
## BREXIT AND DATA PROTECTION DECEMBER 2020

*For information about Brexit generally, see Understanding Brexit on our website.*

The United Kingdom and the European Union have – finally – agreed a Brexit trade deal, the draft EU-UK Trade and Cooperation Agreement ("Agreement"). The Agreement sets out the terms on which the EU and UK will trade following the end of the implementation period at 11 p.m. on 31 December 2020 ("IP Completion"). Provided that the Agreement is approved by the UK Parliament and by the EU Member States before IP Completion, it is expected that it will be provisionally applied from IP Completion onwards, until it can be ratified by the European Parliament early in 2021.

### What does the Agreement say about Data Protection?

A. Interim period allowing for seamless data transfers to UK

In the Agreement, the EU and UK both commit to uphold high standards of data protection[1] . However, the Agreement does not deal with the key question of whether the European Commission determines the UK's data protection regime is "adequate" (i.e. equivalent to the EU's), so as to permit free movement of data from the European Economic Area ("EEA") countries to the UK following IP Completion. Such an adequacy decision is a separate process to a trade deal and has been under consideration by the Commission throughout 2020. It does not appear from the Agreement that an adequacy decision permitting EEA to UK personal data transfers will be reached in time for IP Completion.

In the absence of an adequacy decision, in normal circumstances additional safeguards would have been required from 1 January 2021 in order to transfer personal data from the EEA to the UK in accordance with data protection law. **However, the Agreement allows data flows to continue on an interim basis from the EU and the EEA EFTA States[2] to the UK without any such additional safeguards[3]** . This is an important step that avoids the need for organisations to make any last-minute rush to finalise paperwork.

The Agreement provides that, for an interim period of up to six months[4] from 1 January 2021[5], a **"transmission" of personal data from the EEA to the UK shall not be considered as transfer to a third country under EU**

---

[1] See the Agreement Part Six, Title II, Article COMPROV.10(1)
[2] Note that the EEA European Free Trade Association ("EFTA") States of Iceland, Norway and Liechtenstein must actively notify both the UK and EU in writing for the interim provision to apply to transfers from each of their jurisdictions to the UK (*Agreement Part Seven, Article FINPROV.10A(2)*),
[3] See the Agreement Part Seven, Article FINPROV.10A
[4] Four months is the default period; it will automatically be extended by a further two months if required, unless either the UK or the EU unilaterally objects. The interim period will come to an end when it expires after four or six months or when adequacy is granted; whichever is the earlier (*Agreement Part Seven, Article FINPROV.10A(4)*) - this update assumes that this will take place
[5] See the Agreement Part Seven, Article FINPROV.11 for more detail on the date from which the Agreement comes into force; essentially these provisions have effect from the date on which the Agreement is provisionally applied

**law**. Presumably this wording is also intended to cover remote access to EEA data by someone in the UK, which would otherwise be a transfer to a third country. This means that the restrictions on transfer under Chapter V of the General Data Protection Regulation ("GDPR" or "EU GDPR") will not apply to transfers to the UK – essentially, the position on transfers that applied during the Brexit transition period will be preserved on an interim basis.

The intention appears to be that the *Schrems II*[6] requirements - to assess UK laws and ensure that transferred personal data is protected to a standard essentially equivalent to the EU GDPR - will not apply during the interim period, since they are only relevant for transfers to third countries. Organisations would no doubt welcome guidance from supervisory authorities confirming and clarifying this.

However, as a pre-condition for this interim period to apply, the UK has agreed that it will not: (i) change its data protection laws from the form they take as at 31 December 2020; or (ii) exercise certain "designated powers"[7] relating to international transfers without the EU's agreement, which agreement would be given through the newly-constituted Partnership Council[8] . If the UK changes its data protection laws (other than to align with updates to EU data protection law), or exercises any these designated powers without consent, the interim period will automatically come to an end.

B. Adequacy decisions pending

The interim period is presumably intended to allow time for the EU and UK to each unilaterally adopt an adequacy decision, recognising the other jurisdiction as offering adequate protection for transferred personal data[9].

