The Information Commissioner's Office

Data protection if there's no Brexit deal

September 2019

ico.
Information Commissioner's Office

About this guidance

Does this guidance apply to us?

If you're new to this topic, go to www.ico.org.uk/no-deal first for an overview of the key points you need to know and practical guidance to help you prepare for a no-deal Brexit.

This guidance explains data protection and Brexit in more detail. Read it if you have detailed questions not answered in our other resources, or if you need a deeper understanding of data protection law and how it will change if we leave the EU without a deal.

It is particularly relevant to UK businesses and organisations that rely on international data flows, target European customers or operate inside the EEA.

This guidance is aimed primarily at DPOs and those with specific data protection responsibilities. It is not aimed at individuals and, if needed, we will provide guidance for individuals in due course.

Other resources

Data protection after a no-deal Brexit: check what you need to do (for small businesses)

Keep data flowing from the EEA to the UK – interactive tool

Law enforcement processing and Brexit – five steps to take

Information rights and Brexit – FAQs

The GDPR

Does this section apply to us?

This section applies if:

- you are a UK-based business or organisation; and
- the GDPR currently applies to your processing of personal data.

How can we prepare?

When planning for a no-deal exit, you can use our guidance to assess the impact of legal changes in a few key areas:

- international data transfers;
- EU representatives;
- EU regulatory oversight of any cross-border processing; and
- minor updates to documentation and accountability measures.

Will the GDPR still apply?

The GDPR is an EU regulation. This means it became law in all member states of the EU (including the UK), without the need for a UK Act of Parliament. It also applies to the EEA states.

When the UK exits the EU, the EU GDPR will no longer be law in the UK. However, the UK government intends to write the GDPR into UK law, with the necessary changes to tailor its provisions for the UK (the 'UK GDPR'). It will sit alongside an amended version of the DPA 2018. The government has published a 'Keeling Schedule' for the UK GDPR, which shows the planned amendments.

The key principles, rights and obligations will remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA.

The UK government intends that the UK GDPR will also apply to controllers and processors based outside the UK if their processing activities relate to:

- offering goods or services to individuals in the UK; or
- monitoring the behaviour of individuals taking place in the UK.

There are also implications for UK controllers who have an establishment in the EEA, have customers in the EEA, or monitor individuals in the EEA. The EU GDPR will still apply to this processing, but the way you interact with European data protection authorities will change.

This guidance covers the key new issues you need to consider regarding international data flows and cross-border processing.

Otherwise, you should continue to follow our existing guidance on your general data protection obligations.

Further reading

For more information about how other legislation we regulate is affected by a no-deal Brexit, see Information rights and Brexit – FAQs.

International data transfers

Does this section apply to us?

This section applies if you are a UK-based business or organisation subject to the GDPR and you transfer personal data to or from other countries (including European countries).

This section does not apply to you if:

- you never transfer personal data outside the UK and never receive personal data from outside the UK; or
- you only transfer personal data outside the UK to consumers or only receive personal data from outside the UK directly from consumers.

Examples

A hairdresser in Cheshire has a client database which it uses for bookings and marketing. It stores this database on its office computer. It has never sent any of its client data outside the UK and has no intention of doing so. The hairdresser does not need to consider this section on international transfers.

A hotel in Cornwall takes direct bookings from individuals across the EEA, which includes their names, addresses and other personal information. It receives personal data from those individuals and sends personal data back to them. Neither transfer is restricted under the GDPR nor UK GDPR, as it is made directly with a consumer. The hotel does not need to consider this section on international transfers.

However, if either business uses a cloud IT service which stores and/or processes their data (including personal data) anywhere outside the UK (including in the EEA), it should read this section on international transfers.

How can we prepare?

- The first thing is to look at what you do now. Understand your international flows of personal data. Key transfers to identify will be from the EEA to the UK.
- While all transfers have to be considered, you may want to prioritise transfers of large volumes of data, transfers of special category data or criminal convictions and offences data, and your business-critical transfers.
- Consider how you may continue to receive these transfers lawfully after exit date. Usually the simplest way to provide an appropriate safeguard for a restricted transfer from the EEA to the UK is to enter into standard contractual clauses with the sender of the personal data.

