ALLEN & OVERY

Data Protection Post-Brexit

Where are we now and what happens next? | March 2021

The UK has left the European Union (**EU**), the transition period is over, the UK and EU have agreed a new **Trade and Cooperation Agreement** (the **TCA**), so what now for data protection? We look at the key consequences of Brexit for data protection and the practical impact for organisations: What law applies? What must businesses do to allow for the uninterrupted flow of data to and from the UK? What changes to policies, procedures, privacy notices and documents are required? Should Data Protection Officers and Representatives be appointed or those roles restructured? Many organisations will have taken steps already and certainly the necessary approach to most questions is clear. But beware, all is not set in stone just yet.

The headlines

This PDF contains interactive elements. Click a square to jump to a section.

Data flows from the EEA to the UK can continue without additional safeguards until 30 June 2021.

The GDPR now forms part of "Retained EU law", meaning it has been onshored into UK law with a number of amendments made by a series of statutory instruments – this is generally now known as "UK GDPR".

The Data Protection Act 2018 continues to apply in the UK (with certain amendments to account for Brexit) alongside the UK GDPR and PECR.

The Privacy and Electronic Communications Regulations 2003 (PECR) continue to apply (with certain amendments to account for Brexit), but the EU's proposed E- Privacy Regulation will not come into force in the UK.

European Data Protection Board (EDPB) guidelines and opinions will have reduced status in relation to the interpretation of UK GDPR (but may still be useful).

The Schrems II decision forms part of "Retained EU law", so companies exporting data from the UK must continue to comply with the judgment of the CJEU in Schrems II.

The UK's ICO is no longer a member of the EDPB and can no longer function as a lead supervisory authority under the one-stop-shop, which has particular relevance for companies with BCRs – a company wishing to maintain or seek BCRs for data exports from the EEA and the UK will need to liaise with both an EU lead supervisory authority and the ICO.

UK companies are required to appoint a representative in the EU (and EU companies are required to appoint a representative in the UK) in certain circumstances.

Changes to data protection law

The EU and the UK clearly state in the TCA their respective rights to regulate to achieve privacy and data protection policy objectives but they also commit to ensuring a high level of data protection and to endeavour to work together to promote high international standards.

However, whilst EU and UK data protection laws are for the time being aligned, this will not necessarily remain the case in the longer term, as the UK looks to flex its rights to evolve and introduce its own laws.

Organisations have grown used to regime across the UK and EU which is substantially harmonised. Post-Brexit, things will be more complex.

Organisations operating across the UK and EU should also be mindful that their activities in any country could be subject to multiple applicable data protection laws, due to the extra-territorial effect of UK, EU and certain other data protection laws.

Contracts and policies may require amendments to refer to the new laws which are created as a result of Brexit, in particular the UK GDPR and the distinction between those laws and the laws which preceded them.

This table outlines the application of relevant legislation in the UK and EU as at 1 January 2021. It also considers the interaction of both regimes with laws in the rest of the world.

In the UK

UK law	**EU law applicable**
– UK GDPR – UK DPA 2018 – Privacy and Electronic Communications Regulations (PECR)	– EU GDPR as it applies to controllers and processors established in the UK to the extent caught by the extra-territorial scope of EU GDPR – EU GDPR as at 31 December 2020, in respect of EU data in the UK on 31 December 2020 as well as certain other personal data processed in the context of the Withdrawal Agreement (until any adequacy decision is granted) **Any other data protection laws outside the UK with extra-territorial effect**

In the EEA

EU law	**UK law applicable**
– EU GDPR – E-Privacy Directive – other EU law as it is incorporated into Member State law	– UK GDPR as it applies to controllers and processors established in the EU to the extent caught by the extra-territorial scope of the UK GDPR **Any other data protection laws outside the EEA with extra-territorial effect**

In the Rest of the World

Rest of world laws (eg CCPA)	**EU law applicable** – EU GDPR as it applies to controllers and processors established in the RoW to the extent caught by the extra-territorial scope of GDPR **UK law applicable** – UK GDPR as it applies to controllers and processors established in the RoW to the extent caught by the extra-territorial scope of the UK GDPR **Any other data protection laws outside the relevant jurisdiction with extraterritorial effect**

Helpfully the UK Government has produced so-called **"Keeling Schedules"** to illustrate changes made to the EU GDPR and UK Data Protection Act 2018 (**DPA**) to on-shore and amend the legislation to create the UK GDPR and update- the DPA.

