LIBRARY BRIEFING

HOUSE OF LORDS

HL Bill 30 of 2023–24

Data Protection and Digital Information Bill

Author: Nicola Newson
Date published: 13 December 2023

The Data Protection and Digital Information Bill is due to have its second reading in the House of Lords on 19 December 2023. The bill would amend existing data protection legislation in ways the government says would reduce burdens on organisations while maintaining high data protection standards.

Among other things, the bill would also reform the governance structure and powers of the information commissioner. It would clarify rules on international data transfers, allowing the secretary of state to approve 'data bridges' with other countries. It would establish a regulatory framework for digital verification services providers. It would enable the government to require data holders to share customer data at the customer's request to enable smart data schemes. It would enable law enforcement authorities to retain biometric data obtained from foreign partners for longer. It would allow Ofcom to require social media companies to retain information in connection with an investigation by a coroner into the death of a child who was suspected to have died by suicide. It would establish electronic, rather than paper-based, registers of births and deaths. It would also establish a national underground asset register. It would abolish the biometrics commissioner and surveillance camera commissioner, transferring some of their functions to other regulators.

Table of Contents

Hundreds of government amendments were made to the bill in the House of Commons. Labour argued at report stage that the bill should be recommitted to a public bill committee to allow further scrutiny, but this motion was defeated. Labour welcomed a government amendment at report stage removing the secretary of state's power to veto codes of conduct drawn up by the information commissioner. MPs raised concerns about new provisions added at report stage to enable the government to require banks and financial institutions to provide data about accounts linked to benefit claimants, which the government argues is necessary to tackle benefit fraud. MPs questioned why state pension claimants were included. They also raised concerns about the Department for Work and Pensions (DWP) having powers to look at people's bank accounts without grounds for suspicion. The provisions were added to the bill after a division. Non-government amendments on democratic engagement, high-risk processing of data and safeguards on automated decision-making were defeated at report stage.

1. Background

1.1 Introduction and carry-over

The Data Protection and Digital Information Bill is due to have its second reading in the House of Lords on 19 December 2023.

The government originally introduced a Data Protection and Digital Information Bill in the House of Commons in July 2022, under Boris Johnson's premiership.[1] However, following the election of Liz Truss as the new party leader, the government announced on 5 September

[1] UK Parliament, 'Data Protection and Digital Information Bill', last updated 5 May 2023.

2022 that second reading of the bill would not take place that day as scheduled, to give ministers time to consider the legislation further.[2] 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.[3] 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 current parliamentary session as the Data Protection and Digital Information Bill. It completed its House of Commons stages on 29 November 2023.

Speaking in March 2023, Michelle Donelan, secretary of state for science, innovation and technology, outlined the benefits the government said the bill would bring:

> […] this new bill ensures that a vitally important data protection regime is tailored to the UK's own needs and our customs.
>
> Our system will be easier to understand, easier to comply with, and take advantage of the many opportunities of post-Brexit Britain. No longer will our businesses and citizens have to tangle themselves around the barrier-based European GDPR [General

[2] HC Hansard, 5 September 2022, col 25.

[3] House of Commons, 'Written statement: Data Protection and Digital Information (No. 2) Bill (HCWS617)', 8 March 2023.

Data Protection Regulation].

Our new laws release British businesses from unnecessary red tape to unlock new discoveries, drive forward next generation technologies, create jobs and boost our economy.[4]

1.2 Bill documents

The government has published various documents alongside the bill:

- explanatory notes
- delegated powers memorandum, updated 6 December 2023
- impact assessments: the 'Data Protection and Digital Information (No. 2) Bill: Impact assessment' covering the bill as it was introduced in the House of Commons in March 2023, a 'Regulatory powers for smart data: Impact assessment' (July 2022) relating to part 3 of the bill, and 'DWP third party data gathering: Impact assessment' (November 2023) relating to clause 128 and schedule 11 of the bill
- 'Public sector equality duty assessment for Data Protection and Digital Information (No. 2) Bill', updated 27 November 2023
- 'Data Protection and Digital Information (No. 2) Bill: European Convention on Human Rights memorandum', updated 27 November 2023

[4] Department for Science, Innovation and Technology, 'British businesses to save billions under new UK version of GDPR', 8 March 2023.

1.3 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 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 a 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) incorporated the EU GDPR into UK domestic law as a piece of retained EU law.[5] Secondary legislation made using powers in EUWA modified the EU GDPR to ensure that it would still work in the UK after it left the EU.[6] 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

[5] Following the passage of the Retained EU Law (Revocation and Reform) Act 2023, 'retained EU law' will be known as 'assimilated law' after the end of 2023.

[6] Explanatory notes, p 20.

(broadly the police and other criminal justice agencies).[7] 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.[8] Part 4 of the DPA 2018 sets out rules for processing personal data by the UK intelligence services.

Another piece of retained EU 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 a European 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; privacy of customer data relating to communications networks, such as traffic and location data, itemised billing or caller ID.[9]

The bill would make amendments to these existing sources of data protection law.

A blog by the law firm Linklaters suggested that the result of the bill "is likely to be the most complex data protection law in the world based on detailed interactions between the heavily amended, and

---

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

[8] As above, paras 41–3.

[9] Information Commissioner's Office, 'What are PECR?', accessed 1 December 2023.

soon to be re-amended, UK GDPR and Data Protection Act 2018".[10]

The government published Keeling schedules in May 2023 showing the changes that the bill would make to the UK GDPR, the DPA 2018 and the PEC Regulations.[11] However, these relate to the Data Protection and Digital Information (No. 2) Bill as introduced in the House of Commons; at the time this briefing was written, they had not been updated to reflect the amendments made at the Commons committee and report stages.

2. What would the bill do?

The version of the bill introduced in the House of Lords consists of 157 clauses and 15 schedules. Many of its provisions are highly technical, making amendments to the UK GDPR, the DPA 2018 and other pieces of legislation. This section of the briefing gives an overview of some of the main provisions of the bill. Section 6 of this briefing focuses on the new clauses added and amendments made at report stage. Over 250 amendments were made to the bill at report stage, and several MPs suggested that the House of Commons had not had sufficient time to scrutinise them and that they should be further scrutinised in the House of Lords.

For a full clause-by-clause explanation of the bill, the reader should consult the explanatory notes produced by the government.

---

[10] Georgina Kon, '[EU and UK: Continental drift on data protection?]', Linklaters, 30 November 2023.

[11] Department for Science, Innovation and Technology and Department for Work and Pensions, '[Data Protection and Digital Information Bill: Supporting documents]', published 10 May 2023, last updated 27 November 2023.

Additional background on many of the measures in the bill, including government consultations held prior to the bill's introduction and reaction from stakeholders, is given in the House of Commons Library briefing 'Data Protection and Digital Information (No. 2) Bill 2022–23' (28 March 2023). The numbering of the bill's clauses has changed significantly since that briefing was written; readers may therefore find it helpful to cross-refer to the guide in section 9 of this briefing which shows which number referred to which clause at different stages of the bill's passage to date.

2.1 Part 1: Data Protection

Part 1 of the bill would make changes to the UK GDPR and the DPA 2018 that the government says would "benefit those who process personal data whilst retaining high data protection standards.[12]

2.1.1 Definitions

Part 1 would amend some of the definitions within the current legal framework. Clause 1 would create a test to help organisations understand whether the data that they were processing was personal or anonymous.[13] The government has said this is important because personal data is subject to data protection rules, but anonymous data is not. Clause 4 would insert a definition of consent into part 3 of the DPA 2018, the part that governs processing by law enforcement authorities. The government has said this mirrors the definition of consent in the UK GDPR and would address "the slight risk that

[12] Explanatory notes, p 11.
[13] House of Commons Public Bill Committee, 'Data Protection and Digital Information (No. 2) Bill', 16 May 2023, session 2022–23, 3rd sitting, col 86.

consent may be interpreted inconsistently" between the two regimes.[14]

2.1.2 Scientific research, statistics and archiving

Clause 2 would amend definitions relating to processing for research and statistical purposes. Clause 3 would 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.[15] The government said that these provisions would help researchers with their use of personal data and allow for personal data to be reused for the purpose of longer-term research studies.[16] In addition, clause 11 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.[17] Clause 26 would combine the safeguards in the UK GDPR about the processing of personal data for the purposes of scientific or historical research, archiving in the public interest and for statistical purposes into a new chapter in the UK GDPR.[18]

2.1.3 Data protection principles

Clause 5 would amend article 6 of the UK GDPR, which is concerned

[14] House of Commons Public Bill Committee, 'Data Protection and Digital Information (No. 2) Bill', 16 May 2023, session 2022–23, 3rd sitting, col 95.
[15] Explanatory notes, p 30.
[16] As above, p 11.
[17] House of Commons Public Bill Committee, 'Data Protection and Digital Information (No. 2) Bill', 16 May 2023, session 2022–23, 3rd sitting, col 118.
[18] Explanatory notes, p 46.

with the lawful grounds for processing personal data. It would create a new ground for lawful processing, namely that the processing is necessary for a 'recognised legitimate interest'. Schedule 1 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:

- safeguarding national security or protecting public safety
- responding to an emergency
- detecting, investigating or preventing crime or apprehending or prosecuting offenders
- safeguarding vulnerable individuals

It would also include where the processing was necessary for the purposes of democratic engagement. The secretary of state would be able to make regulations to amend the recognised legitimate interests set out in the schedule. Clause 8 would insert a provision into schedule 1 to the DPA 2018 setting out where personal data revealing someone's political opinion could be processed for the purposes of democratic engagement. The definition and uses of democratic engagement was discussed at report stage in the House of Commons; this is covered in section 6.2.2 of this briefing.

Clause 6 would set out the conditions under which the reuse of personal data ("further processing") for a new purpose would be permitted.[19] The government has said this would address current uncertainty about when controllers can reuse personal data. Clause 7 would make clear that specified international treaties could provide a

[19] House of Commons Public Bill Committee, 'Data Protection and Digital Information (No. 2) Bill', 16 May 2023, session 2022–23, 3rd sitting, col 106.

lawful basis for processing personal data under several grounds in the UK GDPR.[20]

2.1.4 Data subjects' rights

Individuals have a right to request a copy of their personal data, which is referred to as a data subject access request.[21] Clause 9 would amend the UK GDPR to allow a data controller to charge a reasonable fee for, or refuse to act on, a data subject request which was "vexatious or excessive". This would replace the existing provision that allows controllers to refuse or charge a fee for "manifestly unfounded or excessive" requests.

Clause 10 would amend the deadlines for organisations to respond to subject access requests. The government said it would enable organisations to "stop the clock" on the response time if they were unable to respond without receiving further information or clarification from the person making the request.[22] It would also extend by up to two months the time permitted for intelligence and law enforcement agencies to respond to complex requests, which the government said would replicate provisions in the UK GDPR. Clause 12 would mean data controllers would need to carry out only a "reasonable and proportionate" search in response to a subject access request. Clause 13 would enable controllers not to give data subjects material that was subject to legal professional privilege (or the equivalent in Scotland).

---

[20] HC Hansard, 29 November 2023, col 873.

[21] Information Commissioner's Office, 'Right of access', accessed 6 December 2023.

[22] House of Commons Public Bill Committee, 'Data Protection and Digital Information (No. 2) Bill', 16 May 2023, session 2022–23, 3rd sitting, col 117.

2.1.5 Automated decision-making

Clause 14 would amend the restrictions on when solely automated decision-making could be used for decisions that would produce legal effects for an individual or affect them in similarly significant ways. Labour and the SNP tried unsuccessfully to amend this provision at report stage; this is covered further in section 6.3.2 of this briefing.

2.1.6 Obligations of controllers and processors

The government has said the bill would "streamline the requirements the current legislation places on organisations to demonstrate how they are complying with the legislation".[23] For example, clause 16 would remove the requirement for overseas controllers subject to the UK GDPR to appoint a UK-based representative. Clause 17 would replace 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. Clause 18 would require organisations to keep records of their processing activities only where it was "likely to result in a high risk to the rights and freedoms of individuals".

2.1.7 International transfers of personal data

Clause 25 and schedules 5 and 6 would clarify the rules on international transfers and cross-border flows of personal data.[24] The government said schedule 5 would "consolidate the existing provisions on international transfers" by "setting out in clearer terms

---

[23] Explanatory notes, p 11.

[24] As above.

the general principles and listing the same bases under which personal data can be lawfully transferred overseas".[25] It would enable the secretary of state to make regulations approving the transfer of personal data to another country or international organisation, a so-called 'data bridge'. Schedule 6 would make related provision for international transfers of personal data covered by the law enforcement processing regime in part 3 of the DPA 2018.[26]

2.1.8 National security exemption

Clause 28 would amend part 3 of the DPA 2018 to provide an exemption from certain provisions when required for the purposes of safeguarding national security. The government said this would "replace the current, more limited national security exemptions that exist in the law enforcement regime and mirror the existing exemptions in the UK GDPR and intelligence services regime".[27]

2.1.9 Joint processing by intelligence services and law enforcement bodies

Clause 29 would enable joint processing by a qualifying competent authority and an intelligence service under part 4 of the DPA 2018 for the purposes of national security if they were granted permission by the secretary of state to do so. 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

---

[25] House of Commons Public Bill Committee, 'Data Protection and Digital Information (No. 2) Bill', 16 May 2023, session 2022–23, 4th sitting, col 161.
[26] As above, col 162.
[27] As above, col 168.

