Clayden | Law

No-deal Brexit: data protection consequences for UK businesses

This article looks at how UK businesses will be affected by changes in data protection law arising from a no-deal Brexit.

This article was written by Hannah Kirby, a technology commercial solicitor at Clayden Law. Hannah can be contacted for more information on 01865 953542 or hannah@claydenlaw.co.uk.

UK becomes a 'third country'

The headline point is that once we're out without a deal, the UK becomes a 'third country' for the purposes of all EU laws, including EU data protection law. This is EU-speak for any country that isn't a member state of the EU or EEA.

As a third country, the UK will suddenly find itself outside of the mutually-beneficial internal market that enables the unrestricted movement of, and free trade in, personal data between members of the EU/EEA club. Unless and until the European Commission makes an 'adequacy decision' in respect of the UK's legal framework for the protection of personal data, the UK will take its place on the EU naughty list of third countries that don't provide an adequate level of protection for personal data and obtain the unenviable colloquial label of 'non-adequate country'. It will be unlawful for any organisation based in the EU or EEA – and therefore subject to the GDPR – to send personal data to any organisation based in the non-adequate UK unless one of the 'transfer mechanisms' listed in the GDPR can be put in place (see more on transfer mechanisms below).

The GDPR isn't just about protecting individuals from misuse of their personal data: it's as much about allowing personal data to flow freely without restriction between EU/EEA members – to the benefit of all organisations established in member countries.

All organisations based in the EU/EEA effectively benefit from an assumption that they are 'adequate' because they are all subject to the same EU laws pertaining to personal data. UK organisations have benefitted from, and possibly taken for granted, this assumed adequacy and free trade in personal data for decades, but will suddenly find themselves in the same position as their US, Indian, Chinese and Australian competitors – looking enviously in from the outside at the EU/EEA club whilst having to expend considerable resources to put transfer mechanisms in place and comply with additional obligations

imposed on third country organisations under the GDPR if they want to tap into the EU personal data market.

The need for transfer mechanisms and the additional obligations for third country organisations under the GDPR effectively act as barriers to global free-trade, with 'outsiders' seeing the GDPR as a key tool of European protectionism.

A new data protection legal regime for UK businesses

Currently, UK organisations are subject to:

- the **GDPR**, an EU regulation with direct effect in all EU and EEA member countries ('EU GDPR')
- the **UK Data Protection Act 2018** ('DPA 2018'), which replaced the UK Data Protection Act 1998 and currently supplements and tailors the EU GDPR within the UK

After a no-deal Brexit, UK organisations will:

- continue to be subject to the DPA 2018 (as amended to reflect the UK's newly-acquired third country status)
- no longer automatically be subject to the EU GDPR, except where their activities are 'caught' by its extra-territorial provisions (see 'How will this affect my business' below) – in which case all *those activities* will continue to be subject to the EU GDPR
- Become subject to the new **UK GDPR**: this is essentially the EU GDPR but with EU references changed to UK references, with the same core data protection principles, rights and obligations found in the GDPR. The UK is basically adopting the GDPR as its main domestic data protection law, with technical amendments to make it work in a UK-only context from exit day. The UK GDPR and DPA 2018 will operate alongside each other in the same way that the EU GDPR and DPA 2018 currently do.

The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 is the law which will bring the UK GDPR into effect and amends the DPA 2018 and other data protection-related laws: https://www.legislation.gov.uk/uksi/2019/419/contents/made.

Various other data protection-related laws will continue to apply post-Brexit, including:

- **Privacy and Electronic Communications Regulations 2003 (PECR)**: The EU is replacing the current e-privacy law with a new e-privacy Regulation (ePR), which is not yet agreed and is unlikely to be finalised before Brexit. This means the ePR will not form part of UK law if we no-deal Brexit.
- **Network and Information Systems Regulations 2018 (NIS)**: If your business is a UK-based digital service provider offering services in the EU, on exit date it may need to appoint a representative in one of the EU member states in which it offers services and will need to comply with the local NIS rules in that member state. If it also offer services in the UK, it will also need to continue to comply with the UK rules regarding your UK services.
- **Freedom of Information Act 2000**
- **Environmental Information Regulations 2004**

How will these changes affect my business?