We have an interactive tool to help you decide: Do I need to use standard contractual clauses for transfers from the EEA to the UK? We also have template contracts you can use:

- Controller to controller
- Controller to processor

If you prefer, you can use our contract builder to automatically generate the contract. You will need detailed information about the purposes, scope and context of the processing to hand:

- Build a controller to controller contract
- Build a controller to processor contract

Multinational corporate groups should also consider their use of existing EEA-approved binding corporate rules to make transfers into and out of the UK. These will need updating to reflect that, under the EU GDPR, the UK becomes a third country on exit date.

You can continue to make transfers of data from the UK to the EEA under UK adequacy regulations, but you should update your documentation and privacy notice to expressly cover those transfers. Transfers from the UK to other countries can continue under existing arrangements.

If you are receiving personal data from a country, territory or sector covered by a European Commission adequacy decision, the sender of the data will need to consider how to comply with its local laws on international transfers. Check local legislation and guidance, and seek legal advice if necessary.

What are the key changes?

On exit date there will be two sets of rules to consider:

- First, the UK rules on transferring data outwards from the UK.
- Second, the impact of EU transfer rules on those sending you personal data from outside the UK (including from the EEA) into the UK.

In both cases, you can transfer personal data if it is covered by an adequacy decision, an appropriate safeguard or an exception.

If you transfer personal data outside the EEA now, you should already have in place arrangements for making a restricted transfer under the GDPR. Further detail is provided in the international transfers section of our Guide to GDPR. You won't need any new arrangements for transfers from the UK, but you need to put in place safeguards to maintain data flows from the EEA into the UK.

How can we transfer data from the UK?

This section applies if you are sending personal data outside the UK

You are making a restricted transfer outwards from the UK if:

- the UK version of the GDPR applies to the processing of the personal data you are transferring;
- the UK GDPR does not apply to the importer of the data, usually because they are located in a country outside the UK (which may be in the EU, the EEA or elsewhere); and
- you, the sender of the personal data, and the receiver of the data are separate organisations (even if you are both companies in the same group).

Example

A UK company passes employee information to a centralised group human resources service provided by its parent company in Germany. After the UK exits the EU, this will be a restricted transfer under the UK GDPR.

The UK is England, Scotland, Wales, and Northern Ireland. It does not include Crown dependencies or UK overseas territories, including Gibraltar.

The UK government has stated that, after Brexit, transfers of data from the UK to the EEA will be permitted. It says it will keep this under review.

The UK government will allow transfers to Gibraltar to continue.

If your restricted transfer is not to the EEA, you should already have considered how to comply with the GDPR. You will continue to be able to rely on the same mechanisms. In particular:

Adequacy decisions

- You will be able to make the restricted transfer if it is covered by new UK adequacy regulations. Adequacy regulations confirm that a particular country or territory (or a specified sector in a country or territory) or international organisation, has an adequate data protection regime.
- The UK government intends to recognise the EU adequacy decision made by the European Commission before the exit date. This will allow restricted transfers to continue to be made to most organisations, countries, territories or sectors covered by an EU adequacy decision.
- Specific UK arrangements have now been confirmed regarding the recent EU adequacy decision for Japan. This secures the necessary protections for UK data as well as EU data, so that data can continue to flow from the UK to Japan.
- Modified arrangements will apply regarding the EU adequacy decision for the EU/US Privacy Shield, as this is an EU/US-specific arrangement. The UK government is making arrangements for its continued application to restricted transfers from the UK to the USA and there is further information on the US government's Privacy Shield website. If the UK exits the EU without the Withdrawal Agreement ('no deal'), then you as a UK business will continue to be able to transfer personal data to US organisations participating in the Privacy Shield if they have updated their public commitment to comply with the Privacy Shield to expressly state that it applies to transfers of personal data from the UK.
- After a no-deal Brexit, you as a UK organisation wishing to continue to make transfers to US organisations under the Privacy Shield will need to check that they have made the necessary update to their commitment to comply with the Privacy Shield. You can usually confirm this simply by checking the US organisation's publicly available privacy policy.

Appropriate safeguards

- If no adequacy decision covers your restricted transfer, you should consider putting in place one of a list of appropriate safeguards to cover the restricted transfer.
- For most businesses, a convenient appropriate safeguard is the use of standard contractual clauses.