In relation to UK to EEA transfers, the UK has already announced that it will initially treat the EEA countries as adequate for the purpose of UK to EEA transfers, but that it will keep this under review. There appears to be no reason why the UK would depart from its initial position, although the Agreement clearly shows a desire to underline the UK's sovereignty in this regard.

In relation to transfers from the EEA to the UK, adequacy is by no means guaranteed, as there are clearly elements of the UK's data processing regime which may cause the Commission concern (for example, regarding national security processing, particularly in light of the CJEU decision of 6 October 2020 in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others (C-623/17)*, which casts doubt on whether the UK's regime permitting the retention and transmission of bulk data for national security purposes is compatible with EU law.

However, given that the GDPR will be brought into UK national law by virtue of the European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 ("DPA 2018"), there is reason to hope that an adequacy decision may be achievable within this six-month interim period.

C. Other data protection provisions in the Agreement

The Agreement also sees the UK and EU each committing not to adopt any data localisation requirements[10] and it provides for the sharing of Passenger Name Records and criminal record information, as well as cooperation on

---

[6] See the CJEU decision in *Data Protection Commissioner v Facebook Ireland Limited & Maximillian Schrems (C-311/18)* (and see further below)

[7] The "designated powers" that the UK must only exercise with EU consent during the interim period include the power for the Information Commissioner's Office to publish standard contractual clauses for international transfers of personal data from the UK and to approve new codes of conduct, certification mechanisms or Binding Corporate Rules that can be relied upon to make international transfers of personal data.

[8] The Partnership Council will comprise EU and UK representatives and its role will be to oversee the Agreement – see the Agreement Part One, Title III, Article INST.1

[9] Each side will actually need to make two adequacy decisions, since adequacy is required for transfers under the Law Enforcement Directive, as well as under the GDPR.

[10] See the Agreement Part Two, Title III, Article DIGIT.6(1)(b)

DNA, fingerprint and vehicle registration data[11]. To reinforce the mutual commitment to high standards of data protection, either side may unilaterally suspend all or any part of the law enforcement and judicial cooperation provisions in Part Three if there are "serious and systemic deficiencies" in the other side's data protection requirements, including (but not limited to) where an adequacy decision has been revoked by either side[12]. This underlines the importance given in the Agreement to upholding the fundamental right to personal data protection.

D. The trouble with Legacy Data

As there is not (yet) any formal adequacy decision in place, it should also be noted that Article 71(1) of the Withdrawal Agreement[13] will apply immediately from IP Completion. This requires UK organisations to continue to comply with the **EU** (not UK) GDPR - in its form as at 31 December 2020 - in relation to the personal data of non-UK data subjects: (i) already processed under EU law before IP Completion; or (ii) processed from IP Completion on the basis of the Withdrawal Agreement, for example pursuant to a provision of EU law that applies in the UK by virtue of the Withdrawal Agreement, such as its provisions on citizens' rights) ("Legacy Data").

This highly technical issue is unlikely to make much practical difference to the requirements for UK controllers and processors, as the UK is required not to change its laws from their form as at 31 December 2020 as a precondition of the interim period for transfers. This means that the EU and the UK versions of the GDPR are highly likely to stay aligned.

However, organisations may still need to be able to identify which version of the GDPR applies to any given piece of data, as there may be minor differences – for example, UK courts would still need to pay "due regard" to any CJEU decisions made after IP Completion in relation to Legacy Data[14], whereas they would not need to do so in relation to other personal data. If an adequacy decision is granted then the Legacy Data requirements are disapplied and UK organisations may simply apply the UK GDPR to all of their data, including Legacy Data.

