Brexit and Research: what's next?

This Note is part of a series of Brexit notes for research. It sets out the issues that practitioners need to consider in data protection at the end of the transition period.

The Information Commissioner's Office (ICO) is currently keeping their guidance under review and update it as the situation evolves.

MRS is providing this data protection guidance as general information for 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.

December 2020

MRS Evidence Matters™

Contents

Contents 3
Overview 4
International transfers of personal data 5
From the UK to the EEA 5
From the UK to a Third Country 6
Adequacy Regulations 6
Binding Corporate Rules 7
GDPR Code of Conduct 7
Exceptions 7
Standard Contractual Clauses 8
From the EEA to the UK 9
The 6 steps approach: 10
From countries, territories or sectors covered by an EC adequacy decision 11
Data Transfers and where to find them 12
Examples of Inward Data Transfers 12
Examples of Outward Data Transfers 12
European representatives 13
Additional Considerations 15
Privacy notices 15
Documentation and record of processing 15
Data Protection Impact Assessments (DPIAs) 15

Overview

The UK left the EU on January 31st, 2020 and entered a transition period, which ends on December 31st, 2020.

From January 1st, 2021 the GDPR will be retained in domestic law. The key principles, rights and obligations will remain the same, but the UK will have the independence to keep the framework under review.

The 'UK GDPR' will sit alongside an amended version of the Data Protection Act (DPA) 2018.

The government has published a 'Keeling Schedule' for the UK GDPR, which shows the planned amendments[1].

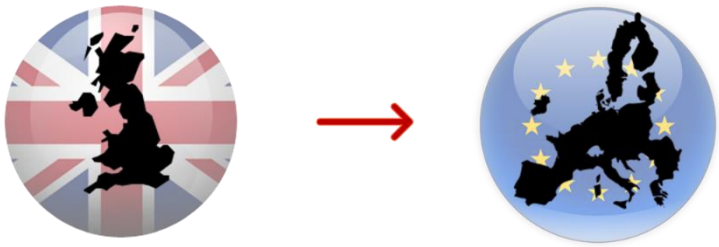
The Information Commissioner's Office (ICO) is currently keeping their guidance under review and updates it as the situation evolves.

In the meanwhile, there are some immediate steps that, if not already taken, practitioners need to adopt and implement in their processes.

[1] According to Article 71 of the Withdrawal Agreement, the EU GDPR must be interpreted in accordance with the relevant case law of the Court of Justice of the European Union handed down before the end of the transition period. This means that the past case law on the EU GDPR as well cases handed down after the end of the transition period will be applicable when UK courts are considering the interpretation of the EU GDPR. At the end of the transition period the EU GDPR will be saved into UK law and will be referenced to as UK GDPR. When interpreting retained EU law, the UK courts will not be bound by judgments of the Court of Justice handed down after the end of the transition period Eleonor Duhs, Fieldfisher, *Legacy data under Article 71 of the Withdrawal Agreement* https://www.fieldfisher.com/en/insights/legacy-data-under-article-71-of-the-withdrawal-agreement

International transfers of personal data

From the UK to the EEA



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

The EEA countries are Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

Practitioners can continue to make transfers of data from the UK to the EEA, but they must update their documentation and privacy notice to expressly cover those transfers.

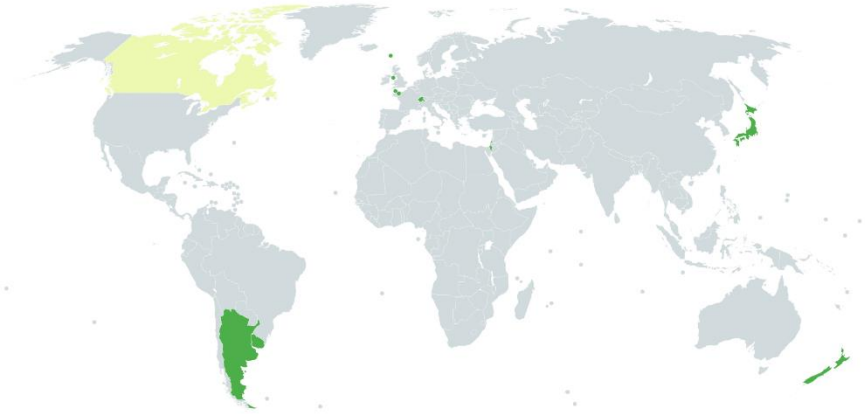
From the UK to a Third Country

Practitioners intending to transfer personal data from the UK to a country out of the EEA should already have considered how to comply with the GDPR. This will not change under the UK GDPR.

