Leaving the EU – six steps to take

1 Continue to comply

Continue to apply GDPR standards and follow current ICO guidance. If you have a DPO, they can continue in the same role for both the UK and the Europe.

2 Transfers to the UK

Review your data flows and identify where you receive data into the UK from the EEA. Think about what GDPR safeguards you can put in place to ensure that data can continue to flow once we are outside the EU.

3 Transfers from the UK

Review your data flows and identify where you transfer data from the UK to any country outside the UK, as these will fall under new UK transfer and documentation provisions.

4 European operations

If you operate across Europe, review your structure, processing operations and data flows to assess how the UK's exit from the EU will affect the data protection regimes that apply to you.

5 Documentation

Review your privacy information and your internal documentation to identify any details that will need updating when the UK leaves the EU.

6 Organisational awareness

Make sure key people in your organisation are aware of these key issues. Include these steps in any planning for leaving the EU, and keep up to date with the latest information and guidance.

Introduction

This checklist highlights six steps you can take now to start preparing for data protection compliance if the UK leaves the EU on 29 March 2019 without a deal.

If you only operate within the UK, you may not need to do much to prepare for data protection after we leave the EU. The UK is committed to the high standards of data protection set out in the General Data Protection Regulation (GDPR), and the government plans to incorporate the GDPR into UK law when we leave. Therefore, your best preparation for the future UK regime is to ensure that you are effectively complying with the GDPR now.

You may however need to ensure adequate safeguards are in place to maintain any data flows from the European Economic Area (EEA), which includes the EU.

If you operate in the EEA, you may need to comply with both the UK data protection regime and the EU regime after the UK exits the EU. You may also need to appoint a representative in the EEA. There is more information below about whether this applies to you.

You can use this checklist to work out whether you will be affected once we leave the EU, and take some key steps to prepare.

We will continue to update our guidance and develop other tools to assist you. Until exit date we continue to work with EU data protection authorities in the European Data Protection Board (EDPB) on GDPR guidelines at European level. However, after exit date, the ICO will only regulate the UK regime. We intend to maintain close links and cooperation with European supervisory authorities (who will have oversight where the EU regime applies).

The ICO is also working closely with trade associations and bodies representing the various sectors – you should also work closely with these bodies to share knowledge about what's happening in your sector.

1 Continue to comply

You should continue to implement GDPR compliance standards and follow current ICO guidance.

The Data Protection Act 2018 will remain in place. The government intends to bring the GDPR directly into UK law on exit, to sit alongside it. There will be some technical adjustments to the UK version of the GDPR so that it works in a UK-only context – for example, amending provisions referring to EU law and enforcement cooperation.

Most GDPR requirements will remain the same. This means the first and most important step is to ensure you comply with GDPR principles, rights and obligations. Our current guidance remains relevant and can help you comply, and we will continue to update it regularly.

If you have a data protection officer (DPO), they may continue in this role. They can combine their future UK responsibilities with any ongoing EU responsibilities, as long as they have expert knowledge of both UK data protection law and the EU regime, and are "easily accessible" from both locations.

2 Transfers to the UK

Review your data flows and identify where you receive data from the EEA, including from suppliers and processors. Think about what GDPR safeguards you can put in place to ensure that data can continue to flow once we are outside the EU.

If you receive data from organisations in the EEA, the sender will need to comply with the transfer provisions of the EU regime. This means the sender needs to make sure there are adequate safeguards in place, or one of the exceptions listed in the GDPR applies.

If the EU makes a formal adequacy decision that the UK regime offers an adequate level of protection, there will be no need for specific safeguards. However, on exit date there may not be such a decision in place. So you should plan to implement adequate safeguards.

You may want to consider putting standard contractual clauses (SCCs) in place if you are receiving data from the EEA. We have produced an interactive tool to help you use the SCCs.

If you are a multinational group with existing binding corporate rules (BCRs) that cover the EEA and UK group companies, with appropriate changes to show the new status of the UK as a third country, these BCRs are likely to permit the transfer from the EEA to the UK. This is subject to confirmation from the EDPB.