"challenges to operational working".[28] 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.

2.1.10 Information commissioner's role

The government has said it does not believe the current legislation provides the information commissioner with a "sufficiently clear framework of objectives and duties".[29] Clause 31 would provide for a principal objective and general duties for the commissioner when carrying out data protection functions. It would require the commissioner to publish a strategy and to report regularly on how they have complied with the duties. Clause 32 would enable the secretary of state to publish a statement of strategic priorities for data protection; the commissioner would have to have regard to this when carrying out their functions. Under clause 35, the government could make recommendations about codes of practice drawn up by the commissioner but would not be able to veto them as had originally been proposed; this is covered further in section 6.2.5 of this briefing. Clause 36 would allow the commissioner to charge a reasonable fee or refuse a request where the request was "vexatious" or "excessive" (replacing the existing test of whether the request is "manifestly unfounded or excessive).

---

[28] Explanatory notes, p 12.

[29] As above, p 11.

2.1.11 Information commissioner's enforcement powers

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

- clarifying that they could require documents as well as information when issuing an information notice (clause 39)
- enabling them to require a report when giving an assessment notice (clause 40)
- enabling them to require people to attend interviews as part of an investigation (clause 41)
- allowing them more time to issue a final penalty notice after issuing a notice of intent (clause 42)

Clause 43 would require the commissioner to produce an annual report on regulatory activity. Clauses 44 to 46 would, according to the government, "streamline and clarify" complaint routes. Data subjects would be able to complain to a data controller if they believed their data protection rights had been infringed. The commissioner could 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.

2.2 Part 2: Digital verification services

Part 2 of the bill would establish a regulatory framework for the provision of digital verification services (DVS) in the UK. The government has said this would "enable digital identities and attributes to be used with the same confidence as paper

documents".[30] The bill would enable public authorities to disclose personal information to trusted DVS providers for the purpose of verifying identity and eligibility (clause 75). Clause 53 would establish a DVS 'trust framework', including a main code that providers would have to comply with to be able to apply for registration. Clauses 63 to 73 contain provisions about the register, including giving the secretary of state powers to set fees and to remove providers from the register. New clauses were added at report stage in the Commons to enable the recognition of supplementary codes applicable to specific sectors; this is covered further in section 6.2.8 of this briefing.

2.3 Part 3: Customer and business data

Part 3 of the bill would give the secretary of state and the Treasury the power to make regulations requiring data holders to make customer data and business data available to customers or authorised third party-providers (ATPs) at the customer's request. The government has said that these smart data schemes will enable the secure sharing of data, for example data held by communications providers or financial services providers, so that ATPs can provide innovative services, such as personalised market comparisons or account management through account aggregation (for instance, a visual dashboard of accounts displayed on a smartphone app).[31] Part 3 includes provisions on enforcement and financial penalties that could be imposed by the enforcer. It also includes provisions on fees, a levy and financial assistance in connection with meeting the costs associated with part 3. New clauses were added at report stage to enable 'interface bodies' to be set up to develop common standards

[30] Explanatory notes, p 9.
[31] As above, pp 9 and 74.

on arrangements for data sharing; this is covered further in section 6.2.9 of this briefing.

2.4 Part 4: Other provision about digital information

2.4.1 Cookie pop-ups

Clause 109 of the bill would amend the PEC Regulations in relation to 'cookies'. The so-called 'cookies rule' in the regulations governs when an organisation can store or gain access to information stored on a person's device (such as a computer, tablet or mobile phone). Currently, organisations do not have to seek the user's consent to place cookies that are strictly necessary to provide a service requested by the user, such as to detect fraud or to remember items in the user's online shopping basket. Clause 109 would remove the requirement for organisations to seek consent for what the government has described as "several low privacy risk purposes".[32] This would apply to cookies for the following purposes:[33]

- collecting statistical information about how an organisation's service was being used (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 installation of software updates on a user's device that are necessary for security reasons (subject to

[32] House of Commons Public Bill Committee, 'Data Protection and Digital Information (No. 2) Bill', 23 May 2023, session 2022–23, 7th sitting, col 237.
[33] Explanatory notes, pp 87–8.

certain conditions)

- 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

The government has said these provisions would "reduce annoying cookie pop-ups".[34] This clause 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.

2.4.2 Unsolicited direct marketing communications

Clause 110 would enable the information commissioner to investigate and take action against organisations responsible for generating unsolicited direct marketing communications, regardless of whether the communications are received by the intended recipient.[35] The government has said that the wording of the law at present implies that such communications need to reach their intended recipient for the commissioner to be empowered to investigate. This clause would also amend the definition of "communication" to make clear that it would cover communications such as texts and emails.

2.4.3 Direct marketing and democratic engagement

Clause 113 relates to when organisations would need to obtain someone's consent to use their personal details for direct marketing

---

[34] Department for Science, Innovation and Technology, 'British businesses to save billions under new UK version of GDPR', 8 March 2023.

[35] Explanatory notes, p 89.

purposes and when the organisation could rely on a soft opt-in.[36] Clause 114 would enable the secretary of state to make exemptions from the direct marketing provisions in the PEC Regulations for the purposes of democratic engagement. Clause 115 sets out definitions for key terms used in clause 114. These provisions were amended at report stage, and a Labour amendment to remove clause 114 from the bill was defeated. This is covered in more detail in section 6.2.2 of this briefing.

2.4.4 Unlawful direct marketing

Clause 116 would place a duty on communications service providers and network providers to report suspicious activity relating to unlawful direct marketing to the information commissioner.[37] It would also set the penalties for non-compliance and require the commissioner to publish guidance on what might constitute reasonable suspicions.

2.4.5 Information commissioner's enforcement powers in relation to privacy and electronic communications

Clause 117 would apply what the government describes as the "more modern enforcement provisions" in the DPA 2018 to the

---

[36] Commercial organisations are allowed to use the so-called 'soft opt-in' in relation to personal data for direct marketing. This is where commercial organisations can send electronic marketing communications to a person without consent if their contact details were collected during the sale of a product or service, or negotiations of a sale. The communication must be in relation to similar goods and services and the person must also be offered a simple means of opting out of receiving further communications (House of Commons Library, 'Data Protection and Digital Information (No. 2) Bill', 28 March 2023, p 85).

[37] Explanatory notes, p 91.

PEC Regulations.[38] The government said this would mean that the maximum penalty that the information commissioner could impose for the most serious breaches of the PEC regulations would be increased to the same levels that can be imposed under the UK GDPR and the DPA 2018, namely up to 4% of a company's annual turnover or £17.5mn, whichever is higher.[39] The government has said these penalties could apply to senders of nuisance calls and texts.[40]

2.4.6 Trust services

Clauses 120 to 124 relate to trust services provided by providers outside the UK. 'Trust services' include services specifically relating to electronic signatures, electronic seals, timestamps, electronic delivery services and website authentication.[41] The provisions would enable the UK to unilaterally recognise EU-qualified trust service providers and would allow the secretary of state to make regulations to recognise products provided by other overseas trust service providers.

2.4.7 Sharing of information

Clauses 126 and 127 would enable 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. The government has stated that such agreements would be subject to

[38] Explanatory notes, p 92.
[39] House of Commons Public Bill Committee, 'Data Protection and Digital Information (No. 2) Bill', 23 May 2023, session 2022–23, 7th sitting, col 250.
[40] Department for Science, Innovation and Technology, 'British businesses to save billions under new UK version of GDPR', 8 March 2023.
[41] Explanatory notes, p 95.

the usual treaty ratification procedures.[42]

2.4.8 Information for social security purposes

Clause 128 and schedule 11 would enable the government to require banks and financial organisations to provide data about accounts linked to benefit claimants. The government intends to use this information to identify possible benefit fraud. This provision was added at report stage in the House of Commons. MPs questioned why state pension claimants were included in the scope of these measures as state pension fraud is low and entitlement is not linked to savings. They also raised privacy concerns about the DWP having the power to look at people's bank accounts without grounds for suspicion. The addition of schedule 11 to the bill was the only government amendment pushed to a vote at report stage. This is covered further in section 6.2.11 of this briefing.

2.4.9 Retention of information in connection with the death of a child

Clause 129 would enable Ofcom, the communications regulator, to require social media companies to retain information in connection with an investigation by a coroner or procurator fiscal into the death of a child where the child was suspected to have died by suicide. This provision was added at report stage in the House of Commons; it is covered further in section 6.2.12 of this briefing.

---

[42] Explanatory notes, p 97.

2.4.10 Retention of biometric information

Clauses 130 to 132 would enable law enforcement authorities to retain fingerprints and DNA profiles obtained from foreign partners for longer without having to obtain a national security determination. These provisions were added at report stage in the House of Commons and are covered further in section 6.2.13 of this briefing.

2.4.11 Registers of births and deaths

Clauses 133 to 137 would remove the requirement for registers of births and deaths to be held in paper form, enabling all births and deaths to be recorded electronically. This would remove the current duplication where they are registered both electronically and in paper registers.[43]

2.4.12 National underground asset register

Clauses 138 to 141 and schedule 13 would establish the national underground asset register for England and Wales, a digital map showing the location of privately and publicly owned underground pipes and cables. These provisions were added at report stage in the House of Commons and are covered further in section 6.2.14 of this briefing.

2.4.13 Information standards for health and social care

Clause 142 and schedule 14 would make provision about information

[43] Explanatory notes, pp 14–5.

technology and information standards for health and adult social care in England.[44] The provisions would ensure that relevant standards could be extended to IT providers dealing with relevant data, to enable system interoperability and data-sharing.

2.5 Part 5: Regulation and oversight

2.5.1 Information Commission

Clauses 143 to 146 and schedule 15 would establish a new body corporate, the Information Commission, to replace the existing regulator, the information commissioner, which is currently structured as a 'corporation sole'. The government has argued that the corporation sole model, which vests powers and responsibilities in a single individual, "can lead to a lack of the diversity, challenge and scrutiny which are critical to robust governance and decision making".[45] It said most UK regulators function as a body corporate with an independent board.

2.5.2 Oversight of biometric data

Clause 147 would abolish the office of biometrics commissioner.[46] It

---

[44] House of Commons Library, 'Data Protection and Digital Information (No. 2) Bill 2022–23', 28 March 2023, p 94.

[45] Department for Digital, Culture, Media and Sport, 'Data: A new direction—government response to consultation', 23 June 2022.

[46] The Protection of Freedoms Act 2012 established the biometrics commissioner and the surveillance camera commissioner as two separate roles. One person was appointed to do both roles in 2021 (Centre for Research into Information, Surveillance and Privacy, 'Independent report on changes to the functions of the biometrics and surveillance camera commissioner arising from the Data Protection and Digital Information (No. 2) Bill',

would transfer the commissioner's casework functions and oversight of the national security determinations regime to the investigatory powers commissioner. Clause 148 would abolish the office of surveillance camera commissioner and repeal the requirement for a surveillance camera code. The government argues that this would remove duplication as the information commissioner has oversight of personal data, including that captured by surveillance camera systems.[47]

2.6 Part 6: Final provisions

Part 6 contains provisions on consequential amendments, the making of regulations, interpretation, financial provision, extent and commencement. The majority of the bill extends to the whole of the UK, but some provisions, for example changes to the use of biometrics and overt surveillance, are limited to England and Wales and provisions on data in the health and adult social care system apply in England only. Annex A of the explanatory notes to the bill gives a clause-by-clause breakdown of territorial extent and application.

3. Responses to the bill

John Edwards, the information commissioner, said he welcomed the Data Protection and Digital Information (No. 2) Bill when it was introduced in March 2023.[48] He said he supported its ambition to

---

6 October 2023). The government said at the time having one person perform the two previously part-time roles was to "reflect the increasing convergence of those technologies" (HC Hansard, 20 January 2022, col 186WH).

[47] Explanatory notes, p 113.

[48] Information Commissioner's Office, 'ICO statement on re-introduction of Data Protection and Digital Information Bill', 8 March 2023.

"enable organisations to grow and innovate whilst maintaining high standards of data protection rights". He said the bill would ensure the Information Commissioner's Office could continue to operate as a "trusted, fair and independent regulator".

An independent report by the Centre for Research into Information Surveillance and Privacy (CRISP) into changes to the functions of the biometrics and surveillance camera commissioner (BSCC) was published in October 2023.[49] It had been commissioned by the Home Office. The report concluded that the bill did not make provision to replace all of the activities currently carried out by the commissioner, and it dismissed as "unrealistic" that these functions would be picked up automatically by other public bodies. It argued that the bill "fails to recognise the complexities of the current regulatory landscape and the protections offered by the BSCC". It also concluded that without a clear plan for how to replace all the BSCC's functions, "abolishing the BSCC creates oversight gaps and will create, rather than remove, regulatory complexity". Responding to the report, Fraser Sampson (whose tenure as BSCC ended on 31 October 2023), said the decision to abolish the commissioner role was "neither here nor there".[50] However, he argued that what was important was not to "simply junk the protection those roles have provided and instead find a way to retain the functions that this report shows are still clearly needed".

