Browne Jacobson

Data reform in the UK

Since the UK left the EU and are now able to move away from the EU data protection regime, the UK government have implemented a national data strategy with the aim of reducing the burden on organisations but maintaining a high data protection standard.

27 September 2022

Since the UK left the EU and are now able to move away from the EU data protection regime, the UK government have implemented a national data strategy with the aim of reducing the burden on organisations but maintaining a high data protection standard. The Government published a consultation in September last year asking for responses to their proposed changes to the current UK data protection regime (the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA) and Privacy and Electronic Communications Regulations (PECR)), the outcome of which was published earlier this year. On 18 July 2022, the Data Protection and Digital Information Bill had its first reading in the House of Commons.

We consider some of the key proposed changes to the current UK data protection regime and recommend steps to take now to ensure compliance going forward below:

Privacy management programme framework

The government is proposing to remove key accountability requirements such as the requirement for an organisation to have a Data Protection Officer (DPO), to undertake Data Protection Impact Assessments and to maintain a Records of Processing Activities (RoPA) and replace it with a requirement for organisations to implement a more flexible and risk-based “privacy management programme” based on the level of processing activities and the volume and sensitivity of personal data they handle. Organisations will still be required to appoint a senior person to be responsible for data protection, however they will not be subject to the statutory obligations DPOs currently are. Organisations will be given more freedom to implement risk assessment tools and take a more flexible approach to record keeping.

For now, we recommend organisations look at the Information Commissioner’s Office’s (ICO) current accountability framework to determine their current compliance level. If an organisation is reasonably compliant under the current framework, it is most likely to be compliant under the new regime going forward.

Cookies and cookie consent

The government is proposing to remove the cookie consent requirements from Regulation 6 of PECR in respect of certain less privacy intrusive cookies, including analytics (the Bill refers to use of cookies ‘for statistical purposes’ to improve a service or website), and some functional cookies. The effect of the proposed changes is that those cookies would be treated in a similar way that ‘strictly necessary’ cookies are treated under the current regime. There are still restrictions on the use of those cookies in that the data must not be shared with any other party (e.g. Google) and that website users should be able to object to the use of their data. The proposed changes however will not impact on the consent requirements for more privacy intrusive cookies such as those which collect personal data for the purposes of real-time bidding and targeting advertisements/marketing, which will remain in place.

For now, we recommend organisations map the cookies used on their websites and make sure they have a good awareness of any privacy intrusive cookies used (such as those which track users across multiple websites, targeted advertising cookies and those used to build a profile about an individual), as they are likely to continue to need to get consent to drop those cookies going forward under the new regime.

Subject access requests (SARs)

SARs are often used by disgruntled individuals as a weapon against organisations, causing them to use lots of precious time and money in order to comply with the request for personal data. Under the current regime, an organisation can only refuse to comply with a SAR where the request can be deemed to be manifestly unfounded and/or excessive. The government propose to change this wording to bring it in line with the Freedom of Information Act wording i.e., where a request is vexatious and/or excessive. It is not clear as of yet what the practical impact of this change will be, however it is hoped that this will allow organisations to take a more practical approach when responding to SARs and refuse to respond when dealing with a vexatious individual where it would be disproportionate to do so.

For now, we recommend that organisations concentrate on making sure they have appropriate retention and deletion practices in place, to ensure there is only minimal data to deal with when complying with a SAR.

This is of course just a draft bill and may change as it goes through various stages in Parliament.

Contact

Ella Greenwood

Associate

ella.greenwood@brownejacobson.com

+44 (0)330 045 2469

Related expertise

Services

Data protection and higher education

Data protection and information sharing in academy schools and trusts

Data protection and privacy

Data protection for retail

Digital and data

Information law