The UK government intends to recognise EC-approved standard contractual clauses as providing an appropriate safeguard for restricted transfers from the UK. We have template contracts you can use:

- Controller to controller
- Controller to processor

Example

A UK travel company organises educational visits overseas for schools. It sends personal data of those going on the trips to hotels in Spain, Uruguay and Mexico. The travel company, the schools and each hotel are separate controllers as each is processing the personal data for its own purposes and making its own decisions. The personal data of students is passed from the schools to the UK company and then to the hotels. The travel company is making a restricted transfer to the hotels. It does not need to take additional steps when transferring personal data to:

- the Spanish hotel (as the UK government will recognise EEA countries as ensuring an adequate level of data protection under UK law); and
- the Uruguayan hotel (as the UK government will recognise the EC's adequacy decision regarding Uruguay).

To transfer personal data to the Mexican hotel, the company will need to take additional steps to comply with the provisions on restricted transfers in the UK GDPR. The most appropriate action is likely to be using standard contractual clauses.

- For restricted transfers from a UK public body to a non-EEA public body, where one party is unable to enter into a binding contract, an appropriate safeguard may be an administrative arrangement between these bodies which has been approved by the ICO.
- For restricted transfers from the UK but within a corporate group or to a group of overseas service providers, another convenient method of providing an appropriate safeguard is binding corporate rules.
- The UK government will recognise binding corporate rules authorised under the EU process **before** the exit date as ensuring appropriate safeguards for transfers from the UK. On that basis, if on exit date you have in place binding corporate rules within your organisation covering the UK sender of data and the receiver (wherever located), the personal data may be sent. You will need to update your EEA binding corporate rules, so that the UK is listed as a third country outside the EEA.
- Other contractual or policies-based mechanisms may provide appropriate safeguards, but so far none have been approved.

Exceptions

If there is no adequacy decision and no appropriate safeguards, but one of the list of exceptions under the EU GDPR applies, you will be able to make the restricted transfer. These exceptions will continue under the UK GDPR.

How can we maintain transfers from the EEA into the UK?

This section applies if you are receiving personal data from the EEA

The EU GDPR will continue to apply to an EEA sender of personal data. To help you understand the obligations on the EEA sender of the personal data to you in the UK, you can use our guidance on international transfers. You should bear in mind that on exit date the UK will be a third country outside the EEA.

The European Data Protection Board (EDPB) has also published an information note on data transfers under the GDPR in the event of a no-deal Brexit.

The EDPB is still finalising detailed guidance on international transfers more generally. We advise you to take a broad interpretation of a restricted transfer, which is that you are receiving a restricted transfer if you are a controller or processor located in the UK and an EEA-located controller or processor sends you personal data.

Under the GDPR, an EEA controller or processor will be able to make a restricted transfer of personal data to the UK if any of the following apply:

Adequacy decisions

- The EEA controller or processor will be able to make a restricted transfer to the UK if it is covered by an EC adequacy decision.
- If we leave the EU without a deal, at exit date there will not be an EC adequacy decision regarding the UK. We will keep you updated as to any plans by the UK Government and the EC regarding an adequacy decision.

Appropriate safeguards

- If there is no EC adequacy decision regarding the UK, but the EEA sender has put in place one of the EU GDPR list of appropriate safeguards, the EEA sender will be able to make the transfer to you.
- For most businesses a convenient appropriate safeguard is standard contractual clauses. We have an interactive tool to help you decide: Do I need to use standard contractual clauses for transfers from the EEA to the UK? We also have template contracts you can use:
  - Controller to controller
  - Controller to processor

For restricted transfers from an EEA public body to a UK public body, where one of the parties is unable to enter into a contract, an appropriate safeguard may be provisions inserted into an administrative arrangement between these bodies. This will need to be authorised by the data protection supervisory authority with oversight of the EEA public body.

Example

A UK regulator makes a request to an EEA counterparty for information about the good standing of an individual who has moved to the UK. The EEA regulator is not able to enter into contracts. The two regulators could agree to an appropriate administrative arrangement, which would need to be approved by the EEA supervisory authority of the EEA counterparty.

