response to consultation [online], 17 June 2022, chapter 2.2

88 As above, chapter 2.2

89 As above, chapter 2.2

90 As above, chapter 2.2

The Bill

Clauses 12 to **20** would make changes to the responsibilities of data controllers and processors. Some of these are briefly summarised below. The Explanatory Notes give further detail.

General obligations

Clause 12(1) would replace the requirement for data controllers to implement "appropriate technical and organisational measures" (Article 24(1) of the UK GDPR) with "appropriate measures, including technical and organisational measures".[91] The Explanatory Notes say the change would give data controllers more flexibility in terms of the measures they put in place to demonstrate and manage risk.[92] Corresponding amendments would be made to Part 3 of the 2018 Act by **clauses 12(5)** to **(10)**.

Removal of requirement for representatives for controllers outside the UK

Clause 13 would omit Article 27 of the UK GDPR so that data controllers that were not established in the UK would no longer need to appoint a data protection representative within the UK.

Senior responsible individuals

Clause 14 would replace the requirements on data protection officers in Articles 37 to 39 of the UK GDPR and sections 69 to 71 of the 2018 Act. It would introduce new requirements for data controllers and processors to designate a "senior responsible individual" to be responsible for data protection risks within their organisations or delegate that task to suitably skilled individuals.

Clause 14(2) would add a new Article 27A to the UK GDPR. This would set out the criteria for when a senior responsible individual would have to be appointed:

- where the controller or processor was a public body (except for courts or tribunals acting in their judicial capacity); or
- where the controller or processor was carrying out processing likely to result in a high risk to individuals (eg where an organisation was processing special category data on a large scale or data relating to criminal convictions).

Organisations would not need to appoint a senior responsible individual if their processing activities were low risk.

The remaining sub-clauses would make further provision about senior responsible individuals.

---

91 Clauses 12(2) and (3) would make similar clarification to Article 25(1) and Article 28(1), (3) and (4)(e).

92 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 187

Duty to keep records

Clause 15 would remove Article 30 of the UK GDPR and section 61 of the 2018 Act relating to records of processing activities. **Clause 15(4)** would insert new Article 30A into the UK GDPR which would require the controller or processor to maintain an appropriate record about the personal data.

New Article 30A (1) is new to the Bill. This would provide that a controller or processor would be exempt from the duty to keep records unless they were carrying out high risk processing activities.

New Article 30A would set out, among other things:

- the information to be included in the record of the data controller.
- the requirements for the data processor's record.
- the factors which controllers and processors would have to consider when deciding what an "appropriate" record was (eg the nature, scope and context of the processing; the risks their processing posed to individuals; and the resources available to the controller or processor).

Where possible, the record would have to include information on how the controller or processor would ensure the data was secure.[93]

Under the withdrawn Bill, a controller or processor that employed less than 250 people would have been exempt from the duty to keep records unless they were carrying out high risk processing activities. This exemption has been removed from the new Bill.

Assessment of high risk processing

Clause 17(2) would amend the heading of Article 35 of the UK GDPR from "Data Protection Impact Assessments" to "Assessments of high risk processing".

Clause 17(3) would omit or amend the requirements in the Article 35. Under the amended provisions, the data controller's assessment of high risk processing would need to include:

- a summary of the purposes of the processing.
- an assessment of whether the processing was necessary and the risks it posed to individuals.
- a description of how the controller would mitigate any risks.

Clause 17(7) would make similar amendments to section 64 of the 2018 Act.

[93] New Article 30A (4) and (7)

Consulting the Information Commissioner prior to processing

Clause 18(1) would amend Article 36 of UK GDPR (prior consultation) in accordance with subsections **(2) and (3)**. **Clause 18(2)** would make optional the previous requirement for controllers to consult the Information Commissioner before processing where an assessment under Article 35 indicated that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Schedule 4 paragraph 10(2) would amend Article 83 of the UK GDPR (general conditions for imposing an administrative fine) to allow the Commissioner to consider any relevant prior consultation under Article 36 when imposing administrative fines on a data controller.

Law enforcement processing and codes of conduct

Clause 19 would insert a new section 71A into the 2018 Act. This would enable expert public bodies, who had sufficient knowledge and experience, to create voluntary, sector-specific codes of conduct to enable controllers to identify and resolve data protection challenges in their sector and demonstrate compliance with data protection law.

Comment

The Open Rights Group has said the Bill's changes to DPIAs would leave data subjects with fewer protections.[94]

3.7 International transfers of personal data

Background

In an August 2021 document, the DCMS noted that the "hyper-connected world" was reliant on data transfers – eg GPS navigation, wearable technology, smart home technologies, and content streaming services.[95] International data transfers underpinned:

- international commerce, trade, and development.
- innovation, research and development across multiple sectors (eg health, higher education).

[94] The Data Discrimination Bill attacks our data protection rights, Open Rights Group blog, 7 March 2023

[95] DCMS/DSIT, International data transfers: building trust, delivering growth and firing up innovation [online], 26 August 2021 (accessed 13 March 2023)

They also supported international cooperation (eg international trade, law enforcement, and national security) and enabled people to connect (eg during the COVID-19 pandemic).

To transfer personal data from the UK to other countries, there must be an "adequacy decision" or an alternative transfer mechanism in place.

Adequacy decisions

The 2021 document explained that "data adequacy" is a status granted by the UK to countries providing high standards of protection for personal data. An adequacy decision means that personal data can be transferred from the UK to a country freely, in accordance with the terms of the decision.

UK adequacy decisions were the most efficient way to freely transfer personal data because they removed the need for UK organisations to use alternative transfer mechanisms, which could be costly to implement. Adequacy could also provide consumers and organisations greater certainty and confidence in the regulatory landscape of another country.

The UK had deemed the EU/EEA members to be adequate. Other adequate countries, jurisdictions or territories included: Andorra, Argentina, Canada (partial), Faroe Islands, Gibraltar, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, and Uruguay.

Under the UK GDPR, the test for adequacy is that when personal data is transferred internationally, the level of protection under the UK GDPR is not undermined. In determining this, the UK considers the overall effect of a third country's data protection laws, implementation, enforcement, and supervision. The DCMS guidance gives further information on determining adequacy.[96]

EU adequacy decisions on the UK

In January 2021, at the end of the transition period, a time-limited "bridging mechanism" was put in place so that personal data could continue to flow from the EU/EEA to the UK until adequacy decisions for the UK were adopted.[97] On 28 June 2021, the European Commission adopted decisions on the UK's adequacy under the EU GDPR and Law Enforcement Directive so that most personal data[98] could flow from the EU and the EEA.[99] Both decisions are expected to last until June 2025.[100]

---

96 As above

97 PQ 132820 [on data adequacy], answered 14 January 2021

98 The adequacy decisions don't cover data transferred to the UK for the purposes of immigration control, or where the UK immigration exemption applies. For further detail on this exemption, see the ICO's Guidance on the GDPR and the immigration exemption (accessed 13 March 2023)

99 EU adopts 'adequacy' decisions allowing data to continue flowing freely to the UK, DCMS press release [online], 28 June 2021 (accessed 13 March 2023)

100 ICO website, Data Protection and the EU (accessed 13 March 2023)

Alternative transfer mechanisms

Alternative transfer mechanisms help provide appropriate safeguards for international transfers of personal data to other countries in a way that ensures the level of protection of individuals guaranteed by the UK GDPR is not undermined. The DCMS guidance explains that these mechanisms are primarily used to transfer personal data to other countries where it is not possible to rely on an adequacy decision. They place obligations on the data exporter and data importer to ensure that personal data is protected when it is transferred outside the UK. Alternative transfer mechanisms for the private sector include:

- Standard and custom data protection clauses.
- Binding Corporate Rules (BCRs).
- Codes of conduct.
- Certification schemes.

Options for the public sector include:

- Legally binding instruments between public authorities/bodies.
- Administrative arrangements between public authorities/bodies.[101]

The ICO website includes further detail on international transfers.[102]

Consultation on data reform

In its September 2021 consultation on data reform, the DCMS said it intended to add more countries to those deemed adequate "by progressing an ambitious programme of adequacy assessments in line with the UK's global ambitions and commitment to high standards of data protection".[103] This would provide UK organisations with a "simple and safe" mechanism for international transfers of personal data.[104] The Government would take a risk-based approach to adequacy assessments. A four-stage procedure would be used to ensure that UK citizens and consumers would have confidence in the adequacy decisions that were made:

> a. Gatekeeping stage: consideration of whether to commence an adequacy assessment in respect of a country, by reference to policy factors, including high standards of data protection and the UK's strategic interests.
>
> b. Assessment stage: collection and analysis of information relating to the level of data protection in another country; this will look at questions based on

[101] As above
[102] ICO website, International transfers after the UK exit from the EU Implementation Period (accessed 13 March 2023)
[103] DCMS, Data: a new direction (PDF), 10 September 2021, p87
[104] As above, p88

> key principles of the safeguards in the UK GDPR, while recognising that countries protect personal data in different ways.
>
> c. Recommendation stage: officials will make a recommendation to the Secretary of State for Digital, Culture, Media and Sport, who will, after consulting the Information Commissioner and any others considered appropriate, decide whether to make a determination of adequacy in respect of a specific country.
>
> d. Procedural stage: making relevant regulations - and laying these in Parliament - to give legal effect to an adequacy determination.[105]

The Government said it would also explore legislative change to ensure that alternative transfer mechanisms were clear, flexible, and provided the necessary protections for personal data – eg through reinforcing the importance of proportionality when assessing risk for alternative transfer mechanisms.[106]

The consultation sought views on creating a new power for the Secretary of State to formally recognise new alternative transfer mechanisms.[107]

Response to the consultation

In its June 2022 response to the consultation, the Government said that around half of respondents agreed with the proposal for a risk-based approach to adequacy.[108] Some respondents thought the UK should be flexible and not prescriptive when making adequacy decisions. Many were clear that an outcomes-based approach should not come at the expense of data protection standards. The Government said it would proceed with reforms to the UK's approach to adequacy. It explained that the reformed regime would:

> … retain the same broad standard that a country needs to meet in order to be found adequate, meaning individuals' data will continue to be well-protected by a regime that ensures high data protection standards. Where countries meet those high data protection standards, the law will recognise that the DCMS Secretary of State may also consider the desirability of facilitating international data flows when making adequacy decisions.[109]

The response noted there were mixed views on the proposal allowing the Secretary of State for Digital, Culture, Media and Sport to create new UK mechanisms for transferring data overseas or recognise in UK law other international data transfer mechanisms. However, the Government said it would proceed with this reform because it would help to future-proof the UK's

105 As above, p89. For further detail, see pp87-92 of the consultation.

106 As above, pp93-5

107 As above, p97. For further detail on the proposals on alternative transfer mechanisms see pp92-101 of the consultation

108 DCMS, Data: a new direction - government response to consultation [online], 17 June 2022, chapter 3.2

109 As above

approach to international transfers by allowing the UK to respond rapidly to international developments.[110]

Most respondents agreed with the Government's proposal to enable data exporters to act pragmatically and proportionally when using alternative transfer mechanisms for data transfer.[111]

The Bill

Schedule 5 of the Bill would amend Chapter 5 of the UK GDPR to reform the UK's regime for international transfers. There would be three legal bases under which personal data could be lawfully transferred:

- where the Secretary of State had made regulations allowing the free flow of personal data to another country.[112]
- where there were appropriate safeguards for the personal data to be transferred (eg through contractual clauses).[113]
- where a transfer could be based on a derogation under Article 49 of the UK GDPR.

  Derogations can only be used in very limited circumstances and under specific conditions, where adequacy and alternative transfer mechanisms are unavailable – eg where a transfer is necessary for important reasons of public interest, or where a transfer is necessary to protect the vital interests of the data subject or of other persons and where the data subject is physically or legally incapable of giving consent.[114]

The Secretary of State would have the power to make regulations approving transfers of personal data to third countries or international organisations.[115]

A data protection test would have to be met before the Secretary of State could make regulations approving transfers.[116] This would be met if the standard of protection for the general processing of personal data in a country or international organisation was "not materially lower than the standard of protection under the UK GDPR and relevant parts of the 2018 Act".[117] In deciding whether the data protection test had been met, the Secretary of State would have to consider, among other things:

---

110 As above
111 As above
112 New Article 45A-C
113 Under Article 46 of the UK GDPR
114 For further detail on the derogations, see DCMS, Data: a new direction (PDF), 10 September 2021, pp100-1
115 New Article 45A(1)
116 Article 45B
117 Article 45B(1). For further detail on the test, see Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 716

- respect for the rule of law and for human rights in the country or the international organisation.
- the existence, and powers, of an enforcement authority.
- arrangements for redress for data subjects, whether that redress is judicial or non-judicial.
- rules about the transfer of personal data from the country or by the organisation to other countries or international organisations.
- any relevant international obligations to which the country or international organisation was subject.
- the constitution, traditions and culture of the country or organisation.[118]

Monitoring

The Secretary of State would have to monitor developments in third countries and international organisations that could affect decisions to make regulations approving transfers of personal data, or decisions to amend or revoke such regulations.[119]

If the Secretary of State became aware that the data protection test was no longer met in a country or international organisation to which transfers had been approved, they would have to amend or revoke the regulations approving the transfers.[120] When regulations had been amended or revoked, the Secretary of State would have to consult with the third country or international organisation to improve the protection provided to data subjects.[121]

The Secretary of State would have to publish a list of third countries and international organisations that had been approved by regulations. A list of the countries that had been, but no longer were, approved by regulations would also have to be published.[122]

Transfers subject to appropriate safeguards

Schedule 5 would also amend the UK GDPR to set out how organisations would have to approach the data protection test for transfers using standard contractual clauses - ie they would have to act "reasonably and proportionately", taking into account all the circumstances of the transfer.

