Brexit and research:
EU-UK Data Transfers

This Note is part of a series of Brexit notes for research practitioners on the implications of the UK withdrawal from the EU on 29 March 2019. It sets out the issues that research practitioners need to consider to continue the lawful transfer of personal data between the EU and the UK post Brexit .

MRS is providing this guidance as general information for research practitioners. It is not legal advice and should not be relied upon as such. Specific legal advice should be taken in relation to any specific legal problems or matters.

MRS Evidence Matters

Overview

The UK will formally leave the European Union on 29 March 2019. At the time of the publication of this note, the terms of the future relationship had not yet been agreed.

Given this considerable uncertainty, we are publishing this note to provide guidance to MRS members and Company Partners to help them comply with the requirements of the General Data Protection Regulation (GDPR) on personal data transfers. Our aim is to present the tools and options that are available for organising your internal operations, allowing for the smoothest possible transition in personal data transfers.

Why are "personal data transfers" a topic of discussion?

By adopting the GDPR, the European Union provided its Member States[1] and the members of the EEA area[2] with a comprehensive framework for data protection. Its major aim is to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union. In order to guarantee legal certainty and transparency for businesses, natural persons and authorities, the GDPR is a regulation that automatically applies to all member states – although it allows them limited opportunities to make provisions for how it applies in their country.

This means that:

- The GDPR is directly applicable to the UK until Brexit day. Unless a ratified withdrawal agreement establishes otherwise, from March 30, 2019 all EU legislation will cease to apply.
- The UK has adopted the Data Protection Act 2018,(DPA 2018) in addition to restating the provisions of the GDPR, the DPA 2018 also sets out tailored national exemptions (in areas allowable under the GDPR) and provides a legal framework for data protection in criminal justice and law enforcement. It also replaces the Data Protection Act 1998 (DPA 1998). In the case of no Brexit deal, the DPA 2018 will be the applicable legislation and the UK will be referred to as a third country.
- Until then, the GDPR and the DPA 2018 must be read side by side.

[1] The EU countries are: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.
[2] The EEA includes EU countries and also Iceland, Liechtenstein and Norway. It allows them to be part of the EU's single market.

Further information on data protection can be found in the **MRS Guidance Note on Data Protection and Research**

What is a personal data transfer and why does it matter so much?

The GDPR defines personal data as information relating to an identified or identifiable natural person; who can be identified directly or indirectly by that data on its own or together with other data. This includes identifiers such as a name, an identification number, location data, device identifiers, cookie IDs, IP addresses and relates to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

The GDPR also requires a higher level of protection when *special categories of personal data* are processed: race; ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where this is used for identification purposes);health data; sex life; or sexual orientation.

International personal data transfers, to countries outside the EEA, is considered a risk for data subjects as they may not receive the same guarantees as provided by the GDPR. This is why, the GDPR restricts the transfer of personal data to countries where the GDPR is not applicable unless a series of safeguards are in place.

If the UK leaves the EU on 29 March 2019 without a deal any flow of personal data from the EEA to the UK AND any onward transfer from the UK to another third country will be allowed only if a series of safeguards are in place.

As mentioned, by analysing the following options we aim to help your organisation making an informed decision about the available tools and hence allow the smoothest transition.

Our assumption for this guidance is a no deal scenario. In preparation for it, practitioners – both controllers and processors, should as a matter of priority:

- Identify key data transfers particularly with organisations that are based in the EU
- Assess data flows focusing on transfers of data from the EU to the UK
- Implement a robust data transfer mechanism

What about UK-EEA transfers?

The UK Government has stated that it will permit transfers of personal data from the UK to the EU. In light of this no additional steps should be necessary for data transfers from the UK to the EU apart from standard GDPR compliance measures, including data processing agreements. However, both controllers and processors should be aware that in the future, individual EU Member States may decide to implement national laws that require additional steps for UK businesses.

Ensuring the Free Flow of Data: what options?