Commenting on the bill's introduction in March 2023, trade association techUK said the bill's smart data provisions would "help spur competition and innovation in the market, while empowering

[49] Centre for Research into Information, Surveillance and Privacy, 'Independent report on changes to the functions of the biometrics and surveillance camera commissioner arising from the Data Protection and Digital Information (No. 2) Bill', 6 October 2023.
[50] Biometrics and Surveillance Camera Commissioner, 'Report finds 'worrying vacuum' in surveillance camera plans', 30 October 2023.

consumers and delivering better outcomes".[51] It welcomed the bill but called for the government to make sure any smart data schemes would be "co-designed with sector-specific experts to ensure they bring real benefits" and to guard against "overlapping regimes or friction between different regulators".

Privacy and rights campaigners have raised concerns about the bill. The Public Law Project has argued it would:

> […] weaken important data protection rights and safeguards, making it more difficult for people to know how their data is being used, how decisions affecting them are being made, and weakening requirements on those who process data to consider the rights and interests of those their actions will affect.[52]

Similarly, the Open Rights Group has argued that the bill will "weaken UK data protection rights, reduce accountability for private businesses and the government and have a negative impact on the UK economy" as "navigating multiple data protection regimes will significantly increase costs and create bureaucratic headaches for businesses".[53]

4. House of Commons: Second reading

The bill's second reading in the House of Commons took place on

[51] techUK, 'Smart data: The UK's new data sharing laws will spur innovation and improve consumer outcomes', 15 March 2023.
[52] Public Law Project, 'House of Commons report stage briefing on the Data Protection and Digital Information Bill', November 2023, p 2.
[53] Open Rights Group, 'Parliamentary briefing: Data Protection and Digital Information Bill: Briefing for the report stage', November 2023.

17 April 2023.[54] Julia Lopez, minister for data and digital infrastructure, said the bill would begin "an evolution away from an inflexible one-size-fits-all regime and towards one that is risk based and focused on innovation, flexibility and the needs of our citizens, scientists, public services and companies".[55] She argued that the existing rules were "too vague, too complex and too confusing always to understand". She said the "simpler, easier, clearer regulation" brought in by the bill would give "the people using data to improve our lives", such as businesses and scientists "the certainty they need to get on with their jobs".[56] She believed it would do this while maintaining high standards for protecting people's privacy and making data "more useful for more people".

Lucy Powell, the then shadow secretary of state for digital, culture, media and sport, said the bill was a "huge missed opportunity", despite the "hype" around it.[57] She argued that despite rapid changes in the way data was being used in the digital age, the bill simply made "tweaks around the edges of the GDPR, making an already dense set of privacy rules even more complex". She said that Labour did not disagree with many of the aims of the bill, but questioned whether it would achieve them in practice.[58] Labour agreed that new legislation was needed following the UK's departure from the EU, and it welcomed better and easier data sharing between public services and the measures to reduce nuisance calls and cookie banners.

However, Ms Powell argued that in many areas the bill "threatens to take us backwards".[59] First, she said it threatened the UK's ability to

[54] HC Hansard, 17 April 2023, cols 67–102.
[55] HC Hansard, 17 April 2023, cols 67.
[56] HC Hansard, 17 April 2023, col 73.
[57] HC Hansard, 17 April 2023, cols 73 and 76.
[58] HC Hansard, 17 April 2023, col 74.
[59] HC Hansard, 17 April 2023, col 74.

share data with the EU, which risked an "astronomical cost to British business". This is a reference to the EU's data adequacy decision on the UK. The EU makes unilateral 'data adequacy decisions' about whether non-EU countries offer what it considers to be an adequate level of data protection.[60] If so, personal data can be transferred between that country and the EU without any further safeguards. The EU adopted data adequacy decisions covering the UK in June 2021.[61] The European Commission is due to begin a review in 2024 to decide whether to extend them for another four years.[62] Ms Powell noted concerns that "the vast expansion of the secretary of state's powers, among other things" in the bill might put the data adequacy decision in doubt. Second, she said that rather than cutting red tape, the "complex requirements" in the bill "threaten to add more hurdles" for businesses trying to understand how to comply with data protection requirements.[63] Third, she argued the bill undermined individuals' rights, reducing protection for citizens and "tilting the rules in favour of the companies that are processing our data".

Ms Powell also argued that important elements were missing from the bill. She suggested it did not focus on the "potential harms of data […] felt well beyond the individual level", such as biases in artificial intelligence.[64] She also suggested it lacked measures to open up data to small businesses and not-for-profit organisations and allow them to "compete with existing giants". Finally, she said the bill did not include measures to boost public trust.

Layla Moran, the Liberal Democrat spokesperson for science,

[60] European Commission, 'Adequacy decisions', accessed 30 November 2023.
[61] Department for Digital, Culture, Media and Sport, 'EU adopts 'adequacy' decisions allowing data to continue flowing freely to the UK', 28 June 2021.
[62] Information Commissioner's Office, 'Adequacy', accessed 7 December 2023.
[63] HC Hansard, 17 April 2023, col 75.
[64] HC Hansard, 17 April 2023, col 76.

innovation and technology, raised similar concerns. She said the bill would undermine data rights, concentrate power with the secretary of state, further complicate the UK's relationship with Europe and, "far from restoring confidence in data protection", would set a "dangerous precedent for a future in which rights and safeguards are undermined".[65]

Closing the debate, Paul Scully, the then parliamentary under secretary of state for science, innovation and technology, agreed data adequacy was very important.[66] He said the government had been speaking to the European Commission on a regular basis about this. He emphasised that the EU did not require exactly the same rules as its own to be in place for it to decide another country was adequate.

The bill received its second reading without a division.

5. House of Commons: Committee stage

Committee stage of the bill took place over eight sittings between 10 and 23 May 2023.[67] Oral evidence was taken from expert witnesses during the first two sittings. A total of 65 government amendments were made to the bill, including the addition of seven new clauses. Most of the government amendments were described as "minor or technical".[68] The new clauses covered the areas set out below.

---

[65] HC Hansard, 17 April 2023, cols 94–5.
[66] HC Hansard, 17 April 2023, col 100.
[67] House of Commons Public Bill Committee, 'Data Protection and Digital Information (No. 2) Bill', 24 May 2023.
[68] House of Commons Library, 'Data Protection and Digital Information (No. 2) Bill: Progress of the bill', 17 November 2023, p 6.

NC2 (now clause 118 in the Lords version of the bill) would require 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.[69] NC1 (now clause 22 in the Lords version of the bill) would make a related amendment to article 41 of the UK GDPR to clarify that bodies accredited to monitor compliance with approved codes of conduct 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.

NC3 and NC4 (now clauses 78 and 79 in the Lords version of the bill) and related amendments would mean that information disclosed by the Welsh Revenue Authority or Revenue Scotland to a person registered in the DVS register under what is now clause 74 in the Lords version of the bill could not be further disclosed, other than for the purpose of providing digital verification services, without the consent of the Welsh Revenue Authority or Revenue Scotland. This would match provisions in clause 74 regarding the disclosure of information from HMRC.

NC5 (now clause 127 in the Lords version of the bill) and related amendments would enable Scottish ministers and Welsh ministers to make regulations under clause 126 in areas where they had devolved competence (for Welsh ministers this would be subject to consent from the UK government if required). The power in clause 126 is for the appropriate national authority to make regulations to implement technical or operational detail of international law enforcement information-sharing agreements.

---

[69] For more information about these regulations, see: Information Commissioner's Office, 'What are PECR?', accessed 4 December 2023.

NC7 (now clause 119 in the Lords version of the bill) would provide that requirements relating to consultation on the PEC Regulations in clauses 109 to 117 could be fulfilled by a consultation before, as well as after, the relevant bill provision came into force. This includes the requirement in clause 114 for the secretary of state to consult the information commissioner before making any regulations that would exempt direct marketing for the purposes of democratic engagement from requirements in the PEC Regulations.

NC6 would have allowed MPs and members of the Welsh Senedd, Scottish Parliament and Northern Ireland Assembly 30 days (instead of the current four) after leaving office after a general election to process 'special category' data following a request by an individual to act on their behalf. '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.[70] This clause was subsequently removed at report stage. In its place, what is now clause 8, added at report stage, would enable MPs and members of the devolved legislatures to process special category data revealing someone's political opinion for 30 days after a general election if it was necessary for discharging the elected representative's functions or for the purposes of their democratic engagement activities. For more on this, see section 6.2.2 of this briefing.

No non-government amendments were made to the bill at committee. Most of the divisions that took place related to Labour amendments on the data protection provisions in part 1 of the bill.

[70] Information Commissioner's Office, 'Special category data', accessed 28 November 2023.

For a fuller summary of the discussions at committee stage, see the House of Commons Library briefing 'Data Protection and Digital Information Bill: Progress of the bill' (updated 17 November 2023). The numbering of the bill's clauses has changed significantly since that briefing was written; readers may therefore find it helpful to cross-refer to the guide in section 9 of this briefing which shows which number referred to which clause at different stages throughout the bill's passage to date.

6. House of Commons: Report stage

Report stage took place in the House of Commons on 29 November 2023.[71] The government tabled 266 amendments, including 38 new clauses and two new schedules. The government described these as "a raft of common-sense changes" to "further improve data security, bolster national security and prevent fraud".[72] All the government's amendments were made to the bill. The Commons voted on only one government amendment, new schedule 1, which set out provisions on a new power for the secretary of state to require information for social security purposes.

No non-government amendments were made to the bill, although amendments on the processing of special category (sensitive) data, automated decision-making, the definition of high-risk processing, and direct marketing for the purposes of democratic engagement were put to a vote.

---

[71] HC Hansard, 29 November 2023, cols 848–1015.

[72] Department for Science, Innovation and Technology, Department for Work and Pensions and Home Office, 'Changes to data protection laws to unlock post-Brexit opportunity', 23 November 2023.

6.1 Recommittal motion

In light of the number of amendments tabled by the government, Sir Chris Bryant, shadow minister for creative industries and digital, moved that the bill should be recommitted to a public bill committee for further consideration.[73] He said the government had tabled 240 of its amendments on the last possible day, and many of them were "very significant", including amendments to "give very extensive new powers to ministers" and to "introduce completely new topics that have never been previously mooted, debated or scrutinised by Parliament in relation to this bill". He accused the government of acting "whether knowingly, recklessly or incompetently" in a way that meant the Commons could not carry out line-by-line scrutiny of dozens of pages of new laws.[74] He said this was "no way to scrutinise a bill".

Sir John Whittingdale, minister for data and digital infrastructure, countered that the bill had been considered "at length" in committee stage and would be further scrutinised at report stage.[75] He said the "vast majority" of the government's amendments were technical, and the reason the overall number sounded high was that "a lot are consequential on original amendments". He said that those which addressed new aspects "represent important additions to the bill".

The recommittal motion was defeated by 275 votes to 209.[76]

David Davis (Conservative MP for Haltemprice and Howden) later

---

[73] HC Hansard, 29 November 2023, col 848.
[74] HC Hansard, 29 November 2023, col 849.
[75] HC Hansard, 29 November 2023, cols 849–50.
[76] HC Hansard, 29 November 2023, cols 850–3.

said that by not accepting the recommittal motion, the House of Commons had "in effect delegated large parts of the work on this important bill to the House of Lords".[77]

6.2 Government new clauses and amendments

6.2.1 Processing in reliance on relevant international law (clause 7)

NC6 was added and is now clause 7 in the Lords version of the bill. It would amend the UK GDPR so the conditions for the lawful processing of personal data would include processing that had a basis in or was authorised by relevant international law. This clause would also amend the DPA 2018 to set out what would be relevant international law for these purposes. A new schedule (A1) to the DPA 2018 would specify that the processing of personal data would be lawful if it was necessary for the purposes of responding to a request made in accordance with the UK-USA Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime.[78] Clause 7 would give the secretary of state power to add other treaties or parts of treaties ratified by the UK to schedule A1, subject to the affirmative resolution procedure.

Sir John Whittingdale said the new clause would make clear that the UK-US data access agreement and other specified international treaties could provide a basis for processing under several grounds in the UK GDPR.[79] He explained the current legislation did not prevent

---

[77] HC Hansard, 29 November 2023, col 888.

[78] For information about the background to this agreement, see: House of Lords Library, 'Crime (Overseas Production Orders) Bill [HL]', 5 July 2018.

[79] HC Hansard, 29 November 2023, col 873.

data disclosures under the UK-US agreement, which has been operational since October 2022. However, he said clause 7 would make it "absolutely clear" to UK telecoms operators that the agreement provided "an appropriate legal basis for processing personal data, special category data and criminal offences data under the relevant provisions in the UK GDPR".

6.2.2 Democratic engagement (clauses 8 and 113 to 115)

NC48 was added to the bill as clause 8. It relates to the processing of personal data revealing political opinions for the purposes of democratic engagement. The definition of democratic engagement in clause 115 was also amended by amendment 256.

Sir John Whittingdale said both the new clause and the amendment included the addition of "a fuller definition of what constitutes 'democratic engagement activities'" which would "help the reader understand that term wherever it appears in legislation".[80] The new clause and amendment 256 set out matching definitions of democratic engagement activities, defining them as "activities whose purpose is to support or promote democratic engagement". They define 'democratic engagement' as:

> […] engagement by the public, a section of the public or a particular person with, or with an aspect of, an electoral system or other democratic process in the United Kingdom, either generally or in connection with a particular matter, whether by participating in the system or process or engaging with it in another way […]

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

Both definitions set out non-exhaustive lists of examples of democratic engagement activities. For instance, activities the purpose of which was to promote the registration of individuals as electors or to support a person to become a candidate for election as an elected representative would be democratic engagement activities. 'Gathering opinions' or 'communicating with electors' may be democratic engagement activities (but would not always necessarily be so).