118 Article 45B(2)
119 Article 45C(1)
120 Article 45C(2)
121 Article 45C(3)
122 Article 45C(4)

Schedule 6 Transfers of personal data to third countries etc - law enforcement processing

Schedule 6 of the Bill would make provision on the transfer of personal data to third countries for the purposes of law enforcement.[123]

Transitional provisions

Part 2 of **Schedule 7** sets out transitional provisions designed to ensure "a smooth transition between the current international transfers regime, and the new regime which will be implemented by the Bill".[124] Paragraphs 767 to 769 of the Explanatory Notes give details of the provisions. The Notes summarise their effect as follows:

> The effect of these provisions is to allow controllers to use pre-commencement transfer mechanisms following commencement of the new regime, so long as those mechanisms satisfy the requirements of existing Article 46(1) and the last sentence of existing Article 44 of the UK GDPR, or existing section 73(3) of the DPA 2018, immediately before the regime commences. Controllers who satisfy these criteria will therefore not need to apply the new data protection test in new Article 46(6) and section 75(5) of the DPA 2018 (unless they seek to enter into new transfer mechanisms post-commencement of the Bill).[125]

The Government has said that these updated provisions would mean that "businesses can continue to use their existing international data transfer mechanisms to share personal data overseas if they are already compliant with current UK data laws. This will ensure British businesses do not need to pay more costs or complete new checks to show they're compliant with the updated rules".[126]

Comment

Sam De Silva, Chair of BCS' Law Specialist Group (the BCS is the Chartered institute for IT), commented on the withdrawn Bill that "any material deviation the UK adopts in relation to data protection" would risk its adequacy status. He therefore hoped there would be a "detailed and objective analysis undertaken to assess whether the benefits from UK's data reform outweigh the risks of not continuing to have an adequacy status."[127]

In its IA on the withdrawn Bill, the Government said that moving to a system that allowed personal data to be transferred more flexibly via adequacy and alternative transfer mechanisms was expected to lower transaction costs and

123 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), paras 741-64
124 As above, para 766
125 As above, para 770
126 British Businesses to Save Billions Under New UK Version of GDPR, Department for Science, Innovation and Technology press release [online], 8 March 2023
127 GDPR reforms must protect the UK's data adequacy arrangement with the EU warns IT body, BCS Comment [online], 17 May 2022 (accessed 13 March 2023)

increase cross-border data flows. The IA estimated an annual benefit to trade of between £80m and £160m.[128]

The IA acknowledged that as the UK diverged from the EU GDPR, the risk of the EU revoking its adequacy decisions would increase. If this happened, there would be a cost to UK businesses:

> ...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....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 £410 million in lost export revenue when taking a micro approach to modelling.

However, the IA noted that adequacy decisions did not require third countries to have the same rules and the Government believed its reforms were compatible with the EU maintaining the free flow of personal data.

3.8 Information Commissioner's role

Background

The Information Commissioner's Office (ICO) is an independent public body with responsibility for overseeing and enforcing data protection law in the UK. Its functions and powers are set out in Parts 5 and 6 of the Data Protection Act 2018. The Department for Science, Innovation and Technology (DSIT) is the ICO's sponsoring department. The ICO website gives further detail on the ICO's management and structure.[129]

Consultation on data reform

ICO structure and governance

In its September 2021 consultation on data reform, the DCMS said the UK GDPR did not provide the ICO with a clear framework of objectives and duties against which to prioritise its activities and resources, evaluate its performance and be held accountable by its stakeholders. The ICO was instead obliged to fulfil a list of tasks, set out in Article 57 of the UK GDPR, but without a strategic framework to guide its work.[130] The Government therefore wanted to introduce a new, statutory framework setting out the strategic

128 Impact Assessment on the Data Protection and Digital Information Bill (PDF)[online], p8

129 ICO website, Who we are (accessed 13 March 2023)

130 DCMS, Data: a new direction (PDF), 10 September 2021, p115

objectives and duties that the ICO would have to fulfil when exercising its functions.[131]

The consultation also sought views on changing the ICO's governance model. The ICO is currently structured as a "corporation sole" (a single legal entity consisting of an incorporated office occupied by a single person). The powers and responsibilities of the ICO lie solely with the Information Commissioner. The consultation observed that most "peer regulators of the ICO" (eg Ofcom or the Financial Conduct Authority) ran a governance board model, including a separate, statutory independent board function which provided direction to, and scrutiny of, the executive function of the organisation. In contrast, a corporation sole was run by the executive function, without a chair or statutory independent board. According to the Government, "a corporation sole model makes the ICO an outlier for a large regulator with a broad and important remit. This model can lead to a lack of diversity, challenge and scrutiny that is critical to robust governance and decision-making".[132]

Complaint handling

The consultation also sought views on changes to the how the ICO handles data complaints from the public. In 2020/21 the ICO received 36,607 complaints. Responding to these required a "significant proportion" of the ICO's resources. The outcomes were sometimes "low-value" for data subjects and "poor value-for-money" for data protection fee payers. The Government said it wanted to create a more efficient and effective model by enabling the ICO to "take a risk-based approach, focusing on upstream activities in order to identify and address problems before they cause widespread harm".[133] It proposed the introduction of:

- a requirement for the complainant to attempt to resolve their complaint directly with the relevant data controller before lodging a complaint with the ICO.

- a requirement on data controllers to have a simple and transparent complaints-handling process in place to deal with data subject complaints.[134]

The Government would also explore whether to introduce criteria by which the ICO could decide not to investigate a complaint.[135]

131 As above, p115
132 As above, pp123-4
133 As above, pp131-2
134 As above, p132
135 As above, pp132-3

Response to the consultation

ICO structure and governance

The Government's June 2022 response to the consultation noted that almost half of respondents agreed that the ICO would benefit from a new statutory framework. However, some expressed concern about the potential risk to the ICO's independence and argued that the current framework was sufficiently clear.[136] The Government said it recognised these views, particularly those around independence, and had carefully considered the need to maintain the ICO's independence in developing its plans to proceed in introducing a new statutory framework of objectives and duties.[137]

There were also mixed views on the proposed change in the ICO's governance model. Those opposing the proposal raised concerns over the ICO's independence or had no issues with the current model. The Government said that having powers and responsibilities spread across a board, rather than with one individual, should ensure greater independence and integrity. It also said reforming the model would not erode the ICO's independence and would ensure "greater diversity in its leadership and its governance".[138]

The Government would legislate so that the ICO would, among other things, be required to be publish:

- a strategy setting out how it will discharge its functions and deliver against its objectives.
- key performance indicators.
- its approach to delivering its new objectives and duties framework.
- a response to the Government's Statement of Strategic Priorities.
- its approach to enhanced consultation and setting up expert panels with regards to codes of practice and statutory guidance.
- its approach to exercising its discretion concerning complaints handling.
- statutory guidance under section 160 of the 2018 Act.

The ICO would also be required to report annually on its approach to enforcement and the use of its powers.[139]

136 DCMS, Data: a new direction - government response to consultation [online], 17 June 2022, chapter 5.2

137 As above, chapter 5.2

138 As above, chapter 5.3

139 As above, chapter 5.4

Complaint handling

Nearly half of respondents to the consultation agreed that the ICO would benefit from a more proportionate approach to handing complaints. Most also supported the proposal to require complainants to attempt to resolve complaints with the data controller before contacting the ICO. Around half of respondents agreed with the proposal to set out criteria in legislation by which the ICO could decide not to investigate a complaint. However, there were some concerns that the criteria should be clear and not too rigid or overly prescriptive. Most respondents agreed with the introduction of a requirement for data controllers to have a simple and transparent complaints-handling process for data subjects' complaints.[140]

The Bill

Duties of the Commissioner in carrying out functions

Clause 27 would insert new sections into Part 5 of the 2018 Act to make changes to the Information Commissioner's role. Under **new section 120A**, the principal objective of the Commissioner when carrying out functions under data protection law would be:

- to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest; and
- to promote public trust and confidence in the processing of personal data.

Under **new section 120B**, the Commissioner would need to have regard to the following when carrying out data protection functions:

- the desirability of promoting innovation.
- the desirability of promoting competition.
- the importance of the prevention, investigation, detection, and prosecution of criminal offences.
- the need to safeguard public security and national security.

New section 120C would require the Commissioner to prepare and publish a strategy setting out how the Commissioner would discharge functions under:

- new sections 120A and 120B of the 2018 Act.
- section 108 of the Deregulation Act 2015 (exercise of regulatory functions: economic growth).

[140] As above, chapter 5.6

- section 21 of the Legislative and Regulatory Reform Act 2006 (exercise of regulatory functions: principles).

New section 120D would require the Commissioner to consult when considering how the exercise of their functions might affect economic growth, innovation and competition. The Explanatory Notes give an example of issues relating to emerging technology.[141]

Clause 27(4) would require the Commissioner to report on what they had done to comply with the duties during a reporting period.

Strategic priorities

Clause 28 would insert new sections into Part 5 of the 2018 Act to make provision for the introduction of a Statement of Strategic Priorities. This would set out the Government's data protection priorities to which the Commissioner would need to have regard.

Under **new section 120E**, the Statement would be prepared, designated and published by the Secretary of State.

New sections 120F(1-2) would require the Commissioner to consider the Statement when carrying out functions under the 2018 Act.

New sections 120F(3-5) would require the Commissioner to publish a response, within 40 days of the Statement's designation, explaining how they would have regard to the Statement.

New section 120G outlines the review process for the Statement.

Under **new sections 120H(1-2)**, a draft Statement prepared by the Secretary of State would be submitted to Parliament for approval via the negative resolution procedure on a non-amendable motion. This means the draft Statement could be rejected in full by either House of Parliament within a 40-day period. The Statement could not be designated until the end of this period. A Statement could not be designated without receiving parliamentary approval.

The Commissioner would have to report on how they had considered the Statement during the reporting period.

Codes of practice as to the processing of personal data

Clauses 29 and 30 would make changes to the statutory process for making codes of practice under the 2018 Act. Paragraphs 277 to 294 of the Bill's Explanatory Notes give further detail.

[141] Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 262

Vexatious or excessive requests made to the Information Commissioner

Clause 32 would amend the threshold for the Commissioner to charge a reasonable fee or refuse a request from a data subject or a data protection officer. The threshold would change from "manifestly unfounded or excessive" to "vexatious or excessive" and would align with the same change in threshold being made across the UK GDPR and the 2018 Act.

Analysis of performance

Clause 33 would insert new section 139A into the 2018 Act providing for the Commissioner to prepare and publish (at least once a year) an analysis of the Commissioner's performance.

Enforcement

Clauses 34 to 42 would make changes to enforcement of the data protection regime.

Clause 34 would amend section 142 (information notices) of the 2018 Act to clarify that the Commissioner could require specific documents as well as information when using the information notice power.

Clause 35 would make provision for the Commissioner to require a report on a specified matter when exercising the power under section 146 of the 2018 Act to give an assessment notice.

Clause 36 would insert **new section 148A** into the 2018 Act to make provision about interview notices. An interview notice could be used to require a person to attend an interview and answer questions when required by the Commissioner.

Penalty notices

Under schedule 16 to the 2018 Act, before issuing a penalty notice to a person, the Commissioner must inform the person of the intention to do so. At present, a penalty notice given in reliance on a notice of intent must be issued within 6 months from when the notice of intent is given.

Clause 37 would amend Schedule 16 to give the Commissioner the power to issue a penalty notice within 6 months of giving a notice of intent, but would allow the Commissioner to issue a penalty notice outside of the 6-month time limit if it was not reasonably practicable to issue a final penalty notice within this timeframe. The Explanatory Notes state that, in such circumstances, the Commissioner would instead be required to issue a final penalty notice "as soon as reasonably practicable" after issuing the notice of intent. This would allow the Commissioner to have sufficient time, after issuing a notice of intent, to consider oral or written representations and complete its investigations, where needed.[142]

[142] Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 364

Annual report on regulatory action

Clause 38 would amend section 139 of the 2018 Act to make provision for the Commissioner to publish an annual report on how it had discharged its regulatory functions ie:

- UK GDPR investigations; and
- the exercise of the Commissioner's enforcement powers.

Under **new section 161A(3)**, the annual report would have to include information on the enforcement powers exercised in relation to law enforcement processing and intelligence services processing.

Under **new section 161A(4)**, the Commissioner would have to publish information on the number of penalty notices issued in the reporting period that were given more than 6 months after the notice of intent was given and the reasons for this.

Complaints to controllers

Clause 39 would amend section 164 of the 2018 Act and insert new sections outlining the procedure for complaints by data subjects to data controllers.

Power of the Commissioner to refuse to act on certain complaints

Clause 40 would amend section 165 of the 2018 Act, by inserting section 165A, to give the Commissioner new powers to refuse to act on data protection complaints when certain conditions were met:

- Condition A: at the time the complaint was made, the complaint had not been made to the data controller.
- Condition B: the complaint had been made to the controller, the controller had not finished handling the complaint, and the period of 45 days beginning with the day the complaint was made to the controller had not expired.
- Condition C: the complaint was vexatious or excessive (as defined in new section 204A).

Under **new section 165B**, the Commissioner would have to publish, and lay before Parliament, guidance on responding to and refusing to act on complaints.

New section 166A would outline the process for appealing against a refusal of the Commissioner to act on a data protection complaint.

Paragraphs 314 to 406 of the Bill's Explanatory Notes give further detail on **clauses 34 to 42**.

Information Commission

The DCMS' June 2022 response to its data reform consultation said that, given the proposed changes to the ICO's governance model, the name "Information Commissioner's Office" might not accurately reflect the organisation, as it would not be the office of one individual. To ensure that the name of the body was not misleading, the Government was considering options for a new name for the regulator.[143]

Clauses 100 to 102 and Schedule 13 would establish a body corporate, the Information Commission, to replace the Information Commissioner, which is structured as a corporation sole. According to the Explanatory Notes to the Bill, the nature of the regulator's role and responsibilities would be "fundamentally unchanged".[144]

Comment

John Edwards, the Information Commissioner, has welcomed the Bill and its proposed reforms.[145]

However, the Open Rights Group has claimed that the Bill gives the Government powers to "interfere with the ICO".[146]

143 DCMS, Data: a new direction - government response to consultation [online], 17 June 2022, chapter 5.3

144 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 650

145 ICO statement on re-introduction of Data Protection and Digital Information Bill, ICO statement [online], 8 March 2023 (accessed 13 March 2023)

146 The Data Discrimination Bill attacks our data protection rights, Open Rights Group blog, 7 March 2023

4 Digital Verification Services

Part 2 of the Bill would establish a regulatory framework for the provision of online digital identity verification services in the UK. More specifically, it would create a legal framework through which 'trusted' private providers of digital verification identity services could be established. This includes a "trust mark" for organisations that have been certified against the framework, a register of providers, and an information-sharing gateway. The "information gateway" would enable public authorities to share government-held personal data with trusted providers for the purposes of identity and eligibility verification.