This on-shoring and amendment process is governed by the European Union (Withdrawal) Act 2018, as amended by the European Union (Withdrawal Agreement) Act 2020 (the **EUWA**). The EUWA also provides that case law decided prior to the end of the transition period by the Court of Justice of the EU (**CJEU**) will be binding on all UK courts (other than the Supreme Court and Court of Appeal) where that case law remains relevant and the underlying law is unmodified. In the context of data protection, this approach therefore on-shores the CJEU judgment in the case of Facebook Ireland Ltd v Maximillian Schrems dated 16th July 2020 (**Schrems II**) such that the resulting question marks over cross border transfer mechanisms such as Standard Contractual Clauses (**SCCs**) and Binding Corporate Rules (an internal agreement that permits data transfers within a corporate group, **BCRs**) also remain in the UK post-Brexit.

Generally, the ICO has also confirmed that whilst **European Data Protection Board (EDPB) Guidelines** are no longer directly relevant to, nor binding under, the UK regime, they may still provide helpful guidance on certain issues.

Alongside extra-territorial application of the EU GDPR, Article 71 of the Withdrawal Agreement (agreed between the EU and UK in October 2019) provides for the post-transition protection of "legacy data" – the personal data of data subjects outside the UK which was processed in the UK under EU law (i.e. the EU GDPR) prior to the end of the transition period. Until the UK is granted an adequacy decision (and to the extent any such decision is subsequently lost), this "legacy data" continues to be subject to the EU GDPR as at 31 December 2020 – the ICO refers to this as the **"Frozen GDPR"**. The DPA is not "frozen" and can continue to be amended as long as it stays consistent with the Frozen GDPR. The intention is to ensure an "adequate level of protection" for personal data that was transferred freely from elsewhere in the EU to the UK before the end of the transition period. In contrast to the position referenced above, EDPB Guidelines continue to apply to the Frozen GDPR and the UK must also have due regard to any new post-2020 CJEU decisions in the context of "legacy data". However, given the TCA bridging provisions (see further below) prevent the UK deviating from EU data protection law until any adequacy decision is granted, we do not anticipate any significant practical impact on organisations.

In future, organisations will need to determine which legal obligations apply to personal data in different circumstances, potentially separating and treating EU and UK data differently. Businesses will resist this where possible, to avoid the complexity it would entail, and most are used to taking a risk-based approach to compliance with data protection laws on a global basis, balancing the need for globally consistent processes with the need to meet local law requirements.

The ICO's role and need to engage with multiple regulators

The ICO is the supervisory authority under the UK GDPR and DPA but no longer has a role under the EU GDPR. It is not a member of the EDPB cannot participate in the cooperation and consistency mechanism under the EU GDPR nor act as a lead supervisory authority under the so called "One Stop Shop" (**OSS**), for cross-border processing across more than one Member State.

Businesses operating across the UK and EU, which have the ICO as their lead supervisory authority in the EU, may wish to consider whether it is possible to identify an alternative EU supervisory authority that could act as their lead supervisory authority under the EU GDPR, to continue to take advantage of the OSS system in relation to cross-border processing activities in the EU.

However, many UK headquartered organisations may not have a 'main establishment' within the EU, or they may only have an EU main establishment for specific and limited cross border processing activities, so the option of 'migrating' to another lead supervisory authority may be unavailable (other than in specific contexts, such as the maintenance of EU BCRs). For others, the situation may be more finely balanced.

If, as a result of Brexit, a business relocates infrastructure and personnel from the UK to the EU (eg to benefit from the financial services passporting regime within the EU), such a structural change may be sufficient to give rise to a main establishment within the EU.

What are the implications for international data transfers?

In the short term, transfers of personal data can generally continue on the same basis as those prior to the end of the transition period. This position may change if the EU does not grant the UK an adequacy decision prior to July 2021 but indications are positive.

In any event, drafting amendments to contracts may be required to reflect the UK's status as a non-EU country and, in relation to BCRs, ICO approval may be necessary to enable uninterrupted data flows (see further below).

Transfers to the UK from the EEA- adequacy decision looks promising

Despite UK hopes, the European Commission had not completed its assessment of the protection offered to personal data by the UK legal regime by the end of the transition period. No adequacy decision was therefore granted at that point.

A Joint Declaration of the EU and the UK on 24 December 2020 did, however, note the European Commission's intention to launch the procedure for adoption of adequacy decisions for the UK and on 19 February 2020, it published positive draft decisions, concluding that the UK maintains an essentially equivalent level of protection for personal data as that granted

under the EU regime. This progress has been welcomed by the UK Government and ICO. The EDPB must now provide an opinion on the same, with further approval from a committee of representatives of EU Member States required before the decisions can be adopted.