Clause 8 and clause 115 as amended by amendment 256 would add this definition of democratic engagement activities to different pieces of existing legislation.

Clause 8 would add it to schedule 1 to the DPA 2018. This governs the processing of special categories of personal data. Special categories of data are defined in Article 9(1) of the GDPR as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". One lawful reason for the processing of special category data is if it meets one of the substantial public interest conditions set out in part 2 of schedule 1 to the DPA 2018. Clause 8 would insert the new definition of democratic engagement activities into this schedule. This would allow registered political parties and the elected representatives listed in clause 8 to process personal data that revealed someone's political opinions if it was necessary for democratic engagement activities. Clause 8 would also allow candidates for election, permitted participants in a referendum and accredited campaigners in a recall election to process special category 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".

Sir John Whittingdale said clause 8 would address an "anomaly" in the current law, where political parties can process sensitive political opinions data without consent for the purposes of their political activities, but elected representatives, candidates, recall petitioners and permitted participants in referendums cannot.[81]

Amendment 256 amended clause 115 to insert a new definition of democratic engagement activities for the purposes of clause 114. Clause 114 would give the secretary of state the power to provide an exception from a direct marketing provision in the PEC Regulations for communications activity for the purposes of democratic engagement.

Currently, if political parties or other campaigners, including candidates, use personal data for unsolicited campaigning material, this is treated as direct marketing and is subject to the PEC Regulations.[82] As the House of Commons Library has explained, different rules on direct marketing apply to communications from different types of sender:

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

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

[82] Leaflet drops and mailings which are unaddressed or addressed to 'the occupier' do not fall within the statutory definition of direct marketing because they are not "directed to particular individuals" (House of Commons Library, 'Data Protection and Digital Information (No. 2) Bill 2022–23', 28 March 2023, p 85).

fundraising, unless they have obtained prior consent to use personal data for that purpose.

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

Non-commercial organisations cannot use 'soft opt-in'.[83]

Clause 113 of the bill would extend the soft opt-in to organisations which have charitable, political or non-commercial objectives when sending electronic marketing communications for the purpose of furthering their objective. Clause 114 (as amended by the government's amendments 253, 254 and 255) would enable the secretary of state to make regulations to exempt certain types of communication from the direct marketing provisions in the PEC Regulations. Similarly to clause 8, a distinction is drawn between elected representatives and political parties, and candidates, permitted participants in a referendum and accredited campaigners in a recall petition. The regulations could exempt the communications of elected representatives and registered political parties if the communications were for the purposes of democratic engagement activities (or, in the case of a registered political party, election activities). The regulations could exempt communications from

[83] House of Commons Library, 'Data Protection and Digital Information (No. 2) Bill 2022–23', 28 March 2023, p 85.

candidates, permitted participants in a referendum or accredited campaigners in a recall petition if the communications were for the purposes of their campaigning.

For the purposes of these exemption regulations, MPs and members of the devolved legislatures would continue to qualify as "elected representatives" from dissolution until the end of the day on which a general election to Parliament or the devolved legislature was held. Clause 115 had originally provided they would continue to qualify for 30 days after the election, but government amendment 263 at report stage reduced this.

Another amendment to clause 115 (amendment 264) means that, if regulations were made to exempt elected representatives from PEC Regulation direct marketing provisions, this would also apply to an MP who was subject to a successful recall petition, until the end of the day on which a by-election for their seat was held, or the next general election (whichever was earlier). Similarly, amendment 277 to schedule 1 would ensure that an MP who was subject to a successful recall petition would continue to count as an elected representative for 30 days after the resulting by-election or general election (if earlier) for the purposes of relying on democratic engagement as a recognised legitimate interest ground for lawfully processing personal data.[84] Sir John Whittingdale said this would "enable them to complete urgent casework or hand over casework to a successor, as they do following the dissolution of Parliament".[85]

---

[84] This aligns with provisions in paragraph 13 of schedule 1 for former MPs and members of the devolved legislatures who would also be able to rely on 'democratic engagement' as a 'recognised legitimate interest ground' for lawfully processing personal data for 30 days after an election.

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

Sir Chris Bryant said that clause 113 meant that any political party or elected representative could engage in direct marketing relying on a soft opt-in procedure.[86] He suggested that this would enable "using data acquired as an MP for the wholly different purpose of seeking re-election as a candidate". He said that clause 114 would allow the secretary of state to make future changes and exemptions "for the very unspecified purposes of 'democratic engagement'". He described this as "a major power grab", enabling the secretary of state to "change the direct marketing rules for elections with the bare minimum of scrutiny".

He noted that the government had explained that "a future government may want to encourage democratic engagement in the run-up to an election by temporarily 'switching off' some of the direct marketing rules".[87] In light of this, Sir Chris said he was worried the government was "trying to slip yet another change through just before an election that will enable the Tories to mine people's information for votes". He argued that clause 113 should be rewritten to remove the soft opt-in provisions for political parties and elected representatives, and clause 114 should be removed altogether.

Sir Chris was also critical of amendment 256 setting out a new explanation of 'democratic engagement'. He dismissed it as "anything that anybody could do in a political party or as an elected representative", arguing it extended rather than clarified the definition.[88]

---

[86] HC Hansard, 29 November 2023, col 885.

[87] Department for Science, Innovation and Technology, 'Letter from Sir John Whittingdale MP to Stephanie Peacock MP regarding issues raised in the Data Protection and Digital Information (No. 2) Bill committee stage debate: clause 83—Direct marketing for the purposes of democratic engagement', 25 May 2023.

[88] HC Hansard, 29 November 2023, col 886.

Speaking for the SNP, Patrick Grady (SNP MP for Glasgow North) said his party echoed Labour's concerns about the clauses on democratic engagement.[89]

Sir Chris moved an amendment (amendment 218) to remove clause 114 from the bill. This was defeated by 275 votes to 194.[90]

6.2.3 Searches in response to data subjects' requests (clause 12)

NC7 was added and is now clause 12 in the Lords version of the bill. It deals with what are known as subject access requests: article 15 of the UK GDPR gives individuals the right to ask an organisation whether or not they are using or storing the individual's personal information and to request a copy of their personal information.[91] Clause 12 would amend this article so that individuals would be entitled "only […] to such confirmation, personal data and other information as the controller is able to provide based on a reasonable and proportionate search". Clause 12 would also amend the DPA 2018 to introduce an equivalent "reasonable and proportionate search" threshold for subject access requests related to data processed by law enforcement and the intelligence services.

Sir John Whittingdale explained that the Retained EU Law (Revocation and Reform) Act 2023 will remove the general EU law principle of proportionality from UK domestic law at the end of 2023.[92] He said the government had therefore tabled this new clause

---

[89] HC Hansard, 29 November 2023, col 894.
[90] HC Hansard, 29 November 2023, cols 986–90.
[91] Information Commissioner's Office, 'Your right of access', accessed 30 November 2023.
[92] HC Hansard, 29 November 2023, col 873.

to ensure that data controllers would "continue to need only to carry out a reasonable and proportionate search" when responding to a subject access request. He said that data controllers should make the best possible efforts to locate all the information requested by a data subject, but there were occasions when this might be unreasonable or disproportionate. In such circumstances, he believed it was "important to continue to allow controllers to limit the efforts they make when searching for information". He said this reflected existing case law, and the amendment would provide greater legal certainty for data controllers.[93]

Sir Chris Bryant said that "limit[ing] a data subject's entitlement to their own data to the controller's ability to conduct a 'reasonable and proportionate' search" would "drive a coach and horses through the rights of people to access their own data and to know who is doing what to their information".[94] He questioned what was the definition of "reasonable and proportionate" and who would determine whether a search had met this threshold. He said Labour did not support this change; however, it was not put to a division.

6.2.4 Duty to keep records and high-risk processing (clause 18)

Clause 18 of the bill would amend the requirements in the UK GDPR about what records data controllers and processers must keep about their processing activities. It would replace the current requirements in article 30 to keep records of all processing activities relating to personal data. Instead, they would be required to keep records of the processing of personal data "which, taking into account the nature,

---

[93] HC Hansard, 29 November 2023, col 874.
[94] HC Hansard, 29 November 2023, col 884.

scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of individuals".

Sir John Whittingdale said at report stage that some organisations had queried whether this meant they would have to keep records in relation to all their activities if only some of their activities were high risk. He explained that this was not the government's intention. He said the government had therefore tabled amendments to "make it absolutely clear that organisations have to keep records only in relation to their high-risk processing activities".[95] A total of 33 amendments were made to clause 18.

Sir Chris Bryant said he was "perplexed" that there was no definition of high-risk processing in the bill, and that the government had removed the existing standard for high-risk processing from the existing UK GDPR.[96] He said this left a "legislative lacuna" for the information commissioner to fill, which he did not believe was right. Sir Chris said he had therefore tabled an amendment (amendment 1) to retain a statutory definition of high-risk processing in the UK GDPR. He said the information commissioner supported this.

In response, Sir John Whittingdale said the government found some of the language in this definition "unclear and confusing", which was part of the reason it wanted to remove it.[97] He believed organisations should have "the ability to make a judgement of risk based on the specific nature, scale and context of their own processing activities". He said that clause 20 of the bill would require the information commissioner to produce a document with examples of high-risk processing.

---

[95] HC Hansard, 29 November 2023, col 878.
[96] HC Hansard, 29 November 2023, col 878.
[97] HC Hansard, 29 November 2023, col 911.

Labour's amendment 1 was defeated by 275 votes to 198.[98]

6.2.5 Codes of practice: Secretary of state's recommendations (clause 35)

The bill was amended to remove a proposed veto for the secretary of state over codes of practice drawn up by the information commissioner.

Currently, the information commissioner is required under sections 121 to 124 of the DPA 2018 to publish four statutory codes of practice, on data sharing, direct marketing, age-appropriate design, and data protection and journalism. The codes must be laid before Parliament before they can come into force.[99] If either House resolves not to approve a code, it cannot come into force. The secretary of state can also require the information commissioner to produce other codes of practice giving guidance on the processing of personal data.[100] These do not have to be laid before Parliament in the same way as the other four codes.

Clause 35 of the bill proposed changing these arrangements so that all codes would be subject to the same approval procedure. It would have required the information commissioner to submit the codes to the secretary of state for approval before they were laid before Parliament. As before, Parliament would have had 40 days in which either House could resolve not to approve a code. If the secretary of state did not approve a code, they would have had to explain the reasons why to the information commissioner, who would then have

---

[98] HC Hansard, 29 November 2023, cols 965–9.
[99] Data Protection Act 2018, s 125.
[100] Data Protection Act 2018, s 128.

been obliged to revise and resubmit the code in light of this.

At committee stage, Labour moved an amendment to this clause that would have enabled the secretary of state to reject the final version of a code only once.[101] Labour argued this was needed to ensure there was no risk to the information commissioner's independence. The government argued it would "unduly limit" its opportunity to give a view before the code was laid before Parliament. The amendment was rejected by nine votes to six.

However, government amendment 45, agreed to at report stage, amended clause 35 to remove the requirement for codes to be approved by the secretary of state. Instead, the information commissioner would have to submit a final version of a code to the secretary of state and publish it. The secretary of state would have 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 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.

Sir John Whittingdale said in making the amendment, the government had listened to "concerns about the perceived impact of the approval powers on the independence of regulators".[102] He said the amendment "balances regulatory independence with democratic

[101] House of Commons Public Bill Committee, 'Data Protection and Digital Information (No. 2) Bill', 18 May 2023, session 2022–23, 5th sitting, col 184 (amendment 111). The relevant clause was numbered 31 at committee stage.
[102] HC Hansard, 29 November 2023, col 874.

accountability", emphasising that the information commissioner would not be bound by the secretary of state's recommendations. He added that the Information Commissioner's Office (ICO) supported the amendment.

Sir Chris Bryant thanked the government for this amendment, saying it achieved "a much better balance between democratic oversight and ICO independence".[103]

Joe Jones, research and insights director at the International Association of Privacy Professionals, commented that this amendment came after stakeholders in the UK and the EU had emphasised the risk that a government veto might impact the independence of the ICO, "by extension, threatening the durability of the EU's adequacy decision for the UK".[104]

Although he did not link the issue directly to this amendment, Sir John Whittingdale noted at report stage that the government appreciated the importance of an EU data adequacy decision for the UK.[105] He said the government was confident that nothing in the bill would put data adequacy at risk, and the ICO shared this opinion.

6.2.6 Notices from the information commissioner (clause 38)

NC8 was added and is now clause 38 in the Lords version of the bill. The DPA 2018 empowers the information commissioner to issue

[103] HC Hansard, 29 November 2023, col 882.
[104] Joe Jones, 'UK GDPR reforms move forward in UK Parliament', The Privacy Advisor Blog, 29 November 2023.
[105] HC Hansard, 29 November 2023, col 872.

different types of notice (information notices, assessment notices, enforcement notices and penalty notices). Section 141 of the DPA 2018 outlines the processes the commissioner may follow to issue notices to individuals and organisations. This includes a provision that a notice can be issued by electronic means with the recipient's consent. Clause 38 would replace this section with a new section to enable the information commissioner to give notices by email without having to obtain the recipient's consent to do so. Sir John Whittingdale said this would allow the ICO to enforce the UK's data protection regime more effectively, particularly against overseas businesses.[106] He added that it would mirror arrangements already in place for some other regulators.