Adequacy Regulations

Practitioners will be able to make restricted transfers if covered by new UK adequacy regulations.

From January 2021, the UK will be able to adopt its own Adequacy regulations. These will confirm that a particular country or territory has an adequate data protection regime.



The countries which have been already approved by the UK adequacy regulations are Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

Specific UK arrangements have now been confirmed regarding the recent EU adequacy decision for Japan.

If no adequacy decision covers the restricted transfer, it is necessary to put in place one of a list of appropriate safeguards.

Binding Corporate Rules

Multinational groups and joint ventures can use Binding Corporate Rules (BCRs), a set of legally binding policies that regulate international personal data transfers from organisations within the same group established in a third country.

BCRs are very useful for multi-national and group ventures intragroup 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 of a corporate a group.

GDPR Code of Conduct

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

MRS is in the process of developing a GDPR Research Code for the UK and we will keep you updated about progress.

Exceptions

The UK GDPR will also provide a set of derogations for specific situations, in the absence of an adequacy decision or appropriate safeguards. Exceptions *have to be interpreted restrictively. They have to be documented in the processing activities. They have to be communicated to the ICO*.

Exceptions are:

- Individual's explicit consent to restricted transfer: a valid consent is specific, informed (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. Consent would be required for every transfer that occurs.
- The transfer is necessary for the performance of a contract between a data subject and a controller or for the performance of a contract concluded in the interest of the data subject.

In all these cases transfers 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 a 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 regularly.

Standard Contractual Clauses

Standard contractual clauses (the SCCs) are one of a number of 'safeguards' which can be used to comply, and the one most likely to be appropriate for small and medium-sized businesses. The SCCs are standard sets of contractual terms and conditions which a sender and a receiver of personal data both sign up to. They include contractual obligations which help to protect personal data.

The ICO has prepared template contracts:

- Controller to controller
- Controller to processor

The ICO has also prepared a contract builder to automatically generate the contract:

- Build a controller to controller contract
- Build a controller to processor contract

A NOTE ON SSCs

In the Schrems II Case, the European Court of Justice (ECJ) invalidated the 'US Privacy Shield' and examined the validity of the Standard Contractual Clauses.

The Court added that validity depends on whether SCCs include effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection essentially equivalent to that guaranteed within the EU by the GDPR and that transfers of personal data according to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them.

Following this judgment, the European Data Protection Board (EDPB) released a series of recommendations on measures that supplement transfer tools that, when definitely adopted, will be mandatory for any EEA business relying on EU SCCs.

At the time of writing the ICO is still reviewing the recommendations and will consider whether we need to publish their own guidance in due course.

Because of the rule of law and Article 71 of the Withdrawal Agreement (effects of ECJ judgments in UK) and most importantly, because of the spirit and the principles of the GDPR, it is recommended, albeit not binding, to follow the SCCs.

From the EEA to the UK

Businesses transferring personal data from the EEA to a third country are bound by the terms of Art. 44-50 GDPR.

In the absence of an adequacy decision, SCCs appear to be the most suitable transfer mechanism.

The European Commission has adopted the following:

EEA controller to non-EU or EEA controller

- decision 2001/497/EC
- decision 2004/915/EC

EEA controller to non-EU or EEA processor

- decision 2010/87/EU

As mentioned, the EDPB published Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, currently under consultation.

These recommendations are meant to help EEA exporters with the complex task of assessing third countries and identifying appropriate supplementary measures where needed and are essential to any UK business will have to assist their EEA counterparts in the assessment for international transfer of data to the UK.

In particular:

- Standard contractual clauses and other transfer tools mentioned under Article 46 GDPR do not operate in a vacuum.
- Controllers or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools.
- In those cases, it is still possible for exporters to implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law.

