LIBRARY BRIEFING

HOUSE OF LORDS

HL Bill 40 of 2024–25

# Data (Use and Access) Bill [HL]

**Author:** Nicola Newson
**Date published:** 1 November 2024

The Data (Use and Access) Bill [HL] is scheduled to have its second reading in the House of Lords on 19 November 2024. The government has said the bill has three core objectives: to grow the economy, improve public services and make people's lives easier. It would seek to achieve those aims through measures such as:

- paving the way for the 'smart data' model to be used in more sectors
- establishing a trust framework for digital verification services
- placing the national underground asset register on a statutory footing
- enabling births and deaths to be registered electronically
- applying information standards to IT services within health and social care to make patients' data more easily transferrable across the NHS
- removing the requirement for police to log a justification each time they access someone's personal data

The bill would deliver on Labour's manifesto commitment to give coroners more powers to access information held by technology companies after a child's death. It would make changes to the UK's data protection legislation, for example by creating a new lawful ground for processing personal data of "recognised legitimate interests" and expanding the lawful base for the use of solely automated decision-making. The bill would change the governance model of the Information Commissioner's Office (ICO).

The bill contains many provisions that are similar or identical to ones in the Conservatives' Data Protection and Digital Information Bill that failed to complete all its stages before the general election. However, some provisions have been removed, including those which would have allowed the government to oversee the ICO's strategic priorities and make recommendations on ICO codes, and which would have modified the current requirements for data protection officers and keeping records of personal data processing. Labour's bill contains some new provisions such as a regulation-making power to create a framework allowing researchers access to data relating to online safety held by tech companies.

## Table of Contents

# 1. Background

## 1.1 Labour Party proposals on data

Labour's manifesto for the 2024 general election described harnessing new technology "to put the country back in the service of working people" as one of the hallmarks of its plans for mission-driven government.[1] It also said that the "revolution taking place in data and life sciences has the potential to transform our nation's healthcare".[2] In terms of specific pledges relating to data, the manifesto said a Labour government would:

- create a National Data Library to bring together existing research programmes and help deliver data-driven public services, whilst maintaining strong safeguards and ensuring all of the public benefit[3]
- create the conditions to support innovation and growth in the financial services sector, through supporting new technology, including open banking and open finance[4]
- give coroners more powers to access information held by technology companies after a child's death[5]

Plans for a data bill were not explicitly mentioned in the King's Speech in July 2024. However, the background briefing notes published alongside the King's Speech said the government would introduce a 'Digital Information and Smart Data Bill'.[6] The government set out three aims for the bill:

- to harness data for economic growth
- to support a modern digital government
- to improve people's lives

---

[1] Labour Party, 'Labour Party manifesto 2024', June 2024, p 12.
[2] As above, p 96.
[3] As above, p 35.
[4] As above, p 28.
[5] As above, p 103.
[6] Prime Minister's Office, 'The King's Speech 2024', 17 July 2024, pp 39–41.

It said this would start delivering on Labour's commitment to "better serve the British public through science and technology". The government said the bill would harness the power of data for economic growth by giving a statutory footing to digital verification services, a national underground asset register and smart data schemes for sharing customers' data on request. It said these schemes would "accelerate innovation, investment and productivity across the UK". In addition, it argued the bill would "improve people's lives and life chances" and "enable more and better digital public services" by enabling it to share data about businesses that use public services, register births and deaths electronically and apply information standards to IT suppliers in the health and social care system. The government also made a commitment that the bill would amend data laws to help scientists make better use of data for research. It also promised that the bill would ensure the public's data was well protected by "modernising and strengthening" the Information Commissioner's Office (ICO).

## 1.2 Introduction of the bill

The Data (Use and Access) Bill [HL] was introduced in the House of Lords on 23 October 2024.[7] The government said measures in the bill would be central to delivering three of the prime minister's five missions, "kickstarting economic growth, taking back our streets and building an NHS fit for the future".[8] It contended that the bill would "unlock the secure and effective use of data for the public interest, without adding pressures to the country's finances". It estimated the bill would "harness the enormous power of data to boost the UK economy by £10bn". This figure represents the net present social value of all the reforms across a 10-year period, taking into account estimated costs and benefits.[9]

The government published various documents alongside the bill:

- 'Explanatory notes', 24 October 2024
- 'Delegated powers memorandum', 24 October 2024
- 'Impact assessment: Data (Use and Access) Bill', 23 October 2024
- Additional impact assessments on particular aspects of the bill: 'Impact assessment: Data (Use and Access) Bill—legislation to deliver the national

[7] The title—Data (Use and Access) Bill—differs from the one initially given in the King's Speech background briefing notes—Digital Information and Smart Data Bill.

[8] Department for Science, Innovation and Technology et al, 'New data laws unveiled to improve public services and boost UK economy by £10 billion', 24 October 2024.

[9] Explanatory notes, p 143.

underground asset register'; 'Impact assessment: Regulatory powers for smart data'; 'Impact assessment: Researchers' access to data'; 'Impact assessment: Data (Use and Access) Bill—open data architecture information standards'; and 'De minimis assessment: Powers for digital identity and attributes initiatives', all 23 October 2024

- 'Data (Use and Access) Bill: European Convention on Human Rights memorandum', 24 October 2024
- Three factsheets on how the bill relates to Labour's missions: 'Data (Use and Access) Bill factsheet: Growing the economy'; 'Data (Use and Access) Bill factsheet: Improving public services'; and 'Data (Use and Access) Bill factsheet: Making people's lives easier', all 24 October 2024

### 1.3 Comparison with Data Protection and Digital Information Bill

Much of the bill is similar or identical to provision included in the Data Protection and Digital Information Bill under the Conservative government (although the parts of the bill are presented in a different order).

The Conservative government originally introduced a Data Protection and Digital Information Bill in the House of Commons in July 2022, under Boris Johnson's premiership.[10] However, following the election of Liz Truss as the new party leader, the government announced on 5 September 2022 that second reading of the bill would not take place as scheduled, to give ministers time to consider the legislation further.[11] In March 2023, Michelle Donelan, secretary of state for science, innovation and technology in Rishi Sunak's government, announced the government was introducing a new Data Protection and Digital Information (No. 2) Bill, superseding the previous bill.[12] She said the new bill followed "a detailed codesign process with industry, business, privacy and consumer groups" to determine how it could improve on the previous version.

The Data Protection and Digital Information (No. 2) Bill completed its second reading and committee stage in the House of Commons in the 2022–23 parliamentary session. It was subject to a carry-over motion and was reintroduced in the 2023–24 parliamentary session as the Data Protection and Digital Information Bill. It completed its House of Commons

[10] UK Parliament, 'Data Protection and Digital Information Bill 2022–23', last updated 5 May 2023.
[11] HC Hansard, 5 September 2022, col 25.
[12] House of Commons, 'Written statement: Data Protection and Digital Information (No. 2) Bill (HCWS617)', 8 March 2023.

stages in November 2023, and had completed its committee stage in the House of Lords by April 2024. However, it did not progress any further before Parliament was dissolved for the 2024 general election. This bill was amended considerably during the parliamentary stages it completed: 65 government amendments were made at House of Commons committee stage, 266 government amendments were made at House of Commons report stage, and 62 government amendments were made at House of Lords committee stage.

Further information about the Conservatives' bill—including the consultations that preceded it and the changes it underwent as it progressed through Parliament—is available in the following briefings:

- House of Commons Library, 'The Data Protection and Digital Information Bill 2022–23', 14 March 2023
- House of Commons Library, 'The Data Protection and Digital Information (No. 2) Bill 2022–23', 28 March 2023
- House of Commons Library, 'The Data Protection and Digital Information Bill: Progress of the bill', 18 December 2023
- House of Lords Library, 'Data Protection and Digital Information Bill: HL Bill 30 of 2023–24', 13 December 2023

Elements that were in the Conservative bill by the time it completed its Lords committee stage, but which have not been included in Labour's bill, are as follows:

- **Information relating to an identifiable living individual**: The Conservative bill would have created a test to help organisations understand whether the data that they were processing was personal or anonymous. Personal data is subject to data protection rules, but anonymous data is not.
- **Democratic engagement**: The Conservative bill would have redefined the term "democratic engagement" to provide what the Conservative government said was "a fuller definition of what constitutes 'democratic engagement activities'".[13] "Democratic engagement" is one of the lawful bases for processing personal data.[14] The Conservative bill would also have included "democratic engagement" as a "recognised legitimate interest" on which data

[13] HC Hansard, 29 November 2023, col 877.

[14] For further information about lawful bases for personal data processing, see: Information Commissioner's Office, 'Lawful bases', accessed on 29 October 2024.

controllers outside public authorities could rely as a lawful ground for the processing of personal data. It would have allowed registered political parties and elected representatives to process personal data that revealed someone's political opinions if it was necessary for democratic engagement activities. It would also have allowed candidates for election, permitted participants in a referendum and accredited campaigners in a recall election to process personal data revealing people's political opinions in more tightly defined circumstances, namely "when necessary" for a campaign but not for more broadly defined "democratic engagement activities".

- **Direct marketing**: Currently individuals must give consent for their personal details to be used for direct marketing at the point their personal data is collected. However, commercial organisations are allowed to use a 'soft opt-in', where they can send electronic marketing communications to a person without their consent if their details were collected during the sale of a product or service. The Conservative bill would have extended the soft opt-in to organisations with charitable, political or non-commercial objectives when sending electronic marketing communications for the purposes of furthering their objective.
- **Direct marketing and democratic engagement**: The Conservative bill would have enabled the secretary of state to make regulations to exempt certain types of communication from the direct marketing provisions in the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the PEC Regulations). The regulations could have exempted the communications of elected representatives and registered political parties if they were for the purposes of democratic engagement activities (or, in the case of a registered political party, election activities). The regulations could have exempted communications from candidates, permitted participants in a referendum or accredited campaigners in a recall petition if the communications were for the purposes of their campaigning.
- **Unlawful direct marketing**: The Conservative bill would have placed a duty on communications service providers and network providers to report suspicious activity relating to unlawful direct marketing to the information commissioner. It would have set penalties for non-compliance and required the information commissioner to publish guidance on what might constitute reasonable suspicions.
- **Vexatious requests**: Current legislation allows data controllers and the information commissioner to charge a reasonable fee for, or refuse to act on, a request that is "manifestly unfounded or excessive".[15] The Conservative bill

[15] UK General Data Protection Regulation, article 12; and Data Protection Act 2018, ss 53 and 135.

would have changed this to "vexatious or excessive".[16] The Labour bill would retain the current wording of "manifestly unfounded or excessive".

- **Requirement for UK-based representative**: The Conservative bill would have removed the requirement for overseas data controllers subject to the UK GDPR to appoint a UK-based representative.
- **Senior responsible individual**: The Conservative bill would have replaced the current requirement for organisations to appoint a data protection officer with a requirement for a 'senior responsible individual' to be responsible for data protection risks within the organisation.
- **High-risk processing**: The Conservative bill would have required organisations to keep records of their activities processing personal data only where it was "likely to result in a high risk to the rights and freedoms of individuals". It would have made it optional for data controllers to consult the information commissioner before processing personal data in a way the data controller had assessed would result in a high risk.
- **Strategic priorities for data protection**: The Conservative bill would have enabled the secretary of state to publish a statement of strategic priorities for data protection, to which the information commissioner would have had to have regard.
- **Codes of practice**: The secretary of state would not have the right to veto or to make recommendations on codes of practice prepared by the information commissioner as proposed at different stages of the Conservative bill. These proposals had raised concerns about the independence of the information commissioner.[17] Under Labour's proposals, the secretary of state would have to be consulted before the information commissioner prepared codes of practice.
- **Complaints by data subjects**: The Conservative data bill would have allowed the information commissioner to refuse to act on a complaint if it had not been raised with the data controller, or if the controller had not finished handling the complaint and less than 45 days had passed since the complaint was made.
- **Cookies**: The Conservative data bill would have allowed storage of/access to information in an individual's equipment for the sole purpose of installing

[16] House of Lords Library, 'Data Protection and Digital Information Bill: HL Bill 30 of 2023–24', 13 December 2023, pp 9 and 11.
[17] See: House of Lords Library, 'Data Protection and Digital Information Bill: HL Bill 30 of 2023–24', 13 December 2023, pp 31–3.

software updates on the equipment that were necessary for security reasons (subject to certain conditions).

- **Implementation of law enforcement information-sharing agreements**: The Conservative bill would have enabled the government (or Welsh or Scottish ministers in areas of devolved competence) to make secondary legislation to implement the technical or operational detail of international law enforcement information-sharing agreements.
- **Information for social security purposes**: The Conservative bill would have enabled the government to require banks and financial organisations to provide data about accounts linked to benefit claimants. The Conservative government intended to use this information to identify possible benefit fraud. The Labour government has said it will introduce a separate Fraud, Error and Debt Bill that will include an eligibility verification measure to require banks and financial institutions to examine their own data to highlight where someone may not be eligible for the benefits they are being paid.[18]
- **Biometrics commissioner**: The Conservative bill would have abolished the office of biometrics commissioner and transferred the commissioner's casework functions and oversight of the national security determinations regime to the investigatory powers commissioner.[19]
- **Surveillance camera commissioner**: The Conservative bill would have abolished the office of surveillance camera commissioner and repealed the requirement for a surveillance camera code.

