Skills Development Scotland

Brexit and Data Protection in the UK

Best Practice Guidance Note 11

February 2020

Where are we currently?

Brexit is now underway. The UK has until 31 December 2020 to negotiate its future relationship with the EU, although it is possible that this deadline will be extended. During the transition period, EU laws, including the EU GDPR (General Data Protection Regulation) will continue to apply in the UK.

Does the UK still need to comply with GDPR?

UK organisations that process personal data are currently bound by two laws: the EU GDPR and the UK DPA (Data Protection Act) 2018. Both laws continue to apply until the end of the transition period on 31 December 2020.

What happens after the transition period?

The EU GDPR will no longer apply directly in the UK at the end of the transition period. However, UK organisations **must still comply** with its requirements after this point. This is because the DPA 2018 enacts the EU GDPR's requirements in UK law.

The UK government has issued a statutory instrument – the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. This amends the DPA 2018 and merges it with the requirements of the EU GDPR to form a data protection regime that will work in a UK context after Brexit.

This new regime will be known as '**the UK GDPR**'.

Impact of Brexit on Data Protection

What's the difference between the EU GDPR and the UK GDPR?

There is very little material difference between the EU GDPR and the proposed UK GDPR. So, organisations that process personal data should continue to comply with the requirements of the EU GDPR.

The EU GDPR's requirements as implemented by Parts 3 and 4 of the DPA 2018 will continue to apply for law enforcement and intelligence purposes.

How does Brexit affect international data transfers?

Now that it is no longer an EU member state, the UK has been reclassified as a 'third country'. This shouldn't make any difference to UK organisations until the end of the transition period.

Under the EU GDPR, the transfer of personal data from the EEA to third countries and international organisations is permitted only in certain circumstances:

- If the European Commission has issued an adequacy decision, stating that there is an adequate level of data protection.
- If appropriate safeguards are in place, such as BCRs (binding corporate rules) or SCCs (standard contractual clauses).
- Based on approved codes of conduct, such as the EU-US Privacy Shield. (No such code has been agreed for transfers from the EEA to the UK yet.)

Most organisations that provide goods or services to, or monitor the behaviour of, EU residents will also have to appoint an EU representative under Article 27 of the EU GDPR.

Adequacy decisions

The UK hopes that by enacting the EU GDPR's requirements in domestic law it should be able to demonstrate that it will continue to enforce international data protection requirements after leaving the EU.

To date, the Commission has adopted 13 adequacy decisions with states such as Argentina, Canada, Japan, Switzerland and the United States (for companies certified under the EU-US Privacy Shield).

Talks with South Korea are ongoing. Both the UK and EU hope to complete the adequacy decision process within the transition period.

Binding corporate rules and standard contractual clauses

If an adequacy decision is not reached by 31 December 2020, organisations in the UK that process EU residents' personal data will have to rely on other safeguards, such as BCRs or SCCs.

After the transition period, the ICO (Information Commissioner's Office) will no longer be a supervisory authority under the EU GDPR. This means it won't be able to approve BCRs for transfers of personal data from the EEA to the UK. These will instead need to be approved by a supervisory authority within the EU 27.

Potential penalties for non-compliance

Infringements of the EU GDPR's requirements for transferring personal data to third countries or international organisations are subject to the higher level of administrative fines: up to €20 million or 4% of annual global turnover – whichever is greater.

Organisations that process EU residents' personal data should therefore put measures in place to ensure they continue to comply with the law after 31 December 2020 in case no adequacy decision is reached.

Transfers of UK personal data to the US

For transfers of UK personal data to the US, the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 makes provision to preserve the effect of the EU-US Privacy Shield in the UK.

US organisations that participate in the Privacy Shield will have to update their public commitments to state specifically that the commitment extends to personal data received from the UK.

Further information can be found on the Information Commissioner's website:

ICO - Data Protection and Brexit Implications