First things first – EEA controllers and processors will be able to transfer personal data which is undergoing processing or is intended for processing to the UK, only if they can successfully apply a two-step process:

- Determine and use an appropriate legal basis for the data processing (together with full GDPR compliance);
- Use applicable GDPR provisions on lawful data transfers

The case for an Adequacy Decision

An adequacy decision is a decision taken by the European Commission establishing that a third country provides a comparable level of protection of personal data to that in the European Union, through its domestic law or its international commitments. As a result, personal data can flow safely from the EEA to that third country, without being subject to any further safeguards or authorisations.

Until now the European Commission has granted adequacy only to Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay.

"Partial Adequacy Decisions" [EU Commission wording] limited in scope are:

- US Privacy Shield: a voluntary scheme that protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States for commercial purposes. The framework also brings legal clarity for businesses relying on transatlantic data transfers.
- Canada sector specific framework: applies only to private entities falling under the scope of the Canadian Personal Information Protection and Electronic Documents Act.

Further information on Adequacy Decisions can be found on the EU Commission website **here**

Adequacy decision or partial adequacy decisions are the best case scenario, but this requires a lengthy political process that can be initiated only once the UK officially becomes a third country on March 29, 2019

The case for Binding Corporate Rules

Multinational groups and joint ventures can use **Binding Corporate Rules (BCR's)**, a set of legally binding policies that regulate international personal data transfers from organisations established in the EEA to organisations (within the same group) that are established in the UK.

BCRs work as a code of conduct, ensuring that all data transfers within a corporate group occur under adequate safeguards. They cover a set of elements such as privacy principles (transparency, data quality, and security); tools of effectiveness (such as audit, training, or complaint handling systems) and an element proving that the rules are binding. After development BCRs must be approved by the relevant data protection authority in the location of the European headquarters of any organisation using BCRs.

The European Commission has developed a toolkit for organizations seeking to develop BCRs, which the ICO has published here

First step
- The company designates the lead authority.This is the authority which handles the EU cooperation procedure with the other European data protection authorities (DPAs).

Second step
- The company drafts the binding corporate rules. These rules have to meet the requirements set up in the working papers adopted by the article 29 working party. This draft is submitted to the lead authority which reviews it and provides comments to the company to ensure that the document matches the requirements set out in paper WP 153.

Third step
- The lead authority starts the EU cooperation procedure by circulating the binding corporate rules to the relevant DPA.The authority will be located where group members transfer personal data to entities located in countries that do not ensure an adequate level of protection.

Fourth step
- The EU co-operation procedure is closed after the countries under mutual recognition have acknowledged of receipt of the BCGs. A mutual recognition procedure has been agreed. Under this procedure, once the lead authority considers that BCGs meet the requirements, the DPAs under mutual recognition accept this opinion as sufficient basis for providing their own national permit or authorisation.

Fifth step
- Once the binding corporate rules have been considered as final by all DPAs, the company shall request authorisation of transfers on the basis of the adopted rules by each national DPA.

The decision as to which DPA should act as the lead authority is based upon relevant criteria such as: the location of the group's European headquarters the location of the company which is best placed to deal with the application, and to enforce the binding corporate rules in the group or the EU country from which most transfers outside the EEA will take place.

BCRs are very useful for multi-national and group ventures intra-group data transfer, but the process for obtaining them can take a long time and require significant investment by organisations. Additionally it is important to note that, they do not provide a basis for transfers made outside the group.

The case for Standard Data Protection Clauses SDPC

Standard contractual clauses provide an important tool: The European Commission has published those that offer sufficient safeguards on data protection for personal data to be transferred from EEA to third countries [for the purposes of this note, from EEA to the UK].

The clauses contain contractual obligations on the EEA data exporter and the UK data importer, and rights for the individuals whose personal data is transferred. Importantly, individuals can directly enforce those rights.

Since 2010, EEA based controllers wishing to rely on Standard Contractual Clauses to legitimise international data transfers to processors outside the EEA, have had to use the updated clauses for new processing operations.

There are three sets of standard contractual clauses **that will remain valid until replaced or amended by the European Commission**

- **2001 EEA controller to third country controller**
  - Available here: https://bit.ly/2tYaMfa
- **2004 alternative EEA controller to third country controller**
  Available here https://bit.ly/2tTAUrA
- **EEA controller to third country processor**
  - Available here https://bit.ly/2PawDgU

It is very important that you keep on checking the websites of the UK ICO at and of the European Commission for further updated information.