[18] House of Commons, 'Written statement: DWP Fraud, Error and Debt Bill (HCWS114)', 8 October 2024.
[19] The two roles of biometrics commissioner and surveillance camera commissioner were carried out by the same person between February 2022 and August 2024, when he stepped down from the roles (Biometrics and Surveillance Camera Commissioner, 'About us', accessed 29 October 2024; HM Government, 'Office of the biometrics commissioner', accessed 29 October 2024; and Biometrics and Surveillance Camera Commissioner, 'Resignation of the biometrics and surveillance camera commissioner', 8 August 2024).

# 2. What would the bill do?

## 2.1 Part 1: Access to customer data and business data

### Background: Smart data

Part 1 of the Data (Use and Access) Bill [HL] deals with access to customer data and business data. The government has said this will pave the way for the 'smart data' model to be used in more sectors beyond its current use in open banking in the finance sector.[20] It explained that the UK General Data Protection Regulation (GDPR) allows individuals to obtain and reuse their personal data, but smart data takes this further by allowing consumers to request their data be directly shared to authorised and regulated third parties whilst ensuring data security. For example, open banking allows customers to aggregate account information from different banks into one dashboard so they can see real-time information about their money in one place.

The government contends that extending the smart data model to open finance would bring the benefits of open banking to a wider range of products including mortgages, pensions, savings and investments.[21] The government believes that by extending the smart data model to other sectors, customers could, for instance, compare prices between energy providers, or use authorised third party providers to act as an intermediary for their data so they could cancel one service and sign up to another with the click of a button.[22] It also suggested that the Department for Energy Security and Net Zero could use the power to introduce a road fuel price data scheme, subject to the government's response to the road fuels consultation, which it said would be published in due course.[23]

---

[20] Department for Science, Innovation and Technology, 'Data (Use and Access) Bill factsheet: Growing the economy', 24 October 2024.

[21] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 4.

[22] Department for Science, Innovation and Technology, 'Data (Use and Access) Bill factsheet: Growing the economy', 24 October 2024.

[23] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 4.

## Data regulations (clauses 1 to 7)

Clause 1 of the bill defines what is meant by 'business data' and 'customer data', 'data holder' and other terms. Customer data includes information relating to the goods, services or digital content supplied or provided to the customer including the price paid, their use or their performance and their quality.[24]

Clause 2 would give the secretary of state or the Treasury the power to make regulations requiring data holders to provide customer data 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. It would also give the secretary of state the power to provide for the production, collection and retention of customer data so that data holders have specific data to hand to ensure that smart data schemes can operate consistently and effectively.[25] Clause 4 would make equivalent provision about business data, with two key differences from the provisions about customer data.[26] As business data does not relate directly to a particular customer, the regulations could require data holders to publish business data, and the provision of data to a third party recipient would not need to be authorised by a customer.

In making data regulations under clause 2 or 4, the secretary of state and the Treasury would have to take certain matters into account, such as the likely effects on existing and future customers, data holders, small and micro businesses, innovation and competition. Clauses 3 and 5 set out further provisions that the regulations made under clauses 2 or 4 may contain, in relation to customer data and business data respectively. For example, the regulations could set out requirements about how customers authorise third parties to act on their behalf, restrictions on who a customer may authorise to receive their data, or provisions for complaints or resolving disputes. The government has said that clauses 3 and 5 "illustrate" provisions that data regulations made under clauses 2 or 4 could make, but the regulations would not have to contain all these provisions and would not be limited only to the illustrative uses set out in clauses 3 and 5.[27]

The regulations could provide for a decision-maker to decide who should be authorised to receive customer data or business data. Clause 6 would enable regulations to make

---

[24] As above.
[25] Explanatory notes, p 30.
[26] As above, p 33.
[27] As above, pp 30 and 33.

provisions about the appointment of a decision-maker and to confer powers on them to monitor compliance with the conditions for being authorised or approved to receive data.

The regulations could also make provision about 'interface bodies'. Further detail about these is set out in clause 7, which provides that the regulations could require a data holder or third party recipient to set up an interface body to do one or more of the following:

- establish a facility or service for providing, publishing or processing customer data or business data (an "interface")—examples could include dashboard services, other electronic communications services and application programming interfaces
- set standards ("interface standards") or make other arrangements ("interface arrangements") for use by others when establishing, maintaining or managing an interface
- maintain or manage an interface, interface standards or interface arrangements

The regulations could also require data holders and/or third party recipients to fund an interface body.[28]

The government explained that 'interface' in this context refers to the interface between the data IT systems of data holders and third party recipients.[29] It said that clause 7 would allow for bodies similar to the Open Banking Implementation Entity (OBIE) to be established. Banking providers were required to set up this body under the existing open banking scheme. The OBIE, known as Open Banking Ltd, delivers application programming interfaces (APIs—mechanisms through which software applications communicate and share data with each other), data structures and security architectures that enable developers to develop easy and secure ways for individuals and small businesses to share the financial information held by the banks with third parties.[30]

[28] Clause 7(4)(b) and (c) and 7(7).

[29] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 5.

[30] Open Banking, 'What is open banking?', accessed 24 October 2024.

## Enforcement (clauses 8 to 10)

Clause 8 would enable the secretary of state or the Treasury to make regulations about monitoring compliance with and enforcing regulations made under part 1 of the bill. This could include specifying a public authority to act as an "enforcer" to monitor and enforce the regulations. Regulations made under clause 8 could enable an enforcer to:

- have powers of investigation, subject to the restrictions set out in clause 9
- issue compliance notices and enforce them as if they were a court order
- impose a financial penalty for providing false or misleading information, or failing to comply with a requirement in regulations made under part 1 of the bill or in a compliance notice; this would be subject to the conditions in clause 10 about what regulations enabling a financial penalty must or may contain

Regulations made under clause 8 could also:

- create offences punishable with a fine (including up to an unlimited amount) for providing false or misleading information, or for preventing an enforcer, interface body or decision-maker from accessing information, documents, equipment or other material
- provide for complaints, review and appeals processes
- enable or require an enforcer to publish information about its monitoring or enforcement activities, or guidance about how an enforcer proposes to exercise its functions

## Fees and financial assistance (clauses 11 to 13)

Clauses 11 to 13 make provision for the funding of smart data schemes. Clause 11 would enable the secretary of state or the Treasury to make regulations allowing data holders, decision-makers, interface bodies and enforcers to charge fees to cover expenses incurred in performing the duties or exercising the powers they are given by part 1 regulations. The government has set out its intention that "a data holder's provision of its data and performance of other obligations should be free to customers and third party recipients".[31]

[31] Explanatory notes, pp 38–9.

However, it added that regulations "might, for instance, allow data holders to charge fees in the case of excessive requests for data".

Clause 12 would enable a levy to be imposed on data holders or third party recipients to meet expenses that certain bodies—decision-makers, interface bodies, enforcers or public authorities that are third party recipients of business data—incur in performing the duties or exercising the powers they are given by part 1 regulations. The government has said the purpose of charging fees and imposing a levy would be to meet all or part of the costs so that the expenses of a smart data scheme may be met by the relevant sector without a cost to the taxpayer.[32]

Clause 13 would allow the secretary of state or the Treasury to give financial assistance to a person to meet expenses incurred in performing duties or exercising powers or other functions under part 1 regulations. Financial assistance could include a grant, loan, guarantee or indemnity, but would not include buying shares in a company. Financial assistance could not be given to data holders, customers, third party recipients (except public authorities that are third party recipients of business data) or a person acting on behalf of any of the above. The government has said the power to provide financial assistance is a "backstop", but it intends smart data schemes should be self-financing through fees and levies.[33]

### Financial services sector (clauses 14 to 17)

Clauses 14 to 17 set out provisions relating to smart data within the financial services sector. Clause 14 would enable the Treasury to make regulations enabling or requiring the Financial Conduct Authority (FCA) to set rules that would oblige financial services providers to use a particular interface, interface standards or interface arrangements. The government has said that, for example, the rules could require data holders to comply with a certain API standard.[34] The rules could also require the use of a particular interface, interface standards or interface arrangements to receive customer data or business data from a financial services provider if the financial services provider is required by data regulations to provide that data. The FCA could also make rules relating to the composition, governance or activities of an interface body, or about the interface, interface standards or interface arrangements, and their use.

---

[32] As above, p 40; and Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 12.

[33] Explanatory notes, p 40.

[34] As above, p 41.

Clause 15 sets out what the government has described as "limitations and safeguards" on the way the FCA can use its rule-making powers.[35] For instance, among other things, the FCA could not require financial services providers to set up an interface body—only the Treasury could do so. Clause 16 sets out provisions relating to the way the Treasury could require or enable the FCA to use its rule-making powers in relation to setting financial penalties and imposing a levy on data holders or third party recipients.

The government has said that clause 14 would allow the FCA to regulate financial services smart data schemes and interface bodies in a manner broadly consistent with its regulation of the wider financial services sector.[36] The FCA already regulates the conduct of all open banking scheme data holders.[37] The government has said it intends to transition oversight of the open banking interface body and scheme from the Competition and Markets Authority (CMA) to the FCA in order to put the open banking scheme on a longer-term footing. It has said that giving the FCA these rule-making powers would facilitate this.

Clause 17 would facilitate coordination between the FCA and other regulators. It would allow the Treasury to make regulations amending the definitions of the FCA's "relevant functions" and "objectives" set out in section 98 of the Financial Services (Banking Reform) Act 2013. The government has said this is intended to ensure the FCA's functions relating to financial services smart data schemes can be brought within the scope of the existing arrangements for coordination between the regulators of payment systems that are set out in that act.[38] Clause 17 is a new provision in the Labour bill for which there was no similar provision in the previous bill under the Conservatives.

### Supplementary provisions (clauses 18 to 26)

Clauses 18 to 26 of part 1 set out supplementary provisions relating to the smart data part of the bill.

---

[35] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 14.
[36] Explanatory notes, p 40.
[37] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, pp 14–15.
[38] As above, p 16.

Clause 18 would permit the secretary of state or the Treasury to make regulations to provide that a public authority cannot be liable in damages when it exercises a function under part 1.

Clause 19 would require the secretary of state and the Treasury to provide for a review of regulations they had each made under part 1 of the bill and to publish a report on whether the regulation remained appropriate. The first report would have to be published within five years of such a regulation coming into force, and subsequent reports would have to be published at least every five years from then on. The reports would have to be laid before Parliament. Information that might harm commercial interests could be omitted. The regulations could allow the secretary of state and the Treasury to carry out a joint review and produce a joint report. This requirement differs from the review requirement in the Conservative bill. That bill contained a review requirement on the face of the bill itself and applied only to data regulations made under what are now clauses 2 and 4.[39] The current bill requires the review requirements to be set out in secondary legislation and it applies to regulations made under all the regulation-making powers in part 1 of the bill.

Clauses 20 and 21 set further conditions on the provisions that could be made by regulations under part 1. For example, clause 20 provides that regulations under part 1 could not be read as authorising or requiring personal data to be processed in a way that breached data protection legislation. As another example, clause 21 would allow regulations to amend, repeal or revoke primary legislation if the regulations were making provision about handling complaints, resolving disputes, appeals, or consequential, supplementary, incidental, transitional, transitory or saving provisions.

Clause 22 sets out which parliamentary procedure would apply, depending on which power in part 1 was used to make regulations. For example, the first regulations made under clauses 2 and 4 that made provision about a particular description of customer or business data would be subject to the affirmative procedure, but subsequent ones could be subject to the negative procedure. The government has said the intention is that regulations to introduce a new smart data scheme would be subject to the affirmative procedure.[40] Clause 22 would also require that before making regulations subject to the affirmative procedure, the secretary of state or the Treasury would have to consult, as they considered appropriate, those likely to be affected by the regulations (such as businesses who would become data holders under a smart data scheme) and sectoral regulators.

---

[39] As above, p 17.

[40] Explanatory notes, p 45.

Clause 23 would make provision about related subordinate legislation. The government has said this is intended to allow smart data provision to be made by amending existing subordinate legislation rather than making new standalone regulations.[41] This could include, for example, amending existing data sharing requirements in financial services legislation such as open banking provisions in the Payment Services Regulations 2017. Clause 24 would repeal existing provisions of the Enterprise and Regulatory Reform Act 2013 that deal with customer data. Clauses 25 and 26 set out definitions of terms used in part 1 of the bill.

## 2.2 Part 2: Digital verification services

### Background: Digital identity

Part 2 of the bill would establish a regulatory framework for the provision of digital verification services (DVS) in the UK. The bill would enable companies that provide tools for verifying identities to get certified against the government's framework of standards. Certified companies would receive a 'trust mark'. The government has said this would enable users to recognise trusted digital identity providers and enable digital identities and attributes to be used with the same confidence as paper documents.[42] The government describes a digital identity as "a digital representation of a person or things about them" which "lets people prove these things without having to present physical documents".[43] The government estimates that efficiency gains from supporting the digital identity sector could generate £4.3bn for the UK economy over the next decade.[44]

The government has sought to explain that its DVS measures are not introducing mandatory identity requirements. In the days after the general election, there was some media speculation about whether Labour might introduce mandatory digital ID cards.[45] This followed a newspaper article in which former Labour Prime Minister Sir Tony Blair suggested digital identity could help control immigration and referred to his own policy when he was in

---

[41] As above, p 46.

