Ministry of Housing, Communities & Local Government

4 March 2019

Accessing data from the European Economic Area (EEA) under no deal Brexit

Guidance for local authorities

Notes: This document is for guidance only. The situation is subject to change, and this general guidance cannot, and is not intended to, cover every eventuality. You should seek your own legal advice regarding the handling of your organisation's personal information assets.

Flow of personal data in a no deal Brexit

Leaving the EU with a deal remains the Government's top priority. This has not changed.

However a responsible government must plan for every eventuality, including a no deal scenario.

In the event that the UK leaves the European Union in March 2019 without a deal the UK will no longer be recognised automatically as compliant with the requirements of the General Data Protection Regulation (GDPR).

The UK will transitionally recognise the EEA as though they have been subject to an affirmative adequacy decision by the UK. This means that, for example, personal data can continue to flow freely **from the UK to the EEA** as if such transfers were made on the basis of an adequacy decision.

However, it is not expected that the European Commission will have made an adequacy decision regarding the UK at the point of exit in March 2019. Therefore, for the purposes of the EU GDPR the UK will be treated as a third country without an adequacy decision. The transfer of personal data **from the EEA to the UK** will be restricted unless appropriate safeguards are in place, or the transfer benefits from one of the statutory exceptions (known as derogations for specific situations).

Further information on international transfers, including a list of appropriate safeguards, is available from the Information Commissioner's Office (ICO).

Working with data processors based in the EEA

There is legal uncertainty regarding the transfer of personal data between data processors located in the EEA and organisations in the UK in the event of a no deal Brexit.

We expect the European Data Protection Board (EDPB) to provide guidance on the transfer of personal data between data processors located in the EEA and organisations in the UK in the event of a no deal Brexit.

Effect of no deal Brexit on transfers of data from EEA processors

As the Government cannot provide legal advice, individual local authorities will need to take their own legal advice about the likelihood of significant disruption to transfers of personal data from processors in the EEA to controllers in the UK. In any assessment, your authorities may want to take into account the following points:

Data processors in the EEA may consider the regulatory risk too high and stop sending data to the UK: data protection authorities in Ireland and the Netherlands, where most data processors are based, generally take a risk based and proportionate approach to regulation, similar to the Information Commissioner's Office (ICO). Even where data protection authorities are less pragmatic, the large data processing companies are used to dealing with them and managing the compliance risk.

The EDPB may declare that these data transfers require additional safeguards: this scenario may be more likely than the first bullet, though the timing of any decision may be some months away. One might expect that EDPB will manage any change to allow for an orderly transition and thus not disrupt existing data flows.

How this affects local authorities

You are best placed to understand the data that you process and are responsible for assessing the risks to your organisation referring to the published guidance (see 'Further information', below) and consulting lawyers and your Data Protection Officer (DPO) as necessary.

Actions for local authorities

You are strongly encouraged to conduct a risk assessment, and seek legal advice where necessary, with regard to any personal data where you are data controller or data processor. What actions you take will depend on your own unique organisational circumstances; some example actions are set out below.

1. Identify each instance of personal data processing in your organisation, where the data is received from or sent to a third party. This includes storage of data in the cloud.
2. Identify where the third party is located, and where the data is located (this may be different to the location of the third party), the nature of the processing activity and the personal data being shared. You should include instances where personal data are exchanged as part of a contract between your organisation and a data service provider, as well as contracts where the third party relies on other data service providers (i.e. data service providers you do not have direct contractual arrangements with).
3. Identify any instances of data being transferred from the EEA to the UK, making a note of the data controller(s) and processor(s) in each instance.
4. Seek legal advice on whether any data transferred from the EEA to the UK that you have identified might benefit from the use of Standard Contract Clauses (i.e. (i) EU controller to UK controller; or (ii) EU controller to UK processor, but **not** (iii) EU processor to UK controller), and generate these as appropriate. You may wish to use the ICO's free interactive tool.
5. Discuss with your data processors what plans they have in place regarding personal data transfers in the event of a no deal Brexit.
6. Identify and prioritise critical personal data and assess risks to the continuation of your critical service delivery should the flow of this personal data to your organisation be disrupted. **Notify your Data Protection Officer of any *critical* datasets that you hold.**
7. Consider whether any mitigating actions are needed (see further advice below)

Standard Contractual Clauses (SCCs)

SCCs (sometimes known as model clauses) are one of the most widely used mechanisms by which controllers established in the EEA can secure an appropriate safeguard for the transfer of personal data to a third country without an adequacy decision. The clauses are in a prescribed standard form that imposes contractual obligations on the importer and exporter to secure safeguards necessary to protect the processing of personal data outside the EEA.