This Part of the Bill has been informed by earlier consultations on the governance of digital identities. A 'UK digital identity and attributes trust framework' is also in development. 'Alpha' versions of the framework were published in 2021 and a 'beta' version was published in June 2022. An overview of the consultations and the development of the framework is outlined below.

4.1 Background: identity verification

Verifying that we are who we say we are is integral to participating in both the 'real world' and in virtual spaces. Tasks such as opening a bank account, applying for a mortgage, renting a home, and buying alcohol and other age-restricted products are examples of situations that require a person to provide evidence of their identity (who they are) and/or their attributes (things about them, such as their age or address). Access to government services, including claiming Universal Credit or applying for a driving licence, similarly require a person's identity to be verified and authenticated. The aim of identity checks is usually to prevent fraud and to confirm entitlement to the service or product.

Traditional authentication methods rely on an individual knowing and recounting key personal details, such as their date of birth or address, and presenting hard copies of documents that corroborate their answers, including a driving licence, a birth certificate, or a passport. Such documents were typically presented in person. The Covid-19 pandemic, however, has underscored the value of identity checks that can be made online.

While there are different types of digital identity verification services, the process generally involves comparing something the person has (such as an ID document, like a passport) with a verified data set (such as passport data held by the Government). It is 'digital' because the comparison process – the

collection, extraction and analysing of ID data – is done online, using computer technology, rather than in person.

According to the Impact Assessment (IA) accompanying the first version of the Bill, current approaches to proving an identity that, for example, rely on presenting 'paper' documents in person, can be "expensive, inefficient, and vulnerable to fraud". While digital approaches to verification could "strengthen and simplify" the verification process, it is stated in the IA that digital identities do not currently "command trust" and lack standards which would enable them to be used across different organisations.[147]

4.2 Digital identities

A digital identity is a digital representation of a person that enables them to prove who they are during interactions and transactions. In some cases digital identities will be single-use: created for the purpose of completing one interaction at a specific point in time, such as an identity check carried out by an employer before a new employee joins the organisation. From the individual's perspective that interaction would be essentially the same as traditional paper-based identity verification, except that it takes place digitally.

Part 2 of the Bill is primarily intended to support the wider adoption of 'reusable' digital identities, which can "be used again and again for different interactions and transactions across organisations".[148] Focus group research conducted by BritainThinks for DCMS explained it as follows:

> Instead of showing my drivers license every time I need to prove who I am, I show my drivers license number once and get a 'digital identity'. The digital identity company check my drivers licence against the central list, and give me back a code. I show this code to anyone who needs to check my identity so they know I am me. But they won't see any other information, like my address.[149]

The Bill aims to provide a legal framework for the digital identity services market by:

- Establishing a 'trust framework' of standards against which digital identity verification service providers will be certified.
- Allowing certified service providers to check people's identity against Government-held data.

147 The Bill's supporting documents page states that an updated impact assessment for the DPDI (No 2) Bill has been submitted to the Regulatory Policy Committee for scrutiny. At the time of writing it has not yet been published.

148 DCMS, UK digital identity and attributes trust framework beta version (0.3), 13 June 2022

149 BritainThinks, Public perceptions of digital identities and attributes: transparency, trust and data, Report for DCMS, March 2022, p17

The Government has emphasised that it has no plans to create a centralised ID database, make digital IDs compulsory, or introduce ID cards.

The Government says that these measures will increase the level of trust individuals and organisations have in how verification service providers create, verify, and secure digital identities.[150]

Digital identity services are offered by the private sector. The Government has emphasised that it has no plans to make digital identities compulsory or to introduce ID cards.[151]

> Digital identity products and services developed under the trust framework are not the same as centralised identity databases or digital identity cards. The trust framework will enable users to choose a range of services created by different organisations that use different technologies to meet diverse user needs.
>
> Anyone can choose to create one or more digital identities (a user may choose to have different digital identities to use in different contexts). They do not have to create a digital identity if they would prefer not to.
>
> [...]
>
> This government is committed to delivering these benefits without the need for a national identity card. This means people will have the choice over if, when, and how they use digital identities.[152]

According to the IA, the following benefits could arise through widespread adoption of digital identities:

1. **Economic gains associated with a functioning digital identity system, enabling the full realisation of the digital economy**
2. **Protection against fraud, for both businesses and people** (The wide scale adoption of secure digital identity solutions has the potential to reduce the opportunity to steal and use stolen documents).
3. **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).
4. **The promotion of inclusive solutions and removal of barriers to inclusion** (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).[153]

150 DSIT, Data Protection and Digital Information Bill – Explanatory notes, March 2023, p14
151 DCMS and Cabinet Office, Government response to the digital identity and attributes consultation, March 2022
152 DCMS, UK digital identity and attributes trust framework beta version (0.3), 13 June 2022
153 DCMS, Impact Assessment, Data Protection and Digital Information Bill (opens PDF), 6 July 2022, pp37-38

For further information see also DCMS, Powers for digital identity and attributes initiatives, 15 September 2021.

4.3 UK digital identity and attributes trust framework

The Government has stated that clear rules and standards, governing the operation and use of digital identity verification systems, are required before such systems can be deployed by private providers – especially when they rely on government-held personal data.[154]

In February 2021, the Government published an 'alpha prototype' of its UK digital identity and attributes trust framework. This is the framework against which digital identity verification service providers will be certified.[155] It covers matters including:

- how organisations should handle and protect people's data;
- what security and encryption standards should be followed;
- how user accounts should be managed;
- how to protect against fraud and misuse.[156]

The aim of the trust framework is to ensure that individuals and organisations can understand and have confidence in how service providers create digital identities:

> One reason why [digital identity verification] does not currently happen is because one organisation does not know how another creates digital identities or attributes. This means they're not able to trust if the processes the other organisation followed are secure and meet their needs.
>
> The trust framework is a set of rules that different organisations agree to follow to deliver one or more of their services. This includes legislation, standards, guidance and the rules in this document. By following these rules, all services and organisations using the trust framework can describe digital identities and attributes they've created in a consistent way. This should make it easier for organisations and users to complete interactions and transactions or share information with other trust framework participants.[157]

154 DCMS, The UK digital identity and attributes trust framework, 11 February 2021

155 Guidance for service providers on the certification process is available at DSIT, Trust framework certification, updated 26 January 2023

156 DCMS, The UK digital identity and attributes trust framework, 11 February 2021

157 DCMS, UK digital identity and attributes trust framework beta version (0.3), 13 June 2022

The Government invited feedback on the framework and published an updated version in August 2021. The current 'beta version' of the framework was published in June 2022.

At the end of 2021, the Government announced its intention to use the trust framework to enable digital right to work, rent and criminal record checks using digital identity providers. This will be the first commercial application of the framework. Guidance for digital identity service providers on how to become certified to carry out identity checks for these purposes was subsequently published in July 2022.[158]

Commenting on the development of the trust framework, Philip James, a partner at the law firm Eversheds Sutherland, highlighted the importance of getting its implementation right:

> Digital ID is becoming an increasingly common cornerstone of transacting online, accelerated by the pandemic. Whilst Digital IDs present a great opportunity for facilitating digital economy growth - as well as preventing potential fraud - if implemented poorly, Digital IDs could significantly damage trust and privacy and prejudice the vulnerable; and, in a worst case scenario, could allow a fraudster to assume another's ID (and even lock out) that individual from their own authorised account/life.[159]

Speaking at a TechUK event in 2021 on Digital ID, Laura Barrowcliff, Head of Strategy at GBG Plc (an identity verification provider) emphasised that the government's approach to digital ID, as set out in the trust framework, "prioritised the right things" in relation to governance, inclusion and interoperability.[160] On inclusion, for example, one of the rules stipulated in the trust framework is that digital identity products and services should be accessible to as many people as possible:

> Making your products and services inclusive means as many people as possible can use them no matter who they are or where they're from. This includes people who do not have traditional identity documents such as passports, or who may find it difficult verifying their identity to access services online.
>
> [...]
>
> Organisations must follow the Equality Act 2010 when considering how to make sure no one is excluded because of their 'protected characteristics'. This applies to all organisations offering services. Public sector organisations or non-public sector organisations carrying out public functions will also need to meet the public sector equality duty (PSED) detailed in the Equality Act 2010.[161]

158 DSIT, Digital identity certification for right to work, right to rent and criminal record checks, updated 24 March 2023

159 Eversheds Sutherland, UK Government aims to lead on trust in Digital IDs, 23 March 2022

160 TechUK, Digital ID: What's the current state-of-play in the UK? , 22 July 2021

161 DCMS, UK digital identity and attributes trust framework beta version (0.3), 13 June 2022

Biometrics

The trust framework also allows the use of biometric technology for identity verification and authentication. Biometrics involve capturing a physical or behavioural attribute of a person in real time (such as their fingerprints or their facial image) and comparing it against a copy of the same trait stored on a database or on a token. Comparison is achieved through the application of a matching algorithm and a match score is generated; the higher the score, the more certain the system is that the two templates belong to the same person.

The Ada Lovelace Institute, an independent research institute focused on data and AI, has cautioned that the "plans to use biometrics in the UK Digital Identity and Attributes Trust Framework need careful consideration". In a blog post on the framework, the Institute stated that biometric systems, such as those that rely on automated facial recognition using Government-issued photo ID documents, can "simplify employment or rental checks significantly". However, it also pointed to problems with this approach:

- not everyone has appropriate government-issued photo identity documents, such as passports [...] Similarly, the pandemic has significantly decreased the number of young people with a driving licence.

- there are still widely acknowledged problems with automated facial recognition technology [...] These issues are often a consequence of biases in the datasets used to train the automated identification systems. In simple terms: if the datasets do not represent society, then the resulting systems will not be usable by everyone in society, even if they have the relevant documents.[162]

The risk of bias and discrimination posed by the application of biometric technologies in certain contexts is explored in further detail in the Ryder Review: independent legal review of the governance of biometric data in England and Wales (June 2022) which was commissioned by the Ada Lovelace Institute.

The Commons Science and Technology Select Committee has also examined biometrics on several occasions since 2014-15, including the Government's biometrics strategy and the work of the biometrics commissioner.[163] The Committee similarly highlighted concerns about bias, discrimination and the lack of governance of biometric systems. In 2018, for example, the Committee stated that "facial recognition technology should not be generally deployed,

[162] Ada Lovelace Institute, Digital identity verification: a problem of trust, 24 May 2022

[163] Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15, HC 734, 7 March 2015; Commons Science and Technology Committee, Biometrics strategy and forensic services, Fifth Report of Session 2017–19, HC 800, 25 May 2018; Commons Science and Technology Committee, The work of the Biometrics Commissioner and the Forensic Science Regulator, Nineteenth Report of Session 2017–19, HC 1970, 18 July 2019

beyond the current pilots, until the current concerns over the technology's effectiveness and potential bias have been fully resolved".[164]

In its 'beta version' of the trust framework, the Government outlined the steps it believes are necessary to ensure that biometric systems for digital IDs are inclusive and non-discriminatory:

> biometric technology needs to be inclusive and accessible. Appropriate testing of biometric technology helps ensure the technology works for a wide range of users. Following feedback from stakeholders in industry and civil society, the trust framework beta includes the strengthened requirement to test biometric technologies following an industry standard, which will apply to all services using biometrics.[165]

4.4 Government consultations

Digital Identity Call for Evidence

The Government published a call for evidence in July 2019 on the development and secure use of digital identities. The consultation document emphasised the Government's view that there are clear benefits to citizens when they can create digital identities that are "under their own control".[166] The Government stated that, via the consultation, it wanted to gather "insights and evidence into how government [could] support improvements in identity verification and support the development and secure use of digital identities and ensure that the potential benefits of this approach are open to all". [167]

In response to the consultation privacy campaign groups, including Privacy International and Big Brother Watch, raised concerns about digital identities, particularly around the potential for personal data held in a centralised location to be used for surveillance and manipulation. Privacy International said in its response to the call for evidence:

> It would be positive for both the UK, and the development of identity systems around the globe, if the UK builds a digital identity ecosystem that becomes a world-leader in respecting the rights of individuals and communities. Yet the risks of digital identity are large, from dangers surrounding the curtailing of people's rights and state surveillance, to the exploitation of their data by private companies. As a result, the highest standards must be in place to meet the promise of a world-leading system.[168]

---

164 Commons Science and Technology Committee, Biometrics strategy and forensic services, Fifth Report of Session 2017–19, HC 800, 25 May 2018, p21

165 UK digital identity and attributes trust framework - beta version - GOV.UK (www.gov.uk), 13 June 2022

166 DCMS and Cabinet Office, Digital Identity: Call for Evidence [opens PDF], July 2019, p2

167 DCMS and Cabinet Office, Digital Identity: Call for Evidence [opens PDF], July 2019, p2

168 Privacy International, Digital Identity: Call for evidence by the Department of Digital, Culture, Media, and Sport, and Cabinet Office, September 2019, p2

The response discusses several features that Privacy International would want to see in a digital identity system, including that:

- The purpose of the digital identity scheme should be clearly defined and legitimate;
- Data should not be held centrally and users should not receive a unique identifier used across multiple services;
- It should be possible to create multiple digital identity accounts;
- When verifying a person's identity, the minimum amount of personal data should be shared;
- The identification system should be as inclusive as possible, for example by allowing a broad range of ways for people to prove their identity;
- The system should be based on strong data protection standards, enforced by regulators.