[42] As above, p 9.

[43] Department for Science, Innovation and Technology, 'Data (Use and Access) Bill factsheet: Making lives easier', 24 October 2024.

[44] As above; and Department for Science, Innovation and Technology et al, 'New data laws unveiled to improve public services and boost UK economy by £10 billion', 24 October 2024.

[45] Kate Devlin, 'Minister rejects Blair's ID card call two hours after refusing to rule it out', Independent, 7 July 2024.

office for national identity cards.[46] In response to this speculation, the business and trade secretary, Jonathan Reynolds, said that ID cards were not part of the Labour government's plans.[47] Peter Kyle, secretary of state for science, innovation and technology, said that when using language about digital identity, his focus was on digital verification that would make it easier for people to verify their identity when accessing services online, rather than a universal system of ID cards.[48]

In a factsheet published alongside the bill, the government confirmed it had no plans to introduce national digital ID cards.[49] It said using digital ID would be voluntary, and people would still be able to prove their identity using physical documents if they wished. It explained the purpose of the bill was to ensure that people who chose to use digital identity products or services could tell which ones met government standards.

### Introductory (clause 27)

Clause 27 sets out the scope of part 2 of the bill and defines "digital verification services".

### DVS trust framework and supplementary codes (clauses 28 to 31)

Clause 28 would require the secretary of state to publish a DVS trust framework setting out rules for the provision of DVS. The secretary of state would have to consult the information commissioner and anyone else the secretary of state considered appropriate before publishing the DVS trust framework. The DVS trust framework could specify different rules for different DVS.

Development versions of a DVS trust framework have already been published under the Conservative government: 'alpha' versions in February 2021 and August 2021 and a 'beta'

---

[46] Tony Blair, 'My advice to Keir Starmer', Times (£), 6 July 2024. The Labour government legislated for a national identity card scheme in 2006, but this was repealed by the coalition government in 2010 (see: House of Lords Library, 'Identity documents in the UK', 8 January 2016).

[47] Kate Devlin, 'Minister rejects Blair's ID card call two hours after refusing to rule it out', Independent, 7 July 2024.

[48] ITV 'Peston' programme, 'Official X account', 8 July 2024.

[49] Department for Science, Innovation and Technology, 'Data (Use and Access) Bill factsheet: Making lives easier', 24 October 2024.

version in June 2022, developed following feedback and testing of the alpha version.[50] The Conservative government had said that it would conduct further testing of the beta version in collaboration with industry, civil society and the public to refine it further.

When the House of Lords Delegated Powers and Regulatory Reform Committee reported on the Conservatives' data bill, it argued that the DVS trust framework should be subject to parliamentary scrutiny.[51] It said the affirmative procedure would be the appropriate level of scrutiny.

Clause 29 would allow the secretary of state to publish one or more "supplementary codes", sets of rules to supplement the DVS trust framework. As with the trust framework, the secretary of state would have to consult the information commissioner and anyone else they considered appropriate before publishing a supplementary code. A supplementary code could make different rules for different DVS. The government has suggested that supplementary codes could be used where individual sectors or use cases have additional requirements that exceed those in the trust framework. For instance, this could be the case if a sector has additional specific legislative or regulatory obligations.[52] Clause 30 would enable the secretary of state to withdraw a supplementary code after publishing a determination giving at least 21 days' notice of the withdrawal.

Clause 31 would require the secretary of state to carry out an annual review of the DVS trust framework and each supplementary code (except supplementary codes that had been withdrawn). As part of the review, the secretary of state would have to consult the information commissioner and anyone else the secretary of state considered appropriate. Clauses 28 and 29 would allow the secretary of state to publish a revised DVS trust framework and supplementary codes following the annual review or at any other time.

---

[50] Department for Science, Innovation and Technology and Department for Digital, Culture, Media and Sport, 'UK digital identity and attributes trust framework alpha v1 (0.1)', 11 February 2021; and 'UK digital identity and attributes trust framework—beta version', last updated 20 July 2023.

[51] House of Lords Delegated Powers and Regulatory Reform Committee, 'Data Protection and Digital Information Bill, Pedicabs (London) Bill [HL]', 14 February 2024, HL Paper 60 of session 2023–24, p 2. The relevant power in the Conservatives' bill was in clause 53. The drafting of clause 28 in the present bill is not identical to clause 53 of the earlier bill.

[52] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 20.

## DVS register (clauses 32 to 44)

Clause 32 would require the secretary of state to establish, maintain and make publicly available a register of persons providing digital verification services. This would be known as the DVS register. A non-statutory version of a DVS register already exists on the government's website. It lists digital identity and attribute services that provide DVS certified against the beta version of the DVS trust framework.[53] The government has said the 49 companies currently certified against the current trust framework are already undertaking hundreds of thousands of right to work, right to rent, and disclosure and barring service (DBS) checks every month.[54]

Clause 33 sets out conditions for registration in the DVS register. It would require DVS providers to be included on the register if they:

- hold a certificate from an accredited conformity assessment body certifying their DVS are provided in accordance with the DVS trust framework
- have applied to be registered for one or more of the DVS for which they hold a certificate
- have complied with the registration requirements set out in a determination made under clause 38
- have paid any fee payable under clause 39

DVS providers could not be registered if they had not fulfilled all the above criteria. The DVS register would have to show which DVS a provider was registered to provide.

Clause 34 would enable the secretary of state to refuse to register a DVS provider if they considered it necessary to do so on national security grounds, or if they were satisfied the provider was failing to comply with the DVS trust framework. The secretary of state would have to provide written notice of their intention to refuse registration, and the provider would have at least 21 days to make representations about this. If the secretary of state decided to refuse registration, they would have to notify the DVS provider. The notification could also state that further applications from the provider would be refused for a period of up to two years.

---

[53] HM Government, 'Guidance: Find registered digital identity and attribute services', 20 September 2024.
[54] Department for Science, Innovation and Technology, 'Data (Use and Access) Bill factsheet: Making lives easier', 24 October 2024.

Clause 35 would allow a DVS provider already on the DVS register to be registered for additional services they provide in accordance with the DVS trust framework. Their registration would have to be updated to include the additional services if they met the relevant criteria of holding a certificate from an accredited conformity assessment body for the additional services, complying with any requirements imposed by a determination under clause 38 and paying any fees required under clause 39.

Clause 36 would allow a provider registered in the DVS register to add a supplementary note to the register recording that they are providing services in accordance with a supplementary code. Clause 37 would allow a provider who already had a supplementary note included in the register to apply to amend it to include additional services. In both cases, the provider would have to hold a certificate from an accredited conformity assessment body confirming their service was being provided in accordance with the supplementary code, comply with any requirements imposed by a determination under clause 38, and pay any fees required under clause 39.

Clause 38 would enable the secretary of state to determine the form and manner in which applications for registration, supplementary notes and amendments to the register would be made. This would include the information and documents to be provided with the application. The requirements could be different for different types of application.

Clause 39 would allow the secretary of state to make regulations about fees for:

- applications for registration, supplementary notes and amendments
- continued registration on the DVS register

These regulations would be subject to the negative procedure. The government has said that the fee structure is "likely to be technical and complex, with different fees to be applied for different purposes".[55] Clause 39 would allow fees to be set at a level higher than cost recovery. The government has said that any additional revenues are intended to "fund wider governance functions that may be considered necessary within the digital identity market".

[55] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 22.

Clause 40 would require the secretary of state to remove a DVS provider from the register if they:

- asked to be removed
- ceased to provide all of the DVS for which they were registered
- no longer held a certificate from an accredited conformity assessment body confirming that they provided at least one DVS in accordance with the DVS trust framework

Clause 42 would create a similar duty for the secretary of state to amend the register to remove particular services (for instance, if a provider was registered for multiple services but stopped providing one of them or no longer held a certificate for one of them). Clauses 43 and 44 would create a similar duty for removing supplementary notes and removing services from supplementary notes.

Clause 41 would give a discretionary power to remove a DVS provider from the register if the secretary of state:

- was satisfied they were failing to comply with the DVS trust framework or a supplementary code
- was satisfied they had failed to provide the secretary of state with information in accordance with a notice under clause 51
- considered it necessary in the interests of national security

Similar to the process for refusing registration, the secretary of state would have to provide written notice of their intention to remove the registration, and the provider would have at least 21 days to make representations. If the secretary of state decided to remove the person from the register, they would have to notify the DVS provider. The notification could also state that applications from the provider for re-registration would be refused for a period of up to two years.

**Information gateway (clauses 45 to 49)**

Clauses 45 to 49 would establish an 'information gateway' to enable public authorities to share information with registered DVS providers. Clause 45 would allow public authorities

to disclose information about an individual to a registered DVS provider if the individual had requested DVS from the DVS provider. However, clause 45 would not authorise a disclosure of information that would breach data protection legislation. Public authorities could charge fees to the DVS provider for sharing the information.

Clause 46 specifies that where HMRC has disclosed personal information under clause 45, the DVS provider must not share that information further without the consent of HMRC other than for the purpose of providing DVS for the individual. Disclosing information in contravention of this clause would be an offence. Clauses 47 and 48 make similar provision about information disclosed by the Welsh Revenue Authority and Revenue Scotland.

Clause 49 would require the secretary of state to publish a code of practice about information shared under clause 45.[56] Public authorities would have to have regard to the code of practice when sharing information with DVS providers. The secretary of state would be required to consult the information commissioner and the devolved governments when preparing or revising the code. The code would have to be approved by both Houses of Parliament. Revisions to the code would be subject to the negative scrutiny procedure in Parliament.

### Trust mark (clause 50)

Clause 50 would enable the secretary of state to designate a trust mark that registered DVS providers could use when providing DVS. The secretary of state could bring civil proceedings for an injunction (or interdict in Scotland) against someone using the trust mark where they were not registered to provide DVS. The government has said the trust mark will be a new logo to show the public which DVS are approved by the new Office for Digital Identities and Attributes (OfDIA) within the Department for Science, Innovation and Technology (DSIT).[57]

[56] The code of practice would have to be consistent with the 'Data sharing code of practice' published under section 121 of the Data Protection Act 2018.

[57] Department for Science, Innovation and Technology et al, 'New data laws unveiled to improve public services and boost UK economy by £10 billion', 24 October 2024.

## Supplementary (clauses 51 to 55)

Clause 51 would give the secretary of state the power to require an accredited conformity assessment body, or a person registered in the DVS register, to provide information that the secretary of state reasonably requires for exercising their functions under this part of the bill.

Clause 52 would allow the secretary of state to make regulations delegating their functions under this part of the bill to a third party. These regulations would be subject to the affirmative procedure in Parliament. However, the secretary of state could not delegate their regulation-making powers to a third party. The government has said that while the DVS market is developing, it believes governance and the trust framework should sit with DSIT. However, it added that in future some or all of the functions might be delegated to another public sector body, a regulator or the private sector.[58]

Clause 53 would require the secretary of state to publish annual reports on the operation of this part of the bill.

Clause 54 sets out an index of defined terms for this part of the bill.

Clause 55 would make amendments to immigration legislation so that the secretary of state could refer to DVS-registered persons when making regulations relating to checks made by employers, landlords and lettings agents that people have the right to live or work in the UK. Completing prescribed checks provides employers, landlords and letting agents with a statutory excuse against the imposition of a civil penalty if they are found to be employing or renting to someone whose immigration status disqualifies them from work or renting in the private rented sector. The government has said this clause would allow the Home Office to legislate to require employers and landlords who use identity document validation technology to carry out their right to work and right to rent checks to use a DVS provider that is registered in the DVS register as complying with designated supplementary rules concerning these checks.[59]

---

[58] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 25.

[59] Explanatory notes, p 12.

## 2.3 Part 3: National underground asset register

### Background: National underground asset register

Part 3 of the bill would put the national underground asset register (NUAR) on a statutory footing. NUAR is a digital map of underground pipes and cables in England, Wales, and Northern Ireland.[60] A separate system, the Scottish community apparatus data vault, already exists in Scotland to share underground pipe and cable information via Scotland's existing road works database.[61]

The government has explained why it believes NUAR is needed:

> There are 600+ owners of underground assets (or "apparatus") across the public and private sectors (including energy, water, telecommunications and local and transport authorities) who hold data about their own apparatus, which they are required by law to share for the purposes of 'safe digging'. However, currently there is no standardised method to do this with multiple organisations having to be contacted for each dig, providing information in varied formats, scales, quality and on different timelines resulting in a complex process for maintaining, operating and repairing buried apparatus.
>
> The bill will streamline the data-sharing process, reduce the risk of potentially lethal utility strikes on apparatus and promote more efficient management and maintenance of underground apparatus, through establishment, on a statutory footing, of the national underground asset register (NUAR).[62]

The government said that NUAR would increase efficiency by accelerating the average data-sharing process from six days to six seconds.[63] It estimates NUAR will deliver at least £400mn per year of economic growth, through "increased efficiency, reduced asset strikes (when underground pipes and cables are accidentally damaged) and reduced disruptions for

---

[60] Department for Science, Innovation and Technology and Geospatial Commission, 'National underground asset register (NUAR)', 15 October 2024.
[61] Office of the Scottish Road Works Commissioner, 'Vault: Access to information on the location of underground pipes and cables', accessed 26 October 2024.
[62] Explanatory notes, p 13.
[63] Department for Science, Innovation and Technology, 'Data (Use and Access) Bill factsheet: Growing the economy', 24 October 2024.

the public and business".[64] It said accidental damage currently costs the economy £2.4bn a year.[65]

An initial private beta (development) version of NUAR is already live across England, Wales, and Northern Ireland. It includes data from over 200 asset owners, including most of the major energy and water providers, several major telecoms companies, and some smaller providers, transport organisations and local authorities.[66] The NUAR platform is expected to be fully operational by the end of 2025.

