ROPES & GRAY

ALERT

London

August 23, 2017

UK Government Sets Forth Approach for GDPR

Attorneys
Rohan Massey
Clare Sellars

With its "Statement of Intent" published on 7 August 2017, the UK Government has taken the first step in the process of cementing the General Data Protection Regulation into UK law. In the statement, entitled "A New Data Protection Bill: Our Planned Reforms" (the "Bill"), the Government commits to updating and strengthening data protection laws through the new Bill in order to fulfil its vision of the UK being "*the best and safest place to live and do business online*". The statement explains that the Government is determined to ensure that the GDPR best supports UK interests and sets out the necessary changes that the Bill will make to the GDPR to this end. Inevitably, it recognises that the proposed Data Protection Bill must be consistent with the GDPR to ensure that safe and uninterrupted data flows continue between the UK, the EU and other key markets such as the US. Some of the main points arising from the statement are considered below, including how the Government intends to invoke any derogations permitted by the GDPR to allow "*a simpler shift for both businesses and consumers*".

Personal data – Reflecting the growth in technology, the definition of personal data will be expanded to include IP addresses, internet cookies and DNA.

Consent to profiling – The rules around consent are strengthened and subject to additional conditions, such as being "unambiguous" and easy to withdraw. Consent must also be "explicit" when processing sensitive personal data. Reliance on default opt-outs or preselected "tick boxes" will become a thing of the past. The GDPR provides that parents or guardians must give consent to personal data processing on behalf of young children using information services. It allows the UK to set the minimum age at which a child can consent to data processing to any age between 13 years and 16 years. As expected, the Data Protection Bill will legislate to allow a child aged 13 years or older to consent to his or her personal data being processed.

Improved data access – Individuals will find it easier to require an organisation to disclose the personal data it holds about them at no charge. The statement says that data controllers will provide better information on how to access information and empower people to take ownership. The Bill will also create a new offence of altering records with intent to prevent disclosure following a subject access request.

Data portability – New rules will make it easier for customers to move data between service providers. The statement explains, for example, that where an individual changes internet service providers, if he or she is using email or file storage services to store personal photographs or other personal data, he/she should be able to move that data.

Right to be forgotten – Subject to certain exceptions, individuals will be able to ask for their personal data to be erased in certain circumstances. This will include provision to allow people to require social media platforms to delete information they posted during their childhood. In certain circumstances, individuals will have the ability to ask social media companies to delete any or all of their posts. For example, a post on social media made as a child would normally be deleted upon request, subject to very narrow exemptions.

Profiling and automated processing – Individuals will have greater say in decisions that are made about them based on automated processing. Where decisions are based on solely automated processing, individuals can request that processing be reviewed by a person rather than a machine. The GDPR allows exemptions where suitable measures are put in place to safeguard the individual's rights. In this respect, the statement says that there are also legitimate functions which are dependent on automated decision-making. For example, a bank, before agreeing to provide a

loan, would be entitled to check the creditworthiness of an applicant. In this context, an automated credit reference check would be an appropriate means of achieving this outcome. In light of this, the Government says that it will legislate to implement this exemption with a view to ensuring legitimate grounds for processing personal data by automated means.

Enforcement – The ICO will continue to have the ability to request information from data controllers and processors, enter and inspect premises, carry out audits and require remedial action. The maximum fine for serious data protection breaches is increased from £500,000 to €20m or, in the case of undertakings, 4% of global turnover, whichever is the greater. The statement adds that offences will be modernised to ensure that prosecutions continue to be effective, and new offences will be introduced to deal with emerging threats. In particular, the Bill will create a new offence of intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data. Offenders who knowingly handle or process such data will also be guilty of an offence, and the maximum penalty would be an unlimited fine.

Processing criminal conviction and offence data – The GDPR only permits bodies vested with official authority to process personal data on criminal convictions and offences. However, the GDPR does allow the UK to legislate to permit other bodies to process this category of personal data. For example, UK legislation could permit a private or third sector employer to obtain details of criminal convictions in order to carry out a criminal records check. To preserve continuity, the statement of intent says the Government will legislate to extend the right to process personal data on criminal convictions and offences so as to enable organisations other than those vested with official authority to process criminal convictions and offences data.

Freedom of expression in the media – The GDPR provides for exemptions to certain areas of data protection to allow for journalistic activity in the public interest. Currently, under s 32 of the Data Protection Act, exemptions exist for personal data which are processed for special purposes if the processing is undertaken with a view to publication, that publication is in the public interest, and compliance with the data protection principles is incompatible with the special purposes. The Government believes that the existing exemptions set out in s 32 "*strike the right balance between freedom of expression of the media and the right to privacy for individuals*". It therefore intends broadly to replicate s 32. The main difference will be to amend provisions relating to the ICO's enforcement powers to strengthen the ICO's ability to enforce the re-enacted s 32 exemptions effectively.

Comment

No surprises here – the Bill will be consistent with the GDPR. This is good news for any organisation planning its UK and EU compliance strategy in preparation for May next year. The derogations set out in the Bill are by definition only such as permitted by the GDPR and the Bill will use them largely to minimise disruption to existing practices which have worked well, for example legitimate processing of offence data and legitimate processing by automated means. The Bill, once enacted, should pave the way for GDPR compliance in the UK and itself become the corner stone for an adequacy finding if Brexit moves the UK out of the EU.