Data Protection Update – Brexit Implications
January 2021

This update keeps you informed about the latest government and ICO guidance on the implications of Brexit for data protection and market research.

The UK formally left the European Union (EU) on 31 December 2020 however the General Data Protection Regulation (GDPR) still applies in the UK.

The GDPR has been incorporated into UK law. So data protection requirements will remain largely the same although the UK will have the independence to keep them under review. The 'UK GDPR' (as it tends to be called) will sit alongside an amended version of the Data Protection Act (DPA) 2018.

What remains the same

Data transfers from UK to EU

These transfers can continue without safeguards because the UK has already designated EEA member countries as providing an adequate level of protection (of personal data for the purposes of the UK GDPR). In addition, the UK has adopted the same adequacy decisions as the EU and so transfers can be made from the UK to these 'adequate' countries e.g. Japan, without additional safeguards.

In addition, the following data protection requirements did not change:

- EU Standard Contractual Clauses (SCCs) can still be used as they are recognised in UK law.
- EU Binding Corporate Rules (BCRs) authorised before 31 January 2020 can be used as they too are recognised.
- The extraterritorial scope of the data protection framework is maintained. So, if an organisation has processing activities in both the EU and UK, or is targeting customers or monitoring individuals in the EU from the UK (or vice versa), it will to be subject to data protection requirements under both the EU and UK versions of the GDPR.
- Organisations do not necessarily need to appoint separate UK and EU Data Protection Officers (DPOs) within the UK and EU, provided that they can still perform their tasks effectively and remain easily accessible to the organisation's employees, regulators and data subjects.

What remains the same . . . for the time being

Personal data transfers from the EU to the UK

On 24 December 2020, the UK and the European Union (EU) agreed the terms of a Brexit deal which includes an interim solution to the issue of personal data transfers from the EU to the UK. This means that there is no need (yet) to put alternative transfer mechanisms (such as standard contractual clauses (SCCs)) in place.

The interim solution allows organisations that transfer personal data from the EU to the UK, to continue to do so, for up to six months (from 1 January 2021) to give time for the European Commission (EC) to hopefully approve an adequacy decision for the UK. During the extension period, transfers of personal data from the EU (and the European Economic Area) to the UK will not be considered transfers to a 'third country' (provided that the UK's data protection law remains the same as it was on 31 December 2020). However:

- The initial four-month extension period will end when adequacy is granted, or may be extended by two further months unless the UK or EU objects;
- If the UK amends its data protection legislation, or exercises certain designated powers without EU agreement during the extension period, the extension period will end.

The Agreement took effect provisionally in EU law on 1 January 2021, pending ratification by the EU Parliament in early 2021. The UK Parliament has ratified the Agreement.

An adequacy decision

The UK Government's goal is to secure an adequacy decision; to do this the EC has to establish that UK law provides an equivalent level of protection to the GDPR. An adequacy decision would allow data to flow into and out of the EU without the need for other safeguards but would not address the ICO's status or the need for a representative.

The EU has stated that it is committed to securing a favourable adequacy decision for the UK. However, the ICO has issued a statement on the Agreement that reminds us that adequacy is not guaranteed and therefore:

> *"As a sensible precaution, before and during this period, the ICO recommends that businesses work with EU and EEA organisations who transfer personal data to them, to put in place alternative transfer mechanisms to safeguard against any interruption to the free flow of EU to UK personal data."*

The UK Market Research Society (MRS) has also advised researchers and analysts to take precautions in case an agreement on data adequacy is not reached. This advice includes having alternative data transfer mechanisms in place, such as SCCs, to ensure there is no disruption to the flow of data between the UK and the EU.

Preparing for no adequacy

If there is no adequacy agreement, 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 different types of standard contractual clauses available from the EC, these remain valid until replaced or amended by the EC:

- EU controller to non-EU or EEA controller
- EU controller to non-EU or EEA processor

Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

It is important to make sure that SCCs are fit for purpose and that they do genuinely provide the security intended.

There are currently no standard clauses for processor to processor agreements. It is 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. Although the UK's Market Research Society (MRS) is working on the development of a GDPR Code for social, opinion and market research which may for those that sign up to it provide a means to secure unrestricted data transfers.

Transfers of personal data to the USA

In July 2020 the 'Privacy Shield' was judged invalid by the EU Court of Justice and so can no longer be used to safeguard transfers between EU and US organisations.

Advice to BHBIA members

- Identify 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 a no adequacy decision e.g. look into using SCCs or examine the practicability of BCRs.
- Update your data protection agreements to make sure that they allow for the transfer of personal data to the UK and include the correct details for Data Protection Officers, local representatives and/or lead supervisory authorities.
- Revise privacy notices so that data subjects are informed of the transfer of their personal data outside the EU.
- Privacy notices, internal policies, contracts and other documents may need to be updated to reflect the applicable regime(s).
- Organisations relying on BCRs for transfers to territories outside the EU/UK may need to have those rules validated by the ICO or an EU supervisory authority.

What has changed

Brexit – Pharmacovigilance (PV)

In January 2021 the UK's role in the European Medicines Agency (EMA) ceased and the Medicines and Healthcare products Regulatory Agency (MHRA) took on the tasks previously performed by the EMA for medicines on the UK market. So the MHRA now has primary responsibility for PV activities in relation to UK Marketing Authorisations. 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 or data analysis) have to be transferred from or to the UK it is essential that the transfer is made by secure and legal means

Brexit – Lead Data Protection Authority

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).

The interim arrangements set out in the UK-EU trade deal do not relieve businesses in either the UK or the EU of their obligation to appoint a representative.

Organisations that do not have an establishment within the EU will have to appoint an EU-based representative. 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.

Government guidance makes it clear that this requirement is expected to work both ways so controllers based outside of the UK need 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-and-legislation/privacy-data

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.

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/about-the-ico/news-and-events/news-and-blogs/2020/01/statement-on-data-protection-and-brexit-implementation-what-you-need-to-do/

Further Information

Market Research Society Brexit Hub https://www.mrs.org.uk/standards/brexit-hub
The MRS's '*Brexit and research: What's Next?*' is likely to be of particular interest.

Government Guidance: Using personal data in your business or other organisation during and after the transition period https://www.gov.uk/guidance/using-personal-data-after-brexit

Information Commissioner's Office: Data Protection at the end of the transition period https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/

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