The Conservatives' data bill made provision for NUAR in England and Wales only, not Northern Ireland. However, the Conservative government had intended to introduce provisions for Northern Ireland in the House of Lords.[67]

The Office of the Scottish Road Works Commissioner has a separate system, the Scottish community apparatus data vault, to share underground pipe and cable information via Scotland's existing road works database.[68]

**National underground asset register (clauses 56 to 60 and schedules 1 and 2)**

Clause 56 and schedule 1 would amend the New Roads and Street Works Act 1991 to insert a number of new sections and a new schedule, as follows:

- New section 106A: The secretary of state would be required to keep a register of information relating to apparatus in streets in England and Wales, to be known as the national underground asset register. A single register could cover England and Wales and Northern Ireland.
- New section 106B: Undertakers would be required to upload information about their apparatus to NUAR before the end of an "initial upload period",

---

[64] Department for Science, Innovation and Technology and Geospatial Commission, 'National underground asset register (NUAR)', 15 October 2024.
[65] Department for Science, Innovation and Technology et al, 'New data laws unveiled to improve public services and boost UK economy by £10 billion', 24 October 2024.
[66] Department for Science, Innovation and Technology and Geospatial Commission, 'National underground asset register (NUAR)', 15 October 2024.
[67] HC Hansard, 29 November 2023, col 877.
[68] Office of the Scottish Road Works Commissioner, 'Vault: Access to information on the location of underground pipes and cables', accessed 26 October 2024.

the date of which would be set by the secretary of state in regulations. In this context, undertaker means someone who has a relevant statutory right to carry out street works or to carry out street works under a licence.[69] Failure to upload the required information would be an offence and would make an undertaker liable to compensate anyone who incurred damage or loss in consequence of the failure.

- New section 106C: The secretary of state could set out in regulations who and in what circumstances a person should be provided with access to information kept in NUAR.[70]
- New sections 106D and 106E: The secretary of state could make regulations setting out a scheme under which undertakers who have apparatus in a street would be required to pay fees to fund the running costs of NUAR and could be required to provide information relating to the new fees scheme.[71]
- New section 106F: The fees scheme would be enforced by a power conferred on the secretary of state to impose monetary penalties for non-compliance.[72] Further information about monetary penalties would be set out in new schedule 5A to the 1991 act, inserted by schedule 1 of the bill.
- New section 106G: The secretary of state could enter into arrangements with one or more other persons to exercise certain functions of the secretary of state, with a requirement that any such persons be prescribed in regulations.[73]
- New section 106H: Any processing of personal data that took place as a result of the new sections or regulations made under them would have to be done in accordance with existing data protection legislation.
- New section 106I: The secretary of state would be required to consult the Welsh government and the Northern Ireland Department for Infrastructure before making any regulations under the new sections.
- New section 106J: This section defines various terms used in the new sections.

---

[69] New Roads and Street Works Act 1991, s 48(4).

[70] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 28.

[71] As above.

[72] As above.

[73] As above.

Clause 58 and schedule 2 would make equivalent provision for Northern Ireland by amendments to the Street Works (Northern Ireland) Order 1995.[74]

Clause 57 would make further amendments to the 1991 act to impose a duty on undertakers in England and Wales to update their NUAR record after placing an item in the street or moving its position, or inspecting, maintaining, adjusting, repairing, altering or renewing it, or receiving information about it from somebody else executing street works. This would have to be done "as soon as reasonably practical" and within a time period prescribed by the secretary of state. The secretary of state would also have the power to prescribe the form and manner in which information should be submitted to NUAR, and to prescribe exemptions from the requirements to record information about apparatus. The secretary of state would have to consult the Welsh government before making such regulations.

Clause 57 would also insert a new section 80 into the 1991 act which would place a requirement on anybody executing street works who had access to NUAR information about that street. If they discovered an item of apparatus was missing from NUAR or incorrectly recorded, they would be required to take "reasonably practicable" steps to inform the undertaker to whom the apparatus belonged. If they were unable to inform the undertaker, they would be required to record the prescribed information about the apparatus on NUAR themselves. It would be an offence to fail to do so. Before making regulations to prescribe what information should be recorded, how it should be recorded or any exemptions, the secretary of state would have to consult the Welsh ministers, representatives of those likely to be affected by the regulations, and anyone else the secretary of state considered appropriate.

Clause 59 would make equivalent provision in Northern Ireland.[75]

Clause 60 specifies that consultations which took place before the bill received royal assent could satisfy the consultation requirements under the amendments made by clauses 56 to 58.

## 2.4 Part 4: Registers of births and deaths

Part 4 of the bill would remove the requirement in England and Wales for registers of births and deaths to be held in paper form. This would enable births and deaths to be recorded

---

[74] Explanatory notes, pp 64 and 116.

[75] As above, p 66.

electronically, and remove the current duplication where they are registered both electronically and in paper registers.[76] The government has said this change would enable people to "get on with their lives without unnecessary admin".[77] With the registration of deaths in particular, the government said this would be "supporting people at one of the most challenging times in life", allowing them to register a death over the phone rather than face-to-face. However, people could still choose to make the registration face-to-face if they preferred.

Clause 61 would amend the Births and Deaths Registration Act 1953 to allow the registrar general to determine the form in which registers of births and deaths are to be kept. The government has said this would allow the information to be registered and stored electronically without the need for paper registers to be kept in a safe.[78] It would also repeal provisions of the 1953 act that require quarterly returns, as these would not be needed with an electronic system.

Clause 62 would require local authorities to provide and maintain equipment and facilities that the registrar general considers necessary for registrars and superintendent registrars to carry out their functions.

Clause 63 would allow the relevant minister to make regulations to provide that if a person complies with specified requirements at the time of registering a birth or death, they are to be treated as having signed the register in the presence of the registrar. This may include requiring them to sign something other than the register to provide evidence of their identity.

Clause 64 would set out arrangements for the retention and disposal of existing paper registers and certified copies. Clause 65 introduces schedule 3, which would make minor and consequential amendments.

---

[76] As above, p 13.

[77] Department for Science, Innovation and Technology et al, 'New data laws unveiled to improve public services and boost UK economy by £10 billion', 24 October 2024.

[78] Explanatory notes, p 67.

## 2.5 Part 5: Data protection and privacy

### Background: Current legal framework for data protection

The processing of people's personal data is covered by various legal frameworks in the UK, depending on the type of processing taking place and who is doing it.

General data processing is covered by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). These pieces of legislation had their origins in EU law on data protection. The EU General Data Protection Regulation (2016/679) (the EU GDPR) applied to the UK from 25 May 2018 as the UK was still an EU member state at that point. As an EU regulation, it applied to the UK directly and did not need to be transposed into UK domestic law. However, the UK also passed the DPA 2018 to supplement it. The DPA 2018 repealed the UK's previous data protection law (the Data Protection Act 1998) and exercised certain derogations that were allowed under the EU GDPR.

At the end of the Brexit transition period, the European Union (Withdrawal) Act 2018 (EUWA 2018) incorporated the EU GDPR into UK domestic law as a piece of retained EU law.[79] Secondary legislation made using powers in EUWA 2018 modified the EU GDPR to ensure that it would still work in the UK after it left the EU.[80] The resulting piece of legislation now on the domestic statute book is known as the UK GDPR.

A separate piece of EU law, EU Directive 2016/680, governed data processing by 'competent authorities' for law enforcement purposes (broadly the police and other criminal justice agencies).[81] This was transposed into UK domestic law by part 3 of the DPA 2018.

Processing of personal data by intelligence agencies was not covered by EU law as national security is outside EU competence.[82] Part 4 of the DPA 2018 sets out rules for processing personal data by the UK intelligence services.

---

[79] Following the passage of the Retained EU Law (Revocation and Reform) Act 2023, 'retained EU law' is now known as 'assimilated law'.

[80] Explanatory notes, p 22.

[81] Explanatory notes to the Data Protection Act 2018, para 37.

[82] As above, paras 41–3.

Another piece of assimilated law, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PEC Regulations), gives people specific privacy rights in relation to electronic communications. Again, the regulations were originally made to transpose an EU directive into domestic law but are now part of the domestic statute book. The PEC Regulations sit alongside the UK GDPR and the DPA 2018. They set out specific rules on marketing calls, texts and emails; cookies and similar technologies; security of public electronic communications services; and privacy of customer data relating to communications networks, such as traffic and location data, itemised billing or caller ID.[83]

The bill would make amendments to these existing sources of data protection law. The government has said that "targeted reforms" to parts of the UK's data protection and privacy framework would support economic growth and a modern digital government.[84]

**Research for scientific and statistical purposes (clauses 67 and 68)**

The UK GDPR and the DPA 2018 contain provisions to enable the processing of personal data for research purposes.[85] These provisions refer to three types of research-related purposes for the processing of personal data:

- archiving purposes in the public interest
- scientific or historical research purposes
- statistical purposes

Clause 67 would insert new definitions into article 4 of the UK GDPR of what constitutes the processing of personal data for research and statistical purposes. This would mean that:

- References to processing personal data for the purposes of **scientific research** cover 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".[86] This could include processing personal data for technological development or demonstration, fundamental research or applied research, as long as those

[83] Information Commissioner's Office, 'What are PECR?', accessed 27 October 2024.
[84] Explanatory notes, p 9.
[85] Information Commissioner's Office, 'What are the research provisions?', accessed 27 October 2024.
[86] Clause 67.

activities could reasonably be described as scientific. However, processing personal data for the purposes of research in public health would meet the definition of scientific research only if the research was in the public interest.

- References to processing personal data for the purposes of **historical research** would include processing personal data for genealogical research.
- References to processing personal data for **statistical purposes** are references to processing personal data for statistical surveys or producing statistical results only where the information produced by the data processing is aggregate data, not personal data, and the data controller does not use the personal data processed, or the information that results from the processing, in support of measures or decisions relating to an individual to whom the personal data relates.

Clause 68 would amend the UK GDPR to clarify how data controllers processing data for scientific research purposes could obtain consent to an area of scientific research where it was not possible to identify fully the purposes for which the data was to be processed at the time it was collected.[87]

The government has said these amendments would make it clear that research organisations can seek broad consent for areas of scientific research and would allow legitimate researchers doing scientific research in commercial settings to benefit from the special position of research in the data protection framework.[88]

### Consent to law enforcement processing (clause 69)

Clause 69 would insert a definition of consent into part 3 of the DPA 2018, the part that governs the processing of personal data by law enforcement authorities. This mirrors the definition of consent in the UK GDPR.[89]

### Data protection principles (clauses 70 to 72 and schedules 4 and 5)

Clause 70 would amend article 6 of the UK GDPR, which is concerned with the lawful grounds for processing personal data. It would make some clarifications to the public tasks

---

[87] Explanatory notes, p 70.
[88] As above, p 14.
[89] As above, p 70.

lawful ground that already exists in article 6. It would also create a new ground for lawful processing, namely that the processing is necessary for a "recognised legitimate interest". Schedule 4 would insert a new annex into the UK GDPR that would set out what would qualify as a recognised legitimate interest. This would include where the processing was necessary for the purposes of:

- making a disclosure to a data controller who needs to process that data for their task in the public interest or exercise of their official authority where the data controller has requested that data
- safeguarding national security or protecting public safety
- responding to an emergency
- detecting, investigating or preventing crime or apprehending or prosecuting offenders
- safeguarding vulnerable individuals

The Conservatives' data bill would also have included "democratic engagement" as one of the new recognised legitimate interests, but this is no longer included in Labour's bill.

Public authorities could not rely on the new recognised legitimate interest ground in the performance of their tasks.[90] The government has explained the reason for this provision as follows:

> Under current law non-public authority data controllers would need to conduct a balancing of interests test to determine whether personal data should be processed for these purposes […] If a data controller is not sure whether its interests outweigh the rights of the individual, it might decide to delay or stop [processing the] data due to worries about liability. The government is keen to encourage personal data processing and sharing for important public interest scenarios and considers that the burden of the balancing test should not be on data controllers in these circumstances.[91]

[90] As above, p 71.

[91] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 64.

The secretary of state would be able to make regulations to amend the recognised legitimate interests set out in the schedule.

When it reported on the equivalent provision in the Conservatives' data bill, the House of Lords Delegated Powers and Regulatory Reform Committee (DPRRC) argued that the grounds for lawful processing of personal data "go to the heart of the data protection legislation, and therefore in our view should not be capable of being changed by subordinate legislation".[92] The committee therefore recommended the power for the secretary of state to amend the list of recognised legitimate interests should be removed from the bill.

