Updated to take account of the version of the Bill published March 2023

DATA PROTECTION AND DIGITAL INFORMATION BILL

The role of secondary legislation

Summary: The Data Protection and Digital Information Bill (the 'Bill') gives wide discretion to the Secretary of State to make fundamental changes to data protection law by statutory instrument, including introducing new, automatic lawful bases for processing[1]. Given that statutory instruments are very rarely rejected by Parliament, this represents a significant medium-term risk to standards of protection for personal data under the new regime. By extension, it leaves a question mark over the UK's adequacy decision from the EU, as the impact of changes introduced by secondary legislation will be subject to anxious scrutiny by the European Commission and privacy and data protection advocates.

The role of secondary legislation by provision

Matters which are of greatest significance in the data protection regime – and which therefore require the most scrutiny if changed – are highlighted orange[2].

Matter/Powers	Relevant Sections	Parliamentary Procedure[3]	Limitations on discretion[4]
List of **recognised legitimate interests**	s.6 Annex 1	Affirmative	Consider Interests, fundamental rights & freedoms of data subjects Consider need to protect children

[1] This is a core concept in data protection: processing of personal data is illegal unless it is done in reliance on a specific 'lawful basis'. The bases which can be relied upon are limited and are set out in Article 6 GDPR.
[2] There are no significant changes to this in the most recent published version of the Bill.
[3] In the 'affirmative' procedure, secondary legislation becomes law only once positively approved by both Houses of Parliament. In the 'negative' procedure, it becomes law *unless voted down* by at least one House. In the 'made affirmative' procedure, secondary legislation becomes law without Parliament considering it, but cannot remain law unless both Houses approve it within a certain time frame.
[4] Note that s.44 of the Bill requires the Secretary of State to consult with the Commissioner in relation to any regulations made under the UK GDPR

Matter/Powers	Relevant Sections	Parliamentary Procedure[3]	Limitations on discretion[4]
List of **compatible secondary purposes**	s.6 Annex 2	Affirmative	New purposes must be necessary to safeguard interests in Article 23 GDPR
Require controllers to publish guidance on fees for data subject requests	s.7	N/A	None
Define decisions as **not significant** for Article 22A (automated decisions)	s.11	Affirmative	None
Amend **safeguards** for 'ordinary' **solely automated significant decisions** in Article 22C	s.11	Affirmative	None
Approval regulations and standard clauses for **international transfers**	s.21 / Sch 5[5]	Affirmative	May consider any matter the SoS considers relevant The data protection test ('not materially lower') must be met
Derogations (for one-off) or restrictions in **international transfers**	s.21 / Sch 5	Affirmative; made affirmative if urgent	None

[5] Similar provisions apply for international transfers in the context of law enforcement processing subject to Part 3 DPA.

Matter/Powers	Relevant Sections	Parliamentary Procedure[3]	Limitations on discretion[4]
Vary **safeguards** required for processing for scientific research[6]	s.22	Affirmative	None
Designation of **joint processing between competent authorities and intelligence services** to bring it within Part 4 DPA	s.25	N/A	Consult the Commissioner[7] Processing must not involve transfers of data outside the UK
Designation of **strategic priorities** for the Information Commissioner	s.28	Laid before Parliament; 40 day waiting period	None
Require Commissioner to prepare **codes of practice**	s.29	Negative	None
Approval of **codes of practice**	s.31	N/A	None
Require controllers to **notify the Commissioner of complaints** in a prescribed form & at prescribed internals	s.39	Negative	None

[6] Core requirements – no decisions about the data subjects, no substantial danger or distress, and data minimisation – cannot be varied or removed by statutory instrument.
[7] Where a specific provision – as opposed to s.44 of the Bill – requires consultation of the Commissioner, it also requires consultation of 'such other persons as the Secretary of State considers appropriate', which does not in practical terms place any further limits on the discretion.