6.2.7 Court procedure in connection with subject access requests (clause 47)

NC9 was added and is now clause 47 in the Lords version of the bill. It 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. Sir John Whittingdale said giving the court access to this material would enable it to assess whether it should have been provided as part of

[106] HC Hansard, 29 November 2023, col 874.

the original response to a subject access request.[107]

Sir Chris Bryant said Labour did not support this, because the party disagreed with "reasonable and proportionate" being the threshold for a search.[108]

6.2.8 Digital verification services supplementary codes (part 2)

Multiple new clauses were added to part 2 of the bill to introduce the concept of supplementary codes on digital verification services. Clause 53 of the bill would enable the government to establish a digital verification services (DVS) trust framework. This would set out "baseline rules that organisations must follow to become a government-approved digital verification service provider".[109] While these baseline rules would apply to all DVS providers certified under the framework, the government said at report stage it recognised that some DVS providers might need to follow additional rules to those in the framework to meet sector-specific requirements, for instance when people were using a DVS to apply for a mortgage or to complete pre-employment checks.[110] The government therefore introduced new clauses at report stage relating to supplementary codes. The bill was also amended (government amendment 50) to provide that the rules set out in the DVS trust framework would be referred to as the 'main code'.

Supplementary codes could be drawn up either by the secretary of

---

[107] HC Hansard, 29 November 2023, col 874.
[108] HC Hansard, 29 November 2023, col 884.
[109] HC Hansard, 29 November 2023, col 874..
[110] HC Hansard, 29 November 2023, col 874.

state or someone else. NC11, added to the bill as clause 55, would enable the secretary of state to draw up a supplementary code and to designate it as complying with the conditions set out in the DVS trust framework. If a supplementary code was drawn up by someone other than the secretary of state, they could apply to have it approved. NC10, added to the bill as clause 54, would require the secretary of state to approve a supplementary code where:

- it met the relevant conditions set out in the DVS trust framework
- the application complied with application requirements set out by the secretary of state
- the applicant paid any relevant fee

NC12, added to the bill as clause 56, would require the secretary of state to maintain and publish a list of designated supplementary codes and approved supplementary codes (known collectively as recognised supplementary codes).

NC13, added to the bill as clause 57, specifies that if the secretary of state made changes to the DVS trust framework that affected an approved supplementary code, the code would lose its approved status 21 days after the changes to the trust framework came into force, unless an application for reapproval of the code was made within that period. The supplementary code would retain its approved status until the secretary of state decided the reapproval application. The secretary of state would have 21 days from the changes to the trust framework coming into force to review all designated supplementary codes and decide whether they continued to meet the conditions in the trust framework.

NC14, added to the bill as clause 58, specifies that if an approved supplementary code was revised, it would have to go through the approval process again to maintain its status. The secretary of state could revise a designated supplementary code only if they were satisfied that the revised version would still meet the relevant conditions in the trust framework.

NC15, added to the bill as clause 59, would enable the secretary of state to determine the process for making a valid application for approval of a supplementary code. NC16, added to the bill as clause 60, would allow them to set fees for approval, reapproval and continued approval of a supplementary code. NC17, added to the bill as clause 61, would enable the secretary of state to 'de-approve' an approved supplementary code on receipt of a valid request. NC18, added to the bill as clause 62, would enable the secretary of state to 'de-designate' a designated supplementary code.

Clause 63 of the bill would require the secretary of state to establish and maintain a publicly available DVS register of organisations providing DVS that have been certified by an accredited body as complying with the DVS trust framework. The government added a group of new clauses at report stage to do with the recording of information in the DVS register:

- NC19 (added to the bill as clause 64) would enable a person to apply to add services to their entry in the DVS register if they had been certified by an accredited body that they provided the additional services in accordance with the main code.
- NC20 (added to the bill as clause 65) would enable a person to apply for a note to be included in the DVS register that

they provide DVS services in accordance with a recognised supplementary code.

- NC21 (added to the bill as clause 66) would enable a person to apply to add services to their supplementary note in the DVS register.
- NC22 and NC23 (added to the bill as clauses 71 and 72) would require the secretary of state to remove services or supplementary notes from the register if the person requested it, if they ceased to provide the service, if they were no longer certified as providing services in accordance with the main code, or if the relevant supplementary code was no longer recognised. NC24 (added to the bill as clause 73) would make similar provision for removing additional services from supplementary notes.

NC25 (added to the bill as clause 83) would add an index of defined terms for part 2 of the bill.

NC26 (added to the bill as clause 84) 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 these checks to use a DVS provider which was registered in the DVS register as complying

with designated supplementary rules concerning these checks.[111] Sir John Whittingdale said this would "provide confidence and security to employers and landlords that the service providers they are using are certified".[112] He said the sector welcomed the use of digital identity service providers "as it represents a more cost-effective practice than manual checks of physical documents".

During the report stage debate, both Dawn Butler (Labour MP for Brent Central) and David Davis (Conservative MP for Haltemprice and Howden) raised concerns about ensuring that people retained the right to use non-digital verification services.[113] Sir John Whittingdale said the bill provided for the use of secure digital identities but did not force businesses or individuals to use them.[114] He emphasised that "individual choice is integral" to the government's approach, and said the bill made clear that digital verification services could only be used at the request of the individual.

As well as the new clauses on digital verification services that were added to part 2 of the bill at report stage, a number of government amendments were made to the existing clauses in this part of the bill. The main changes they made were to:[115]

- require the secretary of state to set conditions for approval or designation of supplementary rules concerning the provision of digital verification services (amendment 49;

[111] Explanatory notes, p 16.
[112] HC Hansard, 29 November 2023, cols 874–5.
[113] HC Hansard, 29 November 2023, col 872 and cols 888–90.
[114] HC Hansard, 29 November 2023, col 913.
[115] Based on member's explanatory statements in House of Commons, 'Data Protection and Digital Information Bill (Amendment paper)', 29 November 2023, pp 75–85.

clause 53)[116]

- provide that the DVS framework and any revised version of the framework must specify when they come into force (rather than the default being they come into force on publication) (amendment 51; clause 53)
- enable the DVS framework to set different rules for different digital verification services, and different conditions for approval or designation for different purposes (amendment 52; clause 53)
- remove a clause that would have allowed registered DVS providers to apply for a top-up certificate if the secretary of state changed or added rules in the trust framework to certify they were providing services in accordance with the new rule (amendment 78)
- replace the removed clause on top-up certificates with provision enabling the DVS trust framework to contain transitional provision about certificates issued before revisions to the main code come into force (amendment 53; clause 53)
- clarify that a person may hold a certificate which covers a wider range of digital verification services than those for which they apply to be registered (amendments 54 and 56; clause 53; and amendment 70; clause 69)
- require the secretary of state to record on the DVS register which services a person is registered in respect of (amendment 57; clause 63)
- provide for how an application is made to add additional services to the DVS register, to include a note in the register or add services to a note (amendment 62; clause 67), and to

[116] The clause numbers given in this list are for clauses as numbered in the Lords version of the bill.

enable the secretary of state to charge fees for such applications (amendment 66; clause 68)

- clarify that a duty to remove a person from the DVS register arises only if the person no longer provides any digital verification services in respect of which they are registered (amendment 69; clause 69)
- clarify that the power to remove a person from the DVS register is exercisable if the person is failing to comply with the main code when providing some or all of the digital verification services in respect of which they are registered (amendment 75; clause 70)
- enable the secretary of state to remove a person from the register if the person has a note in the register that they provide digital verification services in accordance with a supplementary code and they are failing to comply with the code (amendment 76; clause 70)

At report stage, Sir Chris Bryant said that Labour supported part 2 of the bill, establishing a digital verification framework, as amended at committee stage.[117] However, he was concerned that the government had "underestimated the sheer technicality of such an endeavour", as shown by "the last-minute requirement for tens of government amendments to this part of the bill".

6.2.9 Smart data and interface bodies (part 3)

New clauses were added at report stage relating to 'interface bodies' for smart data schemes in part 3 of the bill. Smart data schemes allow for the secure sharing of customer data, such as that held by a

[117] HC Hansard, 29 November 2023, col 882.

communications provider or financial services provider, at the customer's request, with authorised third-party providers (ATPs). ATPs can these use the data to provide services such as personalised market comparisons or account management. An example of a smart data scheme is the implementation by the UK's six largest banking providers of an open banking roadmap mandated by the Competition and Markets Authority.[118] Open banking allows customers to do things such as give permission to an automatic savings app to analyse their current account and move money to a savings account, or enable payments to online retailers without having to fill in payment card details.[119] The bill would extend the government's powers to mandate data holders to participate in smart data initiatives.

Clause 86 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.[120] 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. Clause 88 would make equivalent provision about business data.

At report stage, the government added NC27, which is now clause 91 in the Lords version of the bill. This would specify that regulations made under clause 86 or 88 could make provision about interface bodies. The regulations could require a data holder, an

[118] Competition and Markets Authority, 'Millions of customers benefit as open banking reaches milestone', 12 January 2023.
[119] MoneySavingExpert, 'Open banking explained: How it works and if your data is safe', 28 February 2023.
[120] Explanatory notes, p 74.

authorised person or a 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

NC28 and NC29 were also added and are now clauses 98 and 99 of the bill. They 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 rules could also require businesses to use a particular interface, interface standards or interface arrangements when receiving customer data or business data from a financial services provider.

Sir John Whittingdale said that the amendments would ensure that smart data schemes could "replicate and build on the open banking model by allowing the government to require interface bodies to be set up" by members of a smart data scheme.[121] He said interface bodies would "play a similar role to that of the open banking implementation entity, developing common standards on arrangements for data sharing". He said the regulations would ensure

[121] HC Hansard, 29 November 2023, col 881.

that interface bodies had "appropriate accountability to regulators". John Penrose (Conservative MP for Weston-super-Mare) sought assurance that data standards set by interface bodies within different sectors of the economy would be compatible with each other.[122] Sir John Whittingdale said he would discuss this with him further in due course.[123]

Over 100 other government amendments (amendments 82 to 196) were made to part 3 of the bill at report stage. Sir John Whittingdale said they were "complicated and technical".[124] He said amendments to part 3 would "ensure that the range of data and activities essential to smart data schemes are better captured and more accurately defined". Overall, he said that changes to part 3 would support the government in meeting its commitment "first, to provide open banking with a long-term regulatory framework, and secondly, to establishing an open data scheme for road fuel prices", as well as "more generally strengthen[ing] the toolkit available to government to deliver future smart data schemes.[125]

Sir Chris Bryant said that Labour "warmly welcome[d] and support[ed] this part of the bill", observing that his party and industry had been "urging the government to go much faster in this particular area".[126] However, noting that the government had pledged to "kickstart a smart data big bang" in the autumn statement, he said the FCA "does not think that a big bang approach to open finance is feasible or desirable". Nevertheless, he said many of the government's technical amendments to this part of the bill "indicate a move in the right direction".

---

[122] HC Hansard, 29 November 2023, col 881.
[123] HC Hansard, 29 November 2023, col 881.
[124] HC Hansard, 29 November 2023, col 881.
[125] HC Hansard, 29 November 2023, col 880.
[126] HC Hansard, 29 November 2023, col 882.

6.2.10 Duty to notify the information commissioner of personal data breach: Time periods (clause 112)

NC33 was added to the bill and is now clause 112 in the Lords version. It 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 retained EU law,[127] 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 112 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 delay" if it was not all available at the time of notification.

The new timeframe matches the one already set out in section 67 of the DPA 2018, which requires data controllers to notify the information commissioner without undue delay and, where feasible, not later than 72 hours after becoming aware of a personal data

[127] After the end of 2023, 'retained EU law' will be known as 'assimilated law'.

breach if the breach is likely to result in a risk to the rights and freedoms of individuals.

Sir John Whittingdale said at report stage that the new clause "eases burdens on industry by giving more time for those data controllers to report data breaches".[128] He said it would "allow organisations to gather more detailed information" before reporting the breach, which in turn would "allow the ICO to focus its efforts on assessing that information".

6.2.11 Information for social security purposes (clause 128 and schedule 11)

NC34 and NS1 were added to the bill and are now clause 128 and schedule 11 in the Lords version. They would give the government powers to obtain information for social security purposes. In a press release announcing it was tabling these amendments, the government said they would enable "better use of data to identify fraud—tackling benefits cheats intent on ripping off the taxpayer".[129] The press release went on to explain how the powers were intended to work:

> The changes include new powers to require data from third parties, particularly banks and financial organisations, to help the UK government reduce benefit fraud and save the taxpayer up to £600mn over the next five years. Currently, Department for Work and Pensions (DWP) can only undertake fraud checks on a claimant on an individual basis, where there is already a suspicion of fraud.

---

[128] HC Hansard, 29 November 2023, col 875.

[129] Department for Science, Innovation and Technology, Department for Work and Pensions and Home Office, 'Changes to data protection laws to unlock post-Brexit opportunity', 23 November 2023.

