What does the Brexit deal mean for data protection? (Keep calm and carry on complying)

The end of 2020 brought with it the "deal" on EU-UK trade in the form of the EU-UK Trade and Cooperation Agreement which notably, from a data protection point of view, allows the continued free-flow of personal data from the EU to the UK for potentially up to 6 months from I January 2021. However, this is not the whole story on data protection post Brexit.

Firstly, as an adequacy decision is not guaranteed, a sensible precaution (and one recommended by the ICO) during this bridging period is to put in place alternative transfer mechanisms to safeguard against any interruption to the free flow of EU to UK personal data in the event that an adequacy decision is not granted.

Secondly, there are some changes arising from the end of the Transition Period that businesses need to make from 1 January 2021 which are unrelated to the adequacy decision.

It is still the case that UK businesses need to keep focussed on compliance with data protection law. Even businesses which are solely UK based and have no contracts or customers or data relating to EEA nationals will see little change in their obligations in relation to data from 1 January 2021. This is because the Data Protection Act 2018 essentially adopted the EU General Data Protection Regulation (GDPR) into domestic legislation.

What should businesses be doing now?

If they haven't already done so, all business need to:

- ensure they comply with PECR and GDPR (all businesses should already be doing this and will continue to

need to do this)
- review processes to see whether they handle data relating to EEA residents
- update their privacy notices and other data protection documentation to reflect the UK no longer being part of the EU.

Further steps

The further steps your business needs to take will depend on whether you handle data relating to EEA residents:

- UK businesses which receive personal data from the EEA
- Consider whether the EEA to UK data transfers are still required.
- Put in place contracts between you and the EEA senders of personal data on EU-approved terms, known as standard contractual clauses (SCCs) so that these will apply at the end of the bridging period if an adequacy decision is not granted. SCCs will be required in almost all circumstances, unless the data transfers are between a large multinational group of companies and the group already has approved binding corporate rules (BCRs) in place.
- UK businesses with customers in the EEA or with offices, branches or other establishments in the EEA
- Identify the European countries in which your EEA customers are predominantly based. This is required because your UK activities will be covered by UK law and your European activities will be covered by EU law. Once you know where your customers are based, you should identify how EU data protection law is handled in those countries to ensure you remain compliant.
- Check which European data protection regulator will be your 'lead supervisory authority' as this will help you identify whether you need to register with that authority and how you should handle correspondence with that authority in the event of a data breach etc.
- If you are only based in the UK but you offer goods or services to individuals in the EEA, or monitor the behaviour of individuals in the EEA, you will need to comply with the EU data protection regime in relation to these activities. In most cases you will also need to appoint a suitable representative in the EEA (see below for more details).
- Do we need to appoint an EU Representative?

If you are a UK-based controller or processor of personal data:

- which has with no offices, branches or other establishments in the EEA; but
- which offers goods or services to individuals in the EEA or which monitors the behaviour of individuals in the EEA.

You will need to:

- Appoint a representative in the EEA (unless you are exempt, see below). This representative will need to be set up in an EU or EEA state where some of the individuals whose personal data you are processing are located. Your European representative may be an individual or a company or organisation established in the EEA (for example, a law firm, consultancy or private company).
- Put in place a service contract or other written mandate for your European representative authorising them to act on your behalf regarding your EU GDPR compliance, and to deal with any supervisory authorities or data subjects in this respect.
- Update your privacy notice and website to include contact details and other information about your European representative.

You will not need to appoint a European representative if:

- you are a public authority; or

- your processing is only occasional, of low risk to the data protection rights of individuals, and does not involve the large-scale use of special category or criminal offence data.
- We are an EU business, do we need to appoint a UK Representative?

A business located in the EU (or otherwise outside of the UK), but which is still required comply with the UK data protection law (for example because it offers goods or services to individuals in the UK or because it monitors the behaviour of individuals in the UK), must appoint a UK representative.

Where can I find out more?

If you wish to understand more about the impact of Brexit on data protection compliance, please contact Kathryn Rogers or Elliot Fry.

Other useful links on the subject can be found on the Information Commissioner's Office (ICO) website.

Written by

Kathryn Rogers

Partner