The Information Commissioner's Office

Data protection at the end of the transition period

September 2019

ico.
Information Commissioner's Office

About this guidance

On 28 June 2021 the EU Commission adopted 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. This means that most data can continue to flow from the EU and the EEA without the need for additional safeguards. The adequacy decisions do not cover data transferred to the UK for the purposes of immigration control, or where the UK immigration exemption applies. For this kind of data, different rules apply and the EEA sender needs to put other transfer safeguards in place.

Does this guidance apply to us?

This guidance explains data protection now the UK has left the EU 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 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. If you haven't yet read our in brief page on data protection and the EU, you should read that first.

Adequacy

What is adequacy?

'Adequacy' is a term that the EU uses to describe other countries, territories, sectors or international organisations that it deems to provide an 'essentially equivalent' level of data protection to that which exists within the EU.

An adequacy decision is a formal decision made by the EU which recognises that another country, territory, sector or international organisation provides an equivalent level of protection for personal data as the EU does.

On 28 June 2021, the EU Commission published two adequacy decisions in respect of the UK:

- one for transfers under the EU GDPR; and
- the other for transfers under the Law Enforcement Directive (LED).

These decisions contain the European Commission's detailed assessment of the UK's laws and systems for protecting personal data, as well as the legislation designating the UK as adequate.

Both adequacy decisions are expected to last until 27 June 2025. The European Commission will start work later in 2024 to decide whether to extend the adequacy decisions for the UK for a further period up to a maximum of another four years. If they don't extend the decisions, then they will expire on 27 June 2025.

Can the adequacy decisions end earlier?

Yes. The European Commission must monitor developments in the UK on an ongoing basis to ensure that the UK continues to provide an equivalent level of data protection. Alternatively, EU data subjects or an EU data protection authority can initiate a legal challenge to adequacy decisions. The Court of Justice of the European Union would then have to decide whether the UK did provide essentially equivalent protection.

What does the EU GDPR adequacy decision say?

The EU GDPR adequacy decision says that the UK provides adequate protection for personal data transferred from the EU to the UK under the EU GDPR.

However, transfers of personal data for the purposes of UK immigration control, or which would otherwise fall within the scope of the immigration exemption in the DPA 2018, are excluded from the scope of the adequacy decision. This may also affect which version of the data protection regime applies in the UK to data processed for immigration control purposes. Our section below on receiving EEA data provides information on what you need to consider under these circumstances.

What does the Law Enforcement Directive adequacy decision say?

The LED adequacy decision also 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. Our section on law enforcement processing provides information on what you should consider if you are a UK competent authority processing for law enforcement processing under Part 3 of the Data protection Act 2018.

The UK GDPR

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.

What should we do?

Now the UK has EU adequacy decisions, 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?

Yes. The GDPR is retained in domestic law as the UK GDPR, 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 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 cross-border processing.

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

Further reading

For information about how other legislation we regulate is affected by the end of the transition period, see our Overview – Data Protection and the EU.

International data transfers

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).

The EU GDPR adequacy decision means that data can continue to flow from the EEA in most cases. The decision does not cover data transferred for the purposes of immigration control or where the UK immigration exemption applies.

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.

What should we do?

Map your flows of international data. Because the EU considers the UK GDPR to be adequate, data can continue to flow as before in the majority of cases, and you don't need to consider another appropriate safeguard.

You should identify any transfers you receive for the purposes of immigration control (or data that falls within the UK immigration exemption) as these are excluded from adequacy; they are restricted transfers and fall under different rules.

What about receiving transfers covered by a European Commission adequacy decision?

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.

How can we transfer data from the UK?

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

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

The UK government will allow transfers to Gibraltar to continue.

You should update your documentation and privacy notice to expressly cover these transfers.

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.

What about transfers from the EEA into the UK?

Receiving data transfers from the EEA

Unless you are processing or holding data transferred for the purposes of immigration control (or data which otherwise falls within the UK immigration exemption), data can still flow freely from the EEA because the EU have adopted adequacy decisions about the UK.

Which regime applies?

Whilst the adequacy decisions remain in place, the UK GDPR applies. Both decisions are expected to last until 27 June 2025.

The EU Commission must monitor developments in the UK on an ongoing basis to ensure that the UK continues to provide an equivalent level of data protection. The Commission can amend, suspend, or repeal the decisions if issues cannot be resolved. Also, EU data subjects or an EU data protection authority can initiate a legal challenge to the decisions. The Court of Justice of the European union would then have to decide whether the UK did provide essentially equivalent protection.

In the absence of an EU GDPR adequacy decision, the Frozen GDPR would apply to personal data if:

- it was processed in the UK under the EU GDPR before 01 January 2021; or
- it's being processed in the UK on the basis of the Withdrawal Agreement (for example, in order to comply with legal obligations under the Withdrawal Agreement).

You may need to be able to identify any personal data you've collected before the end of 2020 about individuals located outside the UK.

In addition, you may need to be able to identify any new non-UK personal data that you only process because you're complying with the provisions of the Withdrawal Agreement.

What about the immigration exemption?

Receiving data transfers from the EEA

The EU GDPR adequacy decision does not cover personal data transferred from the EEA for the purposes of UK immigration control, or data which would otherwise fall under the scope of the immigration exemption in DPA2018. EEA organisations can still make these transfers using an appropriate safeguard from the EU GDPR.

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

Which regime applies to data transfers received that engage the immigration exemption?

If you receive data from the EEA for immigration control purposes or where the UK immigration exemption applies, you should consider whether the Frozen GDPR applies. The Frozen GDPR is the EU GDPR almost exactly as it was on 31 December 2020. The Frozen GDPR won't change even if the UK GDPR or EU GDPR are amended.

The Frozen GDPR applies to immigration data if:

- it was processed in the UK under the EU GDPR before 1 January 2021 (personal data you've collected before the end of 2020 about individuals located outside of the UK); or
- it's being processed in the UK on the basis of the Withdrawal Agreement (for example, in order to comply with legal obligations under the Withdrawal Agreement).

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

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.

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

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.

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.

What do we need to do?

- 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 UK has left the EU:

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 UK has left 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 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 UK has left the EU:

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 UK has left 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 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.

Now the UK has left the EU:

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 UK has left 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 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 UK has left the EU: 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 UK has left 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.

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 actions to take

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.

Does this section apply to us?

- You should 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 is 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