Becoming a third country for data protection law purposes presents a number of challenges and hurdles for UK organisations hoping to continue their business-as-usual activities after Brexit, whether this be providing or receiving services, collaborating on international research projects or any other activity that involves the sharing or use of personal data.

The consequences for any particular organisation will depend on its interactions with EEA organisations and individuals. The table below summarises the applicable laws and practical effects for organisations depending on these interactions:

EEA interactions	**Laws that will apply**	**Practical effects/obligations**
No clients / collaborators / partners / other contacts in the EEA **AND** doesn't process personal data relating to people in the EEA	DPA 2018 UK GDPR	Little change, as the DPA 2018 and UK GDPR contain the same basic principles, rights and obligations as the EU GDPR. BUT will have to comply with UK GDPR restrictions and conditions on

		transferring personal data outside the UK. Will be regulated solely by the ICO.
Has an office, branch or other established presence in the EEA	EU GDPR in respect of any processing of personal data *in the context of the activities of the EEA establishment* (even where the processing actually happens in the UK). This is due to the extra territorial effect of Art 3(1) EU GDPR. DPA 2018 + UK GDPR in respect of *all* its data processing activities, including those also subject to the EU GDPR.	Not all the organisation's data processing activities will be subject to the GDPR, only those in the context of the activities of the EEA establishment. However, in practice, it's unlikely to be beneficial or workable to apply EU GDPR requirements to some but not all of the organisation's activities. Will need to identify a new 'lead supervisory authority' to replace the ICO as its regulator for the purposes of the EU GDPR. Will also be regulated by the ICO in respect of its UK activities.
Offers goods or services to individuals in the EEA or monitors the behaviour of individuals in the EEA	EU GDPR in respect of any processing of personal data *relating to offering goods or services to, or monitoring the behaviour of, individuals in the EEA*. This is due to the extra territorial effect of Art 3(2) EU GDPR. DPA 2018 + UK GDPR in respect of *all* its data processing activities, including those also subject to the EU GDPR.	Not all the organisation's data processing activities will be subject to the GDPR, only those relating to offering goods or services to, or monitoring the behaviour of, individuals in the EEA. However, in practice, it's unlikely to be beneficial or workable to apply GDPR requirements to some but not all of the organisation's activities. Will need to appoint an EU representative under

		Art 27 EU GDPR. May need to deal with local supervisory authorities in every EEA country in which it carries out these activities, via its EU representative. Will also be regulated by the ICO in respect of its UK activities.
Receives personal data from organisations in the EEA (regardless of whether it offers goods or services to individuals in the EEA, monitors the behaviour of individuals in the EEA or has an office, branch or other established presence in the EEA)	In addition to the interaction-dependent applicable laws listed above: EU GDPR Chapter V restrictions and conditions on transferring personal data outside the EEA. Although these provisions may not apply directly to the UK organisation, its EEA-based clients, collaborators, partners and other contacts will have to comply with these restrictions and conditions because they are subject to the EU GDPR. DPA 2018 + UK GDPR in respect of *all* its data processing activities, including those also subject to the EU GDPR Chapter V restrictions and conditions	Will need to take extra steps to ensure that it can continue to receive personal data from its EEA-based contacts – i.e. put 'transfer mechanisms' in place, such as standard contractual clauses.

How can we comply with both EU and UK data protection law post-Brexit?

Complying with the dual legal regime should not be too problematic immediately, as the UK GDPR is currently fully aligned with the EU GDPR. However, as time goes on, the UK may change its data protection laws as it 'takes back control' of its laws free of the dictates of Brussels, and if and when the UK and EU regimes diverge, it will become more difficult for UK organisations to comply with both sets of laws. UK organisations may find themselves having to navigate conflicting legal requirements in respect of its data processing activities.