New Contracts

- Use the clauses **in their entirety and without amendment**

New parties in the contract?

- You can add parties (i.e. additional data importers or exporters, both controller and processors) provided they are also bound by the standard contractual clauses

Specificities of the business

- You can include additional clauses on business related issues, provided that they do not contradict the standard contractual clauses.

Remember!

- If you are making a restricted transfer from a controller to a processor, you also need to comply with the **GDPR requirements about using processors**.

Taking into account all the circumstances, such clauses appear to be the most effective way to guarantee a frictionless Brexit transition, until the adoption of more favourable options or frameworks.

The case for a GDPR Code of Conduct

Another contractual option is to adhere to a sectoral **GDPR Code of Conduct**, which has been approved by a Data Protection Authority and by the European Commission. This is a new option and as such will require significant time to be fully operational.

MRS is already developing a GDPR Research Code, together with our European counterparts and European national DPAs. As one of the first sectors actively engaged in the process, we hope to be operational by summer 2019 but this will be dependent on when the Code review and approval process is operational.

The case for Derogations

As previously stated, the adoption of standard contractual clauses appears to be the most effective way to guarantee continuous EEA-UK data transfer for the time being.

The GDPR also provides a set of derogations for specific situations, in the absence of an adequacy decision or appropriate safeguards. **But – the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary**.

Derogations are:

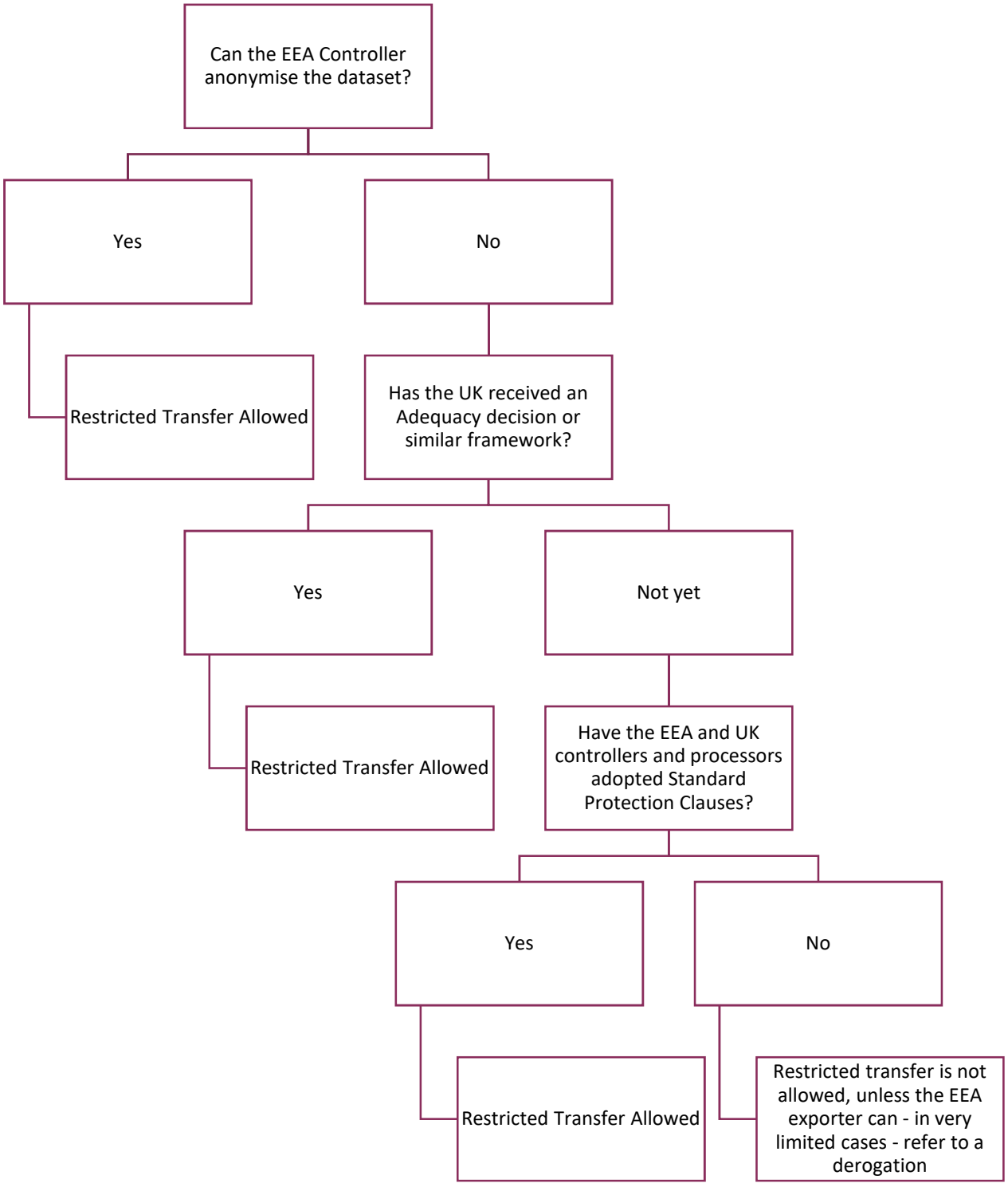
- Individual's explicit consent to restricted transfer: a valid consent is specific, informed (please see GDPR In Brief No.5 on Informed Consent) including all information related to the identity of the receiver, the reasons for the transfer, the kind of data transferred and the risks involved in a transfer to a country which is not deemed to provide adequate data protection. For every time the transfer occurs.
- The transfer is necessary for the performance of a contract between the data subject and the controller or for the performance of a contract concluded in the interest of the data subject.