## Data Protection: what will (and will not) change from 1 January 2021, and what areas of uncertainty are there?

The European Union (Withdrawal) Act 2018 (as amended by the European Union (Withdrawal Agreement) Act 2020) (together, "Withdrawal Act") incorporates the body of EU law as at "IP completion day" - 31 December 2020 - into UK law. In addition, at 11 p.m. on 31 December 2020 (IP Completion) the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020) (together, "Exit Regulations") come into force. The Exit Regulations amend the GDPR to ensure that it operates in a UK-specific context from the end of the Implementation Period. The amended version is referred to as the "UK GDPR". The DPA 2018 will continue to apply, but minor changes will be made to it by the Exit Regulations to implement the UK GDPR as from IP Completion.

In practice, this means that, as from IP Completion at 11 p.m. on 31 December 2020, EU data protection law continues to apply in the UK in the same way as before. There are few substantive changes to the obligations that most organisations must comply with in relation to data protection issues. Three areas of change are nevertheless

[11] See the Agreement Part Three, Titles II (DNA, fingerprints and vehicle registration data, Title III (PNR) and TItle IX (criminal record data), as summarised in the eu-uk_trade_and_cooperation_agreement-a_new_relationship_with_big_changes-brochure.pdf (europa.eu)
[12] See the Agreement Part Two, Title XII, Article LAW.OTHER.137(2)
[13] See the Withdrawal Agreement: *Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community Vol 1*
[14] See Article 4(5) of the Withdrawal Agreement

worth highlighting, which will apply from IP Completion: (1) data transfers; (2) appointment of EU/UK representatives; and (3) the role of the ICO and the one-stop-shop mechanism.

## Data transfers

During the transitional period prior to IP Completion, personal data could still be freely transferred between the UK and the rest of the EEA, with no requirement to enter into transfer safeguards. Under the Agreement, this position is being extended for an interim period of up to six months from 31 December 2020, provided that (i) the UK's data protection laws continue to apply in their form as at 31 December 2020; and (ii) the UK does not exercise certain "designated powers" relating to the permitted mechanisms for international transfers of personal data without the EU's agreement. The extent to which this position changes following the expiry of that interim period depends on which direction the personal data is flowing, and whether an adequacy decision has been reached or not.

For transfers from the UK to the EEA, nothing should change following the interim period, provided that the UK continues to adhere to its stated initial position that all EEA countries will be considered adequate for the purposes of the UK GDPR. Existing adequacy decisions will also, under amendments made to the DPA 2018 by the Exit Regulations, be preserved. Data transfers from the UK to the EEA and to those countries with existing adequacy decisions will therefore be able to continue without any necessary additional safeguards. Each of the 12 non-EEA jurisdictions that currently benefit from an EU adequacy decision (except Andorra, negotiations pending) has also confirmed that data transfers from them to the UK can continue without further safeguards post-IP Completion.

For transfers from the EEA to the UK, following expiry of the Implementation Period **plus** the added interim period of up to six months following IP Completion, if no adequacy decision has yet been made in respect of the UK, transfers of data from the EEA to the UK will need to be based on safeguards such as standard contractual clauses or binding corporate rules, or alternatively to rely on derogations for occasional transfers, such as that they are necessary for the performance of a contract.

In the absence of an adequacy decision for the UK, Article 71 of the Withdrawal Agreement will also apply from IP Completion as set out above. It will apply the EU (rather than the UK) GDPR as it stands at 31 December 2020 to any Legacy Data (personal data of non-UK data subjects processed under EU law before IP Completion, or processed from IP Completion on the basis of the Withdrawal Agreement). If there is UK adequacy, this falls away and processing can continue under the UK GDPR.

Transfers to the UK would not require additional safeguards or derogations if an adequacy decision is made.

## Appointment of EU/UK representatives

UK-based controllers or processors who do not have a branch, office or other establishment in any EU or EEA state but remain subject to the EU GDPR as they either (i) offer goods or services to; or (ii) monitor the behaviour of individuals in the EEA must, following IP Completion, appoint a representative within the EEA, as they will no longer be an EEA-based controller or processor. This position is not affected by the Agreement.

The UK GDPR, like its EU counterpart, has extra-territorial effect. Consequently, it requires that any non-UK-based controller or processor must appoint a UK representative if it processes personal data relating to the offering of goods and services to, or the monitoring of the behaviour of, individuals located in the UK. This applies as from the end of the Implementation Period, which is again unaffected by the interim period for transfers to the UK under the Agreement.