In the interim, the TCA provides for a six month grace period (four months, automatically extendable to end on 30 June 2021) regarding data transfers from the EEA to the UK. During this time EEA states will not treat the UK as a third country in relation to EU GDPR international data transfer requirements, so personal data can continue to flow freely to the UK. However, the bridging mechanism is dependent on the UK continuing to maintain its data protection laws as at 1 January 2021 and not exercising certain "designated powers" regarding data transfers during the period without approval of the TCA's Partnership Council (including, for example, granting adequacy decisions to new third countries, issuing UK standard contractual clauses, approving certain new certification mechanisms and draft codes of conduct, approving new binding corporate rules, authorising new contractual clauses and administrative arrangements). The exception to these restrictions is regards changes made to UK data protection law so as to align with the EU regime. It remains to be seen whether the issuing of UK SCCs in line with new EU drafts, for example, would be an acceptable change.

Planning for a "no adequacy" outcome or loss of an adequacy decision

The ICO has previously suggested that organisations should consider and implement other appropriate safeguards (or identify derogations) as necessary to enable continued data transfers to the UK if no adequacy decision is forthcoming before July 2021. This may include use of SCCs, for example.

It would be surprising if no adequacy decision were to be granted before this deadline. However, it is worth noting that the draft anticipates that the UK's adequacy status will only be valid for a period of four years, after which the finding can be renewed provided that the level of protection in the UK continues to be adequate. It may therefore be prudent for organisations to consider and prepare alternative solutions to enable continued international data transfers should any adequacy decision lapse.

Existing contracts incorporating SCCs for transfers between the EEA and rest of the world may, depending on the specific drafting, already capture transfers of personal data to the UK. However, organisations should consider if contractual amendments are required (for example, to adjust consent to transfer language, to reflect the UK's status as a third country, or the organisation's role as a data exporter and/or data importer) to enable continued data transfers.

Any changes will need to be made in light of the judgment in Schrems II and the potential need for supplementary measures. Organisations should be aware that any Brexit related changes may need to be made in parallel with amendments to reflect the new form of EU SCCs currently under consideration and due to be finalised and adopted by the European Commission in H1 2021.

BCRs

It is likely that few businesses will seek BCRs amidst the current uncertainty created by the Schrems II decision.

However, for those that do, or that have applications already underway, BCRs may provide appropriate safeguards for transfers to the UK in the absence of an adequacy decision.

Existing BCR holders with operations in the EU but with the ICO as its BCR lead supervisory authority were required to transfer those BCRs to a new EU BCR lead (according to the criteria set out in the Article 29 Working Party Working Document 263rev.01) before 31 December 2021. The EDPB recently published a **list of those which had already completed this process**. The EDPB produced an annex containing a checklist of items to be amended in BCR documents in the context of Brexit (see their **information note of 22 July 2020**).

If BCRs were previously approved by the ICO as lead authority under the EU GDPR, by way of the consistency mechanism, it is necessary for the new supervisory authority to (re)approve the BCRs. Approval is not required where BCRs were approved pre-EU GDPR, i.e. under the cooperation procedure under Directive 95/46/EC (though identification of a new BCR lead authority and notification of amendments to that BCR lead will remain necessary).

If a BCR approval process with the ICO, as lead supervisory authority, was ongoing at the end of the transition period that process needs to be reconsidered and re approved by a new EU BCR lead. Organisations should contact the proposed BCR lead in the EU and provide all necessary information to justify why it is the most appropriate authority to assume the role.

Organisations wishing to continue to rely on existing BCRs for international transfers by BCR group members located in the UK to third countries are required to make certain amendments to their BCRs and to notify these to the ICO. EU BCRs approved by the ICO under Directive 95/46/EC remain eligible for use for transfers from the UK, as provided for in the DPA. The ICO further specifies in its **requirements table**, changes to be made to create a UK version of the BCRs that, in this context, must be provided to the ICO on or before the next annual update due date.

Whilst the UK has not given mutual recognition to EU BCRs, the DPA provides that any BCRs approved by a supervisory authority other than the ICO under Directive 95/46/EC, will be recognised by the ICO subject to certain notification and amendment requirements that should be satisfied as soon as possible (as no confirmation of UK BCRs will be issued by the ICO until they are) and in any event by the backstop date of 30 June 2021. The ICO notes that holders of these EU BCRs should contact the ICO for further clarification of its exact requirements. Similarly, where BCRs have been approved under the EU GDPR by a supervisory authority other than the ICO, the BCR holder should have contacted the ICO directly for further guidance on how to obtain UK BCRs, as explained in the ICO's information note **here**. This approach effectively creates two parallel sets of BCRs (i.e. UK BCRs and EU BCRs), either within the same or largely mirrored documentation.

