



Data protection

APRIL 2020

The UK formally left the EU on 31 January 2020 and the transition period established under the Withdrawal Agreement (called the "implementation period" in UK legislation) is due to end on 31 December 2020. This section of our legal guide considers the position both during and after transition in relation to issues of data protection. The main changes will come at the end of the transition period, but in the meantime data is treated the same way as when the UK was a Member State of the EU and EU law continues to be applied in the UK. Once the transition period ends, there will be significant changes and, in particular, unless and until the UK is recognised by the EU as providing adequate data protection, it will be treated by EEA States as a third country and measures will need to be taken by proposed exporters of personal data in the EEA to ensure that adequate protections are in place whenever personal data is being sent to UK recipients.

Data transfers

During the transition period, there is no change to the current position with respect to data transfers – data can be freely transferred between the UK and the EU as the General Data Protection Regulation ("GDPR") continues to apply.

Following the transition period, unless a trade deal is agreed, the UK Government's [no-deal technical note](#), combined with the various Brexit statutory instruments enacted under the [Withdrawal Agreement](#), confirm the following in respect of international transfers of personal data:

- **Transfers from the UK to the EEA:** The UK will recognise all EEA states, EU and EEA institutions, and Gibraltar as providing an adequate level of protection for personal data, meaning that personal data can flow freely from the UK to these jurisdictions. The UK will, however, keep this under review and therefore the UK Government could decide in future that certain Member States do not provide adequate protection and restrict the flow of data to those countries.
- **Transfers from the UK to "adequate" countries outside the EEA:** The UK will preserve the effect of existing EU adequacy decisions for a transition period, meaning

The section is part of our [Brexit Legal Guide](#).

Withdrawal Agreement/ transition period

- Following the UK's withdrawal from the European Union on 31 January 2020, the [Withdrawal Agreement](#) now sets out arrangements for the transition period from 11 pm GMT on 31 January 2020. UK legislation calls this the "implementation period". The transition period is due to end on 31 December 2020 and, as yet, there is no indication that the current COVID-19 pandemic will result in any extension of the transition period. The Withdrawal Agreement would allow an extension until the end of 2021 or 2022, but the UK Government has legislated to prevent Ministers agreeing an extension and it would require further UK legislation, if this position were to be changed.
- The non-binding [Political Declaration](#) on the future relationship between the UK and the EU accompanies the Withdrawal Agreement.

that personal data will be able to flow from the UK to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

The EU - US Privacy Shield currently provides an adequate level of protection to permit the flow of personal data from the EEA to the US. [The Data Protection, Privacy and Electronic Communications \(Amendments etc.\) \(EU Exit\) \(No 2\) Regulations 2019 \(SI 2019/484\)](#) confirm that the UK Government will preserve the effect of the existing Privacy Shield, so that US organisations registered to the privacy shield will continue to be protected under the framework after the UK ceases to be bound by the GDPR. However, Privacy Shield listed companies in the US will need to include a public commitment in their privacy policies to comply with the Privacy Shield principles where the personal data is transferred from the UK to the US. The Government has stated that this will be on a transitional basis, allowing the UK to potentially agree its own Privacy Shield with the US in the future.

- **Transfers from the UK to third countries outside the EEA:** Transfers from the UK to third countries will continue to be restricted under the UK GDPR, meaning that organisations will need to satisfy one of the specified conditions to legitimise such transfers.

The UK Government has confirmed that the current [EU Standard Contractual Clauses](#) will continue to be an effective basis for international data transfers from the UK to a third country under the UK GDPR. However, under the draft regulations, the ICO will also have the power to issue new Standard Contractual Clauses after exit day.

- **Transfers from the EEA to the UK:** The EDPB confirmed in its general information note on [data transfers under the GDPR](#) that in the event of a no-deal Brexit, organisations must comply with the GDPR when transferring personal data from the EEA to the UK, which will become a "third country" for GDPR purposes from exit day. The note states that no new or additional safeguards are contemplated by the EDPB. If the European Commission were to adopt an **adequacy decision** in respect of the UK (determining that the UK ensures an adequate level of protection of personal data under its domestic law or international commitments), this would provide organisations with the simplest and least administratively burdensome option for transfers between the EEA and the UK. The

[Political Declaration](#) confirms that the EU Commission will commence its adequacy process as soon as possible with respect to the UK. However, the European Data Protection Supervisor ("**EDPS**"), Wojciech Wiewiórowski recently noted that the UK is "13th in the row" for an adequacy decision. Even though the EDPS does not participate directly in adequacy decisions, his comments may indicate a general reluctance to let the UK skip the queue in terms of an adequacy decision.