- If you have in place binding corporate rules covering a UK-based entity, which are authorised under the EU process before the exit date, this will continue to provide an appropriate safeguard for personal data transfers from the EEA to the UK.
- Those binding corporate rules would 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.
- The EDPB has published an information note on BCRs which have the ICO as the BCR lead supervisory authority.

Exceptions

If there is no EC adequacy decision regarding the UK and no appropriate safeguards, but one of the list of EU GDPR exceptions applies, your EEA sender will be able to transfer personal data to you. However, in line with EDPB guidance, these must be interpreted restrictively and mainly relate to transfers that are occasional and non-repetitive.

- If there is a medical emergency and you need the data to give medical care to avoid a risk of serious harm to an individual, and the individual is (physically or legally) unable to give consent, then you will be able to rely on an exception. The sender may go ahead and make the transfer on this basis.
- The other exceptions are very limited. Broadly, they cover:
  - the individual's explicit consent;
  - an occasional transfer to perform a contract with an individual;
  - an occasional transfer for important reasons of public interest;
  - an occasional transfer to establish, make or defend legal claims;
  - transfers from public registers; or
  - a truly exceptional transfer for a compelling legitimate interest.
- It is up to the sender in the EEA to decide whether they think an exception applies.

How can we maintain transfers into the UK from countries, territories or sectors covered by an EC adequacy decision?

This section applies if you are receiving personal data from one or more of the following:

Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Isle of Man, Israel, Japan (private-sector organisations only), Jersey, New Zealand, Switzerland, Uruguay, or USA (under Privacy Shield only).

These are the countries, territories or sectors that the European Commission has made a finding of adequacy about.

To have received and to maintain an adequacy decision, the country or territory is likely to have its own legal restrictions on making transfers of personal data to countries outside the EEA. This will include the UK on its exit from the EU.

UK officials are working with these countries and territories to make specific arrangements for transfers to the UK where possible. See the 'other resources' box below for links to the latest information on specific arrangements in each territory (where available).

Otherwise, if you wish to continue receiving personal data from these countries or territories, you and the sender of the data will need to consider how to comply with local law requirements on transfers of personal data, and seek local legal advice.

Other resources

For more information, please check legislation and guidance from the supervisory authority in the sender's country, or seek your own legal advice. These links provide information on specific arrangements in:

- Argentina: resolution (only available in Spanish)
- Canada: existing transfer rules
- Faroe Islands: Ministerial Order (English statement at the bottom)
- Guernsey: legislation change
- Isle of Man: legislation change
- Israel: current privacy law
- Japan: designation of UK as safe destination (only available in Japanese)
- Jersey: legislation change
- New Zealand: existing transfer rules continue
- Switzerland: EU Exit technical notice
- Uruguay: resolution (only available in Spanish)
- US: Privacy Shield and the UK FAQs

We will update this list as we become aware of any further guidance or legislation. However, these links are for information only. The sender should always ensure it checks with its supervisory authority for the latest guidance, and seek legal advice if in any doubt.

European representatives

Does this section apply to us?

This section applies if you are a UK-based controller or processor:

- with no offices, branches or other establishments in the EEA; but
- you are offering goods or services to individuals in the EEA or monitoring the behaviour of individuals in the EEA.

How can we prepare?

- If you do not have any EEA offices, branches or other establishments, you should consider whether you are processing personal data of individuals in the EEA that relates to either:
- offering goods or services to individuals in the EEA; or
- monitoring the behaviour of individuals in the EEA.
- If you are carrying out such processing, and intend to continue after exit date, you will need to consider whether you must appoint a European representative.
- You will need to consider in which EU or EEA state your representative will be based and put in place an appropriate written mandate for that representative to act on your behalf. Information about the representative should be provided to data subjects, for example, in your privacy notice. It should also be made easily accessible to supervisory authorities, for example by publishing it on your website.

What are the rules?

If you are based in the UK and do not have a branch, office or other establishment in any other EU or EEA state, but you either:

- offer goods or services to individuals in the EEA; or
- monitor the behaviour of individuals in the EEA,

then you will still need to comply with the EU GDPR regarding this processing even after Brexit.

As you will not have a base inside the EEA after exit date, the EU GDPR requires you to appoint a representative in the EEA. 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 in this way are located.

