GDPR Update – Brexit Implications 2
April 2019

This update keeps you up to date with the latest government and ICO guidance on the implications of Brexit for data protection and market research. It builds on and replaces the February 2019 bulletin.

At present if a Brexit deal is agreed the UK will exit the EU on 31 October 2019. However, under EU rules, the UK will have to hold European Parliament elections in May, or face leaving the EU without a deal on 1 June 2019. UK data protection standards will remain the same after exit (either on 1 June or 31 October) because the UK's Data Protection Act 2018 and the EU's Withdrawal Act 2018 incorporate the GDPR into UK law. However if there is no Brexit agreement this will impact inter-country data protection issues. This update highlights key aspects of this impact.

Updated Government guidance[1] issued in December 2018 states that regulations will come into force before the UK leaves the EU to make sure that the UK data protection framework continues to operate effectively.

"These regulations would:

- *Preserve EU GDPR standards in domestic law*
- *Transitionally recognise all EEA countries (including EU Member States) and Gibraltar as 'adequate' to allow data flows from the UK to Europe to continue*
- *Preserve the effect of existing EU adequacy decisions on a transitional basis*
- *Recognise EU Standard Contractual Clauses (SCCs) in UK law and give the ICO the power to issue new clauses*
- *Recognise Binding Corporate Rules (BCRs) authorised before Exit day*
- *Maintain the extraterritorial scope of the UK data protection framework*
- *Oblige non-UK controllers who are subject to the UK data protection framework to appoint representatives in the UK if they are processing UK data on a large scale"*

Brexit - Transfers of personal data

The UK Government's hope is to secure a data protection 'adequacy' decision within the withdrawal treaty; this will allow the UK to maintain a free flow of data between the UK and the EU, as we have at the moment. However in the event of no deal, the UK would be a 'third country' when it comes to data protection. This means that some unhindered cross-border transfers of data cannot take place automatically between the UK and the EU.

The Government recently issued extended guidance[1] on the transfers of personal data between the UK and the EU if there is no agreement. Key details are summarised below.

From UK to EU

The guidance states that even if there is 'no deal' personal data can be transferred from the UK to the EU because the UK's DPA 2018 and the EU's Withdrawal Act 2018 incorporate the GDPR into UK law. The Government has stated:

> *"In recognition of the unprecedented degree of alignment between the UK and EU's data protection regimes, the UK would at the point of exit continue to allow the free flow of personal data from the UK to the EU."*

So no changes are expected in this situation. The ICO and the Department of Digital, Culture, Media and Sports have recently reiterated this[2]:

> *"Personal data can continue to flow freely from the UK to EEA countries"*

From EU to UK

If the UK's data protection standards are deemed equivalent to the EU's and an adequacy decision is made, there will be no changes to current practices. However the UK Government has warned that the European Commission (EC) has indicated that an adequacy decision[3] cannot be taken *until* the UK is a third country. This means that there would be a gap between exiting the EU and an adequacy finding. The EC's procedure for reaching an adequacy decision generally takes several months.

The Government's guidance suggests that organisations identify an alternative legal basis for their transfers from the EU to the UK. It suggests that EU standard contractual clauses are likely to be the most appropriate alternative; these approved clauses enable the free flow of data when included in a contract or added as an appendix to a contract. They cover the contractual obligations between both parties to protect the rights of the individuals whose data is being transferred.

There are three standard contractual clauses available from the EC, these remain valid until replaced or amended by the EC:

- 2001 EEA controller to third country controller https://bit.ly/2tYaMfa
- 2004 Alternative EEA controller to third country controller https://bit.ly/2tTAUrA
- EEA controller to third country processor https://bit.ly/2PawDgU

There are no standard clauses for processor to processor agreements. At present it would be expected that the controller would put in place all the necessary data protection agreements/contracts with individual processors. The terms and conditions of any transfers of personal data between (independent) processors should be determined by the controller. Processor to sub-processor contracts would be expected to reflect the data protection terms of the controller-processor contract and should include means by which processor to sub-processor transfers outside of the EEA can be legally made.

Binding Corporate Rules (BCRs) may also be an option for some organisations or group of enterprises engaged in a joint economic activity. Other options such as a GDPR Code of Conduct, the use of a derogation or the research exemption are either unavailable or likely to be of limited value in healthcare business intelligence at present.

It is possible that there will be some form of interim agreement on data protection that allows the UK and EU countries to exchange personal data given that the UK's data protection law is already largely aligned to the EU's.

Transfers of personal data to the USA

At present, upon the UK's exit from the EU, the UK will cease to be part of the Privacy Shield. Although the ICO has said that the UK Government intends to make arrangements for the continued application of the Privacy Shield to transfers of personal data from the UK to the USA.

In anticipation of Brexit, the US Department of Commerce (DOC, which administers Privacy Shield) has published advice that businesses relying on Privacy Shield should take. This advice suggests that organizations can continue to use the Privacy Shield to transfer data from the UK to the USA provided that organisations update their privacy policies before exit from the EU to include an explicit commitment to comply with Privacy Shield making it clear that that the commitment extends to personal data received from the UK.

The ICO recommends that UK organisations check before transferring any personal data that depends on Privacy Shield protection that the US organisation has updated its privacy policy appropriately.

For further information and specimen language for updating the please go to https://www.privacyshield.gov/article?id=Privacy-Shield-and-the-UK-FAQs

Advice to BHBIA members

- Identify existing and future cross border data transfers your organisation makes/is likely to make.
- Review contracts with partners based overseas to check if they exclude transfers of data outside the EU.
- Identify a means to make legal transfers of personal data in the event of no deal on data protection e.g. start drafting standard contractual clauses or examining the practicability of BCRs.
- Review your data protection agreements to make sure that they allow for the transfer of personal data to the UK once it is no longer a member of the EU.
- Prepare to revise privacy notices so that data subjects are informed of the transfer of their personal data outside the EU.
- Check the privacy policies of US organisations to whom you transfer personal data (that relies on Privacy Shield protection) to make sure their policies have been updated appropriately.

