Brexit and Data Protection: The UK Government's New Data Protection Bill

OCTOBER 11, 2017

The UK government has taken an additional step in its attempts to find a way to ensure uninterrupted data flows between the UK and the EU after Brexit. On 13 September 2017, the UK government introduced a draft Data Protection Bill (the Bill, text available here) to the UK Parliament, accompanied by explanatory notes (text available here). The UK Information Commissioner's Office (ICO) welcomed the Bill and published its comments on 9 October 2017 (text available here). The UK Parliament started debating the Bill on 10 October 2017 (recordings of the debate are available here). The Bill is designed to enter into force on 25 May 2018, i.e., when the new EU General Data Protection Regulation (GDPR, text available here) becomes effective. The Bill is a very complex piece of legislation because of its structure, which includes 18 schedules and a substantial number of cross-references to the GDPR. The progress of the legislative process can be monitored here. Here is what we think you should know at this stage.

What Is the UK's Strategy?

The UK will remain an EU Member State where EU law applies until it effectively leaves the EU. Brexit is currently expected to happen on 30 March 2019. Although Brexit could happen before or after this date, the GDPR will apply in the UK before Brexit. Therefore, until the UK leaves the EU, the GDPR will operate in tandem with the Bill. After Brexit, the GDPR will be incorporated into the UK's domestic law under the EU (Withdrawal) Bill, currently before the UK Parliament (Art. 3 of the EU (Withdrawal) Bill, text available here).

As anticipated in our previous alert on Brexit and data protection (text available here), the UK's strategy is to ensure that its data protection law framework is aligned with the GDPR at the date of withdrawal (see the UK government's paper on the exchange and protection of personal data between the UK and the European Economic Area, dated 24 August 2017, text available here). Because the GDPR allows transfers of personal data only to non-EU Member States that ensure an "adequate level of protection" of such data, the UK, by aligning with the GDPR, is working toward ensuring uninterrupted data flows between the EU and the UK. This would still require that the European Commission grant the UK an "adequacy decision" to recognize the adequacy of the UK

framework and to allow transfers from the EU to the UK.

What Are the Scope and Structure of the Bill?

The Bill consists of seven parts and has a much broader scope than the GDPR as it also applies to UK law enforcement authorities and intelligence services. We focus on parts 2 to 4 and part 6, as parts 1 and 7 are less relevant and part 5 grants the ICO the powers that the GDPR grants to Supervisory Authorities. The Bill also includes 18 schedules.

Part 2 of the Bill: Implementing the GDPR Into UK Law

Part 2 of the Bill has two objectives: On the one hand, regarding processing of personal data that is subject to the GDPR, it supplements the legal framework for such processing. On the other hand, it addresses processing that is not subject to the GDPR, by adopting provisions that mirror those of the GDPR.

The UK took the opportunity to further specify certain provisions of the GDPR to model the Bill's flexibilities and derogations to the GDPR on its existing data protection law (the Data Protection Act 1998). The UK government had published a table setting out the flexibilities and derogations in the Bill, the article of the GDPR to which it corresponds, and the UK's reasons for choosing to deviate from the GDPR's default position (available here). These derogations are now part of the Bill, and possible under the GDPR. The most relevant are the following:

- ***Conditions Applicable to a Child's Consent***. The UK decided to set the age at which a child can consent to the processing of data at 13 years old while, by default, the GDPR requires consent of the holder of parental responsibility over the child for children under 16 (Art. 8(a) of the Bill; Art. 8(1) GDPR). The ICO favours an approach whereby even quite young children can access appropriate online services without the consent of a parent or guardian, provided companies have other safeguards.
- ***Processing of Special Categories of Personal Data***. The GDPR prohibits the processing of sensitive data (e.g., personal data concerning health, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership), save exceptions (Art. 9(1) and 9(2) GDPR). The Bill relies on these exceptions to allow such processing for scientific research purposes and to allow employers to fulfill obligations of employment law, all in the absence of the individual's consent (Art. 9 and Schedule 1 of the Bill). The Bill specifies, however, that employers will need to have a "policy document" setting out their procedures for securing compliance with the data protection principles and their retention and erasure policies (Schedule 1, part 1 of the Bill).
- ***Processing of Personal Data Relating to Criminal Convictions and Offences***. The Bill relies on Art. 10 of the GDPR to allow the processing of such personal data by organizations that are not official authorities. For example, employers can process criminal convictions data as part of their pre-employment checks, and insurers can process criminal convictions data for anti-fraud purposes (Art. 10(2), Schedule 1 of the Bill). Again, a policy document is required.
- ***Automated Individual Decision Making***. The Bill allows decisions based solely on

automated processing subject to certain safeguards, including notification to the individual concerned and the right of this individual to request the data controller to reconsider its decision (Art. 13 of the Bill; Art. 22(2)(b) GDPR). This differs from the GDPR's right for data subjects to opt-out of automated decision making (Art. 22(1) GDPR).