## The role of the ICO and the one-stop-shop mechanism

Controllers or processors who carry out "cross-border processing" under the GDPR – that is, processing of personal data which substantially affects or is likely to substantially affect data subjects in more than one EU/EEA state – in theory only need to deal with a single EEA data protection authority (albeit others may seek to get involved in enforcement in some circumstances). This lead supervisory authority will be the relevant authority in the state in which the organisation has its "main establishment". The benefit of the so-called "one-stop-shop" mechanism is that, subject to a few exceptions, organisations will only be investigated by one supervisory authority and will only receive one fine across the EEA.

Following IP Completion, the ICO will no longer participate in the "one-stop-shop" mechanism. Organisations that continue to be involved in processing across the EU should therefore have considered which other EU/EEA supervisory authority will be their lead authority.

The spectre of dual fines may also be on the horizon. Take, for instance, a supplier with one establishment in the UK (its headquarters) and one establishment in Spain (its distribution centre), both of which process personal data originating from across the EU. Before IP Completion, the UK would have been treated as the "main establishment" and the UK ICO would have been the lead authority in enforcing the GDPR across the EU. Following IP Completion, the supplier's only EU establishment will now be in Spain, so the Spanish supervisory authority will be the lead authority for the purposes of the EU GDPR. In the event of a data breach affecting data processed by the supplier involving both UK and EU customers, the supplier will face investigations (and potentially fines) from both the ICO (under the UK GDPR) and the Spanish supervisory authority (under the EU GDPR).

## What are the key issues arising from any changes or uncertainty, and what basic things should be done to address them?

## Transfers from the EEA to the UK

In respect of transfers from the EEA to the UK, following expiry of the post-Implementation Period interim period (of up to six months) and if no adequacy decision has yet been made in respect of the UK, such transfers will need to be based to be based on one of the following safeguards:

- EU standard contractual clauses. These data transfer agreements offer the additional adequate safeguards with respect to data protection that are needed when transferring personal data to a third country. The UK Government has confirmed that it will continue to recognise the European Commission-approved standard contractual clauses for use for transfers from the UK. It should be noted that the Commission is in the process of updating its standard contractual clauses, and it is not yet known whether the UK will recognise and adopt the new Commission versions to safeguard exports from the UK, or whether it will develop its own.

- Binding corporate rules (BCRs). These are internal policies and procedures authorised by relevant data protection authorities which legitimise intra-group transfers, and will in future be available both under the EU GDPR ("EU BCR") and under the UK GDPR ("UK BCR"). Existing authorisations of binding corporate rules made by the Information Commissioner will continue to be recognised in domestic law and BCRs covering a UK-based entity that were authorised before IP Completion will continue to provide an appropriate safeguard for personal data transfers from the EEA to the UK. Holders of EU BCR authorised before the end of the transition period can apply to have UK BCR confirmed, but those with the ICO as their BCR lead supervisory authority should have already moved to a new BCR lead supervisory authority before IP Completion. EU BCRs should have been updated to list the UK as a third country outside the EEA.

Following the CJEU decision in *Data Protection Commissioner v Facebook Ireland Limited & Maximillian Schrems (C-311/18)*, if you are relying on the above transfer safeguards - rather than an adequacy decision - to make a transfer of personal data to a third country, you will **also** need to ensure that you assess whether the data being transferred to the UK can be protected to a standard that is essentially equivalent to that it enjoys under the GDPR. You must consider in particular whether the UK's legal regime permits disproportionate access by public authorities for national security purposes. Such an assessment should be documented and if you decide that the data cannot be properly protected to GDPR standards, you must not transfer it.

Clearly, exporters may find it problematic to assess that a transfer could be appropriately safeguarded if the Commission had failed to find that the UK's laws were "adequate" for data protection purposes. However, it's important to remember that the assessment should take into account how the UK's laws apply to the particular transfer in question. For more information, see our updates: *Privacy Shield invalid: what next for international data transfers?* and *International personal data transfers: EDPB guidance and new Standard Contractual Clauses*.

