The Information Commissioner's Office

Data protection at the end of the transition period

September 2019

ico.
Information Commissioner's Office

About this guidance

The EU Commission announced on 28 June 2021 that adequacy decisions for the UK have been approved. We are in the process of updating our guidance to reflect this decision.

The Brexit transition period ended on 31 December 2020. As part of the new trade deal, the EU has agreed to delay transfer restrictions for at least four months, which can be extended to six months (known as the bridge). On 19 February 2021 the European Commission published its draft decisions on the UK's adequacy under the EU's General Data Protection Regulation (EU GDPR) and Law Enforcement Directive (LED). In both cases, the European Commission has found the UK to be adequate. The draft decisions will now be considered by the European Data Protection Board (EDPB) and a committee of the 27 EU Member Governments. If the committee approves the draft decisions, then the European Commission can formally adopt them as legal adequacy decisions. If adequacy decisions are not adopted at the end of the bridge, transfers from the European Economic Area (EEA) to the UK will need to comply with EU GDPR transfer restrictions. If you receive personal data from the EEA, we recommend you put alternative safeguards in place before the end of April, if you haven't done so already.

Please note that the bridge does not override the provisions of the Withdrawal Agreement, which applied as of 01 January 2021.

We will keep our guidance under review, and update it as the situation evolves. Please continue to monitor the ICO website for updates.

Does this guidance apply to us?

If you're new to this topic, go here first for an overview of the key points you need to know and practical guidance to help you prepare for the end of the transition period.

This guidance explains data protection at the end of the Brexit transition period 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 has changed

It is particularly relevant to UK businesses and organisations that rely on international data flows, target European customers or operate inside the European Economic Area (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 the transition period ends: check what you need to do (for small businesses)

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

Law enforcement processing and the end of the transition period – five steps to take

Information rights at the end of the transition period – FAQs

The GDPR

The EU Commission announced on 28 June 2021 that adequacy decisions for the UK have been approved. We are in the process of updating our guidance to reflect this decision.

Does this section apply to us?

This section applies if:

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

How can we prepare?

Now the transition period has ended, 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.

Does the GDPR still apply?

The GDPR is retained in domestic law now the transition period has ended, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018. The government has published a 'Keeling Schedule' for the UK GDPR, which shows the amendments.

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

The UK GDPR also applies 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 still applies to this processing, but the way you interact with European data protection authorities has changed.

This guidance covers the key 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 the end of the transition period, see Information rights at the end of the transition period – FAQs.

International data transfers

The EU Commission announced on 28 June 2021 that adequacy decisions for the UK have been approved. We are in the process of updating our guidance to reflect this decision.

Does this section apply to us?

This section applies if you are a UK-based business or organisation subject to the UK 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 understand your international flows of personal data. Key transfers to identify will be from the EEA to the UK. Take stock so that you can distinguish between data acquired before the end of the transition period and after. Data you collected before the end of 2020 about people who were located outside the UK at the end of 2020 will be subject to the EU GDPR as it stood on 31 December (known as the 'frozen GDPR'). You may use the latest information you have about where people were living, up to 31 December 2020.

- Personal data acquired since 01 January that is processed on the basis of the Withdrawal Agreement (for example if personal data is processed under a provision of EU law that applies in the UK by virtue of the Withdrawal Agreement) is also subject to the frozen GDPR. Our End of Transition Interactive Tool will help you decide if you are processing 'legacy data' and provides more guidance. As the UK data protection regime is currently aligned with Frozen GDPR, you can continue to read our guidance on the basis that UK GDPR applies. If the EU Commission adopts a GDPR 'adequacy decision' then these requirements will cease to apply.
- 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 if the bridge ends without the adoption of adequacy decisions. 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

We have produced an information note about SCCs after the Brexit transition period.

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 is now a third country.

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.

Further Reading

For more information about the UK Government's view on the application of the Withdrawal Agreement personal data protection provisions (legacy data), read Using personal data in your business or other organisation from 1 January 2021.

What are the key changes?

There are 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 UK GDPR. Further detail is provided in the international transfers section of our Guide to GDPR.

You don't need any new arrangements for transfers from the UK.

Data can still flow freely from the EEA because the EU has agreed to delay transfer restrictions for at least four months, which can be extended to six months (known as the bridge). If the bridge ends without EU adequacy decisions, transfers from the European Economic Area (EEA) to the UK will need to comply with EU GDPR transfer restrictions. We recommend that you put safeguards in place by the end of April, if you have not done so already.

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 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. This is 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 transfers of data from the UK to the EEA are 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 UK

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.
- Specific UK arrangements have 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.

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.
- Before you put in place appropriate safeguards you should read our updated statement on the judgment of the European Court of Justice in the Schrems II case.
- 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 has recognised EEA countries as ensuring an adequate level of data protection under UK law); and
- the Uruguayan hotel (as the UK government has recognised 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 has not given mutual recognition to EU BCRs. However provision has been made to allow holders of EU BCRs authorised before the end of the transition period to have a UK BCR confirmed, provided certain requirements are met. Those requirements are set out in our information note and requirements table.

- 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

Data can still flow freely from the EEA because the EU has agreed to delay transfer restrictions for at least four months, which can be extended to six months (known as the bridge). If the bridge ends without the adoption of adequacy decisions, transfers from the European Economic Area (EEA) to the UK will need to comply with EU GDPR transfer restrictions. We recommend that you put safeguards in place by the end of April, if you have not done so already.

The EU GDPR applies 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 the UK is now a third country outside the EEA.

The European Data Protection Board (EDPB) has also published an information note on data transfers under the EU GDPR in the absence of an agreement at the end of the transition period.