- ***Processing for Journalistic, Academic, Artistic, Literacy, Research and Statistical Purposes***. The Bill also includes exemptions for processing personal data for such purposes (Schedule 2, parts 5 and 6 of the Bill).
- ***National Security and Defence Exemption***. The Bill restricts the application of some provisions, including those concerning individuals' rights, for national security and defence purposes subject to specific safeguards (Art. 24 of the Bill). Under current UK data protection law, this exemption is confined to national security. The ICO said it will follow the debate on this clause to be reassured that the aim is not to grant a blanket exception for everything the Ministry of Defence does.

In addition, the Bill clarifies some concepts that the GDPR refers to but does not define. For example, the Bill provides that, where the GDPR allows the processing of personal data because it is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller, this includes processing of personal data that is necessary for the administration of justice, the exercise of a function of Parliament, the exercise of a function conferred on a person by an enactment, or the exercise of a function of the Crown, a Minister of the Crown or a government department (Art. 7 of the Bill; Art. 6(1)(e) GDPR).

Part 3 of the Bill: Implementing the Law Enforcement Directive Into UK Law

The EU Directive on the processing of personal data by government authorities for the purposes of the prevention, investigation, detection, and prosecution of crime (Directive 2016/680, the Law Enforcement Directive) applies to the cross-border processing of personal data for law enforcement purposes. This directive entered into force on May 5, 2016, and EU Member States, including the UK, have until May 6, 2018, to transpose it into national law.

The Bill applies to both cross-border and domestic processing of personal data for law enforcement purposes. It implements the data protection principles and individuals' rights laid out in the Law Enforcement Directive. The Bill places restrictions on individuals' rights, but only where this is necessary and proportionate to protect specific purposes, including public and national security. The Bill also restricts individuals' access right in relation to documents concerning criminal investigations or prosecution proceedings that are created by or on behalf of a court or other judicial authority (Art. 41 of the Bill). Although individuals can access such information based on other UK laws, the ICO pointed out that this restriction also applies to other individuals' rights, such as the right to rectify inaccurate data.

Part 4 of the Bill: UK Intelligence Services' Processing Activities

National security is outside the scope of EU law, so neither the GDPR nor the Law Enforcement Directive would apply to intelligence services' processing activities. Part 4 of the Bill provides a specific procedure for such processing activities, based on the Council of Europe's Convention 108

(text available here).

Most of the data protection principles and individuals' rights do not apply where such processing activities are necessary to safeguard national security (Art. 108 of the Bill). A minister can certify that an exemption from a specified requirement is necessary in this respect. Such a certificate is to be taken as conclusive evidence of the exemption being required. Individuals who are directly affected by such a certificate can appeal to a tribunal to review the certificate or, where the certificate identifies data by means of a general description, challenge the application of the certificate to specific data.

According to the ICO, there may be concerns that national security exemptions will be widely used and that much of the work of the intelligence services will be taken outside of the Bill safeguards. The ICO insisted that it is important to ensure transparency, to the extent that this is possible. The ICO suggested that any minister issuing certificates could be required to publish information about the issuing of such certificates.

Although national security exemptions already exist under current UK data protection law, they will be of major importance in the context of an adequacy decision analysis post-Brexit. This is because the Court of Justice of the EU made it clear in its October 2015 *Schrems* judgment that a country could not benefit from an adequacy decision where, in this country, the powers of intelligence services go beyond what is necessary and proportionate (the text of the judgment is available here). With this in mind, European Data Protection Authorities might raise criticism of the UK intelligence services' powers. For example, Jan Philipp Albrecht, the European Parliament rapporteur of the GDPR, indicated via his official Twitter account that he doubted whether the UK could obtain adequacy as there would be "less safeguards for intelligence services [in the UK] than in the [United States]."

Part 6 of the Bill: Sanctions and Enforcement

The Bill creates two new offences that do not exist in the GDPR: knowingly or recklessly re-identifying information that is "de-identified" personal data, without the consent of the data controller responsible for de-identifying the data (Art. 162 of the Bill), and altering personal data to prevent disclosure to a data subject requesting access to its data (Art. 163 of the Bill).

Like the GDPR, the Bill enables the ICO to impose fines of up to €20,000,000 or 4% of the company's annual worldwide revenue, whichever is higher. In this context, it is worth noting that Elizabeth Denham, the UK information commissioner, recently made it clear that the ICO does not plan to make early examples of organizations for minor infringements and that maximum fines will not become the norm. She added that predictions of massive fines under the GDPR that simply scale up penalties issued so far, in her view, "are nonsense." The ICO commissioner also stated that the ICO will instead focus on guiding and educating organizations about how to comply. She indicated the ICO will use its powers proportionately and judiciously and will use the other sanctions it can impose, such as warnings, reprimands and corrective orders, where they will be more appropriate.

This alert has been prepared by Frédéric Louis, Martin Braun and Itsiq Benizri of WilmerHale,

Brussels/Frankfurt.

Authors

Frédéric Louis

PARTNER

frederic.louis@wilmerhale.com

+32 2 285 49 53

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207

Itsiq Benizri

COUNSEL

itsiq.benizri@wilmerhale.com

+32 2 285 49 87