The ICO has said that it prefers for the legal instrument making UK BCRs binding to be separate to that which makes EU BCRs binding, which is likely to entail execution of a new or amended agreement for a company wishing to maintain BCRs across the UK and EU.

Subject to the TCA bridging mechanism, under the UK GDPR, the ICO may also approve new BCRs for transfers from the UK to the EEA and the rest of the world.

Transfers from the UK to adequate destinations…

Under the DPA, the UK continues to permit transfers of personal data to EEA states and those destinations already designated as "adequate" by the EU, in each case, without further safeguards. Whilst the DPA provides scope for this approach to be reviewed, data flows from UK to the EEA and other adequate destinations are unlikely to be impeded in the foreseeable future. Indeed, subject to the TCA bridging provisions, the UK may issue its own adequacy decisions in respect of additional third countries in due course.

…or to destinations not deemed to provide an adequate level of protection

Organisations making transfers of personal data from the UK to the U.S. or to other third countries that are not subject to an EU adequacy decision should continue to implement appropriate safeguards or to rely on specific derogations.

Appropriate safeguards and derogations under the UK GDPR and DPA are currently equivalent to those under the EU GDPR, including, for example implementation of SCCs or BCRs (alongside supplementary measures where necessary) but excluding reliance on the EU-U.S. Privacy Shield. As under the EU GDPR and pursuant to the Schrems II judgment, a data exporter should either terminate or suspend transfers from the UK where adequate protection of that data cannot be achieved or notify the ICO where it intends to continue making transfers nonetheless.

Under the DPA, European Commission-approved SCCs continue to be valid for transfers from the UK, accepting the need to make amendments to reflect the UK's departure from the EU (with respect to which the ICO has produced templates to assist). Subject to the TCA bridging requirements, the Secretary of State and the ICO do have the power to issue new SCCs applicable in the UK and the ICO has (informally) indicated that these are likely to mirror or at least take account of the approach to be taken by the EU to its own new draft SCCs. Organisations should consider what, if any, changes are needed to existing SCCs to reflect their use for transfers from the UK.

Is it necessary to update internal policies and procedures?

For the time being, this is unlikely to be required, or the required changes will be minimal.

Currently, the data protection regimes of the EU and UK are closely aligned and therefore large scale updates of policies and procedures are unlikely to be necessary on the basis of Brexit. However, where the processing activities of an organisation are subject to the oversight of more than one regulator, for example the ICO and an EU lead supervisory authority, organisations should consider how these regulatory relationships will be managed going forward in different contexts. For instance, updating procedures to provide for breach notification to more than one regulator, updating policies to require review of more than one set of laws, revising reminders or alerts to flag deadlines of more than one regulator.

Is it necessary to update privacy notices and other documentation?

Articles 13 and 14 of the EU GDPR and UK GDPR require that privacy notices provide details of international data transfers to third countries, as well as the safeguards that have been implemented for the purposes of those transfers.

It is unlikely that privacy notices would need any significant update purely in light of Brexit, but this should be considered. For example, for a business headquartered in the UK, with operations throughout the EU, it may be appropriate, post transition, to refer specifically to the UK as a destination country for data transfers.

It may also be necessary to amend a notice to correct a factual inaccuracy. For example, where data is processed in the UK, privacy notices may have assured individuals that data is processed exclusively within the EU; this will no longer be true.

In any case, unless transfers from the EEA to the UK post-transition are the first example of an organisation transferring personal data outside the EEA (in which case, the privacy notice change should be drawn to the attention of individuals), it is unlikely to be necessary or appropriate to proactively advise individuals of changes to a privacy notice where this is purely due to technical changes due to Brexit (as opposed to more substantive changes due to Schrems II). EDPB guidance on transparency under the EU GDPR is clear that non-material changes are not required to be brought to the attention of individuals proactively. As such, one would hope not to see another flurry of privacy notices being foisted on individuals as was experienced in the run up to 25 May 2018.

Other documentation may require amendment, again as a consequence of the UK's status as a third country post-transition period. For example, the Article 30 record of processing required under both the EU GDPR and UK GDPR may require update to reflect the international nature of data transfers, and organisations may wish to consider if any data protection impact assessments (DPIA) need to be updated on the same basis.