You will need to authorise the representative, in writing, to act on your behalf regarding your EU GDPR compliance, and to deal with any supervisory authorities or data subjects in this respect.

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

You should give details of your representative to EEA-based individuals whose personal data you are processing. This may be done by including them in your privacy notice or in the upfront information you give them when you collect their data. You must also make it easily accessible to supervisory authorities – for example by publishing it on your website.

Your appointment of your representative must be in writing and should set out the terms of your relationship with them. Having a representative does not affect your own responsibility or liability under the EU GDPR.

Example

A UK law firm does not have offices in other EEA countries, but has a regular client base in Sweden and Norway (only). The firm must appoint a European representative to act as its direct contact for data subjects and EU and EEA supervisory authorities. This European representative may be based in Sweden or Norway, but not any other EU or EEA member state.

The firm will have to include the name of its European representative in the information it provides to the data subjects, for example in its privacy notice. It need not inform the supervisory authorities in Sweden or Norway, or indeed the ICO, of this, but the details should be easily accessible to those supervisory authorities.

You do not need to appoint a representative if either:

- 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.

The EDPB has published guidelines on territorial scope which are out for consultation. These contain more guidance on appointing a representative. The EDPB's view is that supervisory authorities are able to initiate enforcement action (including fines) against a representative in the same way as they could against the controller or processor that appointed them.

The UK government intends that after Brexit, the UK version of the GDPR will say that a controller or processor located outside the UK – but which must still comply with the UK GDPR – must appoint a UK representative.

EU regulatory oversight

Does this section apply to us?

This section applies if you are a UK-based controller or processor currently carrying out cross-border processing of personal data, across member state borders, but still within the EEA.

You do not need to read this section if you are based only in the UK and your processing of personal data is unlikely to affect individuals in any other EU or EEA state.

How can we prepare?

- Consider whether any of your processing of personal data involves cross-border processing under the GDPR, and if so who your lead supervisory authority is.
- Consider whether you will continue to carry out cross-border processing after exit date.
- If you will continue to carry out cross-border processing, and your current lead authority is the ICO, review the EDPB guidance, and consider which other EU and EEA supervisory authority will become lead authority on exit date (if any). You may want to contact them closer to exit date.
- If you will no longer carry out cross-border processing after exit date, but your processing will continue to be within the scope of the EU GDPR (for example, if you are 'targeting' individuals in the EEA), this could be a key change for your business and you may want to consider its impact.

What is cross-border processing and One-Stop-Shop?

This is a new concept in the GDPR, designed so that controllers and processors inside the EEA which carry out processing that affects individuals in more than one EU or EEA state only need to deal with a single EEA data protection regulatory authority. The EDPB is still working out how it will operate in practice. We are waiting for it to settle its views on this.

Are we carrying out cross-border processing?

In brief, you may currently be carrying out cross-border processing and benefit from the one-stop-shop if you have an office, branch or other establishment in the UK and your processing is likely to affect individuals in one or more of the other EU or EEA states, for one of the following reasons:

1. You are processing the same set of personal data in the context of the activities of both your UK establishment and one or more EEA offices, branches, or other establishments.

Example

A fashion retailer:

- has a head office in London which handles all its customer data;

- has a distributor in Paris for French sales; and
- sells only in the UK and France.

Before the UK exits the EU, the fashion retailer is cross-border processing its French customer personal data. It is processing that data in the context of both its London head office and Paris distributor.

Or

2. You only have offices, branches or other establishments in the UK, but your processing of personal data is likely to substantially affect data subjects in one or more other EU or EEA states.

Example

A fashion retailer:

- has a single office in London which handles all its customer data; and
- it sells via its website to the UK, France and Italy.

Before the UK exits the EU, the fashion retailer is cross-border processing in the UK, France and Italy, to the extent the London office's processing of the customer data substantially affects data subjects in France and Italy.

If you are carrying out cross-border processing, you benefit from the GDPR One-Stop-Shop system. This means a single supervisory authority will act as the lead on behalf of the other EEA supervisory authorities.

