ADDLESHAW GODDARD

BREXIT AND DATA PROTECTION

Q & A

What happens now?

The UK decision to leave the EU will not affect existing data protection and privacy laws in the UK. These laws (the UK Data Protection Act 1998 (**DPA**) and the Privacy and Electronic Communications Regulations 2003 (**PECR**)) protect people's personal data as well as ensuring that organisations have clear rules and a legal basis when collecting and using such data.

The DPA is the primary source of data protection legislation in the UK. It implements the Data Protection Directive (Directive 95/46/EC) and addresses such items as the definitions of personal data, sensitive personal data, the processing of data, notification and registration requirements, consent, rights of data subjects, collection of data, direct marketing, data transfers and sanctions for non-compliance. This will be the case until the DPA is amended or repealed by Parliament and all UK businesses should continue to comply with the DPA. Previous judgements of both the English and the European courts will continue to be binding in relation to the interpretation of the DPA, at least until the UK leaves the EU (at which point the status of EU jurisprudence will have to be considered).

On May 4th 2016, the EU approved an update to the existing 1995 Data Protection Directive (the EU law from which the UK Act is derived) with what is known as the General Data Protection Regulation (**GDPR**). This new law, due to directly apply across the EU from 25 May 2018, strengthens user control over personal information as well as streamlining the rules, aiming to make it easier to do business across EU markets. It contains new rights and obligations for data subjects and data processors and includes tough new sanctions and fines.

Effect of the EU Referendum vote on the GDPR

The territorial application of the GDPR means that organisations collecting and using personal information from citizens in the EU will need to comply with it regardless of where they are located. The EU Referendum result to leave the EU will not affect this.

The ICO has confirmed that in order for data to be transferred between the UK and the EU, the GDPR will have to be adopted into UK law:

> *"If the UK wants to trade with the single market on equal terms we would have to prove 'adequacy' - in other words, UK data protection standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018. With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations and to consumers and citizens."*

The UK Government will need to decide which EU Directives and Regulations it will choose to adopt or keep as part of UK legislation (including the GDPR). It is possible that the work on this list will not start until later this year when negotiations with the EU to trigger the UK's exit under Article 50 of the Lisbon Treaty are expected to commence. As the GDPR is a regulation rather than a directive, the UK would need to amend current UK legislation for the GDPR to remain in force after the UK exits the EU. Most political commentators suggest the earliest exit date to be January 2019, although it may well be later. This means that the GDPR will apply in the UK from 25th May 2018 until the final exit date unless new legislation is passed in the UK.

Many companies will, therefore, be required to comply with the provisions of the GDPR in order to continue trading in the EU. This, coupled with the ICO's belief, made clear in its statement, that the DPA requires reform, may lead the UK Government to take the simplest path and simply transpose the GDPR into UK law. It may also be a condition of the UK's continued participation in the single market that this regulation, amongst others is fully adopted.

What about the 'cookie law'?

An update to PECR (known as the 'cookie law') in 2011 implemented the revised EU ePrivacy Directive into UK law. This remains in place. Article 5.3 of the Directive replaced the 'notice and opt out' regime for the likes of cookies and other technologies with one based upon consent for, "*the storing of information or the gaining of access to information stored in the terminal equipment of a subscriber or user… having been provided with clear and comprehensive information*".

This law is currently under review by the European Commission (**Commission**) to ensure it is aligned with the GDPR (a public consultation on its revision ends in early July 2016). A new version may arise over the next year or so but it is unlikely that the UK will apply it. Again, it remains to be seen what happens in the UK but the ICO (as well as organisations and citizens) will want to ensure UK law is in line with other EU countries and that there is a balanced and pragmatic approach. Arguably this is now the most important data privacy policy issue to watch.

What about transfers of personal data to other countries?

The DPA (and its counterparts in other European Member States) prohibits transfers of personal data to countries outside the European Economic Area (**EEA**), unless they have been recognised by the European Commission as providing an "adequate form of protection" for personal data.