The BHBIA also recommends that members consult the ICO's guidance:

ICO guidance

We have published guidance and practical tools to help organisations understand the implications ad to help you plam ahead. These comprise:

- a 'Six Steps to Take' guide https://ico.org.uk/media/2553958/leaving-the-eu-six-steps-to-take.pdf
- broader guidance on the effects of leaving the EU without a withdrawal agreement, https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-there-s-no-brexit-deal/ and
- a general overview in the form of Frequently Asked Questions https://ico.org.uk/for-organisations/data-protection-and-brexit/information-rights-and-brexit-frequently-asked-questions/

Brexit – Pharmacovigilance (PV)

If no deal is reached, the UK's role in the European Medicines Agency (EMA) will cease and the Medicines and Healthcare products Regulatory Agency (MHRA) will take on the tasks previously performed by the EMA for medicines on the UK market[4]. So the MHRA would have primary responsibility for PV activities in relation to UK Marketing Authorisations. It is expected that UK based Marketing Authorisation Holders' drug safety departments will have to submit the PV data they need to forward, directly to the MHRA.

Advice to BHBIA members

If details of adverse events that include personal data (collected during the course of market research) have to be transferred from or to the UK it is essential that the transfer is made by secure and legal means e.g. with EU standard contractual clauses in place. As detailed above this may require your organisation to put new transfer mechanisms in place.

Brexit – Lead Data Protection Authority

If the UK becomes a third country (unless a Brexit agreement provides otherwise), the ICO can no longer be a Lead Supervisory Authority (LSA) for EU GDPR purposes. If a UK organisation has appointed the ICO as its LSA, then to be able to continue to benefit from the 'one stop shop' approach, it will need to appoint a LSA in an EU Member State instead, if this is practical. An organisation that doesn't have a main or a single establishment within the EU cannot have a LSA or benefit from the one stop shop.

The one stop shop allows a single designated data protection authority to act as a central point for any cross-border data processing issues that require Data Protection Authority input.

Advice to BHBIA members

If this impacts your organisation, review and consider which LSA is most appropriate for you.

Brexit – Nominating a Representative

Organisations that offer goods and services to EU citizens or monitor the behaviour of EU citizens, but are based outside the EU and don't have an establishment within the EU, must nominate a representative within an EU member state (Article 27). This is different from the role of Data Protection Officer (DPO).

When the UK leaves the EU, organisations that do not have an establishment within the EU will have to appoint an EU-based representative (unless a Brexit agreement specifies otherwise). This is *not* required if the data processing is carried out by a public authority/body, or is occasional, does not include large scale processing of special category data and is unlikely to result in a risk to the rights and freedoms of natural persons.

Recent government guidance[2] restates this and makes it clear that this requirement is expected to work both ways:

> *"The EU GDPR requires a controller or processor not established in the EEA to designate a representative within the EEA. The Government intends to replicate this provision to require controllers based outside of the UK to appoint a representative in the UK."*

This means organisations may have to deal with more than one supervisory Data Protection Authority (DPA): the ICO in the UK and an EU-based DPA.

For more information on appointing a representative please see the BHBIA's update on 'Brexit Implications - Nominating a Representative'
https://www.bhbia.org.uk/guidelines/gdprupdates.aspx

Advice to BHBIA members

Organisations meeting the criteria detailed above should appoint an EU representative if they do not have an EU establishment and update privacy notices so that they include their representative's identity and contact details.

EEA Implications

The Government's guidance notes that "*Norway, Iceland and Liechtenstein are party to the Agreement on the European Economic Area and participate in other EU arrangements. As such, in many areas, these countries adopt EU rules. Where this is the case, these technical notices* [such as the guidance given on personal data transfers] *may also apply to them, and EEA businesses and citizens should consider whether they need to take any steps to prepare for a 'no deal' scenario.*"

Subject to change

The BHBIA's guidance is subject to change. We will do our best to keep members up to date but please monitor news from the ICO https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/whats-new/

References

[1] https://www.gov.uk/government/publications/data-protection-law-eu-exit/amendments-to-uk-data-protection-law-in-the-event-the-uk-leaves-the-eu-without-a-deal-on-29-march-2019

Original guidance – https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal

[2] DCMS website https://bit.ly/2EhN1pa

[3] http://www.dpnetwork.org.uk/brexit-gdpr-data-protection-uk/

[4] https://www.gov.uk/government/publications/how-medicines-medical-devices-and-clinical-trials-would-be-regulated-if-theres-no-brexit-deal/how-medicines-medical-devices-and-clinical-trials-would-be-regulated-if-theres-no-brexit-deal

Other sources

Market Research Society Brexit Hub https://www.mrs.org.uk/standards/mrs-policy
The MRS's '*Brexit and research: EU-UK Data Transfers*' is likely to be of particular interest.

ABPI http://www.abpi.org.uk/publications/

http://www.abpi.org.uk/media-centre/news/2018/november/abpi-and-bia-input-to-mhra-consultation-on-eu-exit-no-deal-contingency-legislation-for-the-regulation-of-medicines-and-medical-devices/

European Commission Standard Contractual Clauses https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

British Healthcare Business Intelligence Association
Ground Floor, 4 Victoria Square, St. Albans, Herts AL1 3TF
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk

A Private Limited Company Registered in England and Wales No: 9244455