Matter/Powers	Relevant Sections	Parliamentary Procedure[3]	Limitations on discretion[4]
Prepare **DVS** Trust Framework, Register & code of practice	ss.47-60	N/A	Consult the Commissioner
Provisions for **access to business and customer data**, including enforcement, levies etc.	ss.61-75	Mostly affirmative; negative for more minor matters	Likely effects on customers, data holders, businesses, innovation, competition, and digital markets. Consult persons likely to be affected. Consult sectoral regulators.
Add conditions in which cookies can be used under PECR Provide for automatic consent/object signal technology	s.79	Affirmative	Consult the Commissioner
Make exemptions from direct marketing rules for democratic engagement	s.83	Affirmative	Consult the Commissioner Consider impact on the privacy of individuals
Amend fixed penalty for PECR breaches	s.85-6	Affirmative	None

Matter/Powers	Relevant Sections	Parliamentary Procedure[3]	Limitations on discretion[4]
Provisions for recognition of trust services (e.g. online signatures)	s.89-90	Negative	New signatures/seals must be of equivalent reliability to existing recognised ones
Provisions for sharing of information for law enforcement purposes in international agreements	s.93	Negative	None
Changes to role & name of Forensic Information Database Strategy Board	s.105	Affirmative	None
Appointment of Chair and non-executive board members of the Information Commission[8]	Sch 12A	N/A	Appointments must be based on merit and subject to open and fair competition

Risk to data rights

1. In general, the more consequential areas in which the Secretary of State has discretion are subject to the (relatively more accountable) affirmative resolution procedure. This means that any regulations will not take effect unless positively approved by both Houses of Parliament, and therefore subject to a degree of Parliamentary scrutiny.

2. However, secondary legislation subject to this procedure is typically debated in small, delegated legislation committees, then sent for approval by the House of Commons without debate. It is very rare for secondary legislation not to be

[8] There are a range of other more minor powers for the Secretary of State relating to the day to day operation of the Information Commission, e.g. payments to board members.

approved under this procedure. The last time the House of Commons failed to pass an affirmative instrument was in 1978, while the House of Lords last failed to do so in 2015[9].

3. The Bill provides for some *fundamental aspects of data protection law* – highlighted orange above, including the lawful bases on which data can be processed – to be changed by the Secretary of State. Given that even under the affirmative resolution procedure, Parliamentary scrutiny of such change is likely to be limited in practice, this represents a significant medium-term risk to standards of protection for personal data under the new regime.

Risk to adequacy

4. Predicting the impact of this on the UK's adequacy determination requires a distinction between (i) the status and impact of the Bill itself on the day it becomes law, and (ii) the potential for longer-term change to the UK's data protection regime.

Immediate impact

5. By leaving important matters of data protection subject to change through secondary legislation (i.e., without further primary legislation) and therefore full parliamentary scrutiny, it could be argued that the Bill creates a data protection regime that is too ill-defined and/or liable to change over time for the UK's adequacy decision to be meaningful. That is, the European Commission would not be able to assess whether or not standards of data protection in the UK meet the relevant test in the EU GDPR for data adequacy.

6. It is unclear however, the extent to which the Commission is likely to inquire into the specifics of how secondary legislation is made in the UK, or whether it would be willing to effectively imply that the use of statutory instruments is arbitrary or not consistent with the rule of law. Article 45 EU GDPR also already provides for the protection of personal data in countries with adequacy to be monitored, which would allow the Commission to respond to any future fundamental reductions in

[9] The Institute for Government: https://www.instituteforgovernment.org.uk/explainers/secondary-legislation

data protection in the UK via statutory instrument. It is unlikely that the mere presence in the Bill of the *ability* to create secondary legislation would prevent the Commission from renewing the UK's adequacy determination, once it becomes law.

Longer-term impact

7. Over time, secondary legislation may lead to significant changes to the UK's data protection regime. There is likely to be anxious scrutiny of the way the UK's data protection regime is developing from the European Commission. Major changes could well prompt the Commission to reconsider whether the UK continues to meet the test in Article 45 GDPR.

8. Data adequacy is moreover not only a political matter for the European Commission. It will face scrutiny before courts and by data protection authorities. Individuals may bring cases resulting in references being made to the CJEU (as has happened in relation to adequacy for the US) where they consider secondary legislation has changed the UK's regime to such an extent that an adequacy decision from the European Commission should no longer stand.

9. Thus while the role of secondary legislation in the Bill does not necessarily imperil the UK's adequacy on the day it becomes law, it leaves a real question mark over the long-term future of the UK's adequacy decision, depending on how that secondary legislation is used to change the data protection regime. This in turn will undermine business confidence and investment.

10. To address the risks to data rights and adequacy, the Government should consider limiting the role for primarily legislation to less consequential aspects of the regime (i.e. as a starting point, removing the ability for the Secretary of State to make changes to the provisions highlighted in the above table). Whilst a requirement for public consultation in relation to significant changes would improve their democratic accountability, it would not by itself prevent the UK's data protection regime from drifting far enough from the EU's – without full parliamentary scrutiny – so as to permit a successful challenge to the UK's adequacy decision.