Is it necessary to relocate or reappoint a DPO?

Despite Brexit, no action is required regarding existing DPOs.

Although the EDPB suggests locating a DPO in the EU, the EU GDPR is silent as to where (geographically) a DPO should be based and simply states that they must: (a) be easily accessible from each establishment for which it performs the role; and (b) have expert knowledge of data protection law.

Equivalent requirements regarding the appointment and nature of a DPO apply under the UK GDPR and therefore, as long as the individual has expert knowledge of UK data protection law (as it develops) and is clearly designated to fulfil both roles, the same person can be appointed to act as a DPO under both regimes.

Is it necessary to appoint a representative?

Under the EU GDPR, as part of its extra-territorial effect, any controller or processor based outside the EEA that processes personal data relating to the offering of goods and services to, or the monitoring of the behaviour of, individuals located in the EEA, must, subject to certain exceptions (including an exception accounting for the frequency and scale of processing, the nature of the personal data and the risk to the rights of the data subjects), appoint a representative in the EEA. This representative should be designated to act on that organisation's behalf and to liaise with supervisory authorities. Therefore:

a) any UK company that offers goods and services to, or monitors the behaviour of, individuals located in the EEA, must consider whether they should appoint a representative in the EEA; and

b) any company that has appointed a representative in the UK with a view to satisfying the requirements of the EEA representative under the EU GDPR should consider relocating or reappointing in the EU.

An equivalent provision applies under the UK GDPR and therefore organisations based outside the UK should now also consider the appointment of a representative in the UK.

Contacts

Jane Finlayson-Brown
Partner – London
Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

Nigel Parker
Partner – London
Tel +44 20 3088 3136
nigel.parker@allenovery.com

David Smith
Special Adviser – London
Tel +44 20 3088 6842
david.a.smith@allenovery.com

Adam Smith
Senior Associate – London
Tel +44 20 3088 7322
adam.smith@allenovery.com

Karishma Brahmbhatt
Senior Associate – London
Tel +44 20 3088 2158
karishma.brahmbhatt@allenovery.com

Emma Keeling
Senior PSL – London
Tel +44 20 3088 2182
emma.keeling@allenovery.com

Filip Van Elsen
Partner – Antwerp
Tel +32 3 287 73 27
filip.vanelsen@allenovery.com

Peter Van Dyck
Partner – Brussels
Tel +32 2 780 25 12
peter.vandyck@allenovery.com

Prokop Verner
Partner – Prague
Tel +420 222 107 140
prokop.verner@allenovery.com

Jakub Cech
Senior Associate – Prague
Tel +420 222 107 157
jakub.cech@allenovery.com

Romaric Lazerges
Partner – Paris
Tel +33 1 40 06 53 44
romaric.lazerges@allenovery.com

Laurie-Anne Ancenys
Counsel – Paris
Tel +33 1 40 06 53 42
laurie-anne.ancenys@allenovery.com

Tina Gausling
Senior Associate – Munich
Tel +49 89 71043 3151
tina.gausling@allenovery.com

Catharina Glugla
Senior Associate – Düsseldorf
Tel +49 211 2806 7103
catharina.glugla@allenovery.com

Balazs Sahin-Toth
Counsel – Budapest
Tel +36 1 429 6003
balazs.sahin-toth@allenovery.com

Livio Bossotto
Employment Counsel – Milan
Tel +39 02 2904 9678
livio.bossotto@allenovery.com

Catherine Di Lorenzo
Counsel – Luxembourg
Tel +352 44 44 5 5129
catharine.dilorenzo@allenovery.com

Nicole Wolters Ruckert
Counsel – Amsterdam
Tel +31 20 674 1401
nicole.woltersruckert@allenovery.com

Anna van der Leeuw-Veiksha
PSL – Amsterdam
Tel +31 20 674 1783
anna.vanderleeuw@allenovery.com

Zuzana Hecko
Senior Associate – Bratislava
Tel +421 2 5920 2438
zuzana.hecko@allenovery.com

Antonio Martinez
Partner – Madrid
Tel +34 91 782 99 52
antonia.martinez@allenovery.com

Krystyna Szczepanowska-Kozlowska
Partner – Warsaw
Tel +48 22 820 6176
krystyna.szczepanowska@allenovery.com

Justyna Ostrowska
Senior Associate – Warsaw
Tel +48 22 820 6172
justyna.ostrowska@allenovery.com

UK
CS2101_CDD-62737_ADD-94689