It should mean that, regarding your cross-border processing only, you deal with a single lead supervisory authority, which is responsible for regulating your cross-border processing and enforcing the GDPR (including issuing fines), acting on behalf of the other interested EEA authorities. So if you breach the GDPR regarding your cross-border processing, you are only investigated by one supervisory authority and only receive one fine across the EEA.

There are exceptions to this. For example, the lead supervisory authority may agree that another supervisory authority can take its own enforcement action if complaints only come from within the other authority's jurisdiction.

Examples

Following the example above, the lead supervisory authority for the fashion retailer is the ICO, as its head office is in the UK.

If (before the UK exits the EU) there is a data security breach of the fashion retailer relating to UK, French and Italian customers, the ICO would investigate and bring enforcement action, such as a

fine.

The French and Italian supervisory authorities would provide input to the ICO investigation and enforcement action, but **they would not be able to carry out their own investigation or take independent enforcement action.** This means the fashion retailer would receive only a single fine but it would reflect the impact of the breach on individuals in the UK, France and Italy. This is a key benefit of the One-Stop-Shop.

If (before the UK exits the EU) a French citizen wants to complain about the fashion retailer regarding a failure to respond to a subject access request, the French citizen may put their complaint to the French supervisory authority. The French authority will contact the ICO, and the ICO may choose to investigate the complaint itself or agree to the French authority investigating.

What is the regulatory impact on cross-border processing?

If you are established in the UK and carry out cross-border processing (as described above), there will be changes to which data protection authorities you need to deal with.

One of four scenarios may apply to you.

Scenario 1

- You are currently cross-border processing in relation to two establishments: one in the UK and one in another EU or EEA state.
- Your processing **is not likely** to substantially affect individuals in any other EU or EEA state.

After exit date:

You will no longer be cross-border processing. You will no longer be processing personal data in the context of the activities of establishments in two or more EU or EEA states.

The One-Stop-Shop and lead authority arrangements will no longer apply to your processing. You will have to deal with both the ICO and the supervisory authority in the other EU or EEA state where you are established.

Example

A fashion retailer:

- has a head office in London, which handles all its customer data;
- has a distributor in Paris for French sales; and
- sells only in the UK and France.

Before the UK exits the EU:

The fashion retailer is cross-border processing its French customer personal data. It is processing French customer data in the context of both its London head office and Paris distributor.

After the UK exits the EU:

The fashion retailer is no longer cross-border processing. It will have only a single EEA establishment (the Paris distributor), which distributes to customers only in France.

If there is a security breach of the retailer's customer database affecting UK and French customers, it will be investigated by the ICO under UK data protection law and the French supervisory authority under the EU GDPR. The retailer could be fined by both.

Scenario 2

- You are currently cross-border processing for two establishments: one in the UK and one in another EU or EEA state.
- Your processing in the context of the activities of both the UK and EEA establishment **is likely** to substantially affect individuals in other EU or EEA states.

After exit date:

Processing in the context of your UK establishment is no longer cross-border processing.

Processing in the context of your EEA establishment, which substantially affects data subjects in other EU or EEA states, will continue to be cross-border processing. Its local supervisory authority will be the lead supervisory authority in the EEA in respect of that cross-border processing.

You will have to deal with both the ICO and the EEA lead supervisory authority.

Example

A fashion retailer:

- has a head office in London, which handles all its customer data;
- has a European distribution centre in Paris; and
- sells online to the UK, France, Italy and Spain.

Before the UK exits the EU:

The fashion retailer is cross-border processing its customer data in the context of both the London office and Paris distributor. The ICO is likely to be the lead authority.

After the UK exits the EU:

The fashion retailer is no longer cross-border processing in the context of the London office.

The fashion retailer is cross-border processing in the context of the Paris distributor, for French, Italian and Spanish customer data.

The French supervisory authority is the lead authority as the fashion retailer has an establishment only in France.

If there is a security breach of the retailer's customer database affecting French, Italian and Spanish

customers, it will be investigated by the ICO under UK data protection law and the French supervisory authority under the EU GDPR. The retailer could be fined by both.

Scenario 3

- You are currently cross-border processing in relation to three or more establishments: one in the UK and two or more in other EU or EEA states.
- Your processing may or may not substantially affect individuals in any other EU or EEA state.

After exit date:

The UK establishment is no longer cross-border processing.

