Department of Health & Social Care

Guidance for health and social care organisations: end of transition period data preparedness

October 2020

Contents

Checklist of top 4 critical actions

These are the top 4 critical actions for your organisation to take before the end of the transition period:

1. **Data transfers:** Identify your personal data flows from the EU/European Economic Area (EEA). Work with your EU based counterparts to put in place Alternative Transfer Mechanisms to allow these data flows to continue in a 'no adequacy' scenario.

   The relevant guidance sections for more information are:

   - Using Standard Contractual Clauses - p. 5
   - Administrative Arrangements - p. 9
   - Alternative Transfer Mechanisms under Article 46 GDPR: legally binding instruments and custom contractual clauses - p.10
   - Derogations for exceptional circumstances - p.12

2. **Data storage:** Identify where your data is stored by EEA based processors, for example cloud storage providers in the EU. Engage with them to gain written assurances that data will continue to flow back to the UK in a 'no adequacy' scenario.

   - Working with data processors based in the EU - p.19

3. **Data audit:** Conduct an audit of all your personal datasets, ensuring information is up to date and relevant meta-data is held, including geographical origin of the data and the legal basis for transfer. This should help you to comply with the data provisions set out in the Withdrawal Agreement, where EU GDPR may continue to apply to some of your datasets.

   - Application of the Withdrawal Agreement Provisions - p.21

4. **Data protection:** Ensure you are compliant with UK GDPR.

   - Data protection compliance – p.23

‘No Adequacy’ Preparedness

What will happen to the flow of personal data without an adequacy decision from the EU?

- **Flows from the UK to the EEA:** The UK has legislated so that personal data for general processing can flow freely, on a transitional basis, from the UK to the EEA, as well as the EU and EEA Institutions. This means that personal data for general processing can continue to flow freely from the UK to the EEA. As legally required by UK law, central government will review the ‘adequacy’ of these arrangements within four years of them coming into effect (i.e. by 1 January 2025).

- **Flows from the EEA to the UK:** In the event that the European Commission has not recognised the UK as adequate by the end of the transition period, the transfer of personal data from the EEA to the UK will be restricted unless alternative transfer mechanisms (also referred to as 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 alternative transfer mechanisms, is available from the Information Commissioner’s Office (ICO).

What this means for you

The UK has one of the best data protection regimes in the world, based in law on the EU’s GDPR. Despite this, the EU may not deem the UK “adequate” for data protection purposes. Given our aligned regimes, the UK will recognise the EU as adequate, and so data to the EU is unaffected. However, if the EU has not deemed the UK to be adequate by the end of the transition period, you will need to have put in place alternative transfer mechanisms for your personal data to continue to flow legally and uninterrupted from the EU/EEA to the UK.

The following sections of the guidance set out the alternative transfer mechanisms that are available and help you:

- decide which mechanisms your organisation can use;
- understand the benefits and limitations of each; and
- how to practically implement them.

Using Standard Contractual Clauses

This section is designed to help you:

- decide whether you can use Standard Contractual Clauses (SCCs) as an alternative transfer mechanism; and
- practically implement SCCs into new or existing arrangements.

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.

Benefits: 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).

Limitations: 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.

Actions for organisations

The following steps will help you understand where SCCs can and should be adopted in relation to contracts you have with third parties in the EU:

Step 1: Create a spreadsheet that identifies each of the business areas in your organisation that process personal data.

Step 2: For each area, outline the key arrangements in place that involve personal data being received from or sent to a third party. Identify, where available, details of where the third party is located (UK or another country), where the data is located (bearing in mind this may be in a different location from 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).

Step 3: Review your spreadsheet to identify specific arrangements involving the transfer of data from the EEA to the UK and in each of those cases, note the nature of the transfer (e.g. controller to controller, controller to processor, processor to controller).

Step 4: Engage your commercial lawyers and/or use the ICO free interactive tool to determine which of the EEA to UK transfers identified at Step 3 may benefit from SCCs (i.e. (i) EU controller to UK controller; or (ii) EU controller to UK processor, but **not** (iii) EU processor to UK controller). Start generating SCCs to support those transfers using template SCC Addendum published alongside this guidance if desired, unless existing contracts with these organisations already adopt SCCs or provide a mechanism to accommodate automatic application of SCCs in the event of no adequacy. As appropriate, you should get in touch with all relevant third parties to inform them of the need to adopt SCCs.

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 of which there are currently three types:

- Controller to controller (2001);
- Controller to controller (2004); and
- Controller to processor (2010).

It is expected that the European Commission will issue new SCCs following the validation of this transfer mechanism in the Schrems II judgment. UK data controllers should continue to monitor the ICO website for updated guidance. Further advice will be circulated in the event that new SCCs are published before the end of the transition period.

