Data Protection and Digital Information Bill – CSA overview

Link: Data Protection and Digital Information Bill
Publication: 18 July 2022

Following its consultation on data protection reform, the government has now published the draft Data Protection and Digital Information Bill, the legislation intended to bring in the proposed reforms. The Bill is currently going through the Parliamentary process.

We have noted below some of the key areas of change and relevant proposals in the Bill. **Please note that these are subject to review or change as the Bill faces scrutiny in Parliament and could also be impacted by the outcome of the Conservative leadership campaign.**

Definition of personal data

- There is an effort to redefine *"personal data"* with a focus on what constitutes "*identifiable"*.
- The Bill aims to distinguish between *"direct identification"* (where no additional information is required for it to be identifiable) and *"indirect identification"* (where additional information is required for it to be identifiable).
- For it to be identifiable, data is required to be, or be likely to be, identifiable by a third party by reasonable means i.e. in the case of data that is indirectly identifiable, they would reasonably have access to the additional information required for identification. Where a third party does not reasonably have access to such information, it could be argued that the data is not identifiable in those circumstances.
- In relation to pseudonymisation, the Bill clarifies that any additional information that would be required for identification must be kept separate and be subject to security measures to prevent the data becoming directly identifiable.

Data Subject Access Requests (DSARs)

- The right to refuse *"manifestly unfounded or excessive requests"* becomes the right to refuse "*vexatious or excessive"* requests.
- The controller would be required to demonstrate that a request is vexatious or excessive.
- The Bill notes that relevant factors in determining the nature of a request include the repetitive nature of a request, the time elapsed since the last request, resources available to the controller and overlaps with other requests.
- Vexatious requests may include those that are an abuse of process or that are not made in good faith.
- In refusing a request, a controller would have to explain this to the data subject and offer referral to the ICO.
- Where identification is required in order to respond to a request, the Bill makes clear that it is permissible to delay the response until such identification is received.
- The Bill also notes that extending the response timeframe by up to 2 months can take account of the number of requests received by the firm – however, it is unclear whether this is based on the number of requests received by a particular individual, or whether it concerns the number of DSARs the firm has received overall.
- When determining whether it would be disproportionate to provide information, factors affecting this include the number of data subjects, the age of the data and applicable safeguards.

International transfers

- International data transfers to third countries will still require equivalent protection. Such transfers should be subject to the *"data protection test"*.
- The explanatory notes state that such a test would not require a point-by-point comparison between the two countries' regimes – the assessment would be based on outcomes. What is "*reasonable and proportionate"* is to be determined by reference to all circumstances, including the nature and volume of personal data.

Complaints

- Controllers would be required to have a complaints process and must acknowledge receipt of a complaint within 30 days of receipt.
- The ICO can refuse complaints if the complainant has not yet complained to the controller or if the controller is still dealing with the complaint and 45 days have not yet elapsed.
- The ICO can also refuse a complaint that it considers vexatious or excessive.

Accountability and Privacy Management Programmes (PMPs)

- Surprisingly, the Bill contains no provisions around a 'privacy management programme' scheme.
- However, the provisions associated with the original proposals – removing requirements for data protection officers, data protection impact assessments, and records of processing – are in the Bill.

Data Protection Officers (DPOs)

- Firms will no longer need to appoint a data protection officer. But firms carrying out processing likely to result in high-risk to individuals will have to appoint a "*senior responsible individual"*.
- For those firms in scope, the senior responsible individual will need to be part of the organisation's senior management, so this could mean that this is not the same person who is currently data protection officer, if they are not sufficiently senior.
- The senior responsible individual will have various tasks that they are responsible for performing or for ensuring are performed, including monitoring data protection compliance, organising training for employees, dealing with complaints and breaches, and liaison with the ICO.
- Controllers are required to support the senior responsible individual with appropriate resources.
- The Bill also removes article 27 of the UK GDPR, which requires controllers or processors outside the UK that are processing UK data subjects' personal data to designate a representative in the UK.

Data Protection Impact Assessments (DPIAs)

- DPIAs will now become Assessments of High-Risk Processing.
- At a minimum, such assessments should include a summary of the purposes of the processing, an assessment of the necessity of processing, an assessment of the associated risks and a description of any mitigation.

- Consultation with the ICO for certain high-risk processing assessments will no longer be mandatory and are now optional.

Record-keeping

- Firms will still be required to maintain an appropriate record of their processing, but not to the degree required under GDPR.
- The Bill requires firms to maintain a record of processing including at a minimum – where data is, the purposes of processing, any data sharing and recipients, details of retention, and whether there is any special category or criminal offence data.
- The record should ideally also document how the data is kept secure.
- For processors, they must have a record of the relevant name and contact information for the controller, where data is and relevant security measures, where possible.
- These records must be made available to the ICO upon request.

Legitimate interests

- The legislation would exempt some defined processing activities from the legitimate interests assessment, creating *"recognised legitimate interests"*.
- These will include processing in emergencies (as defined by the Civil Contingencies Act 2004); processing for detecting, investigating or preventing crime; and safeguarding a vulnerable individual.
- The Bill also identifies certain circumstances where processing will be treated as compatible with the original purpose, which includes crime prevention; protecting the vital interests of a data subject or another individual; safeguarding a vulnerable individual; where necessary for compliance with a legal obligation; and the collection of a tax or duty.

Automated decision-making

- The new section concerning automated decision-making is fairly similar to existing provisions.
- A "*significant automated decision"* is one which produces a legal or similarly-significant effect.
- Decisions that are solely automated and significant are only permissible where they meet one of the following conditions: the decision is based on explicit consent; It is a decision necessary for entering into, or performing, a contract between the data subject and controller; it is required or authorised by law; or it meets a substantial public interest condition.
- Significant decisions must be subject to certain safeguards. These include a requirement that the data subject is given information about the decision, they must be enabled to make representations about such decisions and be able to obtain human intervention from the controller, and they must be contestable by the data subject.

Information Commissioner's Office

- The role of the Information Commissioner would be abolished and the functions transferred to the "Information Commission".
- The ICO would now have objectives to secure appropriate level of protection and promote trust and confidence in processing.
- The ICO would be required to prepare a strategy for achieving its objectives and functions.
- The ICO will have some new enforcement powers, including the power to require a report, which sounds similar to the FCA's section 166 request powers.

Research

- Processing for purposes of scientific research would be broadened to cover *"processing for the purpose of any research that can reasonably be described as scientific, whether publicly or privately funded, including processing for the purpose of technological development or demonstration, fundamental research or applied research."*

Cookies

- The circumstances in which cookies can be used / placed without express consent is extended beyond only those that are 'strictly necessary'.
- The Bill would make it permissible for those being used for web analytics (provided that they are not shared with any other person except for the purpose of enabling that person to assist with making improvements to the service or website) and for installing automatic security updates.

Privacy of Electronic Communications Regulations (PECR) enforcement

- The fines for breaches of PECR will be brought in line with breaches of data protection law.