> The new proposals would allow regular checks to be carried out on the bank accounts held by benefit claimants to spot increases in their savings which push them over the benefit eligibility threshold, or when people spend more time overseas than the benefit rules allow for. This will help identify fraud take action more quickly [sic]. To make sure that privacy concerns are at the heart of these new measures, only a minimum amount of data will be accessed and only in instances which show a potential risk of fraud and error.[130]

Schedule 11 would insert a new schedule 3B into the Social Security Administration Act 1992. This would give the secretary of state the power to give an account information notice to a person of a prescribed description requiring them to provide information about an account they administer or have access to.[131] The secretary of state could use this power only to assist in "identifying cases which merit further consideration to establish whether relevant benefits are being paid or have been paid in accordance with the enactments and rules of law relating to these benefits".

The account information notice would require the recipient to give the secretary of state the names of account holders they identified as being 'matching accounts' in relation to a specified 'relevant benefit' and other specified information.[132]

---

[130] Department for Science, Innovation and Technology, Department for Work and Pensions and Home Office, 'Changes to data protection laws to unlock post-Brexit opportunity', 23 November 2023.

[131] Paragraph 1 of new schedule 3B to be inserted into the Social Security Administration Act 1992.

[132] Paragraph 2 of new schedule 3B.

'Relevant benefits' would be defined as:[133]

- a relevant social security benefit as defined in section 121DA(7) of the Social Security Administration Act 1992. These are benefits under the following legislation, except statutory sick pay and statutory maternity pay:
  - Social Security Contributions and Benefits Act 1992
  - Social Security Administration Act 1992
  - Pensions Schemes Act 1993, except part III
  - section 4 of the Social Security (Incapacity for Work) Act 1994
  - Jobseekers Act 1995
  - Social Security (Recovery of Benefits) Act 1997
  - parts I and IV of the Social Security Act 1998
  - part V of the Welfare Reform and Pensions Act 1999
  - State Pension Credit Act 2002
  - part 1 of the Welfare Reform Act 2007
  - part 1 of the Welfare Reform Act 2012
  - part 4 of the Welfare Reform Act 2012
  - part 1 of the Pensions Act 2014
  - part 5 of the Pensions Act 2014
  - Social Security Pensions Act 1975
  - Social Security Act 1973
  - subordinate legislation made under the above provisions
- a child tax credit or working tax credit under the Tax Credits Act 2002

[133] Paragraph 16 of new schedule 3B.

- a payment, as mentioned in subsection (2)(d) of section 2 of the Employment and Training Act 1973, under arrangements made under that section.

'Matching accounts' would be defined as accounts:

(a) linked to the receipt of the benefit, and

(b) in relation to which specified criteria relevant to that benefit, or specified criteria including such criteria, are met (for example, criteria about account balances or transactions outside the United Kingdom) [134]

An account would be regarded as 'linked' to the receipt of the benefit if:[135]

- the benefit had been paid into it
- the benefit was being paid into it or would be paid into it in future
- it was held by the same account-holder as an account that met either of the above conditions

An account information notice could require information relating to a person who holds a 'matching account' even if that person does not claim a relevant benefit.[136]

An account information notice could not require the recipient to

[134] Paragraph 2(3) of new schedule 3B.
[135] Paragraph 2(5) of new schedule 3B.
[136] Paragraph 2(2) of new schedule 3B.

interrogate data that was more than a year old.[137] It could require information to be provided at specified intervals for a period of up to a year from the date of the notice.[138]

The secretary of state could use the information only for the purposes of, or purposes connected with, the exercise of "departmental functions".[139] These are defined in section 127 of the Welfare Reform Act 2012 as functions relating to social security, employment or training or the investigation or prosecution of offences relating to tax credits.

The secretary of state could (but would not be obliged to) issue a code of practice in connection with account information notices.[140] It could include provision about considerations relevant to issuing account information notices and imposing penalties, assisting people to comply with account information notices, and complaints about account information notices.

The secretary of state would be able to impose a penalty if they had "reasonable grounds to believe that [a] person has failed to comply with the account information notice and had no reasonable excuse for the failure".[141] The secretary of state could impose a fixed penalty of up to £1,000, a daily rate penalty of up to £40 per day, or both. The secretary of state could apply to a tribunal to have the daily rate penalty increased if, more than 30 days after a daily rate penalty was imposed, the person was continuing not to comply with the account information notice. The tribunal could increase the daily rate penalty

[137] Paragraph 2(7) of new schedule 3B.
[138] Paragraph 3(2) of new schedule 3B.
[139] Paragraph 5 of new schedule 3B.
[140] Paragraph 6 of new schedule 3B.
[141] Paragraphs 9 to 12 of new schedule 3B make provision about monetary penalties.

up to a maximum of £1,000 per day. There would be a right of appeal to the tribunal against account information notices and against penalty notices.[142]

Part 2 of schedule 11 would make similar amendments to the Social Security Administration (Northern Ireland) Act 1992, giving the Northern Ireland Department for Communities the power to issue account information notices.

Speaking at report stage, Sir John Whittingdale explained the government wanted to introduce these powers to help tackle benefit fraud:

> In 2022–23 the Department for Work and Pensions overpaid £8.3bn in fraud and error. A major area of loss is the under-declaration of financial assets, which we cannot currently tackle through existing powers. Given the need to address the scale of fraud and error in the welfare system, we need to modernise and strengthen the legal framework […]
>
> The amendment will enable the DWP to access data held by third parties at scale where the information signals potential fraud or error. That will allow the DWP to detect fraud and error more proactively and protect taxpayers' money from falling into the hands of fraudsters.[143]

The explanatory notes to the bill state that the DWP would use the data as intelligence to help determine whether there was a need to

---

[142] Paragraphs 13 to 15 of new schedule 3B make provision about appeals.
[143] HC Hansard, 29 November 2023, col 879.

look into a claim in more detail.[144]

At report stage, Sir John said this amendment implemented an action in the DWP's plan for 'Fighting fraud and error in the welfare system', published in May 2022. This plan stated:

> Better access to data held by third parties, in particular banks, would be hugely beneficial in identifying fraud and error in the welfare system, especially in detecting undeclared capital in claims, the second highest type of welfare fraud. In universal credit alone, this type of fraud was estimated to be £0.9bn in 2020–21. It would also help us to check if someone is fraudulently claiming benefits from abroad.
>
> Third parties are restricted in the support they can provide us to fight fraud. Current powers mean we can only request information from third parties such as banks on an individual basis, where we already have a suspicion of fraud. We need to submit a request that can identify a specific individual by name or description (for instance, account number, sort code or address) to a bank so they can check that individual's capital holdings or whether they show signs of living abroad. This cannot be done swiftly at scale, and by the point of identification of an individual who we want to verify, it is likely that benefits may already have been being acquired fraudulently for some time. This hinders our ability to proactively identify fraud such as capital and abroad fraud that may be unknown to us but visible in third party data.
>
> We will legislate, when parliamentary time allows, for powers to require the transfer of data from third parties to enable the

[144] Explanatory notes, p 13.

> department to more proactively identify potential fraud, such as where claimants might have savings above the capital limit. We want to focus the initial use of this power with banks, where we could have the greatest initial impact. Almost all benefit payments go into current accounts and around 90% of capital fraud and error is identified in high street or online accounts. A small test has been run with a bank to assess the potential of using a feed of banking data to identify possible capital and abroad fraud and error, with very encouraging results.[145]

At report stage, Sir Chris Bryant and Sir Stephen Timms (Labour MP for East Ham), chair of the House of Commons Work and Pensions Committee, questioned repeatedly why the powers extended to looking at the bank accounts of people who claim the state pension.[146]

Sir Chris said he would "back 100% any attempt to tackle fraud" in the welfare system.[147] However, he criticised the government's approach on several grounds. First, he argued the power was "very broad" and "poorly delineated".[148] He questioned why it was drafted to include the bank accounts of people in receipt of benefits that the government said it did not plan at the moment to look at. Second, he expressed concern the power would "mean that millions of bank accounts could be trawled without the Department for Work and Pensions […] even suspecting anything untoward before it asked for the information". Third, he objected to NS1 being tabled on the last day for consideration, without the opportunity for full scrutiny in the House of Commons. He questioned why it had been tabled at this

[145] Department for Work and Pensions, 'Fighting fraud and error in the welfare system', May 2022, CP 679.
[146] HC Hansard, 29 November 2023, col 879, col 880, cols 886–7.
[147] HC Hansard, 29 November 2023, col 887.
[148] HC Hansard, 29 November 2023, col 886.

point given the government had run a test project in 2017, and also questioned why the minister had not mentioned to him in recent private discussions the government was planning to add this measure to the bill.[149] Fourth, he questioned the basis on which the government had made its estimates about how much money could be saved in the next five years, especially since the government was not intending to use the power until 2027.

Sir Chris said the Labour Party was willing to work with ministers to get the measure "right". He suggested meetings between Labour and the government would help "ensure that the debates in the Lords are well informed".

Sir Stephen Timms said the Work and Pensions Committee had received "substantial concerns" about the proposed measure, including from Citizens' Advice and the Child Poverty Action Group (CPAG).[150] He said many people agreed with CPAG's argument that people should not "have fewer rights, including to privacy, than everyone else in the UK simply because they are on benefits". He also highlighted that the government had introduced the measures "in such a way that we are not able to scrutinise what it is planning". He found the proposal "for surveillance where there is absolutely no suspicion at all" was a "substantial expansion of the state's powers to intrude".

In particular, Sir Stephen questioned why the government was including people claiming state pension when entitlement to that benefit was not based on the level of people's income or savings. He said the minister had failed to give a reason why it was necessary for

---

[149] HC Hansard, 29 November 2023, col 887.
[150] HC Hansard, 29 November 2023, col 899.

the government to be empowered to "inspect the bank account of anyone who claims a state pension, which is all of us". He also questioned whether the government had any plans to use the power to automatically identify people who would be entitled to claim benefits but do not do so, for example pension credit.[151]

David Davis said that MPs across the House understood the importance of stopping fraud in the welfare system.[152] However, he argued that a power "where the state seeks the right to put people under surveillance without prior suspicion" needed to be "restricted very carefully indeed". He believed the power needed to be made more targeted, and urged the government to address this further when the bill reached the House of Lords.

Speaking for the SNP, Patrick Grady (SNP MP for Glasgow North) echoed Sir Chris Bryant's points about the timing of the introduction of these measures to the bill. He questioned why, if the government had been planning to take these powers since the welfare fraud action plan was published in 2022, they were not in the original draft of the bill, or not brought in for detailed scrutiny at committee.[153] Mr Grady argued that the new schedule "provides little in the way of safeguards for people who may be subject to such checks". He also suggested there was a contradiction between assurances from the government that "only a minimum amount of data will be accessed" and their plans to carry out checks "proactively and at scale".

Throughout the debate on these provisions, Sir John Whittingdale maintained that "the state pension will not currently be an area of

---

[151] HC Hansard, 29 November 2023, col 900.
[152] HC Hansard, 29 November 2023, col 880.
[153] HC Hansard, 29 November 2023, col 891.

focus for the use of those powers".[154] He said the new measure was "specifically about ensuring that means-related benefit claimants are eligible for the benefits for which they are currently claiming".[155] Winding up the debate, Sir John said he agreed that "to the extent that levels of fraud in state pensions being currently nearly zero, the power is not needed in that case".[156] However, he said the government wished to "retain an option should the position change in the future". He said he expected that the question would be examined further by the Work and Pensions Committee and during the Lords stages of the bill.[157]

The new schedule was put to a division. The government won by 274 votes to 52 and the schedule was added to the bill.[158]

Privacy campaigners have also voiced objections to the measures on social security information. Open Rights Group said it believed the data could "easily be misinterpreted and benefits sanctions incorrectly imposed".[159] It argued that the policy would treat "vulnerable populations", such as migrants, refugees and people who are disabled, sick or in need of care, as "potential criminals rather than people in need of support". Big Brother Watch said it was "wholly inappropriate for the UK government to order private banks, building societies and other financial services to conduct mass, algorithmic, suspicionless surveillance and reporting of their account

---

[154] HC Hansard, 29 November 2023, col 879.
[155] HC Hansard, 29 November 2023, col 880.
[156] HC Hansard, 29 November 2023, col 912.
[157] HC Hansard, 29 November 2023, col 913.
[158] HC Hansard, 29 November 2023, cols 1007–9.
[159] Open Rights Group, 'DPDI Bill: New 'welfare surveillance' proposals target vulnerable people', 28 November 2023.

holders on behalf of the state".[160] It argued that "this level of auditing and insight into people's private lives is a frightening level of government overreach—more so, for some of the most marginalised in society".[161]

The House of Commons Public Accounts Committee published a report on 6 December 2023 that examined the scale of fraud and error in the benefit system.[162] It found that the level remained "unacceptably high". It said the DWP had overpaid some £8.2bn in 2022–23, of which £6.4bn was due to benefit fraud. This had fallen only slightly since the previous year. The committee said it was concerned that the DWP does not expect fraud and error to return to pre-pandemic levels until 2027–28. It said the DWP needed to implement its plan to tackle the increase in fraud and error and demonstrate a "meaningful reduction".

The committee also highlighted there had been "yet another historic underpayment of state pension" which the DWP estimated "may have left some 210,000 pensioners out of pocket by a total of £1.3bn". The committee said the DWP should "do more to detect underpayments before they build up and have a significant impact on pensioners and other claimants".