Post-Brexit trade deals with countries outside the EU are likely to involve a reduction/removal of current protections for personal data in the UK. In particular, US businesses consider these protections to be a non-tariff barrier to trade. According to the Huffington Post, US industry lobbyists have made submissions to the Office of the United States Trade Representative on this point: "US insurers have noted that compliance with data regulations in the UK, particularly with regard to the EU's General Data Protection Regulation (GDPR), is overly burdensome. We suggest that the UK-US negotiations be used to reduce that burden." (See https://www.huffingtonpost.co.uk/entry/us-lobbyists-brexit_uk_5c5b26c6e4b00187b5579f64?guccounter=1&guce_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8&guce_referrer_sig=AQAAAN4WjxyYuTKpjolulNWKTUx4oVD9TF68Q3qn4OGIaD22IFjgOt479k4F_OIdxADR70EJXPk5_tvl3WBGhCCchWRoQtUU7NF5ix_9IqQUtpwABnTIfwCu6SYgCS23ky5DOM9A0i2K9ZsyDl4fdgLog836Pyumpuy7g7qstpUv7seL). These aims are also reflected in the US-UK Negotiations Summary of Specific Negotiating Objectives February 2019 (see https://ustr.gov/sites/default/files/Summary_of_U.S.-UK_Negotiating_Objectives.pdf section on 'Digital Trade in Goods and Services and Cross-Border Data Flows') and in the 2019 National Trade Estimate Report on Foreign Trade Barriers (see https://ustr.gov/sites/default/files/2019_National_Trade_Estimate_Report.pdf page 207).

Any reduction in the protection of personal data under UK law as a condition of securing a trade deal with the US or any other country will have the probable outcome that the UK will not receive an 'adequacy decision' from the EU Commission, and will make it more difficult for UK organisations to do business and share personal data with clients, partners and collaborators in the EEA who are obliged under the EU GDPR to ensure the protection of any personal data they transfer outside the EEA.

Will we be able to send and receive personal data across borders post-Brexit?

A no-deal Brexit will introduce additional restrictions and conditions in respect of cross-border personal data flows ('transfers'). Essentially this means UK organisations will need to ensure there is a 'transfer mechanism' in place for any transfers it sends or receives. 'Transfer mechanism' isn't an official GDPR term, but is colloquial short-hand for the 'conditions' listed in Chapter V of the EU GDPR which must be fulfilled before transfers can be made. Transfer mechanisms include:

- **Adequacy decisions**: where the EU Commission has made a formal decision that a particular country, sector within a country or international organisation ensures an adequate level of protection for personal data. The EU-US Privacy Shield is an example of this.
- **Appropriate safeguards**: these are contractual- or policy-based mechanisms such as:
    - **standard contract clauses** – standard data protection clauses adopted by the EU Commission, which can be used between any organisations
    - **binding corporate rules** – contractually binding terms, approved by a supervisory authority, between companies within a corporate group, which apply to transfers between companies within that corporate group
    - **administrative arrangements** – non-contractual documented arrangements, approved by a supervisory authority, between public bodies in different countries, which apply to transfers between the public bodies named in those arrangements

    In the future there may be further appropriate safeguards in the form of approved codes of conduct and certification mechanisms, but none exist as yet.
- **Derogations for specific situations**: these are context-specific exceptions that may be relied on if applicable in the absence of an adequacy decision or appropriate safeguards, such as obtaining explicit consent of the individuals whose personal data is to be transferred or an occasional transfer to perform a contract with an individual, for important reasons of public interest or to establish, make or defend legal claims. These derogations must be interpreted restrictively and mainly relate to transfers that are occasional and non-repetitive.

The 'order of preference' for these transfer mechanisms in the EU GDPR is: (1) an adequacy decision; (2) an appropriate safeguard; and (3) a derogation as a last resort. The UK GDPR essentially replicates the EU GDPR rules on transfer mechanisms, but with amendments to make it work in a UK-only context.