These recommendations provide exporters with a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place.

The 6 steps approach:

Know your transfers	• Map your transfers • Verify that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country
Verify the transfer tool	• In the absence of an adequacy decision, you need to rely on one of the transfer tools listed under Articles 46 • Only in some cases of occasional and non-repetitive transfers you may be able to rely on one of the derogations provided for in Article 49 GDPR, if you meet the conditions
Third Country Assesment	• Is there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer? • Specific attention to any relevant laws and in particular requirements to disclose personal data to public authorities and granting public authorities powers of access to personal data
Supplementary Measures	• Technical measures: state of the art encryption and Pseudonymisation • Contractual measures: for example exporter reinforcing power to conduct audits or request importers to provide transparency about laws applicable to it that would permit access to data by public authorities • Organizational Measures: such as internal policies, appointing internal team or applying stricter data minimization
Formal procedural steps	• Ensure that additional clauses cannot be construed in any way to restrict the rights and obligations in the SCCs or in any other way to lower the level of data protection
Re-evaluate	• Monitor at appropriate intervals if there have been or there will be any developments that may affect

From countries, territories or sectors covered by an EC adequacy decision

Practitioners receiving personal data from one or more of the following countries: Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Isle of Man, Israel, Japan (private-sector organisations only), Jersey, New Zealand, Switzerland and Uruguay need to consider that these will have their own legal restrictions on making transfers of personal data to countries outside the EEA. This will include the UK at the end of the transition period.

UK officials are working with these countries and territories to make specific arrangements for transfers to the UK where possible.

Practitioners that are UK importers and senders of personal data will need to consider how to comply with local law requirements on transfers of personal data and seek local legal advice.

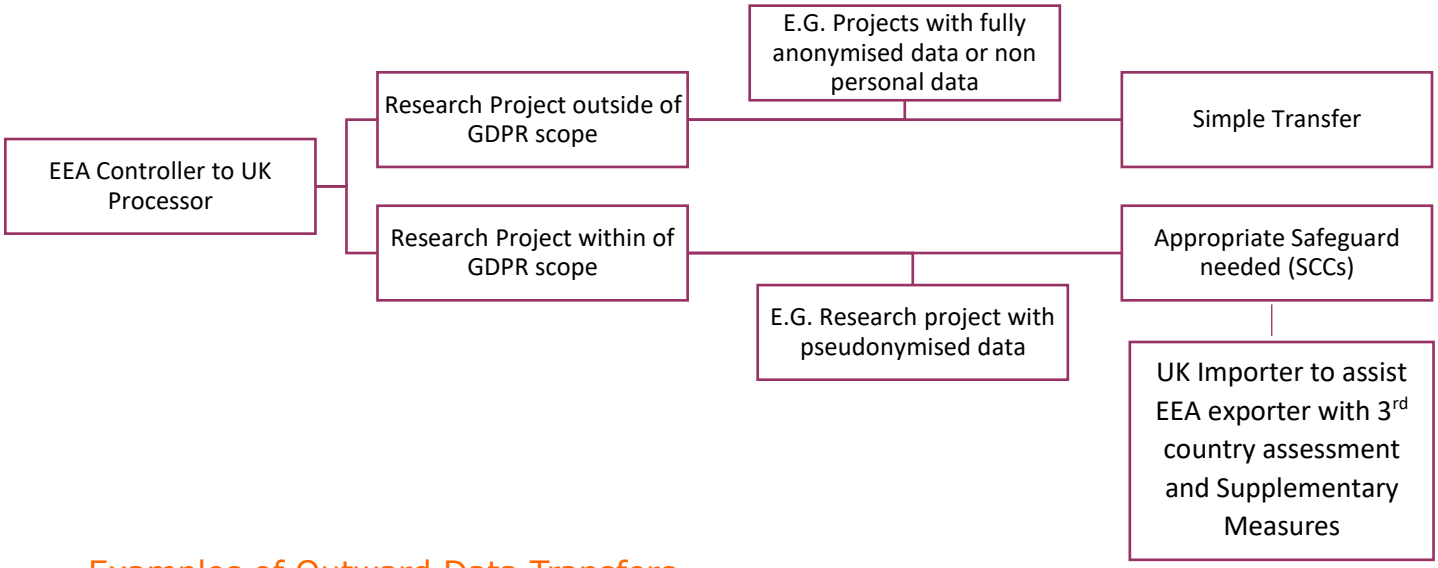
At the time of writing the ICO has compiled the following list (for information purposes only):

