Data protection if there's no Brexit deal

Summary
How the collection and use of personal data would change if the UK leaves the EU in March 2019 with no deal

Detail
If the UK leaves the EU in March 2019 with no deal, find out how the rules governing data protection would change. This includes:

- sharing personal data collected by EU organisations with UK organisations
- sharing personal data collected by UK organisations with EU organisations

A scenario in which the UK leaves the EU without agreement (a 'no deal' scenario) remains unlikely given the mutual interests of the UK and the EU in securing a negotiated outcome.

Negotiations are progressing well and both we and the EU continue to work hard to seek a positive deal. However, it's our duty as a responsible government to prepare for all eventualities, including 'no deal', until we can be certain of the outcome of those negotiations.

For two years, the government has been implementing a significant programme of work to ensure the UK will be ready from day 1 in all scenarios, including a potential 'no deal' outcome in March 2019.

It has always been the case that as we get nearer to March 2019, preparations for a no deal scenario would have to be accelerated. Such an acceleration does not reflect an increased likelihood of a 'no deal' outcome. Rather it is about ensuring our plans are in place in the unlikely scenario that they need to be relied upon.

This series of technical notices sets out information to allow businesses and citizens to understand what they would need to do in a 'no deal' scenario, so they can make informed plans and preparations.

This guidance is part of that series.

Also included is an [overarching framing notice](https://www.gov.uk/government/publications/uk-governments-preparations-for-a-no-deal-scenario/) explaining the government's overarching approach to preparing the UK for this outcome in order to minimise disruption and ensure a smooth and orderly exit in all scenarios.

We are working with the devolved administrations on technical notices and we will continue to do so as plans develop.

Purpose

This notice sets out the actions UK organisations should take to enable the continued flow of personal data between the UK and the EU in the unlikely event that the UK leaves the EU in March 2019 with no agreement in place.

This notice does not consider sector-specific requirements, for example in relation to processing personal data for law enforcement purposes.

Before 29 March 2019

Rules governing the collection and use of personal data are currently set at an EU-level by the General Data Protection Regulation (GDPR). In the UK, the Data Protection Act 2018 and the GDPR provide a comprehensive data protection framework. Most other EU countries have their own supplementary legislation.

Under GDPR rules, organisations are only permitted to transfer personal data outside the EU if there is a legal basis for doing so. Transfers of personal data within the EU are not restricted.

After March 2019 if there's no deal

If the UK leaves the EU in March 2019 with no agreement in place regarding future arrangements for data protection, there would be no immediate change in the UK's own data protection standards. This is because the Data Protection Act 2018 would remain in place and the EU Withdrawal Act would incorporate the GDPR into UK law to sit alongside it.

However, the legal framework governing transfers of personal data from organisations (or subsidiaries) established in the EU to organisations established in the UK would change on exit. As set out below, you would need to take action to ensure EU organisations were able to continue to send you personal data.

You would continue to be able to send personal data from the UK to the EU. In recognition of the unprecedented degree of alignment between the UK and EU's data protection regimes, the UK would at the point of exit continue to allow the free flow of personal data from the UK to the EU. The UK would keep this under review.

What you would need to do

The EU has an established mechanism to allow the free flow of personal data to countries outside the EU, namely an adequacy decision. The European Commission has stated that if it deems the UK's level of personal data protection essentially equivalent to that of the EU, it would make an adequacy decision allowing the transfer of personal data to the UK without restrictions. While we have made it clear we are ready to begin preliminary discussions on an adequacy assessment now, the European Commission has not yet indicated a timetable for this and have stated that the decision on adequacy cannot be taken until we are a third country.

If the European Commission does not make an adequacy decision regarding the UK at the point of exit and you want to receive personal data from organisations established in the EU (including data centres) then you should consider assisting your EU partners in identifying a legal basis for those transfers.

For the majority of organisations the most relevant alternative legal basis would be standard contractual clauses. These are model data protection clauses that have been approved by the European Commission and enable the free flow of personal data when embedded in a contract. The clauses contain contractual obligations on you and your EU partner, and rights for the individuals whose personal data is transferred. In certain circumstances, your EU partners may alternatively be able to rely on a derogation to transfer personal data. We recommend that you proactively consider what action you may need to take to ensure the continued free flow of data with EU partners. Further detail on the availability of each legal basis, and the processes associated with making use of them, is available from the [Information Commissioner's website](https://ico.org.uk/).

Before and after leaving the EU, we are committed to the highest standards of data protection and all organisations should continue to comply with their broader obligations under data protection law, including the GDPR (as incorporated into UK law). The Information Commissioner's Office would produce additional guidance outlining the steps organisations would need to take to continue to meet their obligations. EU organisations should seek guidance from their respective data protection authorities.

The Information Commissioner will remain the UK's independent supervisory authority on data protection and the UK will continue to push for close cooperation and joined up enforcement action between the Commissioner's office and EU data protection authorities.

More information

This notice is meant for guidance only. You should consider whether you need separate professional advice before making specific preparations.

It is part of the government's ongoing programme of planning for all possible outcomes. We expect to negotiate a successful deal with the EU.