Clause 71 would set out the conditions under which the reuse of personal data ("further processing") for a new purpose would be permitted in accordance with the "purpose limitation principle".[93] The "purpose limitation principle" in article 5 of the UK GDPR prohibits further processing that is not compatible with the original purpose for which the personal data was collected. Schedule 5 would insert a new annex 2 into the UK GDPR which would set out under what circumstances processing of personal data for a different purpose would be treated as compatible with the original purpose.[94]

The secretary of state would have the power to amend the list of conditions in annex 2 that are to be treated as being compatible with the original purpose.[95] When it reported on the Conservatives' data bill, the DPRRC recommended that the equivalent power should be removed from the bill.[96] It said it was "inappropriate" for subordinate legislation to be used to make changes to a "fundamental principle" of the UK GDPR.

Clause 72 would amend the UK GDPR to make clear that relevant international law can be used as the basis for lawful processing in certain circumstances. Currently, the UK GDPR

---

[92] House of Lords Delegated Powers and Regulatory Reform Committee, 'Data Protection and Digital Information Bill, Pedicabs (London) Bill [HL]', 14 February 2024, HL Paper 60 of session 2023–24, p 2. The relevant power in the Conservatives' bill was in clause 5.

[93] Explanatory notes, p 72.

[94] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 65.

[95] Explanatory notes, p 73.

[96] House of Lords Delegated Powers and Regulatory Reform Committee, 'Data Protection and Digital Information Bill, Pedicabs (London) Bill [HL]', 14 February 2024, HL Paper 60 of session 2023–24, p 2. The relevant power in the Conservatives' bill was in clause 6.

specifies that the processing of personal data in the following cases is lawful only if authorised by domestic law:[97]

- personal data and special category data (personal data that is more sensitive in nature) on public interest grounds under articles 6(1)(e) and 9(2)(g) of the UK GDPR
- personal data relating to criminal offences and convictions under article 10 of the UK GDPR
- further processing under the new article 8A(3)(e) to be added to the UK GDPR by clause 71 of the bill

Clause 72 would amend these articles to specify that personal data could also be processed on these grounds if the process has a basis in or is authorised by "relevant international law". It would also amend the DPA 2018 to specify that processing would have a basis in or be authorised by relevant international law if it met a condition in schedule A1 to the DPA 2018. New schedule A1 lists one condition: that processing is necessary to respond to a request in accordance with the 'UK-USA: Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime'. This agreement permits telecoms operators in the UK to share information about serious crimes with law enforcement agencies in the US and vice versa.[98] The secretary of state would have the power to add further conditions to the new schedule. Any condition would have to relate to an international treaty ratified by the UK.

### Processing of special categories of personal data (clauses 73 and 74)

"Special category" data is sensitive personal data that needs more protection because it reveals someone's political opinions, racial or ethnic origin, religious or philosophical beliefs, trade union membership, is genetic or biometric data, or concerns their health, sex life or sexual orientation.[99] Article 9(1) of the UK GDPR prohibits the processing of special category data except under the conditions set out in article 9(2), together with any associated conditions in schedule 1 of the DPA 2018 where required.[100]

---

[97] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 66.

[98] As above, pp 66–7.

[99] Information Commissioner's Office, 'Special category data', accessed 27 October 2024.

[100] Explanatory notes, p 74.

Elected representatives are permitted to process special category data when they are acting on behalf of individuals in connection with their casework functions.[101] Someone who is an MP or a member of the Welsh Senedd, Scottish Parliament or Northern Ireland Assembly can continue to do so over a dissolution period and for up to four days after a general election to Parliament or the relevant assembly is held. Clause 73 would extend this period to 30 days.

Clause 74 would give the secretary of state regulation-making powers to amend the UK GDPR and the DPA 2018 in respect of new special categories of data. The powers could be used to:[102]

- add new special categories of data and categories of sensitive processing to the relevant regimes
- remove those categories of special category data, or sensitive processing that have been added by regulations (but not those that are currently set out in the UK GDPR and DPA 2018)
- make provision that any of the existing exceptions in the UK GDPR or conditions in DPA 2018 can or cannot be relied on in relation to any new category added by regulations
- make provision to vary any of the existing exceptions or conditions, but only as it relates to any new category added by regulations

The secretary of state would have to consult the information commissioner and such other person as the secretary of state considered appropriate before making any regulations using this power.

The government has said this would enable it to respond rapidly to future technological and societal developments.[103] It said the need for this power had been highlighted by recommendations from the Regulatory Horizons Council to add neurodata to the list of special categories of personal data, and from the Ada Lovelace Institute to include 'biometric categorisation' as a special category in addition to the existing 'biometric identification'

---

[101] As above.

[102] As above; and Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 68.

[103] Explanatory notes, p 75.

special category.[104] Currently, the list of special categories and associated safeguards can be changed only by primary legislation. This is a new provision that was not included in the Conservatives' data bill.

**Data subject's rights (clauses 75 to 79)**

Individuals have a right to request a copy of their personal data, which is referred to as a data subject access request.[105] Section 53(1) of the DPA 2018 allows data controllers operating under part 3 of that act to refuse to respond to requests that are deemed to be "manifestly unfounded or excessive", or to charge a reasonable fee for responding to them.[106] Clause 75 would enable the secretary of state to make regulations to require data controllers to publish guidance on the fees they charge for such requests. Clause 75 would also require that if data controllers refuse such a request, they must inform the data subject of their reasons for doing so. They would also have to inform the data subject of their right to complain to the information commissioner.

Clause 76 would amend the deadlines for organisations to respond to subject access requests. Generally, organisations must respond within one month of receiving the request, but the amendments made by clause 76 would clarify exceptions to this.[107] For example, the deadline could be extended by two months where necessary because of the number or complexity of the data subject's requests. Additionally, counting of the time taken to respond could be paused if a data controller could not reasonably proceed without obtaining further information from the data subject.

Clause 77 would provide researchers, archivists and those processing personal data for statistical purposes with a new exemption from providing certain information to individuals when they are reusing datasets for a different purpose.[108] They could rely on this exemption where there would be disproportionate effort to provide the required information to data subjects and where the research was in line with new safeguards for research introduced by clause 85.

---

[104] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 77.
[105] Information Commissioner's Office, 'A guide to subject access', accessed 27 October 2024.
[106] Explanatory notes, p 77.
[107] As above, pp 77–8.
[108] As above, p 78.

Clause 78 would mean data controllers would need to carry out only a "reasonable and proportionate" search in response to requests for information and personal data. The government has stated that this codifies the principle currently set out in domestic case law. Clause 78(5) stipulates that the amendments to the UK GDPR and the DPA 2018 made by this clause are to be treated as having come into force on 1 January 2024.

Clause 79 would amend the DPA 2018 to enable data controllers covered by part 3 (law enforcement processing) not to give data subjects material that was subject to legal professional privilege (or the equivalent in Scotland). The government has said that this would mirror the current exemption under the UK GDPR for such material.

### Automated decision-making (clause 80 and schedule 6)

Clause 80 is intended to expand the lawful base for the use of solely automated decision-making to make significant decisions about individuals and to clarify the safeguards that must be in place.[109] Automated decision-making is the process of making a decision by automated means without human involvement.[110] The Information Commissioner's Office explains that these decisions can be based on factual data as well as on digitally created profiles or inferred data. Examples of where it might be used include an online decision to grant a loan or a recruitment aptitude test that uses pre-programmed algorithms and criteria.

Currently, under article 22 of the UK GDPR, if a decision about an individual would produce legal effects for that individual, or "similarly significantly" affect them, an organisation can make the decision using solely automated processing only if the decision meets one or more specified conditions, namely that the decision was:[111]

- necessary for the entry into or performance of a contract
- authorised by domestic law applicable to the data controller
- based on the individual's explicit consent

---

[109] As above, p 14.

[110] Information Commissioner's Office, 'What is automated individual decision-making and profiling?', accessed 28 October 2024.

[111] Information Commissioner's Office, 'Rights related to automated decision making including profiling', accessed 27 October 2024.

Clause 80 of the bill would remove the existing article 22 from the UK GDPR and replace it with new provisions. Under new article 22A, a decision would qualify as being "based solely on automated processing" if there was "no meaningful human involvement in the taking of the decision". A decision would qualify as being a "significant decision" if it produced "a legal effect for the data subject" or had a "similarly significant effect for the data subject". New article 22D would give the secretary of state the power to make regulations to describe cases that are or are not to be taken to have meaningful human involvement, or what is or is not to be taken as a significant decision. The government has said this would allow it to determine when meaningful human involvement and significant decisions had taken place in light of constantly emerging technologies and changing societal expectations.[112]

New article 22B would maintain restrictions similar to the existing ones for solely automated decision-making where the decision was based wholly or partly on 'special category' data. 'Special category' data is sensitive data that needs more protection because it reveals someone's political opinions, racial or ethnic origin, religious or philosophical beliefs, trade union membership, is genetic or biometric data, or concerns their health, sex life or sexual orientation.[113] Data controllers could use solely automated decision-making to take a decision based entirely or partly on special category data only if one of the following conditions applied:

- The data subject had given explicit consent.
- The decision was necessary for reasons of substantial public interest on the basis of domestic law or relevant international law, and either necessary for the entry into or performance of a contract, or required or authorised by law

Data controllers could not rely on the new 'recognised legitimate interest' ground created by clause 70 to take a decision using solely automated processing.

Fewer restrictions would apply for decisions taken solely by automated processing that were based wholly or partly on personal data (rather than special category data), but new article 22C would require certain safeguards to be in place for such decisions. The data subject would have to:

- be provided with information about decisions taken about them

[112] Explanatory notes, pp 80–1.
[113] UK GDPR, article 9(1) and Information Commissioner's Office, 'Special category data', accessed 29 October 2024.

- be enabled to make representations about such decisions
- be enabled to obtain human intervention in relation to such decisions
- be enabled to contest such decisions

New article 22D would allow the secretary of state to make regulations to make further provisions about these safeguards, for example to specify additional safeguard measures. The government has said this power would allow it to provide legal clarity on the safeguards which must apply as new technologies emerge.[114] However, the regulations could not amend article 22C.

The Conservatives' data bill would have allowed the secretary of state to use this power to "vary" the safeguards in article 22C. The DPRRC expressed concerns at the time that this power could have been used to make changes which in some way would limit the scope of a particular safeguard.[115] It recommended that the power should explicitly be made subject to the condition that it could only be exercised where doing so would not reduce the protection afforded by article 22C.

As well as amending the UK GDPR, clause 80 would also make similar—but not identical—amendments to part 3 of the DPA 2018, which covers data processing by the police and other law enforcement authorities. The government has highlighted the main differences between the changes to the two regimes as follows:[116]

- A "significant decision" under part 3 of the DPA 2018 would be one that produces an adverse legal effect or similarly significant adverse effect for the data subject. The government has said that this is because under part 3, data subjects are "unlikely to perceive the majority of decisions taken by the competent authorities as positive, whereas the effect of a significant decision under the UK GDPR may be more nuanced".
- Significant decisions based entirely or partly on the processing of sensitive personal data (the equivalent of special category data in the UK GDPR) could be made solely via automated processing only where the data subject has consented or where it is required or authorised by law. Processing for

[114] Explanatory notes, p 81.
[115] House of Lords Delegated Powers and Regulatory Reform Committee, 'Data Protection and Digital Information Bill, Pedicabs (London) Bill [HL]', 14 February 2024, HL Paper 60 of session 2023–24, p 4. The relevant power in the Conservatives' bill was in clause 14.
[116] Explanatory notes, p 81.

entering into a contract is not a valid basis for taking such a decision, as the government considers it unlikely such a situation would arise under part 3.

- There would be exemptions from the safeguards that would otherwise apply to significant decisions taken solely by automated processing based wholly or partly on personal data. The safeguards would not apply if the decision was to avoid obstructing or prejudicing an investigation, or to protect public security, national security or the rights and freedoms of others. However, where a decision was taken solely by automated processing relying on one of these exemptions, it would have to be reviewed as soon as reasonably practicable with meaningful human involvement.

Schedule 6 would make minor and consequential amendments.

### Logging of law enforcement processing (clause 81)

Section 62 of the DPA 2018 introduced a requirement that law enforcement authorities must keep logs of their data processing activities. This means that each time a police officer accesses or discloses someone's personal data, they have to record the reason for accessing or disclosing it, as well as other information such as the date, time and if possible the identity of those accessing, disclosing or receiving the data.[117] Accessing personal data would include, for example, looking up a suspect or person of interest on the police database. The government has argued that recording a justification each time is "burdensome, time consuming and does not achieve the purpose envisaged for keeping logs, which is limiting the misuse of data".[118] The government maintains that manually input justifications are "of little value and are rarely relied upon, as persons misusing data are highly unlikely to admit this in a formal log or to enter an honest justification".

Clause 81 would therefore remove the requirement for a competent authority to record a justification in the log when consulting or disclosing personal data. The government estimates this would free up to 1.5mn hours of police time and save around £42.8mn in taxpayers' money every year.[119] However, the requirement would remain to log the time and date the personal data was consulted or disclosed.[120]

---

[117] Department for Science, Innovation and Technology, 'Data (Use and Access) Bill factsheet: Improving public services', 24 October 2024.
[118] As above.
[119] Department for Science, Innovation and Technology et al, 'New data laws unveiled to improve public services and boost UK economy by £10 billion', 24 October 2024.
[120] Explanatory notes, p 15.