- *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)*

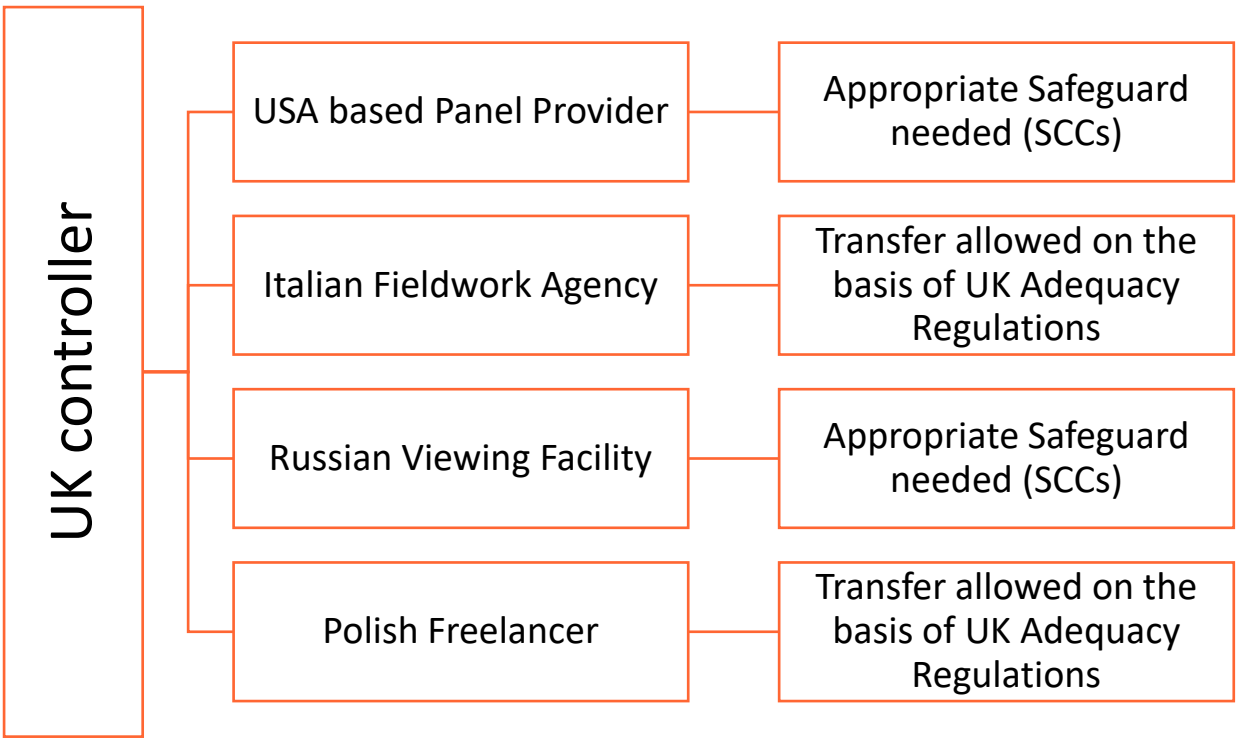
We will update this list as we become aware of any further guidance or legislation. However, these links are for information only. The sender should always ensure it checks with its supervisory authority for the latest guidance and seek legal advice if in any doubt.

Data Transfers and where to find them

Examples of Inward Data Transfers



Examples of Outward Data Transfers



European representatives

Under Article 27 of the GDPR data controllers or processors subject to the GDPR are under the obligation to designate a representative in the European Union if they are offering goods or services to individuals in the EEA or monitoring the behaviour of individuals in the EEA.

Failure to appoint an EU representative, where required, makes the organisation liable to a Tier 2 fine of up to 2% of worldwide turnover or 10 million euros.