You may also rely on one of the other derogations set out in the GDPR (consent or necessity for a contract, for example), however, these derogations should only be relied on in limited cases where the transfer in question is occasional and non-repetitive.

## Requirement to appoint an EU/UK representative

Organisations should consider whether they need to appoint an EU and/or UK representative.

If you (i) do not have branches, offices or other establishments in the EU or EEA but you remain subject to the EU GDPR as you (ii) offer goods or services to individuals in the EEA or monitor the behaviour of individuals located in the EEA, you must appoint an EEA representative. For example, an organisation which has to date only had a single EU/EEA outpost in the UK – and has accordingly had no need for an EU representative – will need to have appointed one from IP Completion.

The representative will need to be set up in an EU or EEA state where some of the individuals whose personal data is being processed are located.

The representative will need to be authorised in writing to act on behalf of the UK-based client regarding their GDPR compliance, and to deal with any supervisory authorities or data subjects on the client's behalf.

The representative may be an individual, or a company or organisation established in the EEA, and must be able to represent the client in respect of its obligations under the GDPR (e.g. a law firm, consultancy or private company).

Following IP Completion, if you are a non-UK controller but you process personal data relating to the offering of goods and services to, or the monitoring of the behaviour of, individuals located in the UK, you should have appointed a UK representative. This appointment should have been made in line with the requirements of the UK GDPR (which closely follow the EU GDPR).

Third country organisations may need **both** a UK and an EU representative, if the extra-territoritality provisions of the GDPR and the UK GDPR apply to them.

## The role of the ICO and the one-stop-shop mechanism

If your lead supervisory authority was the ICO, and you continue to engage in EU cross-border data processing, make sure you are clear on whom your lead supervisory authority within the EU is following IP Completion. This will depend on the location of your "main establishment" in the EU/EEA, typically where your central administration – a headquarters, for example – exists. However, if decisions about the purposes and means of EU personal data processing take place separately from the place of central administration, then it will likely be this establishment

which will be deemed the "main establishment" for the purposes of identifying your lead supervisory authority. "Forum shopping" is not permitted.

## How have other companies/the market been dealing with these issues?

Companies have been reviewing their data flows to understand whether any personal data transfers from the EEA to the UK are carried out, and have prepared EU standard contractual clauses to ensure that these data flows can continue after the post-IP Completion interim period set out in the Agreement, should there be no adequacy decision for the UK. It would also be wise to map data flows in the opposite direction, given that the UK has the power under the UK GDPR to make its own adequacy decisions in relation to each of the EEA states.

Where companies already have agreements based on standard contractual clauses or binding corporate rules in place, they are considering whether any updates need to be made to take account of Brexit and ensure that intragroup cross-border transfers of personal data can carry on unimpeded after the UK's exit from the EU. Those with the ICO as their EU BCR lead supervisory authority should have obtained authorisation from an EU BCR lead supervisory authority before IP Completion in order to continue to use them for EU GDPR purposes.

In addition to the above, companies are considering whether it is necessary for them to appoint a representative in the EEA and/or the UK and taking steps to prepare for making such appointment.

Organisations have also been updating their privacy notices to include details of any newly-appointed EEA or UK representatives. Privacy notices should also accurately describe data flows in light of Brexit – for example, they may now need to specify that data is being transferred to or stored in the UK, as well as EU Member States. Contracts may also need to be updated; for example where they restrict the processing of personal data "outside of the EEA", on the (now outdated) assumption that the UK is part of the EEA.

## What relevant materials do we have on our website?

Our Brexit page, Understanding Brexit, contains links to our Data Protection bulletins, which cover Brexit and related developments.

## Contact us

Naomi Leach
Partner
T: +44 20 7809 2960
E: naomi.leach@shlegal.com

Katie Hewson
Senior associate
T: +44 20 7809 2374
E: katie.hewson@shlegal.com