The provisions allow data subjects to directly enforce the obligations set out in the clauses against both the importer and the exporter.

SCCs are straightforward to adopt, requiring no special authorisation once signed by the two organisations involved in the data transfer. SCCs can be signed on a standalone basis, or can be incorporated into an existing or future contract (typically as a schedule or appendix to that contract).

An important limitation on the adoption of SCCs is that they are currently only approved for personal data transfers between controllers and controllers, or between controllers and processors where the controller is in the EEA.

SCCs are valid for scenarios involving the receipt of personal data from an EEA organisation acting as a controller (i.e. where the EEA organisation is solely or jointly responsible for defining why and how personal data in the relevant database are to be used, collected and shared).

An example of where SCCs may be appropriate:

A local authority contracts out its bin collection services to a Belgian company. The Belgian company collects household data which it shares with the local authority and the company also analyses this data to determine the best routes for waste collection. Both the Belgian company and the local authority are data controllers in this case and a controller- controller SCC would be appropriate.

SCCs are **not applicable** in cases where the EEA based organisation is holding the personal data as a processor (i.e. where the EEA based organisation acts only on the instructions of the controlling UK organisation).

SCCs are also **not viable** in cases where one or both of the organisations involved cannot enter into a contractually binding arrangement. Seek legal advice if you believe this may be the case.

Please do take into consideration the following important constraints on using SCCs:
The SCCs adopted must follow one of the forms which have been approved by the European Commission ("Commission") of which there are currently three types:
- Controller to controller (2001);
- Controller to controller (2004); and
- Controller to processor (2010).

Do not change any part of the SCCs – the clauses must be incorporated without amendment. You can include additional clauses on commercial / business related issues - insofar as they do not contradict the substance of the SCCs.

In particular, do not make changes to any of the references within the SCCs to the data protection laws which predated the GDPR. The ICO advises that the Commission is intending to update the existing SCCs for the GDPR but until those revised clauses are adopted existing contracts incorporating the current SCCs can continue to be used for transfers and should not be adjusted to accommodate the GDPR.

Additional mitigations

If you do not consider the assurances you gain from suppliers independently to be sufficient to mitigate your risk, you may wish to consider:

- **Administrative Agreements as Alternative Transfer Mechanisms under Article 46**

  Standard contractual clauses (SCCs) should be the first option for public authorities or bodies engaging in international transfers of personal data where applicable. Where these cannot be used, it may be possible to rely on other appropriate safeguards for transferring personal data under Article 46.

  The ICO has provided further information on appropriate safeguards.

- **Reliance on derogations under Article 49**

  European Data Protection Board (EDPB) guidance suggests that derogations should only be used where transfers are necessary and occasional. However, you may wish to consider whether suppliers could rely on a derogation in Article 49 of the GDPR as a stopgap solution while awaiting further guidance on the EEA processor issue from EDPB.

  The ICO has provided its own detailed analysis of the derogations (referred to as "exceptions").

- **Moving data outside the EEA**

  In the unlikely event that local authorities believe they must localise critical data outside the EEA, they must notify their Data Protection Officer.

  You should consider the likely associated risks of moving data, including security, cost, lead times, and technical capability.

It is likely that in most cases, repatriating data would not be a proportionate response for all but the most critical data sets given the range of factors above. If you are planning to localise data please inform your Data Protection Officer and at the earliest opportunity.

Please note that it is unlikely that changing the contractual terms with a supplier so that your agreement is with part of a counterparty incorporated outside the EEA will mitigate the regulatory risk if the data is still located in the EEA.

Further information

The ICO has published a suite of no deal guidance on their website:

- FAQ
- Blog
- Six steps
- Detailed guidance
- Guidance on SCCs

Guidance has also been published on gov.uk:

- Policy statement
- Excerpt of the ICO's six steps guidance

Definitions

In this note the terms "personal data", "controller" and "processor" are afforded the definitions provided by Article 4 of the General Data Protection Regulation ("GDPR"). "Personal data" is a broad concept that covers any information that relates to an identified or identifiable individual. A data "controller" refers to a person, company, or other body that determines the purpose and means by which personal data is processed. A data "processor" is a person who handles personal data on the instructions of a controller (for example storing, collecting or analysing data as part of a service provided to the controller).