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 EU 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.
- On 19 February 2021 the European Commission published its draft decisions on the UK's adequacy under the EU's General Data Protection Regulation (EU GDPR) and Law Enforcement Directive (LED). In both cases, the European Commission has found the UK to be adequate.

The draft decisions will now be considered by the European Data Protection Board (EDPB) and a committee of the 27 EU Member Governments. If the committee approves the draft decisions, then the European Commission can formally adopt them as legal adequacy decisions.

Appropriate safeguards

- On 19 February 2021 the European Commission published its draft decisions on the UK's adequacy under the EU's General Data Protection Regulation (EU GDPR) and Law Enforcement Directive (LED). In both cases, the European Commission has found the UK to be adequate.
- The draft decisions will now be considered by the European Data Protection Board (EDPB) and a committee of the 27 EU Member Governments. If the committee approves the draft decisions, then the European Commission can formally adopt them as legal adequacy decisions.
- If the EC adopt the adequacy decisions before the bridge ends, this will allow restricted transfers to continue to be made to most UK organisations, countries, territories or sectors covered by the decision. If there is no EC adequacy decision regarding the UK, but if 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, this will continue to provide an appropriate safeguard for personal data transfers from the EEA to the UK.
- Those binding corporate rules need to be updated, 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, at the end of the , the EC have not adopted the GDPR 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 and Uruguay.

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 includes the UK.

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)

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

The EU Commission announced on 28 June 2021 that adequacy decisions for the UK have been approved. We are in the process of updating our guidance to reflect this decision.

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 the end of the transition period, 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 still need to comply with the EU GDPR regarding this processing.

As you do not have a base inside the EEA, the EU GDPR requires you to appoint a representative in the EEA. This representative needs 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 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. These contain more guidance on appointing a representative.

UK representatives

The EU Commission announced on 28 June 2021 that adequacy decisions for the UK have been approved. We are in the process of updating our guidance to reflect this decision.

Does this section apply to us?

This section applies if you are a controller or processor that is located outside of the UK:

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

How can we prepare?

If you do not have any UK offices, branches or other establishments, you should consider whether you are processing personal data of individuals in the UK that relates to either:

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

If you are carrying out such processing, and intend to continue after the end of the transition period, you will need to consider whether you must appoint a UK representative.

You will need to 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 outside of the UK and do not have a branch, office or other establishment in the UK, but you either:

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

then you will need to comply with the UK GDPR regarding this processing after the end of the transition period.

As you will not have a base inside the UK after the transition period ends, the UK GDPR will require you to appoint a representative in the UK.

You will need to authorise the representative, in writing, to act on your behalf regarding your UK GDPR

compliance, and to deal with the ICO and data subjects in this respect.

Your representative may be an individual, or a company or organisation established in the UK, and must be able to represent you regarding your obligations under the UK 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 UK-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 will not affect your own responsibility or liability under the UK GDPR.

Example

An EEA based sales firm does not have offices in the UK, but has a regular client base in the UK. The firm must appoint a UK representative to act as its direct contact for data subjects and the ICO.

The firm will have to include the name of its UK representative in the information it provides to the data subjects, for example in its privacy notice. It need not inform the ICO of this, but the details should be easily accessible to the ICO.

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.

If you are not sure about any aspect of appointing a representative, you may wish to take independent legal advice.

EU regulatory oversight

The EU Commission announced on 28 June 2021 that adequacy decisions for the UK have been approved. We are in the process of updating our guidance to reflect this decision.

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 EU GDPR, and if so who your lead supervisory authority is.
- 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 at the end of the transition period (if any).
- If you no longer carry out cross-border processing, 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 the regulatory impact on cross-border processing?

If you are established in the UK and carry out cross-border processing (by carrying out processing that affects individuals in one or more EEA states), there are 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 a EU or EEA state.

Now the Brexit transition period has ended:

your processing is no longer cross-border processing. You are no longer 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 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.

Now the Brexit transition period has ended:

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 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.

Now the Brexit transition period has ended:

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.

Now the Brexit transition period has ended:

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 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 the end of the transition period:

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.

Now the Brexit transition period has ended:

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 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.

Now the Brexit transition period has ended: you are not carrying out cross-border processing under the EU GDPR as you have no office, branch or other establishment in the EEA.

You 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 in the UK that handles all customer data; and
- markets and sells online across Europe.

Now the Brexit transition period has ended:

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.

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

The EU Commission announced on 28 June 2021 that adequacy decisions for the UK have been approved. We are in the process of updating our guidance to reflect this decision.

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?

- Take stock so that you can identify overseas data processed before the end of the transition period (known as 'legacy data'). In the absence of adequacy, data processed before 01 January will be subject to the EU GDPR as it stood on 31 December (known as the 'frozen GDPR')
- 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 – 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 both require that your DPO is 'easily accessible from each establishment' in the EEA and UK.
- Codes of conduct and certification – Currently there are no approved codes of conduct and certification schemes acting as safeguards for international transfer tools. However, we are working on

developing codes of conduct and certification schemes and this work will continues.

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.

What do we need to do?

- 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 need to notify the ICO (section 77(7)).

How has the law enforcement regime changed?

Part 3 of the Data Protection Act 2018 brought the EU Law Enforcement Directive EU2016/680 into UK law. This complements the UK GDPR and sets out requirements for processing personal data for criminal law enforcement purposes. Part 3 of the Data Protection Act 2018 continues to be law now that the transition period has ended, 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 key area to consider is:

- transferring personal data out of the UK (sections 73 and 74).

How can we transfer data out of the UK?

EU member states are now 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 transitional provisions to permit transfers to EU member states, EEA countries outside of the EU, Switzerland and Gibraltar for law enforcement purposes on the basis of new UK

adequacy regulations.

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?

You can continue to receive transfers as before. The LED adequacy decision says the UK provides adequate protection for personal data transferred from EU authorities responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

- 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