The Government Response was published on 8 September 2020. According to the Response, consultees wanted "legal certainty on how to use digital identity, and legal gateways to check identity attributes against government data".[169] The Government stated that it had "plans to update existing laws on identity checking" so that digital IDs could be used in the "greatest number of circumstances". It added, however, that further work and consultation on the matter was required first:

> The government will consult on developing legislation to set provision for consumer protections relating to digital identity, specific rights for individuals, an ability to seek redress if something goes wrong, and where the responsibility for oversight should lie. The government will also consult on the appropriate privacy and technical standards for secure digital identities. We will look at how to establish sufficient oversight of these standards to build trust and facilitate innovation - providing organisations with a handrail to develop new future facing products.[170]

In addition, the Government's Digital Identity Strategy Board published principles to "frame digital identity delivery and policy in the UK" as part of the Government Response (see Box 1). It explained that these principles would inform the Government's development of a legal framework to enable the "use of secure digital identities" while simultaneously "establishing safeguards for citizens".

1 Digital identity principles

169 DCMS and Cabinet Office, Digital Identity: Call for Evidence Response, updated 8 September 2020
170 DCMS and Cabinet Office, Digital Identity: Call for Evidence Response, updated 8 September 2020

- **Privacy** – When personal data is accessed citizens will have confidence that there are measures in place to ensure their confidentiality and privacy. Where possible, citizens select what personal data is shared. Organisations will have privacy standards to uphold and will need to prove their ongoing compliance.
- **Transparency** – Citizens must be able to understand by who, why and when their identity data is used [when using digital identity products].
- **Inclusivity** – This means those who want or need a digital identity should be able to obtain one. We will look at how citizens could use different attributes (eg name, date of birth etc.) held across government and by other parties to support identity proofing.
- **Interoperability** – Setting technical and operating standards for use across the UK's economy to enable international and domestic interoperability.
- **Proportionality –** User needs and other considerations such as privacy and security will be balanced so digital identity can be used with confidence across the economy.
- **Good governance –** Digital identity standards will be linked to government policy and law. Any future regulation will be clear, coherent and align with the government's wider strategic approach to digital regulation.

Source: DCMS and Cabinet Office, Digital Identity: Call for Evidence Response, updated 8 September 2020

Digital identity and attributes consultation

A second consultation on 'Digital identity and attributes' was launched in July 2021 and sought views on three areas:

5. Creating a digital identity governance framework

   […] to support the trust framework there will need to be a responsible and trusted governance system in place which can oversee digital identity and attribute use and make sure organisations comply with the rules contained within the trust framework. We are using this consultation to solicit views on the exact scope and remit of this governing body. As the consultation makes clear, it will be vital to ensure that this body works closely with other regulators that have oversight of digital services, and supports our wider goals of establishing a coherent regulatory landscape that unlocks innovation and growth.

6. Enabling a legal gateway between public and private sector organisations for data checking

   […] to unlock the benefits digital identities can bring, we need to make it possible to digitally check authoritative government-held data. We need the digital equivalent of checking data sources such as a passport. That's

> why we are also consulting on how to allow trusted [private] organisations to make these checks.
>
> 7. Establishing the validity of digital identities and attributes
>
> Finally, we want to firmly establish the legal validity of digital identities and attributes, to build confidence that they can be as good as the physical proofs of identity with which we are familiar.[171]

The consultation ran between July and September 2021 and a Government Response was published on 10 March 2022. It emphasised that it would "seek to introduce legislation on measures detailed in [the] response when parliamentary time allows".[172] A brief overview of responses to the three consultation proposals is set out below.

Proposal 1: Creating a digital identity and attributes governance framework

The Government stated that feedback from consultees, and from its wider "stakeholder engagement", supported its proposal for the governance of the digital identity framework to be placed in an existing regulator. There was no agreement, however, on which existing regulator should be responsible.

> We will establish an interim governance function in the Department for Digital, Culture, Media and Sport, to be named the Office for Digital Identities and Attributes (OfDIA). This function will stand up a governance and coordinating role for the trust framework, which will not itself be set in legislation, and trust mark. Working with the UK Accreditation Service and certifying bodies, it will own the list of trust-marked organisations. The list of trust-marked organisations will be publicly available to give organisations and end users the opportunity to verify the provider they are interacting with is trust framework certified.

Proposal 2: Enabling a legal gateway between public and private sector organisations for data checking

The majority of respondents agreed that private organisations should sign up to (be 'members' of) the Government's trust framework, in order to be eligible to make identity checks against government-held data. The Government said that:

> […] there are clear advantages to requiring digital identity and attribute organisations who wish to make checks through the proposed legal gateway to prove they follow the rules of the trust framework. It will build public trust, protect people's data, and ensure user control of data is at the heart of this gateway. It will also help streamline due diligence processes.
>
> We will therefore require such private sector organisations to become certified against the trust framework before they are able to make checks against

171 DCMS and Cabinet Office, Digital identity and attributes consultation, July 2021

172 DCMS and Cabinet Office, Government response to the digital identity and attributes consultation, March 2022

> government-held data through the proposed legal gateway. We do not think this requirement presents an unnecessary commercial restriction.

The Government added that organisations certified against the trust framework would be given a 'trust mark' to demonstrate their compliance and would be defined, and listed publicly, as being a trust-marked organisation.

A majority also agreed that there should be a requirement in legislation or standards to allow an 'alternative pathway' for those who fail a digital check (for example because the service they are trying to access has outdated home address information). 96% of respondents agreed that there should be a code of practice clarifying the obligations that public sector organisations are required to meet when using the legal gateway. The Government said that it would proceed with both. The code of practice will be "consistent with" the Information Commissioner's data sharing code of practice.

Proposal 3: Establishing the validity of digital identities and attributes

More than 90% of respondents agreed that it would be helpful for the Government to confirm the legal standing of digital identities. The Government said that it recognised that this would "help build confidence" and that it would introduce legislation to "to affirm that digital identities and digital attributes can be as valid as physical forms of identification, or traditional identity documents."

Identity cards

In response to concerns expressed about the principle of digital identity systems, the Government stated that it had no plans to make the use of digital ID services compulsory or to introduce ID cards:

> Many of the individuals who responded to the consultation said they were against digital identities in principle. The government has heard this and has no plans to make the use of digital identities compulsory. The government also understands that there is no public support for ID cards in the UK and has no plans to introduce ID cards.
>
> The proposals brought forward in this document will not require the introduction of ID cards. They are limited instead to creating trust and confidence in digital methods of proving identity and eligibility. This means that, when it suits people to prove things about themselves or others on the basis of a digital identity, this can be achieved with as much ease and security as is offered by physical proofs of identity such as a passport.[173]

2 Cabinet Office consultation

[173] DCMS and Cabinet Office, Government response to the digital identity and attributes consultation, updated 10 March 2022

The Cabinet Office has a related but distinct programme of work on digital identity underway. This is to support the rollout of GOV.UK One Login, a service being developed by the Government Digital Service (GDS).

According to GDS there are currently over 190 different ways people can create accounts to access government services online.[174] One Login will replace this system of multiple accounts and identity checks with a single, reusable account.

From January to March 2023 the Cabinet Office consulted on draft legislation to enable identity checking for One Login by adding a new public service delivery objective to the data sharing provisions in the Digital Economy Act 2017.[175] The new objective would allow specified public authorities (in England, Scotland, and Wales) to share personal data for the purpose of verifying the identity of an individual who is seeking to access public services.

4.5 The Bill

Part 2 extends to England and Wales, Scotland and Northern Ireland.

Clause 46 defines a digital verification service (DVS) as meaning identity "verification services provided to any extent by means of the internet" and sets out that DVS's will consist of 4 parts:

- a trust framework.
- a register.
- an information gateway.
- a trust mark.

Trust framework

Clause 47 covers the establishment of the trust framework, namely the "rules concerning the provision of digital verification services" (subsection 1). It states that the trust framework document should be prepared by the Secretary of State (subsection 2), following consultation with the Information Commissioner – whose responsibility it is to uphold information rights in the public interest – and anyone else the Secretary of State thinks it is important to consult (subsection 3). Subsection 4 stipulates that the consultation can take place before **Clause 47** comes into force.

174 GDS, One Login for Government December 2021 update, 1 December 2021

175 Cabinet Office, Consultation on draft legislation to support identity verification, 3 January 2023

Subsection 5 requires the Secretary of State to review the trust framework at least every 12 months, with the same requirements to consult as those set out in subsection 3. Under subsection 6, the Secretary of State can issue a revised and republished trust framework following a subsection 5 review, or at another suitable time. Subsections 7 and 8 specify when the trust framework, or a revised version of the trust framework, can come into force.

There is no Parliamentary procedure associated with the preparation and publication of the trust framework. According to the Delegated Powers Memorandum, this is because the framework is concerned with "technical matters", while the powers to update and revise it will "ensure organisations are being assessed against the most up to date rules and industry standards".[176]

Digital Verification Services (DVS) register

Under Clause 48, the Secretary of State must establish and maintain a DVS register, listing those bodies that provide DVS, while also making it publicly available (subsections 1-3). Subsection 4 sets out the criteria that must be met to be listed on the register. Service providers must:

- Hold a certificate confirming compliance with the trust framework;
- Comply with all registration requirements under clause 49;
- Pay the fee set under clause 50.[177]

Subsection 6 explains when a certificate would not be valid and thus cannot be used for the purpose of registering an organisation on the DVS register, including that it has expired (Clause 48(6)(a)) or has been withdrawn (Clause 48(6)(b)).

Clause 49 provides further details about applying to be registered on the DVS register. Subsection 1 (a-d) specifies that the Secretary of State can make a "determination" (a decision) on the form of the application, how it is to be submitted, as well as the information and documents to be provided in support of the application. The Secretary of State may revise a decision on these matters (subsection 4) though subsections 3 and 5 state that the Secretary of State must publish both the original, and any revised, decisions.

The Secretary of State may also make a determination about charging fees, and setting the amount to be paid, as part of the DVS registration process (**Clause 50(1-3)**). Under subsection 5, unpaid fees can be recovered as a civil debt.

176 DSIT, Data Protection and Digital Information Bill – Delegated powers memorandum, March 2023, p21

177 DSIT, Data Protection and Digital Information Bill – Explanatory notes, March 2023, p60

The conditions under which an entity must be removed from the DVS register, by the Secretary of State, are stipulated in **Clause 51(1)(a-c).** They include that the organisation has:

- asked to be removed;
- stopped providing DVS;
- no longer holds a certificate from an accredited conformity assessment body or;
- no longer holds a valid certificate (eg it has expired or been withdrawn – Clause 51(2)(a-c)).

Clause 52(1) gives the Secretary of State the power to remove a person / organisation from the DVS register, so long as they are satisfied that the organisation is failing to adhere to the DVS trust framework when providing DVS services, or that they have not provided information requested by the Secretary of State when a notice has been issued under **Clause 58**.

Written notice that an organisation is to be removed must be sent to the organisation (subsection 2). It should include, among other things, the reason(s) for removal, that the organisation has the right to make written representations about the intention to remove them from the register (subsection 3) and that it has a minimum of 21 days, following receipt of the notice, to make such representations (subsection 4). If the organisation is removed from the DVS register, any application to be re-registered must be refused for the period specified in the notice, which must not exceed 2 years (subsections 9 & 10).

If the Secretary of State revises and republishes the DVS trust framework, **Clause 53** allows for rules to specify that an organisation has to obtain a "top-up certificate", certifying that they are providing DVS in-line with the revised trust framework (subsections 1 & 2).

Supplementary information

Clause 58(1) gives the Secretary of State the power to require an accredited conformity assessment body, or a person/organisation registered on the DVS register, to provide information that the Secretary of State "reasonably requires" to exercise their functions under this Part of the Bill. A notice must state why the information is required (subsection 2) and disclosure is not required if it would contravene data protection legislation or the Investigatory Powers Act 2016 (subsection 7).

Information gateway

The Explanatory Notes to the Bill state that the current legal framework places "restrictions" on information sharing between public bodies and

private entities, for the purposes of providing digital identity verification service.[178]

Clause 54 (1-2) would grant public authorities the power to share information with a registered DVS provider when an individual makes a request to the registered provider to verify their identity. The Bill makes clear that such a disclosure does not breach "any obligation of confidence owed by the public authority making the disclosure" (subsection 3(a)) but adds that it does not authorise public authorities to disclose information that would contravene data protection legislation or is prohibited under the relevant parts of the Investigatory Powers Act 2016 (subsection 4(a & b)).

HM Revenue and Customs (HMRC) is one such public authority that can share information under Clause 54. **Clause 55**(2) stipulates that any information shared by HMRC with a registered DVS provider, for the purposes of DVS, must not be shared further (unless consent has been obtained from the Commissioners of HMRC). This also applies to any third party who receives the information (subsection 3). Subsection 4 sets out that the offence of wrongful disclosure under section 19 of the Commissioners for Revenue and Customs Act 2005 applies if information is disclosed in contravention of this section of the Bill.

The establishment of the information gateway may also be relevant to the operation of Clause 57 of the Online Safety Bill, which requires providers of certain services to offer adult users the option to verify their identity. The then Minister for Tech and the Digital Economy, Chris Philp, described this approach as giving users "more control over who they interact with online". He added that it:

> only applies to high risk, high reach services. Users who do not want to verify themselves will not have to do so. This ensures that legitimate uses of anonymity are not restricted.[179]

The law firm Pinsent Masons suggests that the establishment of the information gateway, and the sharing of information between public authorities and a registered DVS provider, could:

> play a part in compliance with the Online Safety Bill, which is set to introduce an obligation for certain service providers to offer users the option to verify their identity and cites age verification as a way to comply with various obligations. [180]

Code of practice

To assist public authorities with disclosing information under Clause 54, a Code of Practice must be published by the Secretary of State that is consistent with the Data Protection Act 2018 (**Clause 56(1-2)**). The Code of Practice may

[178] DSIT, Data Protection and Digital Information Bill – Explanatory notes, March 2023, p19

[179] PQ 25841 [on Internet: Proof of Identity], 6 July 2022

[180] Pinsent Masons, UK Data Protection and Digital Information Bill: in detail, 20 July 2022

be revised and republished (subsection 4) and, when it is being prepared, the Secretary of State must consult with the Information Commissioner and anyone else thought appropriate (subsection 5).

The first version of the Code must not be formally published unless a draft of the Code has been "laid before, and approved by a resolution of, each House of Parliament" (the 'affirmative procedure' – subsection 7). Any subsequent revisions, and republications, of the Code are to be subject to the draft negative procedure (subsection 8). The Delegated Powers Memorandum describes this approach as providing an "appropriate level of Parliamentary scrutiny".[181]

Public authorities must have regard to the code of practice when disclosing information under Clause 54 (subsection 3).