In all these cases the transfer might take place only if it is occasional, necessary, not repetitive and concerns only a limited number of data subjects.

A data transfer that occurs regularly within a stable relationship between the data exporter and a specific data importer is deemed as systematic and repetitive. As it is the case of a data importer that is granted access to a database on a general basis.

Derogations have to be interpreted restrictively. They have to be documented in the processing activities. They have to be communicated to the ICO.

International Data Transfer Decision Tree



Research Scenarios

In any international research project, there are several occasions in which a transfer can occur.

Key Terms

- Simple transfer: a transfer of data inside the protection of the GDPR, within the EEA
- Restricted transfer:
  - A transfer of:
    - data that are regulated by the GDPR, in the countries and circumstances in which it applies.
  - A transfer to:
    - a receiver that is located outside the EEA
    - a receiver that is not your direct employee
    - a receiver that is not a branch of your company
- Transit
  - Personal data that is just electronically routed through a non-EEA country and the transfer is from one EEA country to another EEA country.

Scenario 1.

An Italian digital brand, the controller, has commissioned an UK research agency, the processor, to carry out research with a branded on-line community established for this purpose. Client and agency included Standard Data Protection Clauses (SDPCs) in the contract. The UK agency is considering sub-contracting with an US based agency to host the online community.

- Restricted transfer from Italy to the UK allowed because of SDPCs
- Restricted onward transfer from UK to US, allowed if the US subcontractor is Privacy Shield certified

Scenario 2.

A Dutch client, the controller, commissions a research project to a French multinational research agency, the processor, providing sample of its customer database. The Paris branch appoints the research to the Bristol branch. The Bristol branch subcontracts a London translator and a Tel Aviv analyst.

- Restricted transfer from Paris to Bristol allowed if Binding Corporate Rules have been adopted by the group.
- Restricted onward transfer from Bristol to London allowed only if SDPCs are adopted.
- Restricted onward transfer from Bristol to Tel Aviv allowed because of Israeli Adequacy decision.

Scenario 3.

A Belgian Pharma company, the controller, commissions a research to an UK agency, the processor, on a sample collection that will be provided directly by a Spanish fieldwork recruiter.

- The restricted transfer between the Spanish contractor and the UK agency will be allowed only if SDPCs are adopted.
- The restricted transfer from the UK agency to the Austrian client allowed because data go back to the EU.

Data Transfers and where to find them