

Data Protection and Digital Information Bill

Briefing note November 2022.

The Bill proposes amendments to the Data Protection Act 2018, UK GDPR and Privacy and Electronic Communications Regulations (PECR).

The Bill is currently making its way through parliament.

Progress of the Bill can be viewed here: [Data Protection and Digital Information Bill – Parliamentary Bills – UK Parliament](#)

Proposals in the Bill that would impact the council:

1) Definition of personal data

Revised back to pre-GDPR times. Only if data controller can identify, or person they are giving it to can identify (directly or indirectly).

This limits the assessment of identifiability of the data to the controller/processor and person to receive the data rather than anyone in the world.

This could make it easier for organisations to achieve data anonymisation-no longer need to consider potential future identifiability only identifiability at the time of processing. But this does not change the risk of indirect identification.

2) Subject Access Requests

Can refuse requests as 'vexatious or excessive'

This would replace the provisions in UK GDPR currently to refuse "manifestly unfounded" or "excessive" requests.

Examples of vexatious requests in the Bill are those intended to cause distress, not made in good faith, or that are an abuse of process.

Arguably the proposed new provision already exists in the current provision of "manifestly unfounded".

3) Data Subject's Complaints

The Bill expressly provides that data subjects can complain to the controller (council). The council must acknowledge within 30 days and respond, "without undue delay".

The Bill provides that if the data subject has not made a complaint first to the controller the Information Commissioner's Office (ICO) may refuse to act on the complaint.

This should prevent data subject's making complaints directly to the ICO without first seeking address through the council's complaints procedures.

The council may also be required to provide the ICO with the number of complaints on request, so these types of complaints will need to be recorded separately.

4) Data Protection Impact Assessments

DPIAs would be referred to as 'Assessments of High Risk Processing' (of the envisaged processing operations on the protection of personal data) proposing to be a leaner and less prescriptive with no requirement to refer any residual high risks to the ICO (optional).

SRI would not be required to sign off the new assessments.

5) Records of Processing Activities

The Bill proposes to replace with leaner “Record of Processing of Personal Data”

6) Use of personal data for a different purpose

Proposes data controllers have more scope for re-using data for a compatible purpose.

7) Automated processing

The Bill proposes to weaken current provision in UK GDPR providing a right not to be subject to decisions based solely on automated processing.

It would only apply to “significant decisions” rather than decisions that produce legal or similarly significant effects.

It is unclear whether this will make any practical difference.

8) Politicians

The Bill proposes political parties and representatives, and candidates have more ability to directly market and process data about individuals, including 'democratic engagement' as a 'recognised legitimate interest' to over 14s.

9) Law enforcement processing

The Bill proposes to remove requirement to have logging audit trails.

10) International transfers of personal data

The Bill proposes a leaner “data protection test” in replacement to the current Transfer Impact Assessment (TIA).

This would involve determining if the standard of protection provided to data subjects in the recipient country is not materially lower than the standard in the UK.

The explanatory notes to the Bill state the assessment would be based on outcomes for the overall protection for a data subject rather than a point-by-point comparison.

This lighter touch approach may attract the attention of the EU when deciding whether to extend the UK's current adequacy decision.

11) Data Protection Officer

The Bill proposes the removal of the legal obligation to appoint a Data Protection Officer.

Replaces for public bodies (the council) and those carrying out high risk processing the legal requirement for a Senior Responsible Individual (SRI)

SRI tasks or securing tasks are performed by another person:

- (a) monitoring compliance by the controller with the data protection legislation;
- (b) ensuring that the controller develops, implements, reviews and updates measures to ensure its compliance with the data protection legislation;
- (c) informing and advising the controller, any processor engaged by the controller and employees of the controller who carry out processing of personal data of their obligations under the data protection legislation;

- (d) organising training for employees of the controller who carry out processing of personal data;
- (e) dealing with complaints made to the controller in connection with the processing of personal data;
- (f) dealing with personal data breaches;
- (g) co-operating with the Commissioner on behalf of the controller;
- (h) acting as the contact point for the Commissioner on issues relating to processing of personal data.

The SRI must be part of the senior management team

("senior management", in relation to an organisation, means the individuals who play significant roles in the making of decisions about how the whole or a substantial part of its activities are to be managed or organised).

The SRI must delegate to someone else where there is a conflict of interest in performing one of their tasks above.

The SRI does not need expert knowledge themselves in data protection.

SRI is independent (but can delegate and must if conflict of interest) or given resources etc.

If the SRI delegates their tasks they must consider

- a) the other person's professional qualifications and knowledge of the data protection legislation,
- (b) the resources likely to be available to the other person to carry out the task, and
- (c) whether the other person is involved in day-to-day processing of personal data for the controller or processor and, if so, whether that affects the person's ability to perform the task.

12) Regulators

The Bill proposes to abolish the Information Commissioner's Office and replace with an Information Commission (with a chair and mainly same role and responsibilities)

Abolish Biometrics Commissioner and (some of) their functions transferred to the Investigatory Powers Commissioner.

Abolish Surveillance Camera Commissioner and Surveillance Camera Code of Practice for state (including the council) use of CCTV and ANPR.

13) Information sharing

The Bill proposes to extend powers to allow data sharing to deliver public services and businesses.

The extended powers are stated in the proposals to enable businesses to access government services and support more easily, giving them easier access to information, guidance, and business support services.

The proposals states this is to support appropriate data sharing across the wider health and adult social care sector, beyond the current crisis (with information standards)

14) Privacy and Electronic Communications Regulations

The Bill proposes to permit organisations which have charitable, political, or non-commercial objectives to send electronic marketing communications without consent where they have an existing supporter relationship with the recipient.

Also proposes to increase fines for infringement of PECR from a maximum of £500,000 to UK GDPR levels (up to 17.5 million or 4% of global turnover whichever the higher)

15) Cookies

The Bill proposes to allow cookies to be used without consent for the purposes of web analytics and to install automatic software updates.

16) Research

Proposes potential to use data already collected for research purposes without having to give new privacy notice if disproportionate effort.

17) Future reform

The Bill proposes the Secretary of State can amend the provisions through regulations, avoiding Parliament.