Trust mark

Clause 57(1-3) provides that the Secretary of State can designate a trust mark to be used only by those organisations on the DVS register. The Secretary of State may enforce this through civil proceedings or an interdict (a civil court order) in Scotland (subsection 4).

Arrangements for third party to exercise functions

Clause 59(1) enables the Secretary of State, by regulation, to delegate some or all of the functions under Part 2 to another person to carry out. The regulations are subject to the affirmative procedure (subsection 3). The Delegated Powers Memorandum provides the following justification for the procedure:

> While certain functions are administrative and operational in nature, for example, the duty to establish and maintain a register of digital verification services providers, there are functions, such as the duty to set the rules of the trust framework and the power to remove digital verification services organisations from the verification services register, that are substantive functions. Parliament should therefore have the opportunity to scrutinise and debate the proposed arrangements for another person to take on these functions. It is considered that the affirmative procedure provides the appropriate level of scrutiny.[182]

Report on the operation of Part 2

Clause 60 requires the Secretary of State to publish reports on the operation of Part 2, at least every 12 months, beginning on the day which section 47 comes into force.

---

[181] DSIT, Data Protection and Digital Information Bill – Delegated powers memorandum, March 2023, p23

[182] DSIT, Data Protection and Digital Information Bill – Delegated powers memorandum, March 2023, p24

5 Customer data and business data

Background

The UK GDPR gives consumers the right to request that businesses provide their data to Third Party Providers (TPPs) in a commonly used format (ie through the right to data portability). "Smart data" is an extension of the right and enables consumers to securely share their data with third parties to enable them to provide services.[183] In a June 2019 document, the Government said it considered the key benefits of smart data initiatives to be:

- the immediate provision of data by the data holder to TPPs following a request from a consumer (rather than the 30 days permitted in the right to data portability).
- the use of Application Programming Interfaces (APIs) to share data securely, but only once the consumer has verified their identity and the TPP has received their express consent to do so.
- where appropriate, an ongoing transfer of data between businesses and TPPs, rather than a one-off transfer.
- adherence to common technical standards, data formats and definitions to ensure interoperability and to minimise barriers for TPPs.
- provision of certain product and performance data, such as tariffs or geographical availability of services, in addition to consumer data, if necessary, to enable innovation.[184]

Open Banking is one example of smart data. This requires the largest UK banks to use APIs to provide customer transaction data, in real time and in a common format, to regulated third parties (who have the customer's consent) to provide innovative services. It also enables consumers to initiate payments via regulated third party services. Some of the services developed through Open Banking include:

- aggregation services that allow consumers to view multiple current accounts and credit cards in a single app, move funds between accounts and make payments.
- services that use transaction data to monitor a consumer's expenditure and regular payments (for example, mortgage repayments, TV subscriptions or utility bills) and find better deals.

183 BEIS, Smart data: putting consumers in control of their data and enabling innovation (PDF) [online], June 2019, p11 (accessed 13 March 2023)

184 As above, p11

- "sweeping" services that move cash into and out of current accounts automatically to avoid bank overdraft charges and provide a higher rate of return on cash balances.

- tools for businesses that can track business expenses and manage VAT and tax self-assessments.

- the assessment of eligibility for mortgages or legal aid, without consumers having to provide physical bank statements.

- tools for debt advisors that use a client's transaction data to populate financial statements. These can help advisors provide better support and do so more efficiently.[185]

In June 2019, the Department for Business, Energy and Industrial Strategy (BEIS) published a consultation on smart data. This claimed that, while the benefits of smart data were clear, consumers' data was often "locked away in a manner that works against consumers and innovators". The consultation sought views on:

- accelerating the development of innovative data-driven services in consumer markets.

- using data and technology to help vulnerable consumers.

- ensuring consumers and their data were protected.[186]

In a September 2020 document, BEIS said that respondents to the consultation were in favour of the extension of smart data.[187] They also agreed that it was important to have a strong mechanism to incentivise industry to deliver smart data initiatives.[188] Except for some communications providers, the proposal to legislate to mandate industry involvement was broadly supported by respondents.[189] The document noted that the UK GDPR gave a right to consumer data. In addition, sections 89-91 of the Enterprise and Regulatory Reform Act 2013 could be used to mandate that firms participate in sharing consumer data. However, the Government said these powers were insufficient to deliver the full benefits (and safeguards) that it considered necessary (eg existing powers do not include the sharing of product data, or the requirement for TPPs to be accredited).[190]

The Government would therefore use primary legislation to extend its powers to mandate participation in smart data initiatives.[191]

---

185 As above, p15

186 As above, p10

187 BEIS, Next steps for smart data: putting consumers and SMEs in control of their data and enabling innovation (PDF) [online], September 2020, p6 (accessed 13 March 2023)

188 As above, p13

189 As above, p13

190 As above, p13

191 As above, p14

The Bill

Part 3 of the Bill would give the Secretary of State for BEIS and the Treasury the power to issue regulations requiring "data holders" to make available "customer data" and "business data" to customers or third parties, as well as regulations requiring the processing of this data. Sections 89 to 91 of the Enterprise and Regulatory Reform Act 2013 would be repealed (**clause 76**).

Clause 61(2) defines the key terms and concepts of Part 3:

- "Business" data is information about goods or services and digital content supplied by the relevant trader (eg data about the products the trader offers and their prices (to enable price comparison).
- "Customer data" means information relating to the customer of a trader (eg information on a customer's usage patterns and the price paid to aid personalised price comparisons).
- A "data holder" is a trader or a person who, in the course of business, processes the data.
- A "trader" is a person who supplies or provides goods, services or digital content in the course of a business whether acting personally or through another person. The concepts of "goods", "services", "digital content" reflect Part 1 of the Consumer Rights Act 2015.

Under **clause 61(3) and (4)**, "customers" covers persons who have at any time purchased or received goods or services from the trader whether or not the customer had done so in the course of a business. "Customers" include consumers, but also business customers.

Power to make provision in connection with customer data

Clause 62(1) would enable the Secretary of State or the Treasury to make regulations requiring data holders to provide customer data either directly to a customer at their request, or to a person authorised by the customer to receive the data at the request of the customer or the authorised person. The Explanatory Notes state that it is envisaged that data would be provided to an authorised person, rather than the customer, because the authorised person would be best able to make use of the data on the customer's behalf (eg in the provision of account management services via a visual dashboard of accounts, displayed on a smartphone app). However, the regulation-making powers had been kept broad to allow for direct provision of data to customers in the future.[192]

Clause 62(2)(a) would enable the regulations to provide for the production, collection, and retention of customer data so that data holders would have

[192] Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 465

specific data to hand in to ensure that smart data schemes could operate consistently and effectively.

Clause 62(2)(b) would enable the regulations to require or enable data holders to make changes to customer data if requested by the customer or an authorised person on behalf of the customer.

Clause 62(3) would enable the Secretary of State or Treasury to make regulations to provide for an authorised person who received the customer data to be able to exercise the customer's rights in relation to the person who is the data holder in relation to that data.

Clause 62(4) would ensure that in deciding whether to make regulations for customer data, the Secretary of State or the Treasury would have to consider the effect of the regulations on customers, data holders, small and micro businesses, and on innovation in the supply of goods and products and competition.

Clause 63 outlines non-exhaustive provisions that regulations relating to customer data may, among other things, contain. The Explanatory Notes give further detail on the provisions.[193]

Power to make provision in connection with business data

Clause 64(2) would enable the Secretary of State or the Treasury to make regulations to enable the production, collection, and retention of business data.

Clause 64(3) would ensure that, in deciding whether to make regulations relating to business data, the Secretary of State or the Treasury would have to consider the effect of the regulations on customers, data holders, small and micro businesses, and on innovation in the supply of goods and products and competition.

Clause 65 outlines non-exhaustive provisions that regulations relating to business data may, among other things, contain. The clause largely mirrors clause 63.

Decision makers

Clause 66 outlines non-exhaustive provisions relating to decision makers that the regulations could, among other things, provide for. The Explanatory Notes give further detail on the provisions.[194]

Enforcement

Clause 67 would enable enforcement of the regulations by a public body specified in the regulations (an "enforcer"). The enforcer's powers of

193 As above, paras 471-8

194 As above, paras 494-502

investigation could include powers to require provision of information, and powers of entry, inspection, search and seizure (under **clause 67(3)**

Clause 68 would restrict the enforcer's powers of investigation. Under **clause 68(1)**, regulations could not authorise the enforcer to enter a private dwelling without a court-issued warrant.

Under **clause 68(1)(b)**, regulations could not require a person to give an enforcer information to which **subsections (2) to (7)** applied. This would consist of information:

- the provision of which would infringe the privileges of Parliament.
- in respect of a communication between a professional legal adviser and the adviser's client and in connection with legal advice to the client regarding the regulations.
- in respect of a communication between a professional legal adviser and the adviser's client or another person, in connection with proceeding arising out of the regulations, and for the purpose of any such proceedings.
- the provision of which would expose a person to prosecution for an offence other than an offence under the regulations or other legislation listed in subsection (7).

Clause 68(2) would require the amount of a financial penalty to be imposed by an enforcer to be specified in, or determined in accordance with, the regulations.

Fees

Clause 70 would enable the Secretary of State or the Treasury to make regulations so that data holders, decision-makers, enforcers, and others[195] to require the payment of fees to meet any expenses incurred in performing duties or exercising powers under Part 3.

Levy

Under **clause 71**, the Secretary of State or Treasury could make regulations imposing, or providing for a specified public body to impose, a levy on data holders. The levy would meet all, or part of the costs, incurred by enforcers and decision-makers or persons acting on their behalf. The intention is to ensure that expenses would be met by the relevant sector without incurring a cost to the taxpayer.[196]

[195] ie any other persons on whom duties would be imposed, or powers conferred, by regulations under Part 3.

[196] Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF) para 532

Financial assistance

Clause 72 would enable the Secretary of State or the Treasury to give financial assistance to decision makers or enforcers to meet any expenses in the exercise of their functions.

Duty to review regulations

Clause 75 would require the Secretary of State or the Treasury to review the regulations made under Part 3 at least every five years.

Comment

In a news item on the withdrawn Bill, the Investing and Savings Alliance (TISA) welcomed the Bill's provisions on smart data. Harry Weber-Brown, chief executive at TISA Digital, said:

> Smart data and open finance will revolutionise the way we access financial services. We are therefore pleased that the government is determined to support this while maintaining privacy standards, thus addressing the chief barrier to wider adoption of open finance in practice.
>
> We welcome the bill as published today, because it achieves the twin aims of enabling an effective digital finance ecosystem while retaining privacy standard.
>
> The UK was at the forefront of open finance when open banking was launched. However, recent years have seen other jurisdictions adopt more effective data standards and move ahead on open finance implementation. Smart data receiving government backing in such a significant way should provide the boost necessary to finally allow UK consumers to reap the benefits of open finance.[197]

[197] TISA welcomes smart data inclusion in data protection bill, Peer2Peer Finance news [online], 19 July 2022 (accessed 10 March 2023)

6 Further provisions about digital information

Part 4 of the Bill would make changes about digital information in various contexts.

6.1 Privacy and electronic marketing

Clauses 79 to 86 are concerned with privacy and direct marketing electronic communications. If enacted, the clauses would amend the Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426), referred to in the Bill as the "the PEC Regulations." The Regulations sit alongside the Data Protection Act 2018 (the 2018 Act) and the UK GDPR.

Background: current legal position

Relevant definitions

As defined by current regulation 2 of the PEC Regulations, the term "electronic communications" has an intentionally broad meaning to include new forms of messaging. It is defined as:

> [...] any text, voice, sound or image message sent over a public electronic communications network which can be stored in the network or the recipient's terminal equipment until it is collected by the recipient and includes messages sent using a short message service.

Direct marketing is defined in section 122(5) of the 2018 Act as:

> the communication (by whatever means) of advertising or marketing material which is directed to particular individuals.

This definition not only incudes direct advertising or marketing of a good or service but also material promoting the aims or ideas of not-for-profit organisations (eg a charity or political party campaigning for support or funds).

Genuine market research does not count as direct marketing. However, market research calls, where the caller is trying to sell goods or services or collect data to help it (or others) to contact people for marketing purposes in the future, is direct marketing.

Routine customer service messages do not count as direct marketing, for example, emailing existing customers to provide information they need about a current contract (such as delivery arrangements, changes to terms and conditions, or tariffs). According to the ICO, general branding, logos or straplines included in these electronic messages do not count as marketing. If, however, the messages include significant promotional material aimed at getting customers to buy additional products or services or to renew contracts that are coming to an end, they would count as direct marketing and the rules in the PEC Regulations would apply.

PEC Regulations

The current PEC Regulations give people specific privacy rights in relation to electronic communications, by restricting the way organisations can carry out unsolicited direct marketing (that is, direct marketing that has not specifically been asked for). There are specific rules on:

- Marketing by electronic means, including marketing calls, texts, emails, faxes, and picture or video message or by using an automated calling system. There are different rules for different types of communication.

  However, the PEC Regulations do not apply to other types of marketing, such as mailshots or online advertising, but the 2018 Act and the UK GDPR would apply, and if the online advertising used cookies or similar technologies, the provisions about cookies would also apply.[198]

- The use of cookies or similar technologies that track information about people accessing a website or other electronic service.

- Keeping public electronic communications services secure.

- Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID and call return), and directory listings.

Rules set out in the PEC Regulations apply and use the UK GDPR standard of consent (see below). This means that if an organisation sends electronic marketing or use cookies or similar technologies they must comply with both the PEC Regulations and the UK GDPR. There is some overlap, both aim to protect people's privacy, but there are some important differences. For example, the PEC Regulations will apply even if the organisation is not processing personal data.

The ICO is responsible for compliance with the e-marketing rules in the PEC Regulations and the lawful collection and use of personal data under the UK GDPR for direct marketing purposes. Enforcement methods currently available to the ICO include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner can also serve a monetary penalty

[198] "Cookies" or similar technologies track information about people accessing a website or other electronic service.

notice imposing a fine of up to £500,000 on the organisation or its directors. These powers are not mutually exclusive.