### Codes of conduct (clauses 82 and 83)

Clause 82 would amend article 41 of the UK GDPR to clarify that bodies accredited to monitor compliance with approved codes of conduct for the processing of personal data would have to notify the information commissioner that they had taken action for an infringement of the code only if they suspended or excluded a person from the code. The government has said that this would reflect the information commissioner's operational approach and would ensure consistency with amendments to the Privacy and Electronic Communications Regulations 2003 made by clause 114 of the bill.

Clause 83 would amend the DPA 2018 to enable expert public bodies to create codes of conduct relating to law enforcement processing of personal data. An "expert public body" would be one that, in the information commissioner's opinion, had the knowledge and experience needed to produce such a code of conduct. The government has said that this would mirror the existing provision for codes of conduct under the UK GDPR.[121] The government also said that law enforcement agencies would be expected to monitor their compliance with any code of conduct produced under the law enforcement processing regime through existing internal auditing mechanisms.

### International transfers of personal data (clause 84 and schedules 7 to 9)

Clause 84 would introduce schedules 7, 8 and 9, which deal with the rules for transfers of data to other countries and international organisations. Schedule 7 would make amendments to the UK GDPR in relation to the international transfer regime. Schedule 8 would make amendments to part 3 of the DPA 2018 in relation to the international transfer regime for law enforcement purposes. Schedule 9 would make minor and consequential amendments and transitional provision. The government has said that these amendments would clarify the rules on international transfers of data and contends that they would provide "a clearer and more stable framework" which would facilitate international trade.[122]

### Safeguards for processing for research purposes etc (clauses 85 and 86)

Clause 85 would combine the existing safeguards in the UK GDPR and the DPA 2018 about the processing of personal data for the purposes of scientific or historical research, archiving

---

[121] As above, p 82.
[122] As above, p 14.

in the public interest and for statistical purposes into a new chapter 8A in the UK GDPR.[123] This would include safeguards that would apply to the processing of personal data for research, archives and statistics (RAS) purposes:

- The processing could not be likely to cause substantial damage or substantial distress to a data subject.
- It could not be used to make decisions about an individual data subject to whom the personal data relates, except where the processing was being carried out for the purposes of approved medical research.
- Technical and organisational measures would have to be in place to ensure respect for the principle of data minimisation (collecting the minimum amount of personal data needed to fulfil the purpose).[124]

The secretary of state would have the power to make regulations which make further provisions about these safeguards, for example to specify additional safeguard measures, and to vary or omit any additional safeguard measures that had been added by regulations. However, the regulations could not be used to vary or omit any of the safeguards listed above, other than to change the definition of "approved medical research". The government has said this power would ensure that safeguards for RAS purposes could be kept up to date as technology changes.

Clause 86 would make consequential amendments.

### National security exemption (clause 87)

Clause 28 would amend part 3 of the DPA 2018 to provide exemptions from certain provisions when required for the purposes of safeguarding national security. The government has said that the provisions that may be disapplied in such circumstances include the majority of the data protection principles, the rights of the data subject, certain obligations on competent authorities and processors and various enforcement provisions.[125] The government has said that this clause would ensure that law enforcement authorities would have the same national security exemptions that already exist for organisations (such as

[123] As above, p 83.
[124] Information Commissioner's Office, 'Principle (c): Data minimisation', accessed 28 October 2024.
[125] Explanatory notes, p 83.

businesses) operating under the UK GDPR/section 26 of the DPA 2018, and for intelligence services under section 110 of the DPA 2018.

### Intelligence services: Joint processing (clauses 88 and 89)

Clause 88 would enable joint processing by a "qualifying competent authority" and an intelligence service under part 4 of the DPA 2018 when required for the purposes of safeguarding national security. Part 4 of the DPA 2018 is the regime that governs the processing of personal data by the intelligence services. Clause 88 would enable the secretary of state to designate any of the "competent authorities" listed in schedule 7 of the DPA 2018 (including, for instance, police forces and the National Crime Agency) as a "qualifying competent authority". Any joint processing of personal data carried out would be subject to the controls and safeguards in part 4 of the DPA 2018. Clause 88 sets out various conditions that would apply to the designation notices.

The government said because law enforcement bodies (such as the police) and the intelligence services are governed by different data protection regimes, this can present "challenges to operational working".[126] It said the bill would enable operational partnerships to respond to national security threats and protect the public, "particularly where the processing of data requires complex decisions at pace". It said it was introducing this provision in response to the terrorist incidents that took place at Manchester Arena in 2017 and Fishmongers' Hall in 2019.

Clause 89 would make consequential amendments.

### Information commissioner's role (clauses 90 to 95)

The government has said that the core aims of the bill would be "underpinned by a revamped Information Commissioner's Office".[127] While part 6 of the bill (see below) makes structural changes, replacing the office of information commissioner with an Information Commission, clauses 90 to 95 make changes to the duties, enforcement powers, reporting requirements, data protection complaints process and development of statutory codes of

---

[126] As above, p 15.

[127] Department for Science, Innovation and Technology et al, 'New data laws unveiled to improve public services and boost UK economy by £10 billion', 24 October 2024.

practice. The government has said that these reforms would "give the regulator new, stronger powers and a more modern structure, while maintaining its independence".[128]

Currently, section 2(2) of the DPA 2018 requires the information commissioner to "have regard to the importance of securing an appropriate level of protection for personal data, taking account of the interests of data subjects, controllers and others and matters of general public interest". Clause 90 would create a new principal objective for the information commissioner, which would be:

(a) 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

(b) to promote public trust and confidence in the processing of personal data.

The commissioner would also be required to have regard to the following duties as the commissioner considered to be relevant according to the circumstances:

- 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
- the fact that children may be less aware of the risks and consequences associated with the processing of personal data and of their rights in relation to such processing

The commissioner would be required to publish a strategy within 18 months of the relevant section coming into force, review it from time to time and revise it as appropriate. The commissioner would also be required, when they thought it appropriate, to consult other regulators about how the manner in which the commissioner exercised their functions may affect economic growth, innovation and competition.

[128] Explanatory notes, p 9.

The commissioner is already required to provide a general report annually to Parliament. Clause 90 would require this report to cover what the commissioner had done to comply with the principal objective and other duties, including the duty to consult with other regulators, and the operation of the strategy.

The Conservatives' data bill would have enabled the secretary of state to publish a statement of strategic priorities for data protection, to which the information commissioner would have had to have regard. This provision is not included in Labour's bill.

Currently, the information commissioner is required to produce four statutory codes of practice and may be required by the secretary of state to prepare other codes giving guidance as to good practice in the processing of personal data.[129] Clause 91 would amend the DPA 2018 to ensure that all the codes, whether they are mandated by the DPA 2018 or requested by the secretary of state, would be subject to the same parliamentary approval process, requirements for publication and review and would have the same legal effect.[130]

The Conservatives' data bill initially proposed that the codes of practice (both the four statutory ones and any others required by the secretary of state in regulations) would have to be approved by the secretary of state before they could be laid before Parliament under the negative procedure. Labour argued that this could risk the independence of the information commissioner.[131] At report stage in the House of Commons of the Conservative bill, a government amendment was agreed to remove the requirement for the secretary of state to approve the codes. Instead, the secretary of state would have had 40 days to decide whether to make written recommendations to the commissioner about the code. Any recommendations would also have to be published. The commissioner would have had 40 days (or longer by agreement with the secretary of state) to respond to the recommendations and could decide to withdraw the code. If the code was not withdrawn, it would then be laid before Parliament. If the code was withdrawn, it could be resubmitted to the secretary of state, with or without modifications. This provision is not included in Labour's bill. Under Labour's bill, the information commissioner would be required to consult the secretary of state before drawing up a code or amending it (except for the data

---

[129] As above, p 86. The four statutory codes of practice are on: data sharing (section 121 of the DPA 2018); direct marketing (section 122 of the DPA 2018); age-appropriate design (section 123 of the DPA 2018); and data protection and journalism (section 124 of the DPA 2018).

[130] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 80.

[131] House of Lords Library, 'Data Protection and Digital Information Bill: HL Bill 30 of 2023–24', 13 December 2023, pp 31–3.

protection and journalism code, where there is no requirement for consulting the secretary of state).[132]

Clause 92 would require that when preparing these codes of practice, the information commissioner must establish a panel of experts and stakeholders likely to be affected to consider the code and report to the commissioner on it. The commissioner would be required to make any alterations to the code they considered appropriate in light of the panel's report and, if they did not accept a recommendation from the panel, to explain why. The secretary of state could disapply or modify this requirement for a panel for codes that were required by regulations, but not for the four statutory codes of practice required by sections 121 to 124 of the DPA 2018.

Clause 92 would also require the information commissioner to prepare impact assessments for codes of practice, both the four statutory ones and any the secretary of state required through regulations.

Clause 93 would amend the DPA 2018 to make clear that the commissioner may:[133]

- charge a reasonable fee or refuse a request where the request is "manifestly unfounded or excessive"
- refuse to deal with a manifestly unfounded or excessive request made by any person

Clause 94 would require the commissioner to publish an analysis of their performance at least annually, using key performance indicators.

Clause 95 would replace the existing provisions that govern the ways in which the commissioner can give notices, for example clarifying the way in which notices could be given by email and making arrangements for how notice is given to individuals, bodies corporate, partnerships and unincorporated bodies.

---

[132] Data Protection Act 2018, ss 121–4 and clause 91.

[133] Explanatory notes, p 88.

## Enforcement (clauses 96 to 104 and schedule 10)

The bill would also amend the commissioner's enforcement powers, by:

- clarifying that they could require specific documents as well as information when issuing an information notice (clause 96)
- enabling them to require a report on a specified matter when giving an assessment notice (clause 97)
- removing Ofsted's exemption to the information commissioner's assessment notice power; this would allow the ICO to audit Ofsted's function as a registration authority in the event of a suspected data breach (clause 98)
- enabling them to require people to attend interviews as part of an investigation (clause 99)
- allowing them more time to issue a final penalty notice after issuing a notice of intent (clause 100)

Clause 101 would require the information commissioner to publish an annual report on the regulatory action they had taken, providing details about investigations begun, continued, or completed and enforcement actions taken during the reporting period.

Clause 102 would require data controllers to facilitate the making of complaints by data subjects, and to respond to and make enquiries into the subject matter of complaints from data subjects.[134] It would also enable the secretary of state to make regulations requiring a data controller to notify the information commissioner of the number of complaints received in a specified period. The government has said this clause is intended to enable more complaints to be resolved directly between data controllers and data subjects, allowing the information commissioner to take a more risk-based approach to complaints.[135] Clause 102 also introduces schedule 10, which contains minor and consequential amendments.

The Conservative data bill would have allowed the commissioner to refuse to act on a complaint if it had not been raised with the data controller, or if the controller had not

---

[134] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 83.
[135] As above.

finished handling the complaint and less than 45 days had passed since the complaint was made. This provision is not included in Labour's bill.

Clause 103 would insert a new section into the DPA 2018 about court procedure in relation to legal disputes about subject access requests under both the UK GDPR and, for law enforcement and intelligence services processing of personal data, the relevant provisions of the DPA 2018. It would allow the court to require the data controller to make available to the court whatever information is available to the data controller. The data controller could not be required to carry out a search for the information that was more extensive than the reasonable and proportionate search required for the original subject access request. The court would not be allowed to require the information to be disclosed to the data subject unless or until the matter under dispute had been determined in their favour. The government has said this provision would ensure that courts in relevant cases may inspect material that has been withheld in response to a subject access request when determining whether or not the material is exempt from disclosure.[136] It explained that similar provision was included in the Data Protection Act 1998 but was absent in the DPA 2018. The High Court had rejected an argument that this meant Parliament intended the courts should not be able to inspect the material in the absence of the claimant.[137] The government said clause 103 would put this beyond doubt.

Clause 104 would amend schedule 2 of the Electronic Identification and Trust Services for Electronic Transactions Regulations (SI 2016/696) (the EITSET regulations) in order to apply the changes made by other provisions in the bill.[138] Schedule 2 currently applies—with appropriate modifications—certain enforcement provisions contained within the DPA 2018 so the information commissioner has enforcement powers as the supervisory body for trust services providers. For further information about trust services providers, see section 2.7.7 of this briefing.

### 2.5.1 Protection of prohibitions, restrictions and data subject's rights (clause 105)

The government has explained that clause 105 would amend the DPA 2018 to ensure there are clearer rules about the relationship between key elements of the data protection legislation and:[139]

---

[136] Explanatory notes, pp 95–6.

[137] X v The Transcription Agency and another [2023] EWHC 1092 (KB).

[138] Explanatory notes, p 96.

[139] As above.

- other provisions in legislation or rules of law relating to the processing of personal data
- restriction or prohibitions in legislation on disclosures of personal data

The government says this is needed as a result of the changes to the interpretative effects on EU-derived legislation, such as the UK GDPR, made by the European Union (Withdrawal) Act 2018 and the Retained EU Law (Revocation and Reform) Act 2023.