It is unclear whether the UK would become a member of the EEA if it left the EU. If it decides to choose to sit outside the EEA, it would no longer be an automatically "safe" destination for EU personal data. It would have to be approved as providing adequate protection for personal data by the Commission. Until that happened, companies operating in the EU would need to revise the methods they use to transfer data to the UK (such as implementing Model Clauses or Binding Corporate Rules). This could pose serious issues for the large number of businesses which currently process personal data of EU citizens in the UK. These approved mechanisms for lawfully transferring data add an additional administrative layer and vary between jurisdictions. In some Member States, such as Spain, organisations would also have to obtain prior authorisation from the local supervisory authority before making any such transfer.

Whilst one might reasonably expect that the UK would be approved as providing an adequate level of protection given that the DPA 1998 is based on the Directive, it is not certain. The Commission has reportedly written to the UK Government in the past criticising it for not implementing the Directive fully and international data transfers are a politically sensitive issue within the EU in the post-Snowden/ Safe Harbour era. It is possible that the activities of GCHQ and other security services in the UK might lead the EU Commission to require additional safeguards to protect the rights of UK citizens against intrusive and mass surveillance to be implemented before an "adequacy" ruling would be given.

What about the Privacy Shield?

The EU-US Privacy Shield replaces the EU-US Safe Harbour scheme, which was ruled invalid in October 2015 by the Court of Justice of the European Union. On 24th June 2016, agreement was reached between the US and the EU to improve the new Privacy Shield following criticism from MEPs, the European Data Protection Supervisor, and the Article 29 Working Party. The main concern was the need to provide, "*adequate protection against indiscriminate surveillance" and "obligations on oversight, transparency, redress and data protection rights*".

The Privacy Shield's main protections include:

- The US will create an ombudsman to handle complaints from EU citizens about the Americans spying on their data;
- The US Office of the Director of National Intelligence will give written commitments that Europeans' personal data will not be subject to mass surveillance; and
- The EU and US will conduct an annual review to check the new system is working properly

Some of the additional changes agreed on 24th June include:

- A written commitment from the White House, stating that bulk collection of data sent from the EU to the US can only occur under specific preconditions and must be "as targeted and focused" as possible;
- More explicit data retention rules: companies now have to delete data that no longer serves the purpose for which it was collected; and
- A specification that the ombudsman will be independent from national security services.

A spokesman for the European Commission said, "*This new framework for transatlantic data flows protects the fundamental rights of Europeans and ensures legal certainty for businesses*."

The EU is hoping for the Privacy Shield to be operational from July of this year.

Whatever happens, eventually the UK will probably need to have its own 'adequacy' arrangements for data transfers to the US and other countries and this will no doubt shine a light on its own security surveillance operations, particularly with current proposals to extend the UK's 'investigatory powers'. It may be the case that the UK will require its own Privacy Shield even if it adopts the GDPR.

Conclusion

As far as data protection is concerned, the UK's decision to leave the EU should not be seen as an immediate cause for panic. Current laws continue to apply and depending on the exact route chosen for "Brexit", existing and forthcoming directives and regulations such as the GDPR may apply too. Our advice to clients who are preparing or commencing their GDPR compliance programs is that they should continue with the same pace as before. Steps such as carrying out a data audit, creating a data flow map showing where data is and who accesses it, and ensuring appropriate contractual provisions are in place with data processors are all good practice initiatives which will reduce risk and ensure compliance with existing laws.

For further information or for a copy of our "Timeline for GDPR compliance to May 2018", please contact Toni Vitale, Legal Director on 020 7160 3158 or toni.vitale@addleshawgoddard.com.

addleshawgoddard.com

Doha, Dubai, Hong Kong, Leeds, London, Manchester, Muscat, Singapore and Tokyo*

*a formal alliance with Hashidate Law Office