Where a company pays a subcontractor (eg a marketing agency) to do all its marketing, it remains responsible with the subcontractor for complying with the PEC Regulations. According to the ICO, if it is required to take enforcement action, it will usually take it against the company as the "instigator", although it might consider also act against a specialist subcontractor as well if they deliberately or persistently breach the rules.

Consent to direct marketing

Individuals (data subjects) have rights in relation to their personal data, including the right to object to their personal data being used for marketing purposes. The UK GDPR sets a high standard for consent, "specific consent" is required to send unsolicited direct marketing material.[199] In other words, giving consent involves the individual taking some form of clear positive action (for example, ticking an "opt in" box, clicking an icon, sending an email) to say they want to receive the direct marketing material. Pre-ticked opt-in boxes do not give valid consent. There is no set time limit for consent, how long it lasts will depend on the context, but the individual is entitled to withdraw their consent at any time.

The ICO has published Guidance on direct marketing (2018) (PDF) and Guidance on consent (undated).

The Bill

Clauses 79 to 86 are highly technical and, if enacted, would amend the PEC Regulations.

Direct marketing is defined in section 122(5) of the 2018 Act. The PEC Regulations draws its definition of direct marketing from the Data Protection Act 1998 (the 1998 Act). **Clause 81** of the Bill would not alter this definition but would place it directly into PEC Regulation 2(1) to improve the readability of the legislation-n. Other notable changes proposed in the Bill are summarised below.

Storing information in terminal equipment of a subscriber or user

The PEC Regulations sets out rules on the use of cookies[200] and similar tracking technologies and on the confidentiality of terminal equipment (eg computers, mobile phones, wearable technology, smart TVs and connected

[199] See Articles 4(11), (6(1)(a), 7, 8, and 9(2)(a)

[200] When a person visits a website a "cookie" is a small file of letters and numbers that is downloaded on to their terminal equipment. Cookies can do many things, for example, remembering a person's preferences, recording what they have put in their online shopping basket, and counting the number of people looking at a website.

devices, including the 'Internet of Things'[201]). The ICO is responsible for enforcing these rules.

Current regulation 6(1) prohibits an organisation from storing information or gaining access to information stored in the terminal equipment of an individual, unless the individual is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and the individual has given consent. An exception to the consent requirements exists where the cookie is "strictly necessary" for the provision of a service explicitly requested by the individual.

The Bill would extend the circumstances under which cookies or other technologies (e.g tracking pixels) could be used to store or access information on people's devices without their express consent. Specifically, **clause 79(2)(a)** would introduce the following exceptions to the consent requirement in regulation 6(1) of the PEC Regulations for certain purposes that are considered to present a "low risk" to people's privacy:

- Where the tracking technologies are used to collect information for statistical purposes with a view to making improvements to the service provided (**new paragraph (2A)**). In other words, "non-consent" use of cookies would be permissible if it were being deployed or the purposes of web analytics, although only if the information is not shared with any other person except for the purpose of enabling that other person to assist with making improvements to the service or website. As a further safeguard, the exception would only apply where the user is provided with clear and comprehensive information about the purpose and is given a simple and free means of objecting to the storage or access.[202]

- To enable the way an information society service ("ISS") appears or functions when displayed on a subscriber or user's device, to adapt to the preferences of that subscriber or user (eg their font preferences) (new **paragraph 2B(b)(i)**).

- To enable an enhancement of the appearance or functionality of an ISS when displayed on a user's device (new **paragraph 2B(b)(ii)**). This exception would apply only where the subscriber or user is provided with clear and comprehensive information about the purpose and is given

- To enable the installation of software updates on a subscriber or user's device that are necessary for security reasons (new **paragraph 2C**). This exemption would be subject to certain conditions, for example, users should be able to object to the software update and be able to remove or disable the update after it has taken effect.

[201] The "Internet of Things" is a term used to describe physical objects with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the internet or other communication networks.

[202] New paragraph (2A)(c)

- Where the sole purpose is to enable the geographical position of a subscriber or user to be ascertained so that assistance could be provided in response to the user or subscriber's emergency communication from their terminal equipment (new **paragraph 2D**).

In relation to cookies and similar technologies, key technical definitions in the PEC Regulations would be largely unchanged by the Bill. Some have questioned whether this a lost opportunity, the definitions are over two decades old and reflect an internet that was very different from today.[203] That said, two proposed changes should be noted:

- First, for the purposes of the Bill, a reference to an organisation storing information (or gaining access to information stored) in the device of a subscriber or user, would include a reference to the person instigating the storage or access.[204]

- Secondly, the Bill would insert new paragraph 6(b) into regulation 6 of the PEC Regulations, to clarify that a reference to "gaining access to information stored in the terminal equipment of a subscriber or user would include a reference to collecting or monitoring information automatically emitted by the terminal equipment" (so-called "emissions data").[205] This suggests that device and browser fingerprinting[206] would be covered by the Bill.

Significantly, **clause 79(3)** of the Bill would insert new regulations **6A** and **6B** into the PEC Regulations. Under new regulation 6A, the Secretary of State would have the power[207] to add further exceptions to the cookie consent requirements or omit or vary any existing exceptions.[208] Under new regulation 6B, the Secretary of State would have the power to make regulations prohibiting relevant organisations, (eg browser and device suppliers) from supplying "information technology" of a specified description unless it meets the requirements specified in the regulations.[209] The Bill's definition of "information technology" is deliberately broad and future-proofed to ensure there is sufficient technology available to enable subscribers or users to express their consent preferences.

Under new regulations 6A and 6B, before making any new regulations the Secretary of State would have to consult the Information Commissioner and

---

[203] The Data Protection and Digital Information Bill – an initial view, Mishcon de Reya, 19 July 2022 (accessed 13 March 2023)

[204] Clause 79(2)(d) would insert new paragraph 6(a) into regulation 6 of the PEC Regulations

[205] Clause 79(2)(d)

[206] "Device fingerprinting" is a technique that involves combining a set of information elements to uniquely identify a particular device.

[207] New regulation 6A(1)(a)

[208] New regulation 6A(1)(b) would enable the Secretary of State to make consequential, incidental or supplementary provisions to give effect to exceptions made by regulations made under these provisions.

[209] New regulation 6B(5) would enable the Secretary of State to make consequential, incidental or supplementary provisions amending the regulations made under this new power.

"such other persons as the Secretary of State considers appropriate". [210] Regulations would be subject to the affirmative resolution procedure.[211]

Unreceived communications

Part 4 of the Bill would extend the reach of the PEC Regulations in respect of nuisance calls. Specifically, **clause 80** would enable the Information Commissioner to investigate and act against organisations responsible for generating unsolicited direct marketing communications regardless of whether they are received[212] by the intended recipient.[213] This clause would also amend the definition of 'communication' in the PEC Regulations to make it clear it covers "transmitted" communications, such as texts and emails.[214]

Electronic mail: extending the "soft opt-in" rule

The term "soft opt-in" describes the rule about commercial organisations sending electronic marketing communications (eg emails or texts) to existing customers, using data they gathered when that customer bought or expressed interest in their products or services. There are certain criteria which needs to be met to rely on this rule. The rule only applies to existing customers, it does not apply to prospective customers or new contacts (eg from bought-in data lists). Marketing communications with an existing customer must be in relation to similar goods and services. The existing customer must also be offered a simple means of opting out of receiving further communications.

Currently, the soft opt-in rule does not apply to non-commercial promotions, for example, charity fundraising or political campaigning. However, if enacted, **clause 82(3)** of the Bill would add a new subsection (3A) to PEC regulation 22 to permit organisations which have charitable, political or non-commercial objectives to send electronic marketing communications for the purposes of furthering their objective. The following safeguards would apply:

- The recipient's contact details must be obtained from the individual "in the course of" that person expressing an interest or providing support for the objectives of the organisation.[215]

---

210 New regulation 6A(3) and new regulation 6B(6)

211 New regulation 6A(4) and new regulation 6B(7)

212 **Clause 80(2)** would amend the definition of "calls" in Regulation 2(1) of the PEC Regulations to make it clear it includes all calls, whether or not they connect with the intended recipient.

213 **Clause 80(3)** would insert new **paragraph (1A)** into Regulation 2 of the PEC Regulations to clarify the meaning of "recipient" in the context of calls or communication that are sent or generated but not received. It provides that in this context, a reference in the Regulation to a recipient should be taken to mean the "intended recipient".

214 Currently, regulation 2(1) of the PEC Regulations only refer to communications that are "exchanged or conveyed", which implies they need to reach their intended recipients.

215 New subsection (3A)(b)

- The individual must be given a simple way of opting out of receiving communications, both at the point their data was initially collected and at each subsequent communication.[216]

New duty to notify the Commissioner of unlawful direct marketing

Clause 85 of the Bill is significant. It would insert new direct marketing regulations 26A-C into the PEC Regulations which, in turn, would impose a **new duty** on public electronic communication service providers[217] and public communication network providers[218] to report to the Information Commissioner any "suspicious activity" relating to unlawful direct marketing within **28 days** of first becoming aware of such activity.[219]

The Information Commissioner would be required to publish guidance on what might constitute "reasonable" grounds for such suspicions [220] having first consulted with Ofcom, the telecoms companies, the Secretary of State and any other interested parties.[221] The Explanatory Notes give the example of a high number of calls originating within a very short space of time from the same number or from a small batch of numbers. "Phoenix companies" might also raise suspicions of unlawful activity, specifically, where a non-compliant company becomes insolvent and the director(s) then contact the service or network provider to set up a new business to continue operations. The Commissioner would be required to amend and update this guidance as and when necessary.[222]

If enacted, this new duty on service and network providers would be a significant development.[223] The Bill sets out the penalties for non-compliance, the circumstances in which the Commissioner could impose a fixed penalty of £1,000[224] on a service or network provider, and the procedures for issuing notices of intent to impose a fixed penalty.[225] The Commissioner would be required to refer to the published guidance before determining to issue a fixed

216 New subsection (3A)(c)

217 As defined in section 151 of the Communications Act 2003 as: "any electronic communications service that is provided so as to be available for use by members of the public".

218 As defined in section 151 of the Communications Act 2003 as: "an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public".

219 New regulation 26A(3)

220 New regulation 26C(1)

221 New regulation 26C(3)

222 New regulation 26C(2)

223 New regulations 26A(1), 26A(2), and 26A(4)

224 New regulations 26B(1) and (2), the Secretary of State could adjust the fixed monetary penalty amount by laying a statutory instrument in Parliament, subject to the affirmative resolution procedure (new regulations 26B(13) and (14)).

225 New regulations 26B(3) to (7)

penalty notice.[226] Service and network providers would have a right to appeal a fixed penalty.[227]

Enhancement of Commissioner's enforcement powers

Regulation 31 of the PEC Regulations apply the enforcement powers in the 1998 Act to the PEC Regulations, subject to certain modifications. These modifications are currently set out in Schedule 1 of the PEC Regulations. These provisions remain in force for the purposes of the PEC Regulations, even though the 2018 Act replaced the 1998 Act for most other purposes.

If enacted, **clause 86(5)** of the Bill would substitute current regulation 31 of the PEC Regulations with a new regulation that would make it clear that certain enforcement powers in Parts 5 to 7 of the 2018 Act would be applied to the PEC Regulations. Current Schedule 1 to the PEC Regulations would also be substituted with a new Schedule (set out in Schedule 10 of the Bill), which would make modifications to the enforcement provisions in the 2018 Act so that it could be applied to the PEC Regulations.[228]

Under current regulation 5A of the PEC Regulations, service providers have a specific obligation to notify the Information Commissioner about a 'personal data breach' and keep a log of those breaches. Regulation 5C sets out the penalties that can be imposed on service providers for failing to report security breaches. **Clause 86(4)** of the Bill would add new sub-paragraphs 13 and 14 to the end of regulation 5C to provide the Secretary of State with a power to amend the amount of the fixed monetary penalty that could be imposed.[229] Any changes would be made via regulations laid in Parliament and subject to the affirmative resolution procedure.

The application of certain powers in Parts 5 to 7 of the 2018 Act to the PEC Regulations (subject to the modifications in Schedule 10 of the Bill) would have a significant impact on its enforcement regime. In particular, the following should be noted:

- The Information Commissioner would have the power to impose information notices under section 142 of the 2018 Act on any person or communications provider.[230] The requested information to help the

[226] New regulation 26C(4)

[227] New regulation 26B(8)

[228] Clause 86(8)

[229] Currently, the fixed monetary penalty that can be imposed is £1000 or £800 if paid within 21 days of receipt of the notice of intent.

[230] If enacted, clause 86(6) and (7) would remove regulation 31A and regulation 31B of the PEC Regulations, which currently allow the Commissioner to impose "third party information notices" on communication providers to gather information held on electronic communications networks, or by electronic communications services, for investigating compliance with the regulations; and set out rights of appeal against the imposition of a notice. These provisions would be redundant if the powers contained in section 142 of the 2018 Act (and associated appeal rights) were applied to the PEC Regulations.

Commissioner determine whether the person has or is complying with the PEC Regulations.

- The Information Commissioner would have the power to issue assessment notices under section 146 of the 2018 Act,[231] interview notices, enforcement and penalty notices. The relevant rights of appeal for persons who wish to appeal against the imposition of such notices would also be available.

- Relevant criminal offences would be available, such as the offence in section 148 of the 2018 Act which is committed when a person deliberately frustrates an ICO investigation by destroying or falsifying information.

- PECR fines would be brought in line with the 2018 Act. If enacted, **Schedule 10** to the Bill (paragraph 18) would modify section 157 of the 2018 Act for the purposes of its application to the PEC Regulations. A modified section 157 would make provision about the maximum fines that could be imposed for infringements of a provision of the PEC Regulations or a failure to comply with an information notice, interview notice, assessment notice or an enforcement notice. Paragraph 18(b)(ii) would list the PEC Regulations for which a penalty notice could impose the higher maximum penalty in the event of an infringement. The higher maximum penalty would be £17,500,000 or (in the case of an undertaking) 4% of the undertaking's total annual worldwide turnover, whichever were higher.[232]

Infringement of the remaining PEC Regulations would be subject to the standard maximum penalty of £8,700,000 or (in the case of an undertaking) 2% of the undertaking's total annual worldwide turnover, whichever is higher.

