How will Leaving the EU Affect **UK Data Privacy**

By Pulina Whitaker, Partner, Morgan Lewis & Bockius

The UK's data protection laws are derived from EU legislation, such as the Data Protection Act 1998 ("DPA") and the Privacy and Electronic Communications Regulations which implement European Directives. The new General Data Protection Regulation ("GDPR"), which will replace the DPA, will be in force on 25 May 2018. The GDPR will be effective in the UK immediately on this date, without any further UK laws being required. As it is unlikely that the UK will have left the European Union by that time, the Government will need to enact domestic data privacy legislation to replace the GDPR when the UK exits the EU. The UK's data protection authority, the Information Commissioner's Office, has already advised the Government that UK data protection standards will need to be equivalent to those in the GDPR if the UK wishes to trade with the European single market post-Brexit.

Pulina Whitaker, Partner, Morgan Lewis & Bockius.

Territorial scope of the GDPR

The GDPR has extra-territorial effect, in contrast to the current Data Protection Directive. The GDPR applies to:

- processing activities by data controllers and data processors established in the EU, whether or not the processing takes place in the EU;
- the processing of personal data of data subjects who are in the EU by a data controller or data processor not established in the EU where the processing activities relate to offering goods or services to data subjects in the EU; and
- the processing of personal data of data subjects who are in the EU by a data controller or data processor not established in the EU where the processing activities relate monitoring their behaviour in the EU.

The extra-territorial scope of the GDPR represents a significant expansion of EU data protection obligations to cover all processing activities relating to EU-based data subjects.

Most UK businesses are almost certainly going to need to transfer personal data to Europe and also to other countries outside the EU such as the US. Currently, whilst the UK remains part of the EU, there are restrictions against transferring personal data outside the EU, without consent from the individual, other than to certain "adequate" countries such as Canada or Switzerland or unless the business has in place a legally permissible mechanism, such as model clauses or binding corporate rules.

GDPR and the UK Post Brexit

When the UK exits from the EU, within two years from 29 March 2017 when the Government has said it will start the exit process, the GDPR will only continue to apply to a UK organisation to the extent that it falls within the extra-territorial scope summarised above. For purely UK processing activities relating to UK individuals, the GDPR will no longer apply although the UK is highly likely to have a broadly equivalent replacement data protection law at that stage for domestic processing activities. Therefore, the Government will need to pass UK data privacy legislation in place of the GDPR for UK data processing and, perhaps, also processing of personal data of UK citizens by non-UK based organisations. The scope and stringency of this new legislation will be critical to whether the UK is still deemed to have "adequate" data privacy standards when it leaves the EU. This is, of course, relevant to whether or not data transfers to the UK from the remaining EU states are restricted or whether they are permissible without further obligations needed by those EU-based data exporters.

Processing of personal data under the GDPR

Where the GDPR applies to the processing of personal data, UK companies should conduct an initial assessment as to whether it (or its affiliates) are acting as a data controller or a data processor in these processing activities. Different obligations will apply depending on the UK organisation's role.

The data controller is ultimately responsible for compliance with the data protection principles which are that personal data must be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Personal data is lawfully processed if the data subject has consented to the processing or a permitted derogation applies such as legal or contractual necessity. Further, there are strict conditions imposed on whether consent is validly obtained by the data controller.

The data controller must provide a privacy notice to data subjects regarding the processing of their personal data. The information contained in the privacy notice is summarised below and must be provided at the time of the collection of the personal data or, if it was collected via a third party, within a reasonable period of being collected. The privacy notice must specify certain information and ensuring that privacy notices are compliant with the GDPR is likely to be a complex process for many organisations. The privacy notice must be concise, transparent, intelligible and easily accessible, written in clear and plain language and provided free of charge.

There are also direct obligations on data processors under the GDPR (unlike the current DPA) regarding:

- the security of processing operations;
- appointment of a Data Protection Officer;
- the engagement of sub-processors; and
- the notification of any breach of data protection obligations (including data security incidents) to the data controller.

Data breaches

The DPA does not have a mandatory data breach reporting obligation. The GDPR, however, does include a mandatory obligation to notify the data protection authority within 72 hours of becoming aware of the breach and without undue delay and, in certain circumstances, the individuals affected by the breach. The Government will, therefore, need to decide if it will include a data breach notification obligation in the new data privacy legislation, either similar to the stringent GDPR requirement or an alternative obligation, perhaps with a longer notification period and which is triggered for significant data breaches only, which may be more pragmatic and more suited to the UK's approach of business-friendly legal requirements.

Recommended steps to comply with the GDPR

Organisations can consider taking steps to prepare for the GDPR such as the following:

1. conduct an assessment of what personal data is processed or otherwise stored or held by the organisation and/or its affiliates, where it is held, the categories of data subjects (e.g. employees, contractors, contact points at commercial organisations, customers etc), the nature of the personal data (including if it is sensitive personal data), for how long is it being retained, whether it is current or historical, how it was obtained (so far as possible), how it is used and with whom it is shared and where the locations are of the recipients of the personal data (i.e. identify the data flows);
2. review the consents (or other applicable lawful processing derogations) obtained for the processing of the personal data and any privacy notices, policies or other information provided to data subjects for this processing and update the notices or policies as necessary under the GDPR;
3. identify any international data flows and any applicable data transfer agreements (including model clauses approved by the European Commission) or pursuant to the Privacy Shield and ensure that all international data flows are conducted on a lawful basis;
4. review and update as necessary any procedures for responding to data subjects accessing personal data or exercising any other rights such as rectification or blocking of personal data;
5. review data security processes and review and update any (or prepare a) data security incident response plan;
6. consider if the organisation (or one of its EU affiliates) needs to appoint a Data Protection Officer (this is required where there is regular and/or systematic monitoring of individuals or processing on a large-scale of sensitive personal data or criminal conviction data); from our understanding, this may not be required but we can discuss in more detail with you if needed;
7. review and, as necessary, amend processing provisions with data processors; and
8. conduct a privacy impact assessment (ideally on a legally privileged basis) to determine any risk areas for the group including in relation to data security.

Opinion

Although the UK was one of the dissenting voices in negotiations about the GDPR and was particularly vocal about the onerous impact on UK businesses, it seems unlikely that the UK will reduce the extent of data protection obligations on UK businesses. To do so will necessarily reduce the current level of data privacy protections afforded to individuals. The UK is unlikely to want to be seen as being out-of-step with the rest of Europe which will, to a large extent, remain a significant trading partner.

The Government will need to decide if it will retain the same restrictions for cross-border transfers or adopt an alternative solution. The EU-US Privacy Shield will no longer apply to the UK post-Brexit and neither with the protections afforded to EU citizens under the Umbrella Agreement or the Judicial Redress Act to enforce privacy breaches in the US courts. The UK will need to decide if it will adopt a similar model to the Privacy Shield for data transfers from the UK to the US if the current restriction on such data transfers is retained.

Additionally, the UK is likely to apply to the European Commission for a decision of "adequacy" allowing European countries to transfer personal data to the UK without restrictions. Obtaining an "adequacy" decision, of course, depends on whether the Government has passed laws which are materially similar to the GDPR.