The effect of the EU position is that where an EEA business wishes to send personal data to a UK recipient, it will need to have adequate protections in place, likely to be in the form of a contract between the EEA exporter and the UK importer, incorporating the EU standard contractual clauses, at least unless and until an adequacy decision has been made by the EU which covers the intended data supply.

Extra-territorial effect/dual legislative regimes

Even after the transition period, the extra-territorial nature of the GDPR means that it will directly apply to UK organisations processing personal data about data subjects in the EEA in connection with offering them goods or services, or monitoring their behaviour.

Therefore post-transition, UK organisations may still need to comply with the GDPR when trading with the EEA and will also need to comply with the UK GDPR. Vice versa, non-UK organisations trading with the UK in the same way will potentially need to comply with the UK GDPR, in addition to the existing EU GDPR.

In essence, pan-European organisations are likely to have to comply with two separate, but similar legislative regimes, with the consequential risk of dual enforcement action in the event of any breach.

Role of the UK ICO

According to the updated ICO guidance on Brexit, during the transition period the ICO will continue to engage in the co-operation and consistency mechanism under GDPR and continue to be a lead supervisory authority.

However, whilst the [ICO's Brexit guidance](#) states that the UK Government "will continue to work towards maintaining the close working relationships between the ICO and the EU supervisory authorities once the UK has left the EU", the UK regulator is expected to take on a very limited European role following Brexit. The ICO would no longer form part of

- Data protection features in both the Withdrawal Agreement and the Political Declaration, reflecting the significance of data protection rules and data flows between both the EU and the UK.
- The position with respect to data protection is effectively "business as usual" during the transition period with the GDPR continuing to apply in the UK.

At the end of the transition period

- The position following the transition period will depend upon whether or not a new trading relationship is agreed between the UK and the EU. Both sides have set out their respective [negotiating positions](#). The [EU has published](#) its version of the draft EU-UK FTA and the UK has sent its draft to the EU, but has not yet released it publicly - for further updates, please [subscribe](#) to our [Brexit blog](#). However, there will be no clarity as to what will happen until towards the end of 2020 and the adage "plan for the worst, hope for the best" continues to apply. See accompanying section: [Leaving the EU: The process and preparations](#).
- In the event that no trading relationship is agreed prior to the end of the transition period:
 - direct applicability of the GDPR in the UK will end, although this cannot prevent the GDPR's extra-territorial reach where applicable under EEA laws; and
 - the [UK Withdrawal Act 2018](#) will incorporate the GDPR, as supplemented and amended by related Brexit secondary legislation (including the [draft Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) \(No.2\) Regulations 2019](#)) into domestic UK law as part of "retained EU law": see accompanying section: [The UK's new legal order post-Brexit: A new class of UK law](#).
- The fundamental data protection principles, obligations on organisations and rights for individuals will remain broadly the same under UK law (the "**UK GDPR**").

the regulatory co-operation and co-ordination mechanisms under the GDPR and will therefore no longer have a seat on the EDPB.

Following the transition period, the ICO will also no longer be able to act as a "lead supervisory authority" for pan-European organisations with their European headquarters in the UK. Affected organisations will therefore need to consider their European footprint and whether there is an alternative supervisory authority within the EEA that could take on responsibility for enforcing the GDPR in respect of cross-border processing instead or whether the organisation is no longer able to take advantage of the "one stop shop" under the GDPR.

The draft Brexit statutory instruments do, however, provide the ICO with certain powers in respect of the UK GDPR (eg to authorise UK binding corporate rules).

"At least in the short term, data protection laws in the UK will likely replicate the EU regime as much as possible following the transition period. However, in the long term, it is possible that there may be divergence, particularly as the Government potentially takes steps to foster innovation and technology in the UK, often perceived to be "blocked" by GDPR barriers"

MIRIAM EVERETT

Key contacts



Miriam Everett

Partner, Head of Data Protection and Privacy
T +44 20 7466 2378
miriam.everett@hsf.com



Duc Tran

Senior Associate
T +44 20 7466 2954
duc.tran@hsf.com