6.2 Direct marketing for the purposes of democratic engagement

Background

Personal data has always played an important role in political campaigning. One of the key sources of personal data is the electoral register. Access to the electoral register is regulated and can only be used for certain purposes. This

[231] If enacted, **clause 86(2)** and **(3)** would omit paragraph 6 of regulation 5 and paragraph 5B of the PEC Regulations, both concerned with the Commissioner's powers to audit measures taken by public electronic communication service providers to safeguard the security of their services and inform certain parties of a personal data breach. These provisions would be redundant if the powers contained in section 146 of the 2018 Act were applied to the PEC Regulations.

[232] Infringement of the remaining PEFC Regulations would be subject to the standard maximum penalty of £8,700,000 or (in the case of an undertaking) 2% of the undertaking's total annual worldwide turnover, whichever were higher.

includes 'electoral purposes', and the right of candidates and parties to use the electoral register for election campaigning is protected in electoral law.

Parties, elected representatives and candidates also may have access to other personal data. This may be emails or telephone numbers they have collected while canvassing or campaigning more generally, or data they have purchased from other sources. Personal data collection must comply with GDPR and data protection requirements.[233]

The Data Protection Act 2018 makes clear that processing personal data for democratic engagement falls within the lawful 'public interest tasks' but organisations must also identify a separate legal basis elsewhere in the law which explains the nature and purposes of the processing.

If this data is then used to contact individuals for political campaigning, whoever is using the data is then subject to direct market rules.

The electoral register

There are two versions of the electoral register, the 'full' and 'open' registers. The full register lists everyone registered to vote. By contrast, individuals can opt out of appearing on the open register. Electors are asked at the time they register whether they wish to opt out of the open register and can do so at any time.

The open register is available for sale for any use. Access to the full register is regulated and can only be used for specific purposes. It is an offence to disclose details of someone who is on the full register and who is not on the open register.

The right of elected representatives and those standing for election to have access to the full electoral register is set out in electoral law. They have the right to request the full register for the area they represent, or where they are standing for election.[234] The information can be used for 'electoral purposes'. This is not defined in the legislation but is interpreted broadly as anything to do with the process of campaigning and getting elected, including fundraising.[235] Electors do not have a right to opt out of their full entry on the electoral register being used in this way.

Candidates at some elections, including UK Parliamentary elections, also have the right to send one piece of unsolicited mail to voters in the mail free of postal charges. This is why potential voters sometimes receive election leaflets from parties and candidates that they do not support. This is not a breach of data protection rules and is not considered to be direct marketing.

---

233 ICO Guidance for the use of personal data in political campaigning (online) (updated 21 February 2023) gives the key requirements on Collecting personal data

234 Library briefing CBP 1020, Supply and sale of the electoral register, has more detail on who has access to the electoral register

235 As above, section 3

Registered political parties, third-party campaigners and referendum campaigners registered with the Electoral Commission are also entitled to the full registers for electoral purposes.

Individuals and organisations entitled to the full register must still comply with data protection law. For example, they must ensure the data held is accurate and held securely.

Direct marketing

If political parties or other campaigners, including candidates, use personal data for unsolicited campaigning material, this is treated as direct marketing. It is therefore subject to the Privacy and Electronic Communications Regulations 2003, as amended, (PECR).

Because direct marketing covers communications 'directed to particular individuals', leaflet-drops and mailings which are unaddressed, or addressed merely to 'the occupier', do not fall within the statutory definition of direct marketing.

The information Commissioner's Office (ICO) guidance for those undertaking political campaigning notes the majority of political messaging directed to particular individuals is considered to be direct marketing. This is defined by section 122 of the 2018 Act as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals". The exception, as noted above, is where candidates have the right to send a free piece of campaign literature in the post. Other exceptions are administrative communications and genuine opinion research.[236]

Individuals must give consent for their personal details to be used for direct marketing at the point they are collected. It means that politicians, candidates, or parties must not call, email or text prospective voters for purposes such as campaigning or fundraising, unless they have obtained prior consent to use personal data for that purpose.

Commercial organisations are allowed to use the so-called 'soft opt-in' in relation to personal data used for direct marketing. This is where commercial organisations can send electronic marketing communications to a person without consent if their contact details were collected during the sale of a product or service, or negotiations of a sale. The communication must be in relation to similar goods and services and the person must also be offered a simple means of opting out of receiving further communications.[237]

Non-commercial organisations cannot use 'soft opt-in'.

---

[236] ICO Guidance for the use of personal data in political campaigning explains what constitutes opinion research and gives examples of when opinion research can be considered direct marketing, Political campaigning – opinion research and direct marketing

[237] Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), p78

DCMS consultation on data reform

In its September 2021 consultation on data reform, the DCMS asked about the use personal data for the purposes of democratic engagement:

- whether communications from political parties which promote aims and ideals should continue to be treated as direct marketing for the purposes of PECR.
- if so, whether to extend the 'soft opt-in' to non-commercial organisations.
- whether existing UK GDPR and data protection requirements impede democratic engagement.[238]

Direct marketing

The consultation noted that it was case law that had determined communications from political parties should be classified as direct marketing for the purposes of PECR.[239]

When the then Labour Government consulted on transposing the European Directive on privacy and electronic communications (2002/58/EC) into UK law by PECR, the emphasis was on commercial organisations. The regulatory impact assessment prepared by the Department of Trade and Industry referred to consent to "unsolicited commercial e-mail and SMS."[240]

Political parties were subsequently brought under the rules following a ruling by an Information Tribunal. In advance of the 2005 General Election, the then Information Commissioner issued guidance on political campaigning and in his view the PECR rules extended to political parties. Several parties were using unsolicited automated telephone call to contact voters (covered by rule 19 of PECR). The SNP were issued with an enforcement notice, which it appealed. The Information Tribunal dismissed the appeal and ruled the enforcement notice was legally issued and political parties were subject to direct marketing rules in PECR.

A Conservative Party submission to the Lords Democracy and Digital Technologies Committee investigation on the impact of digital technologies on democracy said of the tribunal decision, "This case has never been tested by the higher courts, and never been ratified or agreed by Parliament."[241] The Party also questioned the rationale that if political parties were covered by PECR then why were they not able to use 'soft opt-in' direct marketing.

238 DCMS, Data: A new direction (PDF)[online], September 2021, section 2.5

239 As above, p83

240 DTI, Regulatory Impact Assessment (PDF) [online], Privacy and Electronic Communications (EC Directive) Regulations 2003, Regulation 22, p5-6

241 Written evidence ZDA0106 (DAD106), Democracy and Digital Technologies Committee, Conservative Party, June 2020

Most respondents to the consultation agreed that political communications should be covered by PECR's rules but there were mixed views on extending 'soft opt-in' to non-commercial organisations. The Government decided to consider further whether political parties should be included within the PECR rules but would extend 'soft opt-in'. It said it would introduce a regulation-making power so that Parliament can make exceptions to the direct marketing rules in the future if necessary.[242]

The Bill

Clause 82 of the Bill would extend the 'soft opt-in' provisions available to allow non-commercial organisations to email without consent for the purpose of furthering a charitable, political or other non-commercial objective. Contact details of the recipient of the electronic mail must have been collected in the course of the recipient expressing an interest in the organisation's objectives. A person must also be offered a simple means of opting out of receiving further communications.

Clause 83 would give the Secretary of state the power to make these regulations to exempt democratic engagement carried out by registered political parties, candidates and other campaigners from PECR rules at a later date. Any regulations made under this power can only be made after the Information Commissioner, and "such other persons as the Secretary of State considers appropriate" have been consulted. They would be subject to the affirmative procedure.

Clause 84 further defines candidates and campaigners in clause 83. This includes referendum campaigners and campaigners in a recall petition.

6.3 Sharing data for public service delivery

Background

Section 35 of the Digital Economy Act 2017 (the 2017 Act) enables the public authorities listed in Schedule 4 to the Act to share information for:

- the improvement or targeting of a public service provided to individuals or households, or
- the facilitation of the provision of a benefit (whether or not financial) to individuals or households.[243]

The purpose of the sharing must also be to improve the improvement of the well-being of individuals or households including:

[242] DCMS, Data: a new direction - government response to consultation, June 2022, 2.5 Use of personal data for the purposes of democratic engagement

[243] Section 35(9) of the 2017 Act

- their physical and mental health and emotional well-being,
- the contribution made by them to society, and
- their social and economic well-being.[244]

Further detail on this area is available in:

- Cabinet Office/DCMS/Home Office, Code of Practice for public authorities disclosing information under Chapters 1, 3 and 4 (Public Service Delivery, Debt and Fraud) of Part 5 of the Digital Economy Act 2017, February 2020 (accessed 10 March 2023).
- ICO, Data sharing across the public sector: the Digital Economy Act codes, October 2021.

The Bill

Clause 92 of the Bill would amend section 35 of the 2017 Act to also enable the sharing of information to improve the delivery of public services to businesses. The purpose would be to assist undertakings in connection with any trade, business, or charitable purpose.

6.4 Trust services

Background

"Trust services" include services specifically relating to electronic signatures, electronic seals, timestamps, electronic delivery services, and website authentication.

The eIDAS Regulation (the Regulation)[245] sets the legal framework and specifications for trust service products and services in the UK.[246] The Regulation requires that trust services meet standards and technical specifications to allow for interoperability across the UK economy. An ICO guide gives this overview:

- The UK eIDAS Regulations set out rules for UK trust services and establishes a legal framework for the provision and effect of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

244 Section 35(11) of the 2017 Act

245 Regulation (EU) No 910/2014 (accessed 13 March 2023)

246 The eIDAS Regulation was retained by the European Union (Withdrawal) Act 2018, and amended by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/89)

- Trust services increase confidence in the use of electronic transactions through mechanisms such as verifying the identity of individuals and businesses online and verifying the authenticity of electronic data e.g. documents.

- The UK eIDAS Regulations are an amended form of the EU eIDAS Regulation and retain many aspects of the EU regulation but are tailored for use within the UK.

- Although the UK eIDAS Regulations allows the legal effect of EU eIDAS qualified services to continue to be recognised and used in the UK, no reciprocal agreement currently exists. This means UK eIDAS Regulation qualified trust services are not automatically recognised and accepted as equivalent in the EU.

- The UK Regulation includes no provisions relating to electronic identification schemes and excludes chapter II of the EU eIDAS regulation.

- The ICO is the supervisory body for UK trust service providers. We can carry out audits, grant qualified' status, and take enforcement action.[247]

The Bill

Clause 88 would add a new Article 24B to the Regulation. The Explanatory Notes explain that this would allow for the recognition of conformity assessment reports issued by the national accreditation body of an EU member state. It would also provide that these reports could be used to grant a trust service provider qualified status under Article 21 of the Regulation, and for the purposes of regular auditing requirements (under Article 20(1)).[248]

Clause 89 would enable the Secretary of State, through regulations subject to the negative procedure, to amend or revoke Article 24A of the Regulation, should the continued unilateral recognition of EU qualified trust services no longer be appropriate.

Clause 90 would insert a new Article 45A into the Regulation. This would give the Secretary of State the power to make regulations, subject to the negative procedure, to recognise and give legal effect to trust service products provided by trust service providers established outside the UK.

Clause 90 would also insert a new Article 45B into the Regulation. The Explanatory Notes explain its purpose:

> ...Existing Articles 27 and 37 of the eIDAS Regulation provide that where public sector bodies require an advanced signature or seal for the use of an online public service, they must recognise electronic signatures and seals which meet advanced standards and additional technical requirements under Commission Implementing Decision 2015/1506. Likewise, where public sector bodies require an advanced signature or seal based on a qualified certificate, they must accept a qualified signature or seal which complies with Commission Implementing Decision 2015/1506. New Article 45B provides the Secretary of State with the power by regulations to recognise, for the use of online public services, specified electronic seals and signatures provided by trust service

247 ICO, What is the eIDAS Regulation? [online] (accessed 13 March 2023)

248 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 612

providers established outside the UK, as equivalent to electronic seals and signatures under Articles 27(1), 27(2), 37(1) and 37(2) of the eIDAS Regulation which comply with Implementing Decision 2015/1506.[249]

6.5 Registers of births and deaths

Background

It is a legal requirement to register the birth, including still-birth, of every child in England and Wales and the death of every person in England or Wales. Information about the current procedure for registering births and deaths is provided at:

- Register a birth: Overview - GOV.UK (www.gov.uk);
- Register a death - GOV.UK (www.gov.uk);
- the Explanatory Memorandum (PDF) to the Births and Deaths Registration (Electronic Communications and Electronic Storage) Order 2021.[250]

Provisions in the Coronavirus Act 2020, which enabled deaths to be registered by telephone, have now expired.[251] Regulations, which came onto effect in December 2021,[252] continue to allow the electronic transfer of documentation, but it is again necessary to register a death in person.

The law also sets out what must be done with the records and registers once registration has taken place.[253] The current legislation provides for a paper-based system and is based on legislation that has been in place since the nineteenth century.

Since 2009, the registers of births and deaths have been kept in both paper and electronic form.[254]

249 As above, para 616

250 SI 2021/1231

251 Section 18, which introduced Schedule 13 of the Coronavirus Act 2020, modified procedures in relation to death registration, including enabling those required to give information about a death to do so by telephone or other means instead of in person.

252 Births and Deaths Registration (Electronic Communications and Electronic Storage) Order 2021 (SI 2021/1231)

253 Births and Deaths Registration Act 1953

254 See Registration of Births and Deaths (Electronic Communications and Electronic Storage) Order 2006 SI 2006/2809

The Bill

Overview

Clauses 94 to 98 and **Schedule 11** would provide for the reform of the process of registering births and deaths in England and Wales. They would remove the requirement for paper registers to be held and stored securely in each registration district and enable all births and deaths in England and Wales to be registered electronically.