### 2.5.2 Miscellaneous (clauses 106 and 107 and schedule 11)

Clause 106 would make provision concerning the form, process and procedure for making regulations under the powers in the UK GDPR. For example, it sets out what is meant by the affirmative, negative and made affirmative resolution procedures. It would require the secretary of state to consult the information commissioner and any other persons the secretary of state considers appropriate before making regulations under the UK GDPR. However, this would not apply for international data transfers where the secretary of state had made an urgency statement setting out reasons why the secretary of state considered it desirable for the regulations to come into force without delay.

Clause 107 would introduce schedule 11 which contains minor amendments to the UK GDPR and DPA 2018.

### 2.5.3 Privacy and electronic communications (clauses 108 to 114 and schedules 12 and 13)

Clauses 108 to 114 would amend the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) in relation to nuisance calls, personal data breach reporting by communications service providers, confidentiality of terminal equipment, the ICO's enforcement powers and sectoral codes of conduct.[140] Clause 108 specifies that the regulations would be referred to as the PEC Regulations.

Clause 109 would amend and insert various definitions in regulation 2 of the PEC regulations. Notably, it would clarify that the definition of "calls" includes all calls, regardless of whether

[140] As above, p 14.

they reach their intended recipient, and clarify the definition of "communications" to make clear it covers texts and emails that are transmitted but may not reach their intended recipient.[141]

Clause 110 would adjust the period within which the information commissioner must be notified of a personal data breach under the PEC Regulations. Currently, regulation 5 requires service providers to notify the information commissioner of a personal data breach "without undue delay". Article 2 of Commission Regulation (EU) No 611/2013, which is now a piece of assimilated law, requires providers of publicly available electronic communications services to notify the information commissioner of a personal data breach "no later than 24 hours after the detection of the personal data breach, where feasible". Clause 110 would amend both the PEC Regulations and Commission Regulation (EU) No 611/2013 to require service providers to notify the information commissioner of personal data breaches "without undue delay and, where feasible, not later than 72 hours after having become aware of it". If the notification was not made within 72 hours, it would have to be accompanied by an explanation of the reasons for the delay. Service providers would be able to provide information about the breach to the information commissioner "in phases, without undue further delay" if it was not all available at the time of notification.

Clause 111 would amend the PEC Regulations in relation to 'cookies'. A cookie is a small file of letters and numbers that is downloaded on to an individual's equipment when they visit a website.[142] A cookie can do things such as remember a user's preferences, record what an individual has put in their online shopping basket or count the number of visitors to a website. Currently regulation 6 sets out rules on the confidentiality of communications in "terminal equipment" such as computers, mobile phones, wearable technology, smart TVs and connected devices.[143] Regulation 6 prevents the storing of information or gaining access to information in an individual's terminal equipment, such as by placing cookies, unless the individual is provided with clear and comprehensive information about the purposes of the storage of or access to that information and has given their consent to the cookie.

Clause 111 would replace the current regulation 6 with new wording that would prevent the storage of or access to information in the terminal equipment of a subscriber unless it was done in accordance with the conditions set out in new schedule A1 to the PEC Regulations. Schedule 12 to the bill contains new schedule A1. The schedule would continue to allow organisations to store information or gain access to information stored in an individual's

---

[141] As above, pp 99–100.

[142] Information Commissioner's Office, 'What are cookies?', accessed 28 October 2024.

[143] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 84.

terminal equipment if the individual had been provided with clear and comprehensive information about the purpose and had given their consent.[144] It would also continue to allow storage of or access to information for the sole purpose of transmitting a communication over an electronic communication network, and where it was strictly necessary for the provision of an "information society service".[145]

The schedule would also create the following new exceptions:

- collecting statistical information about how an organisation's service or website was being used with a view to making improvements (eg how many people are accessing a service or how long they are staying on a page)
- enabling an online service to be displayed on the user's device in a certain way (eg saving the user's font preference, or adapting the display to the size of their device's screen)
- enabling the user's geographical location to be ascertained so assistance can be provided to the user in response to an emergency communication from their device

In the first two cases, the individual would have to be provided with clear and comprehensive information about the purpose and be given a simple and free means of objecting.

Clause 111 would also give the secretary of state the power to make regulations to add new exceptions to the cookie consent requirements after consultation with the information commissioner.

The government has said that clause 111 and schedule 12 would help to "reduce the friction caused by numerous cookie consent pop-ups, banners etc that are used on websites and apps to request user consent to cookies and similar technologies".[146]

---

[144] Explanatory notes, p 131.

[145] An "information society service" is broadly defined as "any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service" (Privacy and Electronic Communications (EC) Regulations 2003, regulation 2 and Electronic Commerce (EC Directive) Regulations 2002, regulation 2).

[146] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, p 84.

The Conservative data bill would have allowed storage of/access to information in an individual's equipment for the sole purpose of installing software updates on the equipment that were necessary for security reasons (subject to certain conditions). This is not included in Labour's bill.

Clause 112 would clarify how the period of time in regulation 16A(6) of the PEC Regulations should be interpreted. This relates to the length of time communications providers have to erase or anonymise users' traffic or location data that the communications provider has processed for the purpose of providing an emergency alert service.

Clause 113 would apply what the government describes as the "more modern enforcement powers" in the DPA 2018 to the PEC Regulations.[147] Currently, enforcement of the PEC Regulations relies on powers in the Data Protection Act 1998. The government has said this would ensure that there is a "more cohesive" enforcement regime between the PEC, the UK GDPR and the DPA 2018.[148] However, some differences would remain. Notably, a fixed fine of £1000 would apply under the PEC Regulations where a service provider failed to inform the information commissioner within 24 hours of becoming aware of a data breach. Under the UK GDPR, data controllers who fail to inform the information commissioner of a data breach within a specified timeframe are subject to a penalty of up to 2% of global annual turnover, or £8.7mn, whichever is the higher. Clause 117 would give the secretary of state the power to change the amount of the fixed penalty fine under the PEC Regulations. The government assesses it is not necessary to change the amount of the fixed penalty at the moment as the scope of the reporting requirements under the PEC Regulations and the UK GDPR is different, and it is satisfied that the £1000 is "presently sufficient due to the information commissioner's relationship with the telecommunications sector".

Clause 113 also introduces schedule 13. This schedule would set out modifications to the enforcement regime in the DPA 2018 so it could be applied to the PEC Regulations.

Clause 114 would insert new regulations into the PEC Regulations requiring the information commissioner to encourage representative bodies (such as trade associations) to design codes of conduct on complying with the PEC Regulations to reflect specific data processing operations within a particular sector. The new regulations would also set out the requirements that would have to be met before the information commissioner could approve a code or accredit a monitoring body for a code.

---

[147] Explanatory notes, p 102.

[148] Department for Science, Innovation and Technology, 'Delegated powers memorandum', 24 October 2024, pp 85–6.

## 2.6 Part 6: Information Commission

Clauses 115 to 118 and schedule 14 would establish a new body corporate, the Information Commission, to replace the existing regulator, which is currently structured as a 'corporation sole'.[149] Clause 115 would establish the new Information Commission. Clause 116 would abolish the office of the information commissioner. Clause 117 would transfer functions from the information commissioner to the Information Commission. Clause 118 would enable the secretary of state to make a scheme to transfer property, rights and liabilities from the information commissioner to the Information Commission. Schedule 14 would make further provision about the Information Commission, such as membership, remuneration and procedural requirements.

The government has said that these governance changes would give the regulator a "more modern structure—while maintaining its independence".[150]

## 2.7 Part 7: Other provision about use of, or access to, data

### 2.7.1 Information standards for health and social care (clause 119 and schedule 15)

The Health and Social Care Act 2012 gives the secretary of state and NHS England the power to set information standards for health services or adult social care in England.[151] An information standard is a document containing standards that relate to the processing of information.[152] These may include technical standards, data standards or information governance standards. Technical standards could relate to the specification of systems and may, for example, include messaging, system interoperability or security requirements. Data standards include defining the structure and type of information to be recorded, for example how to record dates of birth or a clinical condition. Information governance standards could relate to policies, procedures or guidelines on information processing.

Clause 119 and schedule 15 of the bill would amend the 2012 act to make clear that information standards in relation to the processing of information include standards relating

---

[149] Explanatory notes, p 104.
[150] As above, p 9.
[151] Health and Social Care Act 2012, section 250.
[152] Explanatory notes to the Health and Social Care Act 2012, March 2012.

to IT technology or IT services.[153] They would ensure that information standards could apply to IT providers, IT services, or information processing services using IT that were used (or intended for use) in connection with the provision of or in relation to health or adult social care in England. Where an information standard applies to a person, they would be required to comply with it (unless the requirement is waived).[154]

The government has said IT providers in the health and social care system provide products that are "currently not uniformly based on information standards that enable information to be accessed and shared in real time across the entire health and social care system".[155] It believes that ensuring information flows in a standardised, consistent and accessible way would improve data quality, enhance the user experience and enable the government to "leverage innovative technologies and ensure the long-term stability of the NHS". It estimates that better data flows would save staff time, improve the accuracy of patient records, save money by reducing the need for duplicate tests and improve patient safety by reducing medication errors.

### 2.7.2 Smart meter communication services (clause 120 and schedule 16)

Clause 120 introduces schedule 16, which would make provision about granting smart meter communication licences. It would amend the Energy Act 2008 to give the Gas and Electricity Markets Authority the power to make regulations about the procedure to be followed for granting such a licence.

There is an ongoing programme to roll out energy smart meters to all homes and small businesses in Great Britain.[156] Enabling smart meters to send and receive communications is central to the operation of smart metering.[157] The smart metering data and communications infrastructure is currently provided by Smart DCC Ltd (also referred to as DCC), which was awarded the smart meter communications licence by the Gas And Electricity Markets Authority with effect from September 2013, following an open competition.[158]

---

[153] Explanatory notes, p 10.
[154] As above, p 23.
[155] Department for Science, Innovation and Technology, 'Data (Use and Access) Bill factsheet: Improving public services', 24 October 2024.
[156] For information about the progress of the rollout, see: House of Commons Public Accounts Committee, 'Update on the rollout of smart meters', 20 October 2023, HC 1332 of session 2022–23.
[157] Explanatory notes, p 16.
[158] As above; and Data Communication Company, 'Smart meter communication licence and regulation', accessed 29 October 2024.

The current licence is due to end in September 2025. Ofgem has carried out a review to put in place a new regulatory framework for DCC following the expiry of its licence and to identify and appoint a successor licensee.[159] As part of this review, Ofgem recommended there should be more flexibility in the process to appoint a successor licensee.[160] It said a competitive process should remain the preferred approach, but alternatives, such as a direct award to a new or existing entity, should be available in case it reached the view that a competitive procurement was not likely to result in a positive outcome.

This provision is a new one that did not appear in the Conservative data bill.

### 2.7.3 Information to improve public service delivery (clause 121)

Section 35 of the Digital Economy Act 2017 (DEA 2017) provides what the government describes as a "legal gateway" to allow specified public authorities to share information with each other to improve the delivery of public services to individuals and households.[161] Clause 121 would amend the DEA 2017 to enable the sharing of information to improve the delivery of public services to businesses as well as to households and individuals. The government has said that the aim of this is to enable businesses to access government services and support more easily, giving them easier access to information, guidance and business support services.[162]

### 2.7.4 Retention of information by providers of internet services (clause 122)

Clause 122 would require social media companies to keep relevant personal data of a child who has died so the data could then be used in subsequent investigations or inquests. This would implement a Labour manifesto pledge to give coroners more powers to access information held by technology companies after a child's death.[163] This followed campaigns by bereaved families, for instance in the case of Molly Russell, a 14-year-old who ended her life

---

[159] Ofgem, 'DCC review: Process for appointing the successor smart meter communication licence holder', 19 July 2024.
[160] Ofgem, 'Decision: DCC Review—process for appointing the successor smart meter communication licence holder: Conclusions', 18 September 2024.
[161] Explanatory notes, p 35.
[162] As above, p 16.
[163] Labour Party, 'Labour Party manifesto 2024', June 2024, p 103.

in November 2017 after viewing suicide and self-harm content online, and Breck Bednar, a teenager who was murdered by someone he had met online.[164]

Clause 122 would amend the Online Safety Act 2023 to set out a process for Ofcom to issue a notice to a provider requiring them to retain information in connection with an investigation by a coroner (or procurator fiscal in Scotland) into the death of a child. The information would have to be kept for one year. Ofcom could extend this for up to six months at a time, in response to information received from the investigating authority. It would be an offence for someone who had received a notice to delete or alter information required by the notice to be kept if their intention was to prevent the information being available for the investigation into the child's death. A senior manager who failed to take all reasonable steps to prevent information being deleted or altered in this way would also be committing an offence.