The committee did not specifically comment on the measures in the bill, but it noted that the DWP was expanding its use of advanced data analytics to tackle fraud, including piloting the use of machine-

---

[160] Big Brother Watch, 'Big Brother Watch briefing on the Data Protection and Digital Information 2.0 Bill for House of Commons report stage', November 2023, p 13.
[161] As above, p 14.
[162] House of Commons Public Accounts Committee, 'The Department for Work and Pensions Annual Report and Accounts 2022–23', 6 December 2023, HC 290 of session 2023–24.

learning algorithms to identify potentially fraudulent claims. The committee said the DWP had "not yet done enough to understand the impact of machine learning on customers and provide them with confidence that it will not result in unfair treatment".

6.2.12 Retention of information in connection with the death of a child (clause 129)

NC35 was added to the bill and is now clause 129 in the Lords version. It would require social media companies to keep relevant personal data of a child who has died through suicide so the data could then be used in subsequent investigations or inquests.

Clause 129 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 suspected to have taken their own life. 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.[163] The government said during the passage of the legislation that this measure would "help families and law enforcement understand if online activity contributed to their death in any way".[164]

However, when tabling their new clause to the present bill, the government said that current rules did not require social media companies to retain children's personal data, which meant that "data which could prove vital to coroner investigations could be deleted as part of a platform's routine maintenance".[165] It said this was a further step "to help ensure harmful content has no place online".

During the report stage debate, Layla Moran questioned why the new power to require social media companies to retain children's data applied only if the child's death was suspected to have been by suicide.[166] She raised the case of Breck Bednar, a teenager who was murdered by someone he had met online.[167] Ms Moran said the coroner would have wanted access to Breck's online data when investigating this case. Breck's mother had been involved in campaigning to have measures added to the Online Safety Bill to give coroners and bereaved families powers to access social media information that might be relevant to the death of a child.[168] Sir John Whittingdale said the government would continue to work with bereaved families and members of the House of Lords who had

[163] Online Safety Act 2023, section 101.
[164] Department for Science, Innovation and Technology, 'Online Safety Bill bolstered to better protect children and empower adults', 30 June 2023.
[165] Department for Science, Innovation and Technology, Department for Work and Pensions and Home Office, 'Changes to data protection laws to unlock post-Brexit opportunity', 24 November 2023.
[166] HC Hansard, 29 November 2023, col 878.
[167] BBC News, 'Breck Bednar murder: Lewis Daynes sentenced to life in prison', 12 January 2015.
[168] BBC News, 'Online Safety Bill: Bereaved parents win fight for information', 22 June 2023.

raised concerns about this issue.[169]

6.2.13 Retention of biometric data (clauses 130 to 132)

The government introduced several new clauses that would change the way law enforcement authorities are allowed to retain biometric data shared with them by foreign partners.

NC36, added to the bill as clause 130, 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.[170] Sir John Whittingdale explained the government was introducing this amendment to enable counter-terrorism police to retain biometrics received from international partners in a more efficient way.[171] He suggested this would redress the current situation where "police can hold biometrics indefinitely for people who have a conviction for shoplifting in the UK but not for convicted terrorists abroad". The amendment would enable the police to retain an individual's fingerprints and DNA profile 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.[172]

---

[169] HC Hansard, 29 November 2023, cols 878–9 .

[170] Member's explanatory statement in House of Commons, 'Data Protection and Digital Information Bill (Amendment paper)', 29 November 2023, p 37.

[171] HC Hansard, 29 November 2023, col 875.

[172] 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.

Sir John also explained that under current legislation, the police can retain biometrics that identify the person from whom they were obtained, but only for three years.[173] Sir John said that the government's NC37, added to the bill as clause 131, would enable the police to "take proactive steps 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 allow the police to hold pseudonymised biometric data indefinitely.[174] Sir John said that counter-terrorism police had requested this change.

NC38, added to the bill as clause 132, 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.[175] Sir John said this would bring the UK into line with the rules under which other Interpol members retained and used these biometrics.[176] He said this amendment was welcomed by counter-terrorism police, the independent reviewer of terrorism legislation, the Office of the Biometrics Commissioner and the security services.

6.2.14 National underground asset register (clauses 138 to 141 and schedule 13)

The government introduced new clauses and a new schedule to

[173] HC Hansard, 29 November 2023, col 876.
[174] Counter-Terrorism Act 2008, s 18A(4).
[175] Interpol, 'Notices', accessed 7 December 2023.
[176] HC Hansard, 29 November 2023, col 876.

create a statutory national underground asset register (NUAR). Sir John explained that this would be "a digital map that will improve both the efficiency and safety of underground work, by providing secure access to privately and publicly owned location data about the pipes and cables beneath our feet".[177]

The government explained why it believed this was needed:

> There are 700+ owners of underground assets (or "apparatus") across the public and private sectors (including energy, water, telecommunications and local transport authorities) who hold data about their own apparatus, which they are required by law to make available 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 installing, maintaining, operating and repairing buried apparatus.
>
> The bill aims to 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 a national underground asset register.[178]

The government estimates that once it is operational, the NUAR will deliver £490mn per year of economic growth, through "increased efficiency, reduced asset strikes (when underground pipes and cables are accidentally damaged) and reduced disruptions for the public and

[177] HC Hansard, 29 November 2023, col 876.
[178] Explanatory notes, p 15.

business".[179] An initial private beta version of NUAR is already live across England and Wales, including data from the major energy and water providers, several major telecoms companies and some smaller providers, transport organisations and local authorities. The government expects to extend coverage to Northern Ireland in spring 2024 and for the platform to be fully operational by the end of 2025. 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.[180]

NC39, added to the bill as clause 138, would amend the New Roads and Street Works Act 1991 to require the secretary of state to keep a register of information relating to apparatus in streets in England and Wales, to be known as the national underground asset register. NC39, added to the bill as clause 139, would also give the secretary of state the power to make regulations about:

- accessing the information kept in the NUAR
- fees payable by undertakers in relation to the NUAR
- requiring undertakers that have apparatus in the street to provide information to the secretary of state in relation to the payment of fees

Clause 139 would also add a new schedule to the 1991 act (this is contained in schedule 13 to this bill) that would allow the secretary of state to impose monetary penalties on someone who refused to

[179] Department for Science, Innovation and Technology, and Geospatial Commission, 'National underground asset register (NUAR)', 23 November 2023.
[180] Office of the Scottish Road Works Commissioner, 'Vault: Access to information on the location of underground pipes and cables', accessed 1 December 2023.

pay the NUAR fees, who refused to provide information to enable the secretary of state to determine if they were liable to pay fees, or who provided false or misleading information. Sir John Whittingdale said at report stage that the provisions on levying fees would mean that "the running of the register will be funded by those who benefit most" rather than the taxpayer and "ensure that the NUAR is a sustainable service for the future".[181]

NC40, added to the bill as clause 139, would amend the 1991 act to impose new duties on undertakers to keep records of and share information about their apparatus in the streets. 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.[182] They would be obliged to share information about existing apparatus before the end of an 'initial upload period', the date of which would be set by the secretary of state. They would be under an ongoing obligation to update the record "as soon as reasonably practicable" after placing an item in the street or moving its position, or inspecting, maintaining, adjusting, repairing, altering or renewing it. There would also be a duty to report missing or incorrect information discovered while executing street works. Fines would be applicable for failing to record the required information.

Before making regulations under clause 138 or 139, the secretary of state must consult representatives of persons likely to be affected and Welsh ministers. NC41, added to the bill as clause 140, would provide that consultation taking place either before or after the clauses come into force could satisfy this requirement.

---

[181] HC Hansard, 29 November 2023, cols 876–7.

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

NC42, added to the bill as clause 141, would transfer certain powers to make regulations for Wales under section 79 of the 1991 act, as amended by the bill, from the Welsh ministers to the secretary of state.

Sir John noted that the new clauses would allow for the NUAR to operate in England and Wales.[183] He said the government intended to bring forward equivalent provisions for Northern Ireland when the bill reaches the House of Lords.

6.2.15 Disclosure for the purposes of archiving in the public interest (schedule 2)

An amendment was made to schedule 2 relating to archiving in the public interest, and how that relates to 'purpose limitation'. Purpose limitation is one of the key principles that lie at the heart of the general data protection regime.[184] It is set out in article 5(1)(b) of the UK GDPR, which requires that personal data shall be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". In other words, personal data cannot be reused ("further processed") in a way that is not compatible with the original purpose for which it was collected. Article 5(1)(b) also states that "further processing for archiving purposes in the public interest […] shall not be considered to be incompatible with the initial purpose".

Clause 6 would set out the conditions for determining whether the reuse of personal data is permitted in compliance with the purpose

---

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

[184] Information Commissioner's Office, 'A guide to the data protection principles', accessed 1 December 2023.

limitation principle.[185] Related to this, schedule 2 would insert a new annex 2 into the UK GDPR which sets out a number of conditions on further processing.[186] If further processing meets any of these conditions, then it would be treated as being compatible with the original purpose for which it was collected, and therefore a lawful use of the personal data. Government amendment 208, made at report stage, introduced a new condition 2 into schedule 2, which would enable certain further processing of personal data for the purposes of archiving in the public interest, where the original processing was based on the consent of the data subject.[187]

Sir John Whittingdale said the government recognised that "archivists currently have very little agency to dictate what lawful ground was used when obtaining personal data from a wide range of sources".[188] He explained the government's amendment to the bill would "ensure that a controller is able to reuse personal data for the purpose of archiving in the public interest, regardless of the lawful ground the personal data was originally collected on". He said this would be "particularly helpful for archivists that are not public authorities and are therefore unable to use a public task ground for their processing". He said the government had worked closely with the National Archives on this amendment.

6.2.16 Divisions on non-government amendments

Five non-government amendments were defeated on division at report stage. Labour's amendments on democratic engagement and

---

[185] Explanatory notes, p 32.
[186] As above, p 117.
[187] Member's explanatory statement in House of Commons, 'Data Protection and Digital Information Bill (Amendment paper)', 29 November 2023, p 152.
[188] HC Hansard, 29 November 2023, col 875.

high-risk processing are covered respectively in sections 6.2.2 and 6.2.4 above. An amendment on protecting special category data in employment settings tabled by a backbench Labour MP, and Labour and SNP amendments on automated decision-making, are covered below.

6.2.17 Lawfulness of processing (amendment 11)

Kate Osborne (Labour MP for Jarrow) tabled amendment 11 to clause 5. This was intended to clarify that the processing of special category data in employment settings would have to follow established principles for reasonable processing, as defined by paragraph 1 of schedule 1 of the DPA 2018.[189] Ms Osborne argued that the bill would allow employers to share employee's personal data, such as health data, within their organisation without a justifiable reason. She said the National AIDS Trust was concerned this could mean people's HIV status could be shared without their consent, leading to discrimination.[190]

Sir John Whittingdale said that the government agreed with the sentiment of the amendment.[191] However, he deemed the amendment "unnecessary", as the current legal framework already required data controllers to identify an exemption under article 9 of the UK GDPR if they were processing special category data.

The amendment was defeated by 276 votes to 200.[192]

---

[189] Member's explanatory statement in House of Commons, 'Data Protection and Digital Information Bill (Amendment paper)', 29 November 2023, p 61.
[190] National AIDS Trust, 'MPs must act now to protect health data', 17 November 2023.
[191] HC Hansard, 29 November 2023, col 915.
[192] HC Hansard, 29 November 2023, cols 953–6.

6.2.18 Automated decision-making (amendments 5 and 224)

Labour and the SNP both moved amendments to change the bill's provisions on automated decision-making. 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:[193]

- 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

Clause 14 of the bill would remove the existing article 22 from the UK GDPR and replace it with new provisions. This would mean that restrictions on the use of solely automated processing to take significant decisions would apply only where the decision was based wholly or partly on 'special category' data. 'Special category' data, as defined in article 9(1) of the UK GDPR, 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.[194] Under the new provisions, 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

[193] Information Commissioner's Office, 'Rights related to automated decision making including profiling', accessed 4 December 2023.
[194] Information Commissioner's Office, 'Special category data', accessed 28 November 2023.

it produced "a legal effect for the data subject" or had a "similarly significant effect for the data subject". Organisations 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 and either necessary for the entry into or performance of a contract, or required or authorised by law

Clause 14 would include safeguards for decisions taken solely using automated processing, including:

- notifying the data subject after such a decision had been taken
- enabling the data subject to make representations about the decision
- enabling the data subject to obtain human intervention from the organisation (data controller) in relation to the decision
- enabling the data subject to contest the decision

Sir Chris Bryant acknowledged that automated decision-making had "the potential to deliver increasingly personalised and efficient services, to increase productivity and to reduce administrative hurdles".[195] However, he also cautioned that "countless research projects have shown that automated decision making and machine decision making are not as impartial or as blind as they sound". He

[195] HC Hansard, 29 November 2023, col 878.

argued that "most of the world is making it harder to make decisions exclusively using ADM", whereas clause 14 would extend the potential for automated decision-making in the UK. Labour's amendment 5 would have extended the safeguards in clause 14 that apply to decisions made solely on the basis of automated processing so that they would also have covered decisions made partly on the basis of automated processing. Sir Chris argued this would strike "a better balance".[196]

Sir John Whittingdale said there was "no need" to extend the protections to partly automated decisions, since these already involved "meaningful human involvement".[197] He said decisions of this type would be covered by relevant protections in the broader data protection regime.