Your EU or EEA establishments will still be cross-border processing. You will have to deal with both the ICO and your EEA lead supervisory authority. You should review the EDPB guidance to work out which is your lead authority.

Example

A fashion retailer:

- has a head office in London, which handles all its customer data;
- has a global distribution centre in Paris and a global marketing office in Milan; and
- sells online across the world.

Before the UK exits the EU:

The fashion retailer is cross-border processing in the context of the London office, the Paris distributor and Milan office, regarding its customer database. The ICO is likely to be the lead authority.

After the UK exits the EU:

The fashion retailer is no longer cross-border processing in the context of its London office.

The fashion retailer continues cross-border processing in the context of its Paris and Milan offices. Its lead authority would be decided based on EDPB guidance. If the largest customer base was in Italy, the Italian supervisory authority would probably be the lead authority.

If there is a security breach of the retailer's customer database, it will be investigated by the ICO under UK data protection law and the Italian supervisory authority (if it is the lead authority) under the EU GDPR. The retailer could be fined by both.

Scenario 4

- You are currently cross-border processing with an establishment only in the UK, and no establishment in any other EU or EEA state.

- Your processing **is likely** to substantially affect individuals in one or more other EU or EEA state.

After exit date: you will not be carrying out cross-border processing under the EU GDPR as you have no office, branch or other establishment in the EEA.

You may still need to comply with the EU GDPR to the extent that your processing relates to the offering of goods or services to, or the monitoring of the behaviour of, individuals in the EEA.

You may have to deal with the ICO and the supervisory authorities in all EU and EEA states where individuals are located if you process their personal data in connection with those activities.

Example

A fashion retailer:

- has a head office that handles all customer data; and
- markets and sells online across Europe.

Before the UK exits the EU:

The fashion retailer is cross-border processing across the EEA.

After the UK exits the EU:

The fashion retailer is no longer cross-border processing as it has no office, branch or other establishment in the EEA.

All the fashion retailer's processing of personal data will be subject to the UK GDPR and the oversight of the ICO.

All the fashion retailer's marketing activities targeting EEA customers will also be subject to the EU GDPR.

If there is a security breach of the fashion retailer's customer database, it will be investigated by the ICO under UK data protection law. It may also be investigated by any of the EEA authorities if it has affected customers in their member state. In theory, the retailer could be fined by the ICO and the supervisory authority in every EU and EEA state where customers have been affected.

This could be a key change for your business, and you may want to consider how to minimise any risks. For example, you should consider what resources may be needed to deal with enquiries from various EU and EEA supervisory authorities.

After exit day, the ICO may no longer be part of the One-Stop-Shop. But we will still co-operate and collaborate with European supervisory authorities, as we did before GDPR and the One-Stop-Shop system, regarding any breaches of GDPR that affect individuals in the UK and other EU and EEA states.

Other minor updates

Does this section apply to us?

This section applies to all UK businesses and organisations whose processing of personal data is currently subject to the EU GDPR.

How can we prepare?

- You can review your privacy notices, DPIAs and other documentation to update references to EU law, UK-EU transfers and your EU representative (if you need one).
- Ensure your DPO will be easily accessible from both your UK and (if you have them) EEA establishments.

What are the key points?

- Privacy notices – the information required in your privacy notice is unlikely to change. You may need to (a) review your privacy notice to reflect changes to international transfers, (b) review references to your lawful bases or conditions for processing if any refer to 'Union law' or other terminology changed in the UK GDPR, and (c) identify your EU representative (if you are required to have one).
- Rights of data subjects – as a reminder, if the UK GDPR applies to your processing of personal data, it doesn't matter where in the world the individuals whose data you process are located.
- Documentation – the information required in your record of processing activities is unlikely to change. You may need to review it to reflect changes regarding international transfers. If you have chosen to record the lawful basis or conditions for any of your processing, you need to review any references to 'union law' or other terminology changed in the UK GDPR.
- Data Protection Impact Assessments (DPIAs) – existing assessments may need to be reviewed in the light of the UK GDPR; for example, if they cover international data flows that on exit date become restricted transfers.
- Data protection officers (DPOs) – if you are currently required to have a DPO, on exit date that requirement will continue, whether under the UK GDPR or the EU GDPR. You may continue to have a DPO who covers the UK and EEA. The UK and EU GDPRs will both require that your DPO is 'easily accessible from each establishment' in the EEA and UK.
- Codes of conduct and certification – the EDPB is working on guidance regarding codes of conduct and certification, and how those schemes may be used for transfers. We do not expect that any codes of conduct or certification schemes will be authorised before exit date. The ICO's work on introducing codes of conduct and certification schemes in the UK will continue after Brexit.