The Online Safety Act 2023, which received royal assent in October 2023, gives Ofcom the power to require providers of certain online services to provide information about a deceased child's use of the service in connection with an investigation by a coroner (or procurator fiscal in Scotland) into the death of the child.[165] The Conservative government said during the passage of the Online Safety Act 2023 that this measure would "help families and law enforcement understand if online activity contributed to their death in any way".[166] However, the Online Safety Act does not currently require social media companies to retain children's personal data. The amendments made by the bill are intended to ensure that information on the child's social media and internet use are not deleted as part of a platform's routine maintenance while an investigation is active.[167]

When a similar measure was first added to the Conservative data bill, it covered only deaths where the coroner suspected the child might have taken their own life.[168] The bill was amended at committee stage in the House of Lords to extend the provision to all child

---

[164] BBC News, 'Molly Russell: Coroner's report urges social media changes', 14 October 2022; and 'Breck Bednar murder: Lewis Daynes sentenced to life in prison', 12 January 2015.

[165] Online Safety Act 2023, s 101.

[166] Department for Science, Innovation and Technology, 'Online Safety Bill bolstered to better protect children and empower adults', 30 June 2023.

[167] Explanatory notes, p 17.

[168] House of Lords Library, 'Data Protection and Digital Information Bill: HL Bill 30 of 2023–24', 13 December 2023.

deaths, not just suspected suicides.[169] Bereaved families who had been campaigning on the issue welcomed this change.[170]

### 2.7.5 Information for research about online safety matters (clause 123)

Clause 123 would amend the Online Safety Act 2023 to enable the secretary of state to make regulations requiring providers of regulated services to provide information for purposes related to the carrying out of independent research into online safety matters. The government has said this would enable the creation of a framework allowing researchers access to data relating to online safety that is held by tech companies.[171] The Online Safety Act 2023 requires Ofcom to report on how and to what extent independent researchers can access information about online safety from service providers.[172] Ofcom has issued a call for evidence to seek input from stakeholders to inform this report. The call for evidence is open until mid-January 2025. The government has said this report will provide an evidence base to inform the design of the access framework.[173] The secretary of state would have to consult Ofcom, the information commissioner, and other stakeholders before making regulations to create the access framework.

This is a new provision that was not included in the Conservative data bill.

### 2.7.6 Retention of biometric data (clauses 124 to 126)

Clauses 124 to 126 would enable law enforcement authorities to retain fingerprints and DNA profiles (biometrics) for longer without having to obtain a national security determination.[174]

---

[169] HL Hansard, 24 April 2024, col 555GC.
[170] BBC News, 'Bereaved parents win online harm battle', 3 February 2024.
[171] Explanatory notes, p 10.
[172] Ofcom, 'Call for evidence: Researchers' access to information from regulated online services', 28 October 2024.
[173] Explanatory notes, p 17.
[174] For further information about 'national security determinations', see: Home Office, 'Protection of Freedoms Act 2012: Revised guidance on the making or renewing of national security determinations allowing the retention of biometric data', August 2020.

The Counter-Terrorism Act 2008 allows biometrics to be held for up to three years from the point at which they were taken.[175] However, they can be retained indefinitely where an individual has a prior UK conviction for a recordable offence, or where the police do not know the identity of the person to whom the biometrics relate. Where an individual does not have a conviction, but the police consider that it is necessary and proportionate for the purposes of national security to retain the biometrics, they can submit a national security determination. National security determinations require approval by a chief officer. They can be approved for up to five years and can be renewed.

Clause 124 would amend the Counter-Terrorism Act 2008 to enable a law enforcement authority to retain fingerprints and DNA profiles where a person had been convicted of an offence equivalent to a recordable offence in a jurisdiction outside England and Wales and Northern Ireland. This would enable the police to retain the biometrics indefinitely for national security purposes if the individual had a foreign conviction equivalent to a conviction in England, Wales, or Northern Ireland. There would be no need for a chief officer of a police force to make a national security determination to authorise the retention.

Clause 125 would enable the police to pseudonymise biometric data received from international partners so they could hold the material in a form that did not include information identifying the person. Existing provisions in the Counter-Terrorism Act 2008 would then allow the police to hold the pseudonymised biometric data indefinitely.[176] When this provision was added to the Conservatives' data bill, the Conservative government said counter-terrorism police had requested this change.[177]

Clause 126 would insert a new section into the Counter-Terrorism Act 2008 that would enable the police to keep biometrics shared via Interpol, for as long as the relevant Interpol notice remained in force, without having to submit a national security determination. Interpol notices are international requests for cooperation or alerts allowing police in member countries to share crime-related information.[178] When this provision was added to the Conservatives' data bill, the Conservative government said it would bring the UK into line with the rules under which other Interpol members retained and used these biometrics. The amendment was reportedly welcomed by counter-terrorism police, the independent reviewer of terrorism legislation, the Office of the Biometrics Commissioner and the security services.[179] The Labour government has said the change would enable the retention

---

[175] Explanatory notes, p 17.
[176] Counter-Terrorism Act 2008, s 18A(4).
[177] HC Hansard, 29 November 2023, col 876.
[178] Interpol, 'About notices', accessed 29 October 2024.
[179] HC Hansard, 29 November 2023, col 876.

of data the police might otherwise have had to destroy, whilst minimising the intrusion on individual rights.[180]

### 2.7.7 Trust services (clauses 127 to 132)

Clauses 127 to 132 relate to trust services provided by providers outside the UK. A trust service is a service designed to protect electronic data and demonstrate that it can be trusted, for example by identifying the person or organisation that originated the data.[181] Examples of trust services include electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services and website authentication certificates.[182]

A piece of legislation known as the UK eIDAS Regulation governs trust services.[183] This is the UK assimilated version of an EU regulation. The Information Commissioner's Office is the supervisory body for trust services in the UK. It can grant a trust service provider qualified status, which provides assurance in the provider's trustworthiness and compliance with the UK eIDAS requirements.[184]

Clause 128 would amend the UK eIDAS Regulation to allow the ICO to accept reports from accredited conformity assessment bodies in the EU when granting qualified status to trust service providers. Clause 129 would enable the secretary of state to make regulations to end the UK's existing unilateral recognition of EU qualified trust services if it was no longer appropriate. Clause 130 would allow the secretary of state to make regulations to recognise products provided by other overseas trust service providers. The secretary of state would have to be satisfied that the reliability of the overseas trust service product was at least as reliable as an equivalent UK product for it to be granted qualified status under the UK eIDAS Regulation. Clause 130 would also allow the secretary of state to make regulations recognising, for the use of online public services, specified electronic seals and signatures provided by trust service providers established outside the UK as equivalent to ones that met certain standards in the eIDAS Regulation.

---

[180] Explanatory notes, p 17.

[181] Information Commissioner's Office, 'Guide to eIDAS: Key definitions', accessed 29 October 2024.

[182] Information Commissioner's Office, 'Guide to eIDAS: Qualified trust services', accessed 29 October 2024.

[183] Its full name is Regulation (EU) 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. The version that applies in the UK is the assimilated law version, as amended by SI 2019/89.

[184] Information Commissioner's Office, 'Guide to eIDAS: Qualified trust services', accessed 29 October 2024.

Clause 131 would allow the secretary of state to make regulations to designate certain overseas regulators or supervisory bodies as ones with which the information commissioner could cooperate in the interests of effective regulation or supervision of trust services.

Clause 132 would make provision about the interpretation of time periods within the UK eIDAS Regulation and the EITSET regulations.

The government has said that these amendments would enable interoperability with trust services in other countries, which would facilitate international business, reduce trade friction and enhance confidence and security.[185]

### 2.8 Part 8: Final provisions

Clauses 133 to 138 contain provisions on consequential amendments, the making of regulations, extent, commencement, transitional, transitory and saving provision and short title. The majority of the bill extends to the whole of the UK, but some provisions have a different extent. Annex A of the explanatory notes to the bill gives a clause-by-clause breakdown of territorial extent and application.

## 3. Response to the bill

The information commissioner, John Edwards, welcomed the introduction of the bill. He said it was an important piece of legislation that would allow his office to "continue to operate as a trusted, fair and independent regulator and provide certainty for all organisations as they innovate".[186] He said the ICO would issue a response to the bill in due course.

Trade groups within the digital and technology sectors have welcomed the balance struck in the bill. Chris Combemale, chief executive of the Digital Marketing Association, said his members would welcome maintaining a high level of data protection and the current accountability framework.[187] Neil Ross, associate director for policy at techUK, the UK's technology trade association, said the bill marked the start of a "welcome effort" to unlock

---

[185] Explanatory notes, p 18.

[186] Information Commissioner's Office, 'Statement in response to the introduction of the Data Use and Access Bill in the House of Lords', 24 October 2024.

[187] Research Live, 'UK government releases new data bill', 28 October 2024.

the power of data.[188] He described the legislative changes as striking "the right balance between maintaining the UK's existing high data protection standards and driving forward essential reform". However, he said they must be coupled with the "cultural and organisational mindset shift required to seize the full potential advantages of new data-driven technologies".

However, privacy campaigners have voiced strong concerns about it. The Open Rights Group said that the bill would fail to protect the public from harmful uses of artificial intelligence. It was particularly concerned the bill could weaken people's rights and give companies and organisations more powers to use automated decision-making and would fail to protect the public.[189] It said this was "of particular concern in areas of policing, welfare and immigration where life-changing decisions could be made without human review". The group also expressed concern that removing the need for police to log a justification for accessing personal data would reduce accountability and transparency. It claimed it would make abuse more likely. It was also critical of allowing data gathered for the purpose of research to be used for commercial purposes. Additionally, the group maintained that the government's ability to select members of the new Information Commission would interfere with the commission's independence.

Similarly, Big Brother Watch said the bill would water down data protection laws by "simultaneously eroding privacy protections and restricting people's control over their own data".[190] It maintained the bill "threatens to set the UK years behind our international partners when it comes to safeguarding against the threats of new and emerging technologies such as AI".

The law firm A&O Shearman assessed that the bill was likely to be "good news" for the UK's retention of a data adequacy decision from the EU.[191] The EU makes unilateral 'data adequacy decisions' about whether non-EU countries offer what it considers to be an adequate level of data protection.[192] If so, personal data can be transferred between that country and the EU without any further safeguards. The EU adopted data adequacy decisions

---

[188] techUK, 'The Data (Use and Access) Bill: What's changed and what remains from the DPDI Bill?', 25 October 2024.
[189] Open Rights Group, 'Data Use and Access Bill will fail to protect public from AI harms', 24 October 2024.
[190] Big Brother Watch, 'Privacy campaigners raise concerns over government's new data bill', 24 October 2024.
[191] A&O Shearman, 'DUA (Lipa) Bill—Hotter than hell or just a few new rules?', 28 October 2024.
[192] European Commission, 'Adequacy decisions', accessed 30 November 2023.

covering the UK in June 2021.[193] The UK's data adequacy status runs out in June 2025, at which point the European Commission has to decide whether to extend it or let it expire.[194]

While the Conservatives' data bill was going through Parliament, stakeholders in the UK and the EU had suggested that proposals included in the early versions of the bill that were perceived to impact on the independence of the ICO—such as giving the secretary of state power to veto codes of conduct—might put at risk the EU's adequacy decision for the UK.[195]

The House of Lords European Affairs Committee wrote to Peter Kyle, secretary of state for science, innovation and technology, the day before the Data (Use and Access Bill) [HL] was introduced, to make some recommendations it believed could inform Labour's bill and its engagement with the EU on the adequacy renewal process.[196] The committee said that losing EU data adequacy status would "impose significant extra costs and administrative burdens on businesses and public sector organisations which share data between the UK and the EU" and raise new barriers to international trade and economic cooperation. It recommended the government should engage with the European Commission and other EU stakeholders in good time to explain and provide reassurance about any planned data protection reforms, particularly in areas such as the independence of the ICO and any new role for ministers to add new grounds of 'legitimate interest' for data processing. It believed there was scope for beneficial reforms to the operation of the UK GDPR, particularly its cost to businesses, that would "not necessarily jeopardise the UK's adequacy status". It said in preparing its data bill, the government should take account of the amendments to the Conservatives' Data Protection and Digital Information Bill that had been adopted before the bill fell at dissolution.

---

[193] Department for Digital, Culture, Media and Sport, 'EU adopts 'adequacy' decisions allowing data to continue flowing freely to the UK', 28 June 2021.

[194] House of Lords European Affairs Committee, 'British businesses and NHS face huge extra costs if crucial UK-EU data agreement is not reached', 23 October 2024.

[195] Joe Jones, 'UK GDPR reforms move forward in UK Parliament', International Association of Privacy Professionals, 29 November 2023.

[196] House of Lords European Affairs Committee, 'Letter to the Rt Hon Peter Kyle MP, secretary of state for science, innovation and technology, re: UK-EU data adequacy', 22 October 2024.

## About the Library

A full list of Lords Library briefings is available on the Library's website.

The Library publishes briefings for all major items of business debated in the House of Lords. The Library also publishes briefings on the House of Lords itself and other subjects that may be of interest to members.

Library briefings are produced for the benefit of Members of the House of Lords. They provide impartial, authoritative, politically balanced information in support of members' parliamentary duties. They are intended as a general briefing only and should not be relied on as a substitute for specific advice.

Every effort is made to ensure that the information contained in Lords Library briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

## Disclaimer



Authors are available to discuss the contents of the briefings with Members of the House of Lords and their staff but cannot advise members of the general public.

**Any comments on Library briefings should be sent to the Head of Research Services, House of Lords Library, London SW1A 0PW or emailed to hlresearchservices@parliament.uk.**