The SNP moved an amendment (amendment 224) to remove clause 14 from the bill altogether. Patrick Grady quoted the Ada Lovelace Institute, an independent research institute, which had argued that "against an already-poor landscape of redress and accountability in cases of AI [artificial intelligence] harms, the bill's changes will further erode the safeguards provided".[198] Mr Grady said clause 14 "fails to offer adequate protection against automated decision making".[199] For instance, he argued that an individual might grant consent for the processing of their data, but that "does not mean that they will fully understand or appreciate how that data will be processed or, importantly, how decisions will be made".

---

[196] HC Hansard, 29 November 2023, col 879.
[197] HC Hansard, 29 November 2023, col 911.
[198] Ada Lovelace Institute, 'Regulating AI in the UK: Strengthening the UK's proposals for the benefit of people and society', 18 July 2023.
[199] HC Hansard, 29 November 2023, col 892.

In response to this amendment, Sir John Whittingdale pointed out that solely automated decision-making that produces legal or similarly significant effects on individuals was not prohibited under the current legal framework.[200] He argued that clause 14 "clarifies and simplifies" the rules while maintaining high standards of data protection and enabling innovation.

The SNP amendment was defeated by 279 votes to 37.[201] The Labour amendment was defeated by 273 votes to 195.[202]

7. House of Commons: Third reading

Third reading took place immediately after report stage on 29 November 2023.[203] Sir John Whittingdale said the bill would "deliver tangible benefits to British consumers and businesses alike", made possible as a result of Brexit. He said it would establish "a more flexible and less burdensome data protection regime that maintains high standards of privacy protection while promoting growth and boosting innovation".

Sir Chris Bryant said Labour supported the bill, although he expressed his continued concerns about "the extensive powers that ministers are giving themselves", particularly in relation to "switch[ing] off the rules on direct marketing in the run-up to a general election.[204] He said he hoped the House of Lords would be "able to do the line by line scrutiny that [the House of Commons]

---

200 HC Hansard, 29 November 2023, col 913.
201 HC Hansard, 29 November 2023, cols 957–9.
202 HC Hansard, 29 November 2023, cols 959–63.
203 HC Hansard, 29 November 2023, cols 1015–16.
204 HC Hansard, 29 November 2023, col 1015.

have been prevented from doing" on the social security information provisions.

Speaking for the SNP, Patrick Grady also expressed concerns that the bill represented "a further power grab by the executive". He feared it risked doing the opposite of what the government wanted to achieve on making life easier for businesses and improving public confidence in data handling and the use of AI. He said the SNP would oppose the bill. He also believed it was "sub-optimal" that it would "once again fall to the unelected House to more fully interrogate the bill".

There was a division on giving the bill its third reading. The government won the vote by 269 to 31.[205]

8. Read more

- House of Commons Library, 'Data Protection and Digital Information (No. 2) Bill 2022–23', 28 March 2023
- House of Commons Library, 'Data Protection and Digital Information (No. 2) Bill: Progress of the bill', 17 November 2023
- Public Law Project, 'House of Commons report stage briefing on the Data Protection and Digital Information Bill', 28 November 2023
- Open Rights Group, 'Parliamentary briefing—Data Protection and Digital Information Bill', 20 November 2023
- Big Brother Watch, 'Big Brother Watch briefing on the Data Protection and Digital Information 2.0 Bill for House of Commons report stage', November 2023

[205] HC Hansard, 29 November 2023, cols 1016–19.

9. Guide to clause numbering

The table below is intended as a guide to how the numbering of clauses and schedules has changed as the bill was amended in the House of Commons.

HC Bill 265 of session 2022–23 was the Data Protection and Digital Information (No. 2) Bill. The House of Commons Library briefing 'Data Protection and Digital Information (No. 2) Bill 2022–23' (28 March 2023), which provides background to many of the measures, uses the clause numbering in this version of the bill.

HC Bill 1 of session 2023–24 is the version of the bill that was carried over into the current parliamentary session. It incorporates the amendments made to the bill at committee stage in the House of Commons.

HL Bill 30 of session 2023–24 is the version of the bill that was introduced in the House of Lords. It incorporates the amendments made to the bill at report stage in the House of Commons. Unless otherwise specified, this briefing uses the clause numbering from this version of the bill.

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
1	1	1	Information relating to an identifiable living individual

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
2	2	2	Meaning of research and statistical purposes
3	3	3	Consent to processing for the purposes of scientific research
4	4	4	Consent to law enforcement processing
5	5	5	Lawfulness of processing
6	6	6	The purpose limitation
	7		~~Elected representatives responding to requests~~
		7	Processing in reliance on relevant international law
		8	Processing of personal data revealing political opinions
7	8	9	Vexatious or excessive requests by data subjects
8	9	10	Time limits for responding to requests by data subjects
9	10	11	Information to be provided to data subjects
		12	Searches in response to data subjects' requests

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
10	11	13	Data subjects' right to information: legal professional privilege exemption
11	12	14	Automated decision-making
12	13	15	General obligations
13	14	16	Removal of requirement for representatives for controllers etc outside the UK
14	15	17	Senior responsible individual
15	16	18	Duty to keep records
16	17	19	Logging of law enforcement processing
17	18	20	Assessment of high risk processing
18	19	21	Consulting the commissioner prior to processing
	20	22	General processing and codes of conduct
19	21	23	Law enforcement processing and codes of conduct
20	22	24	Obligations of controllers and processors: consequential amendments

HC Bill 265 of 2022–23 session	HC Bill I of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
21	23	25	Transfers of personal data to third countries and international organisations
22	24	26	Safeguards for processing for research etc purposes
23	25	27	Section ~~24~~ 26: consequential provision
24	26	28	National security exemption
25	27	29	Joint processing by intelligence services and competent authorities
26	28	30	Joint processing: consequential amendments
27	29	31	Duties of the commissioner in carrying out functions
28	30	32	Strategic priorities
29	31	33	Codes of practice for the processing of personal data
30	32	34	Codes of practice: panels and impact assessment
31	33	35	~~Codes of practice: approval by the Secretary of State~~ Codes of practice: Secretary of state's recommendations
32	34	36	Vexatious or excessive requests made to the Commissioner

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
33	35	37	Analysis of performance
		38	Notices from the Commissioner
34	36	39	Power of the Commissioner to require documents
35	37	40	Power of the Commissioner to require a report
36	38	41	Interview notices
37	39	42	Penalty notices
38	40	43	Annual report on regulatory action
39	41	44	Complaints to controllers
40	42	45	Power of the Commissioner to refuse to act on certain complaints
41	43	46	Complaints: minor and consequential amendments
		47	Court procedure in connection with subject access requests
42	44	48	Consequential amendments to the EITSET Regulations
43	45	49	Protection of prohibitions, restrictions and data subject's rights
44	46	50	Regulations under the UK GDPR
45	47	51	Minor amendments
46	48	52	Introductory

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
47	49	53	DVS trust framework
		54	Approval of a supplementary code
		55	Designation of a supplementary code
		56	List of recognised supplementary codes
		57	Change to conditions for approval and re-approval
		58	Revision of a recognised supplementary code
		59	Applications for approval and re-approval
		60	Fees for approval, re-approval and continued approval
		61	Request for withdrawal of approval
		62	Removal of designation
48	50	63	DVS register
		64	Registration of additional services
		65	Supplementary notes
		66	Addition of services to supplementary notes
49	51	67	Applications ~~for registration~~ under sections 63 to 66

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
50	52	68	Fees for ~~registration~~ applications under sections 63 to 66
51	53	69	Duty to remove person from the DVS register
52	54	70	Power to remove person from the DVS register
53	55		~~Revising the DVS trust framework: top-up certificates~~
		71	Duty to remove services from the DVS register
		72	Duy to remove supplementary notes from the DVS register
		73	Duty to remove supplementary services from supplementary notes
54	56	74	Power of public authority to disclose information to registered person
55	57	75	Information disclosed by Revenue and Customs
	58	76	Information disclosed by Welsh Revenue Authority
	59	77	Information disclosed by Revenue Scotland
56	60	78	Code of practice about the disclosure of information

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
57	61	79	Trust mark for use by registered persons
58	62	80	Power of Secretary of State to require information
59	63	81	Arrangements for third party to exercise functions
60	64	82	Report on the operation of this Part
		83	Index of defined terms for Part 2
		84	Powers relating to verification of identity or status
61	65	85	Customer data and business data
62	66	86	Power to make provision in connection with customer data
63	67	87	Customer data: supplementary
64	68	88	Power to make provision in connection with business data
65	69	89	Business data: supplementary
66	70	90	Decision-makers
		91	Interface bodies
67	71	92	Enforcement of data regulations
68	72	93	Restrictions on powers of investigation etc
69	73	94	Financial penalties

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
70	74	95	Fees
71	75	96	Levy
72	76	97	Financial assistances
		98	The FCA and financial services interfaces
		99	The FCA and financial services interfaces: supplementary
		100	The FCA and financial services interfaces: penalties and levies
73			~~Confidentiality and data protection~~
		101	Liability in damages
	77	102	Restrictions on processing and data protection
74	78	103	Regulations under this Part
75	79	104	Duty to review regulations
		105	Other data provision
76	80	106	Repeal of provisions relating to supply of customer data
77	81	107	Interpretation of this Part
78	82	108	The PEC regulations
79	83	109	Storing information in the terminal equipment of a subscriber or user

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
80	84	110	Unreceived communications
81	85	111	Meaning of "direct marketing"
		112	Duty to notify Commissioner of personal data breach: time periods
82	86	113	Use of electronic mail for direct marketing purposes
83	87	114	Direct marketing for the purposes of democratic engagement
84	88	115	Meaning of expressions in section ~~87~~ 114
85	89	116	Duty to notify the Commissioner of unlawful direct marketing
86	90	117	Commissioner's enforcement powers
	91	118	Codes of conduct
	92	119	Pre-commencement consultation
87	93	120	The eIDAS Regulation
88	94	121	Recognition of EU conformity assessment bodies
89	95	122	Removal of recognition of EU standards etc
90	96	123	Recognition of overseas trust products

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
91	97	124	Co-operation between supervisory authority and overseas authorities
92	98	125	Disclosure of information to improve public service delivery to undertakings
93	99	126	Implementation of law enforcement information-sharing agreements
	100	127	Meaning of "appropriate national authority"
		128	Power to require information for social security purposes
		129	Retention of information by providers of internet services in connection with death of child
		130	Retention of biometric data and recordable offences
		131	Retention of pseudonymised biometric data
		132	Retention of biometric data from Interpol
94	101	133	Form in which registers of births and deaths are to be kept
95	102	134	Provision of equipment and facilities by local authorities
96	103	135	Requirements to sign register

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
97	104	136	Treatment of existing registers and records
98	105	137	Minor and consequential amendments
		138	National Underground Asset Register
		139	Information in relation to apparatus
		140	Pre-commencement consultation
		141	Transfer of certain functions to secretary of state
99	106	142	Information standards for health and adult social care in England
100	107	143	The Information Commission
101	108	144	Abolition of the office of Information Commissioner
102	109	145	Transfer of functions to the Information Commission
103	110	146	Transfer of property etc to the Information Commission
104	111	147	Oversight of retention and use of biometric material
105	112	148	Removal of provision for regulation of CCTV etc
106	113	149	Oversight of biometrics databases

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
107	114	150	Power to make consequential amendments
108	115	151	Regulations
109	116	152	Interpretation of this Act
110	117	153	Financial provision
111	118	154	Extent
112	119	155	Commencement
113	120	156	Transitional, transitory and saving provision
114	121	157	Short title
Schedule 1	Schedule 1	Schedule 1	Lawfulness of processing: recognised legitimate interests
Schedule 2	Schedule 2	Schedule 2	Purpose limitation: processing to be treated as compatible with original purpose
Schedule 3	Schedule 3	Schedule 3	Automated decision-making: consequential amendments
Schedule 4	Schedule 4	Schedule 4	Obligations of controllers and processors: consequential amendments
Schedule 5	Schedule 5	Schedule 5	Transfers of personal data to third countries etc: general processing

HC Bill 265 of 2022–23 session	HC Bill 1 of 2023–24 session	HL Bill 30 of 2023–24 session	Clause title
Schedule 6	Schedule 6	Schedule 6	Transfers of personal data to third countries etc: law enforcement processing
Schedule 7	Schedule 7	Schedule 7	Transfers of personal data to third countries etc: consequential and transitional provision
Schedule 8	Schedule 8	Schedule 8	Complaints: minor and consequential amendments
Schedule 9	Schedule 9	Schedule 9	Data processing: minor amendments
Schedule 10	Schedule 10	Schedule 10	Privacy and electronic communications: Commissioner's enforcement powers
		Schedule 11	Power to require information for social security purposes
Schedule 11	Schedule 11	Schedule 12	Registers of births and deaths: minor and consequential amendments
		Schedule 13	National Underground Asset Register: monetary penalties
Schedule 12	Schedule 12	Schedule 14	Information standards for health and adult social care in England
Schedule 13	Schedule 13	Schedule 15	The Information Commission

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.