The European Data Protection Board has clarified some key principles around the appointment, operation, and liability of the EU Representative in their Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)[2] as follows:

Designation of a representative

- The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under the GDPR
    - The written mandate shall govern the relations and obligations
    - The easiest way to appoint a representative may be under a simple service contract
    - The role can be assumed by a wide range of commercial and non-commercial entities, such as law firms, consultancies, private companies, etc.
    - When the function of representative is assumed by a company or any other type of organisation, it is recommended that a single individual be assigned as a lead contact and person "in charge" for each controller or processor represented.
- When controller or processor carry out several processing activities, they are not expected to designate several representatives for each separate processing activity.
- The representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with the GDPR.
- the same company/person cannot act as a data protection officer and EU Representative for the same company, due to the risk of a conflict of interest arising; for the same reason, a company should not appoint an organisation which also acts as their data processor.
- As part of their information obligations, controllers shall provide data subjects information as to the identity of their representative in the Union. This information shall for example be included in the privacy notice and upfront information provided to data subjects at the moment of data collection
    - Such information should furthermore be easily accessible to supervisory authorities in order to facilitate the establishment of a contact for cooperation needs.

[2] https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_en

The appointment[3]:

- The representative shall be established in one of the Member States where are data subjects whose personal data are, not in the place where their data is processed.
    - One criterion for establishing in which country to appoint a representative when services are offered across the EU is where the largest number of their data subjects are based.
    - One more general criterion is the EU Member States to which data subject can have the easiest access – because of highest recurrence of research projects or geographical vicinity (e.g. the Benelux region, which includes Belgium, Luxembourg and The Netherlands)

MRS is currently investigating with the ICO and Government departments for additional guidelines on country of establishment, particularly in relation to situations where practitioners collect data from across the EU with no specific country being dominant. We will update this guidance as soon as we receive additional information.

Exceptions to the appointment:

Practitioners don't need to appoint an EU representative if either:

- They are a public authority; or
- their 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 role of the EU Representative:

- the EU Representative has a duty to hold, maintain, and provide to supervisory authorities their clients' records of processing activities, **although** the primary duty for preparing this document rests with the controller/processor which appointed them;
- the EU Representative 'should in principle' communicate with the data subject and EU authority in the language they typically use, unless this results in 'disproportionate effort'.

The liability of the EU Representative:

- the EU Representative should not be held primarily liable for their clients' violations of the GDPR; and
- the EU Representative remains primarily liable under the GDPR for its own failures to comply with GDPR Articles 30 (records of processing activities) and 58 (assisting the supervisory authorities with their investigations).

[3] EU: EDPB guidelines on EU representatives https://www.dataguidance.com/opinion/eu-edpb-guidelines-eu-representatives

Additional Considerations

Practitioners need to consider a few additional details:

Privacy notices

a) Review the privacy notice to reflect changes to international transfers;
b) Review any reference to the lawful bases or conditions for processing referring to 'Union law' or to EU GDPR and reflect the terminology change as will be laid down in the UK GDPR.;
c) List name and contact details for the EU representative.

Documentation and record of processing

a) Reflect changes regarding international transfers;
b) Review any references to 'Union law' or to EU GDPR and reflect the terminology change as will be laid down in the UK GDPR.

Data Protection Impact Assessments (DPIAs)

a) Existing assessments may need to be reviewed in the light of the UK GDPR;
    - for example, international transfers of data to the EEA on exit day will become restricted transfers. The DPIA should reflect this change and address the risk assessment and the safeguards invoked and implemented.

MRS will continue to closely follow the legislation and regulatory framework development, including the adoption of the UK GDPR and how this will apply in practice.

Compliance with Data Protection Regulations is not only a legislative obligation but also a Rule of the MRS Code of Conduct and an ethical duty of the profession.

MRS invests significant effort in supporting its Members and Company Partners via:

- Specialist Guidance Notes, which provide detailed interpretation and application of the data protection framework to the insight sector (available here https://www.mrs.org.uk/standards/data-protection); and
- Codeline, the confidential email advice service, which provides swift, reliable and free advice at Codeline@mrs.org.uk