Law enforcement processing

Does this section apply to us?

This section applies if you are a UK competent authority currently processing personal data for law enforcement purposes under Part 3 of the Data Protection Act 2018.

If you are not a competent authority, or if you are processing personal data for non-law enforcement purposes (eg HR records), this section does not apply.

For further information, see our Guide to law enforcement processing.

How can we prepare?

- The first thing to do is to take stock. Understand your international flows of personal data for law enforcement purposes, especially with your law enforcement partners in the EU.
- Discuss with your partners in the EU whether they need you to put any additional safeguards in place to permit you to receive transfers from the EU into the UK. The sender is likely to be able to consider relying on local law enforcement processing provisions, which should permit transfers under (a) a contract or other legally binding instrument containing appropriate safeguards, or (b) the sending controller's own assessment that appropriate safeguards are in place (taking into account the safeguards in the DPA 2018).
- Update your processing record, privacy notice and logs with details of transfers to law enforcement partners in EU member states. The UK government has confirmed transitional adequacy provisions will allow transfers to the EU and Gibraltar for law enforcement purposes to continue, but you should review our guidance on international transfers under the law enforcement processing regime. If you are making any transfers of personal data for law enforcement purposes to EU recipients who are not relevant authorities, you will need to start notifying the ICO from exit day (section 77(7)).

How will the law enforcement regime change?

Part 3 of the Data Protection Act 2018 brings the EU Law Enforcement Directive EU2016/680 into UK law. This complements the GDPR and sets out requirements for processing personal data for criminal law enforcement purposes. Part 3 of the Data Protection Act 2018 will continue to be law after exit date, with some specific amendments to the transfer provisions to reflect that the UK is no longer an EU member state.

Most of your obligations will not be affected. The two key areas to consider are:

- transferring personal data out of the UK (sections 73 and 74); and
- receiving personal data from the EU into the UK.

How can we transfer data out of the UK?

On exit date, the EU member states will become third countries under Part 3. This means the rules on

international transfers for law enforcement purposes will apply to transfers from the UK to the EU.

The general rule is that you can still transfer personal data to your partner law enforcement authorities in third countries (including EU member states) if the transfer is necessary for law enforcement purposes and the transfer is covered by a UK adequacy decision or an appropriate safeguard, or special circumstances (ie an exemption) applies. You can also transfer personal data to other recipients (who are not relevant authorities) if you meet some additional conditions and notify the ICO. For full details, read the international transfers section of our Guide to Law Enforcement Processing.

The UK government has confirmed that there will be transitional provisions to permit transfers to EU member states and Gibraltar for law enforcement purposes on the basis of new UK adequacy regulations. (For law enforcement purposes, this will not extend to EEA countries outside the EU, where you should continue to consider other safeguards).

The position on transfers to countries outside the EU will remain the same, and you can continue to follow our existing guidance.

How can we maintain transfers from the EU into the UK?

Other EU member states will have similar laws in place that also implement the Law Enforcement Directive. Once we leave the EU, the UK will become a third country and rules on international transfers will apply to transfers to the UK.

The European Commission and EU member states will need to make decisions regarding transfers of personal data to the UK for law enforcement purposes. If the EU Commission makes a formal 'adequacy decision' under the Law Enforcement Directive that the UK regime offers an adequate level of protection, there will be no need for specific additional safeguards. However, if we leave the EU without a deal, there will not yet be such a decision in place.

This means the sender will need to ensure 'appropriate safeguards' are in place under the national law in their member state. The likely options are:

- a contract or other legally binding instrument containing appropriate safeguards; or
- the sender's own assessment that appropriate safeguards exist. The sender can take into account the ongoing protection provided by the DPA 2018 itself when assessing appropriate safeguards.

Other resources

Guide to law enforcement processing – international transfers