For more information see our guidance on international transfers.

3 Transfers from the UK

Review your data flows and identify where you transfer data from the UK to the EEA, or to countries outside the EEA, as these will fall under new UK transfer provisions and documentation requirements.

Transfers from the UK to the EU

The UK government has stated that, when the UK exits the EU, transfers to the EEA from the UK will not be restricted.

This means you will able to continue to send personal data from the UK to the EEA without any additional requirements.

Transfers from the UK to countries outside the EEA

Rules on transfers to countries outside the EEA are likely to remain similar. At this stage you don't need to take any specific steps. We expect the UK government to confirm that the UK will reflect existing EU adequacy decisions, approved EU SCCs and BCRs. For more information, see our detailed guidance on data protection law if there's no Brexit deal.

For more information on the current rules on transfers outside the EEA, see our guidance on international transfers. It will be updated to reflect any changes to the UK rules when we leave the EU.

4 European operations

If you operate across Europe, you should review your structure, processing operations and data flows to assess how the UK's exit from the EU will affect the data protection regimes that apply to you.

Data protection regimes

As a UK organisation, you will need to comply with the UK data protection regime after exit, and the ICO will regulate this regime.

If you also have offices, branches or other establishments in the EEA, the EU regime will still apply to your European activities even after the UK leaves the EU. The ICO will no longer regulate the EU regime.

If you are ONLY based in the UK, but you offer goods or services to individuals in the EEA or you monitor the behaviour of individuals located in the EEA, then the EU regime will also apply to your processing of personal data in relation to those activities. You may have to deal with the ICO and with European supervisory authorities in every EEA and EU state where individuals are affected by these activities.

Lead authority and One-Stop-Shop

If the UK is currently your lead supervisory authority, you should review the structure of your European operations to assess whether you will continue to be able to have a lead authority and benefit from the One-Stop-Shop.

The One-Stop-Shop means you can generally deal with a single European supervisory authority taking action on behalf of the other European supervisory authorities. It avoids your having to deal with regulatory and enforcement action from every supervisory authority in every EEA and EU state where individuals are affected.

After the UK exits from the EU, if you no longer have a lead authority and cannot benefit from One-Stop-Shop, this could significantly affect your business and the resources you need to deal with enquiries from various European data protection authorities.

The EDPB has published guidelines for identifying your lead supervisory authority.

Appointing a European representative

If you are based in the UK, and not in any other EU or EEA state, but you offer goods or services to individuals in the EEA, or you monitor the behaviour of individuals located in the EEA, then to comply with the EU regime you will need to appoint a suitable representative in the EEA.

This person will act as your local representative with individuals and data protection authorities in the EEA. This is separate from your DPO obligations,

and your representative cannot be your DPO or one of your processors. You do not need to appoint a representative if you are a public authority, or if your processing is only occasional, low-risk, and does not involve special category or criminal offence data on a large scale.

The EDPB has published guidelines on territorial scope for public consultation that contain more guidance on appointing a representative.

5 Documentation

Review your privacy information and your documentation to identify any details that will need updating when the UK leaves the EU.

The requirements regarding privacy notices and documentation are unlikely to change. But you need to identify any references to EU law or other EU terminology and be ready to make changes to reflect UK terminology by the exit date. You also need to review what you say about international transfers and reflect any changes, especially for data transfers between the UK and EEA.

You may also need to review existing data protection impact assessments if they involve data transfers between the UK and the EEA.

6 Organisational awareness

Make sure that key people in your organisation are aware of these key issues. Include these steps in any business planning for leaving the EU, and keep up to date with the latest information and guidance.

Key people in your organisation need to be aware of the ongoing importance of GDPR compliance, as well as specific implications for any European operations and data flows. If you have significant operations or relationships in Europe, you can plan ahead. You may find it more difficult to ensure continuity if you leave your preparations until the last minute. It would also be useful to review your organisation's risk register, if you have one.