Clauses in the Bill

Clause 94 would amend the Births and Deaths Registration Act 1953 (BDRA) to enable the Registrar General to determine the form of registers of live-births, still-births and deaths. This would allow the duplication of processes to be removed (that is, registration both in a paper register and in an electronic register, as at present).[255] The Explanatory Notes state that it would no longer be necessary to keep paper registers secure in a safe.[256]

The Registrar General would be able to require that the registers be kept in a form which allows the Registrar General and the superintendent registrar to have immediate access to entries of births and deaths; and the Registrar General to have immediate access to entries of still-births. The Registrar General and the superintendent registrar (where relevant), as well as the registrar, would then be deemed to hold the registered information in connection with their functions.

The Registrar General might provide anything they consider appropriate for the purpose of keeping these registers in the form required and would have a duty to maintain anything so provided. This might include, for example, "providing registrars with the system needed to register births and deaths".[257] The Registrar General would also be obliged to provide the forms required to produce certified copies of entries in the registers (for example, a birth or death certificate).

Clause 94 would also repeal the provisions in the BDRA which, at present, require the registrar and superintendent registrar to make quarterly returns and set out how paper birth and death registers need to be stored.

Clause 95 would insert a new section into the Registration Service Act 1953 to require local authorities (subject to the provisions of local scheme arrangements)[258] to provide and maintain the equipment and facilities which

255 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 629

256 As above

257 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 632

258 Local scheme arrangements are arrangements for each registration district made under section 14 of the Registration Service Act 1953 (Explanatory Notes to the Registers of Births and Deaths Bill, para 20, (PDF) footnote 2)

the Registrar General reasonably considers to be necessary for a superintendent registrar or registrar to carry out their functions.

Clause 96 would amend the BDRA to deal with the requirement to sign the register. Where registration was effected otherwise than in hard copy, the Minister would have power to make regulations to provide that:

- a person's duty to sign the register is instead a duty to comply with specified requirements; and
- a person who complies with those requirements is to be treated as having signed the register at that time, and, where required, to have done so in the presence of the registrar.

Regulations might, among other things, provide for a person to sign something other than the register, and require a person to provide specified evidence of identity.

Regulations would be subject to the affirmative resolution procedure, requiring the approval of both Houses of Parliament to become law.

Clause 97 specifies that there would be no change to the existing requirement for superintendent registrars to keep with the records of their office any registers of live births or deaths which are in their custody immediately before Clause 94 comes into force. The Registrar General would also be required to continue to keep any certified copies (quarterly returns) and any registers of still-births which are in their possession when Clause 94 takes effect.

Clause 97 would also make further provision about the treatment of existing registers and records, including:

- Registrars would be required to send any unfilled paper registers of births and deaths in their possession to the superintendent registrar to be kept with the records of the office.
- Registrars would also be required to send any unfilled paper registers of still-births in their possession to the Registrar General, to be kept in the General Register Office as the Registrar General thinks fit.
- The Registrar General would be able to dispose of certified copies of entries in any register of still-births forwarded to the Registrar General, or any information contained in those entries which is held by the Registrar General in electronic form by virtue of section 27 of the BDRA.

- Subsection (5) specifies how copies of birth and death records held in a form other than hard copy form, in the period from 1 July 2009 to the day before Clause 94 comes into effect, would be treated. [259]

Clause 98 would bring into effect **Schedule 11** which contains minor and consequential amendments to the BDRA and other primary legislation.

Previous Private Members' Bills

The provisions in the Bill on the registration of births and deaths in England and Wales are substantially the same as those in two previous Private Members' Bills which did not complete their passage through Parliament:

- the Registers of Births and Deaths Bill 2019-21 (PDF) was presented to Parliament by Andrew Mitchell (Conservative) on 5 February 2020 as Bill 25 of 2019-21 (the 2020 Bill). This Bill had its second reading on 16 October 2020 and a single sitting in Public Bill Committee on 27 January 2021, when it was reported without amendment. The Bill did not progress any further. Information is provided on the Bill page on the Parliament website.

- The Registers of Births and Deaths Bill 2021-22 (PDF, the 2021 Bill) was presented to Parliament by Saqib Bhatti (Conservative) on 21 June 2021, as Bill 34 of 2021-22. A debate on second reading on 26 November 2021 was not completed,[260] and the Bill made no further progress.

The Home Office prepared explanatory notes to each of these Bills, with the consent of the Members in charge.

In second reading debate on the 2020 Bill, the Government and Opposition expressed their support.[261] Kevin Foster, who was then Parliamentary Under-Secretary (Home Office), spoke of the existing electronic register which had been used by registrars to register births and deaths since 2009 in parallel with the paper registers. However, he said, the current legislation requires a paper record of every event to be kept, resulting in a duplication of effort for registrars and this could be addressed only through primary legislation.[262]

In Public Bill Committee, Tom Pursglove, who was then Assistant Whip, said the 2020 Bill would "move the registration of births and deaths into the 21st century".[263] He considered the Covid-19 pandemic had "clearly highlighted the limitations and inflexibility of the now outdated primary

259 See Explanatory Notes to the Data Protection and Digital Information (No 2) Bill, (PDF), para 646
260 HC Deb 26 November 2021 cc630-650
261 HC Deb 16 October 2020 c719 and cc713-4
262 HC Deb 16 October 2020 c719
263 PBC Deb 27 January 2021 c9

legislation" and said the 2020 Bill would pave the way for the introduction of online registration:

> There is a need to be able to offer more flexibility in how births and deaths are registered by removing the requirement for face-to-face registration. The Bill removes the requirement for the signing of a birth or death register by an informant in the presence of a registrar if specified requirements are met. That paves the way for the introduction of online registration in which informants would be able to register an event online at a time to suit themselves from the comfort of their own home. That will provide more choice and convenience for informants, particularly in difficult and upsetting times such as when registering a death. However, the provision to attend personally at the register office will remain if that is the informant's preferred option. The current legislation is restrictive and does not reflect modern society.[264]

Another Library briefing paper, which deals with the 2021 Bill, includes background and further information about the debate on the 2020 Bill.[265]

6.6 Health and social care

Clause 99 would make provision about information technology and information standards for health and adult social care in England. It would give effect to Schedule 12, which would amend Part 9 of the Health and Social Care Act 2012 (HSCA 2012). The clause is unchanged from the Bill that was introduced in July 2022.

The provisions would ensure that certain information standards within the health and social care sector can be extended to IT providers dealing with patient data.

The Government believe current legislative provisions (under the HSCA 2012, as amended) are not sufficient to ensure IT products used by the health and care sector comply with relevant information standards, particularly those in relation to system interoperability and data sharing. The Government has said that, in the health sector, currently service users and their care teams cannot easily access or share, in real time, all the health and social care information that is relevant to their care.[266] According to the Government:

> 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.[267]

The Explanatory Notes to the Bill (PDF) state:

---

264 PBC Deb 27 January 2021 c9

265 Commons Library analysis of Registers of Births and Deaths Bill 2021-22 - House of Commons Library (parliament.uk)

266 Impact Assessment on the Data Protection and Digital Information Bill (PDF)[online], para 38

267 As above

> 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 (either directly or via professional regulation), this would be insufficient to bring the wholesale change to the supplier market that is needed. This is because the legislation does not concern the providers of the IT on which the processing relies and who can ensure that all information technology supplied meets relevant technical requirements.[268]

The Government says it is the intention of the Bill to remedy this by requiring IT suppliers of products and services to the health and care system in England "to meet specified open data architecture standards to improve patient outcomes".[269]

The Explanatory Notes set out that these provisions of the Bill may result in small costs to the health and adult social care system which include, but are not limited to:

- the imposition of new information standards on IT providers supplying IT to the health and social care sector, including communications to existing IT providers and administration associated with reviewing current contracts or entering new contracts;
- the establishment and operation of a compliance function to monitor compliance with information standards by IT providers, including data collection where required;
- the establishment and operation of an accreditation scheme.[270]

Further information on potential costs and impacts can be found in the Government's Impact Assessment (PDF), and related comment from the Regulatory Policy Committee.[271]

The Explanatory Notes say that the provisions apply to persons involved in services so far as they are used or intended for use in connection with health care or adult social care in England, and as such no Legislative Consent Motion is required from the devolved governments.[272]

268 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill, (PDF), para 69
269 Impact Assessment on the Data Protection and Digital Information Bill (PDF), para 38
270 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 870
271 Regulatory Policy Committee, RPC-DCMS-5180(1) (PDF) [online], 7 July 2022
272 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 98

7 Regulation and oversight

Part 5 of the Bill would make changes to the regulation and oversight of biometrics, closed circuit television (CCTV) and the National DNA Database.

7.1 Biometrics

Background

The Protection of Freedoms Act 2012 (the 2012 Act) introduced two independent commissioners to oversee police use of biometrics (the Commissioner for the Retention and Use of Biometric Material "Biometrics Commissioner") and police and local authority use of overt surveillance (the Surveillance Camera Commissioner), and a Surveillance Camera Code of Practice. Under the Data Protection Act 2018, the Information Commissioner provides independent oversight of all controllers' use of all personal data. This includes the use of biometrics and surveillance cameras.

The Government's September 2021 consultation on data protection reform sought views on simplifying the oversight framework for police use of biometrics, and police and local authority overt use of surveillance cameras. The consultation claimed the current framework was "crowded and confusing":

> ...The Biometrics Commissioner covers police use of DNA samples, DNS profiles and fingerprints, and the Surveillance Camera Commissioner covers all use of surveillance cameras by specified public authorities (including 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.
>
> The government recently simplified these arrangements by appointing one person to take on what were previously the part-time roles of Biometrics Commissioner and Surveillance Camera Commissioner. **The government will explore the potential for further simplifying the oversight framework by absorbing the functions of those commissioner roles into the ICO, which should bring benefits to data controllers and the public with a single route for advice, guidance and redress.**[273]

In its June 2022 response to the consultation, the Government said most respondents were "supportive of simplification".[274] However there was some

[273] DCMS, Data: a new direction (PDF), 10 September 2021, p141, emphasis in original

[274] DCMS, Data: a new direction - government response to consultation [online], 17 June 2022, section 5.8

disagreement over the proposal to absorb the functions of the Biometrics and Surveillance Camera Commissioner into the ICO:

> Some [respondents] said that the ICO might deprioritise oversight, given the breadth of its regulatory scope. Others argued that it would be inappropriate to transfer to the ICO, as a regulator, the quasi-judicial functions of the Biometrics Commissioner, who reviews applications from the police to retain biometrics in very limited circumstances where people have not been convicted.[275]

In its response, the Government said it would simplify the oversight framework for biometrics but would not transfer the Biometrics Commissioner's functions to the ICO. It would instead consider transferring these functions to the Investigatory Powers Commissioner, "acknowledging the relevant expertise they can provide in relation to national security".[276]

The Bill

Clause 104 of the Bill would amend section 20 of the 2012 Act to abolish the office of the Biometrics Commissioner and transfer its casework functions to the Investigatory Powers Commissioner. According to the Bill's Explanatory Notes, this would "reduce duplication and simplify oversight of the police use of biometrics".[277] The Information Commissioner would continue to provide independent oversight of the use of biometrics by all bodies, including the police. The Bill's Explanatory Notes give further detail on the changes that clause 104 would introduce.[278]

7.2 CCTV

Background

Part 2 Chapter 1 of the 2012 Act introduced a requirement for the Home Secretary to prepare a code of practice containing guidance on surveillance camera systems (the Surveillance Camera Code), including Closed Circuit Television (CCTV) and Automatic Number Plate Recognition (ANPR) systems. Under section 33(5) of the Act, local authorities, police and crime commissioners and chief constables must have regard to the Code. Other organisations can voluntarily adhere to the Code. The Act introduced a requirement for the Home Secretary to appoint a Surveillance Camera Commissioner to report on compliance with the Code.

275 As above

276 As above

277 Explanatory Notes to the Data Protection and Digital Information (No 2) Bill (PDF), para 665

278 As above, paras 664-71

The Bill

Clause 105(1) would abolish the office of Surveillance Camera Commissioner. **Clause 105(2)** would repeal Part 2 Chapter 1 of the 2012 Act to remove the requirement for a Surveillance Camera Code. The Bill's Explanatory Notes state that the Information Commissioner would continue to provide independent oversight and regulation of this area, without duplication by the Surveillance Camera Code and Commissioner:

> ...The Information Commissioner already has oversight of the use of personal data under the Data Protection Act 2018, including data captured via surveillance camera systems, by all controllers, including the police and local authorities. The Information Commissioner's Office has also published guidance on the use of such systems. This means that the Information Commissioner will continue to provide independent oversight and regulation of this area, without duplication by the Surveillance Camera Code and Commissioner, making it easier for the police, local authorities and the public to understand and comply with any requirements.[279]

7.3 National DNA Database

Background

Section 24 of the 2012 Act inserted section 63AB into the Police and Criminal Evidence Act 1984 (PACE). This introduced the National DNA Database Strategy Board to oversee the operation of the National DNA Database. This requirement is being delivered through the Forensic Information Databases Strategy Board (FIND-SB).

The Bill

Clause 106 would amend section 63AB of PACE by increasing the scope of the statutory board to also provide oversight of the national fingerprint database (referred to as IDENT1). This would bring the legislation up to date with the latest governance rules for the FIND-SB, which added oversight of the national fingerprint database to the Board's terms of reference.[280]

Clause 106 would also introduce a new power, through regulations subject to the affirmative procedure, for the Secretary of State to change the databases the FIND-SB oversees by adding or removing a biometric database used for policing purposes. The Bill's Explanatory Notes state the new power is intended to enable flexibility in the Board's remit given the pace of technological change and the need for clear and consistent oversight. To support policing to meet the requirements of the Data Protection Act and

[279] As above, para 673
[280] As above, para 675

PACE, the FIND-SB would produce codes of practice on the destruction of biometric material and erasure of this data from a database.[281]

[281] As above, para 676

The House of Commons Library is a research and information service based in the UK Parliament. Our impartial analysis, statistical research and resources help MPs and their staff scrutinise legislation, develop policy, and support constituents.

Our published material is available to everyone on commonslibrary.parliament.uk.

Get our latest research delivered straight to your inbox. Subscribe at commonslibrary.parliament.uk/subscribe or scan the code below:

commonslibrary.parliament.uk

@commonslibrary