The table below sets out which transfer mechanisms may be available for transfers to and from different categories of countries:

	OUTWARD TRANSFERS (from the UK to other countries)	**INWARD TRANSFERS** (from other countries into the UK)
Destination/source	**Available transfer mechanism**	**Available transfer mechanism**
EEA countries	Under the UK GDPR, transfers **to** the EEA will not be restricted. UK organisations will not need to take any additional steps to transfer personal data to organisations in the EEA.	***No adequacy decision:*** EEA-based organisations would be able to transfer personal data to a UK organisation **IF** the UK is covered by a European Commission adequacy decision. A no-deal Brexit will mean that there will not be a UK adequacy decision on exit. Adequacy decisions usually take a long time, so even if the Commission is inclined to do this, it is likely to be many months or years before an adequacy decision comes into effect. As the UK will not be covered by an adequacy decision, EEA organisations will need to put in place one of the EU GDPR **appropriate safeguards**, or if none is available, rely on a **derogation**. ***Appropriate safeguards:*** **Standard contractual clauses** are likely to be the most convenient safeguard for many organisations. **Binding corporate rules** can be used to make intra-corporate group transfers of personal data from EEA-based companies covered by the

		BCRs to UK companies covered by the BCRs. However this only immediately helps businesses who are already covered by approved BCRs. Producing and obtaining supervisory authority approval for new BCRs usually takes several months or years, and the approval will have to come from an EU-based supervisory authority (i.e. not the ICO). Any existing BCRs will need to be updated, with effect on the exit date, to recognise the UK as a third country outside the EEA for the purposes of the EU GDPR. **Administrative arrangements** will allow an EEA public body to transfer personal data to an UK public body that is covered by those arrangements. It will need to be authorised by the supervisory authority with oversight of the EEA public body. ***Derogations***: If no appropriate safeguards are available, EEA-based organisations may be able to transfer personal data to a UK organisation based on one of the EU GDPR derogations. It is the EEA sender's responsibility to decide whether a derogation applies.

	OUTWARD TRANSFERS (from the UK to other countries)	**INWARD TRANSFERS** (from other countries into the UK)
Non-EEA countries <u>with</u> an EU adequacy decision Currently includes: Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Isle of Man, Israel, Japan (private-sector organisations only), Jersey, New Zealand, Switzerland, Uruguay, and USA (under Privacy Shield only)	The UK GDPR will recognise existing EU adequacy decisions made by the European Commission before Brexit. This will allow restricted transfers to continue to be made to organisations, countries, territories or sectors covered by an EU adequacy decision, subject to some extra steps in respect of Japan and the US: ***Japan***: Specific UK arrangements have been confirmed which secures the necessary protections for UK data as well as EU data, so that data can continue to flow from the UK to Japan. ***US***: Modified arrangements will apply regarding the EU-US Privacy Shield, as this is an EU/US-specific arrangement. The UK government is making arrangements for its continued application to transfers from the UK to the US (see further information on the US government's Privacy Shield website https://www.privacyshield.gov/article?id=Privacy-Shield-and-the-UK-FAQs). UK organisations will continue to be able to transfer personal data to US organisations participating in the Privacy Shield **IF** the US organisation	These countries, territories or sectors are likely to have their own legal restrictions on making transfers of personal data to countries outside the EEA, which will include the UK on a no-deal Brexit. According to the ICO, UK officials are working with these countries and territories to make specific arrangements for transfers to the UK where possible. In the meantime, the organisations will need to cooperate to consider how to comply with local law requirements on transfers of personal data and seek local legal advice. The ICO provides links to legislation and guidance from the supervisory authorities in these countries: https://ico.org.uk/for-organisations/data-protection-and-brexit/data-protection-if-theres-no-brexit-deal/the-gdpr/international-data-transfers/

	has updated its public commitment to comply with the Privacy Shield to expressly state that it applies to transfers of personal data from the UK. UK organisations will therefore need to check that the US organisation's publicly available privacy policy states these magic words.	
	OUTWARD TRANSFERS (from the UK to other countries)	**INWARD TRANSFERS** (from other countries into the UK)
Non-EEA countries <u>without</u> an EU adequacy decision	UK organisations will need to find an **appropriate safeguard** or failing that a **derogation** set out in the UK GDPR. ***Appropriate safeguards:*** **Standard contractual clauses** are likely to be the most convenient safeguard for many organisations. The UK GDPR will recognise European Commission-approved standard contractual clauses as providing an appropriate safeguard for transfers from the UK. **Binding corporate rules** can be used to send personal data to any group company also covered by the BCRs (wherever located). The UK GDPR will recognise BCRs authorised under the EU process before Brexit as ensuring appropriate safeguards for transfers from the UK. However this only	There are no restrictions or conditions on UK organisations receiving personal data from organisations in these countries under the UK GDPR. However, the organisations will need to cooperate to comply with any legal requirements for transfers of personal data in those countries and seek local legal advice.

	immediately helps businesses who are already covered by approved BCRs. Producing and obtaining supervisory authority approval for new BCRs usually takes several months or years. Any existing BCRs will need to be updated so that the UK is listed as a third country outside the EEA. **Administrative arrangements** approved by the ICO would allow UK public bodies to send personal data to public bodies that are covered by the arrangements in these countries. ***Derogations***: If no appropriate safeguards are available, UK organisations will have to rely on one of the derogations in the UK GDPR, which mirror those in the EU GDPR.	

What if we need to appoint an EU representative?

If your business is required to appoint an EU representative because it offers goods or services to individuals in the EEA or monitors the behaviour of individuals in the EEA, it will need to:

- consider in which EU or EEA state the representative will be based – this must be a country where some of the individuals whose personal data it processes in relation to those activities are located
- put in place a written mandate for that representative to act on its behalf regarding its EU GDPR compliance and to deal with any supervisory authorities or data subjects in this respect
- provide information about the representative to data subjects, e.g. in its privacy notice or in upfront information given to them when it collects their data, and make it easily accessible to supervisory authorities, e.g. by publishing it on its website

An EU representative may be an individual, a company or organisation established in the EEA and must be able to represent the UK organisation regarding its obligations under the EU GDPR (e.g. it could be a law firm, consultancy or private company). In practice the easiest way to appoint a representative may be under a simple service contract.

Having an EU representative does not affect an organisation's own responsibility or liability under the EU GDPR.

Is there anything else we need to do?

As you might expect there are a number of general sweeping-up tasks all UK organisations will need to do in respect of their data protection housekeeping:

- Review and make any necessary changes to your **privacy notices**, **processing records**, **data protection impact assessments (DPIAs)**, **binding corporate rules** (if you have them) etc to reflect changes regarding international transfers, update references to EU or 'union' law in respect of your lawful bases for processing, identify your EU representative (if you need one) and reflect the UK's third country, non-EEA status.
- If you have any EEA establishments, ensure your **data protection officer** (**DPO)** will be easily accessible from both your UK and EEA establishments and think about which EEA supervisory authority will become your lead authority on exit date - you may want to contact them before then.
- Review any existing **Data Protection Impact Assessments (DPIAs)** in light of the UK GDPR, particularly where they cover international data flows that will become restricted transfers on exit date or rely on any EU law to provide a lawful basis.

Concluding remarks

As this article shows, a no-deal Brexit is set to make things much more difficult for UK organisations to continue activities involving the processing of personal data, particularly where those data relate to individuals in the EEA or are obtained from organisations in the EEA.

Understandably, many UK organisations are reluctant to commit the necessary staff time and financial resources now to prepare for these changes at a time of such uncertainty about whether there will be a deal or not, whether we will Brexit or not and if we do, when.

Do get in touch will us if you'd like any advice about how your business will be affected by a no-deal Brexit and what steps it can take to address those effects.