Template SCCs and cover letter: Published alongside this guidance is a template letter to suppliers and contract addendum to support you in implementing the SCCs in applicable contracts, including call-offs and direct contracts. The list of frameworks included in this guidance will be indicative of the types of contract which may potentially involve the supplier acting as data controller and therefore the SCCs applying.

The addendum sets out the 2004 Controller to Controller Provisions and makes use of option (iii) in Clause II(h) which requires the public authority (as the data importer) to comply with the data processing principles set out in Annex A of Appendix A. This will be readily achieved by maintaining compliance with existing UK data protection laws under the Data Protection Act 2018. Use of option (i) would have required compliance with the laws where the supplier is based, which was not deemed appropriate because of lack of familiarity with overseas laws. Option (ii) would only be relevant if the UK secures an adequacy decision (although SCCs should not be required where one has been granted). In any event this is not imminent.

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. It is expected that the European Commission will make these updates if and when they publish new SCCs.

What should I insert into Annex B of the SCCs? – Annex B of the SCC should be completed to provide a full description of the personal data being shared between the supplier and the contracting authority under the contract. The description may be drafted in similar terms to the approach recommended for insertion in supplier contracts in preparation for GDPR compliance, as per the template "*Annex A - Part 2: Schedule of Processing, Personal Data and Data Subjects*" in PPN 03/17. If a description of the relevant processing activity has already been prepared within the existing contract, it is possible to simply cross-reference that within Annex B of the SCCs. It is likely that the Supplier (as the data exporter) is best placed to complete this section as this information may be less visible to the contracting authority. You should send the addendum out unsigned so that you can verify that the information populated is sufficient before signing the SCC.

What should I do if the supplier refuses to sign the SCCs? – If the supplier is processing personal data in the EEA, it is important to remind them that their data protection regulators will expect them to enter into the SCCs before transferring any personal data to a non-adequate country. If they do not do this, they risk being in breach of the GDPR. The EDPB has issued guidance on this position which you may find helpful to refer to when engaging with suppliers.

Further information

Applicability and limitations of SCCs: 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). 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 government entity). In that case, please see the section below on 'Working with data processors based in the EEA without adequacy'. SCCs are also not viable in cases where one or both of the organisations involved cannot enter into a contractually binding arrangement. In that case, if both parties are public bodies, an administrative arrangement may be an appropriate option.

Schrems II: On 16 July 2020, the Court of Justice of the European Union ruled (in the "Schrems II" case) that SCCs can in principle be valid for international data transfers to non-adequate third countries, which would include the UK in a 'No Adequacy' scenario. However, the ruling makes clear that this validity depends on whether the SCCs (together with any other additional measures), when used for a particular third country, provide the level of protection required under EU law. The court is clear that there is an obligation on a controller or processor in the EU to assess the level of protection provided to personal data transfers relying on SCCs on a case-by-case basis. In particular, SCCs will not secure the appropriate level of protection, and therefore will not be a valid basis for a transfer, if third country's laws prevent compliance with the SCCs'

provisions. – i.e. an assessment should be done as to whether the legal regime in the third country provides a level of protection of personal data which does not undermine the level of protection guaranteed to data subjects under EU law and if not, whether supplementary measures (e.g. legal / technical / organisational) can be provided to ensure equivalence of protection. Further guidance is awaited from the European Data Protection Board (EDPB) as to what supplementary measures could be provided and further information will be shared once the position from the EDPB is clear.

The ability or willingness of EU data controllers to use SCCs to send personal data to the UK may be compromised if, at the end of its adequacy assessment of the UK, the European Commission declines to make an adequacy decision in favour of the UK and raises concerns as to the ability of UK laws and practices (as they currently stand) to provide an appropriate level of protection for the personal data transferred from the EU. Further dedicated advice will be forthcoming in this scenario.

Central approach – SCC implementation on behalf of UK government departments:
During no deal preparations, Crown Commercial Service (CCS) wrote to suppliers on the following frameworks to vary the framework so that all future template call-off contracts under them included SCC wording and an obligation to invoke them where required. These variations are still 'active' and in place.

- Vehicle Hire Services (RM1062)
- Corporate Finance Services (RM3719)
- Payment Solutions (RM3828)
- Postal Goods and Services (RM1063)
- NetWork Services (RM1045)
- Network Services 2 (RM3808)
- HSCN Access Services (RM3825)
- Workforce Management (RM1072)
- Language Services (RM1092)
- Employee Services (RM3704)
- Multidisciplinary Temporary Healthcare Personnel (RM3711)
- e-Disclosure Services (RM3717)
- Management Consultancy (RM3745)
- Management Consultancy Two (RM6008)
- Rail Legal Services (RM3756)
- General Legal Advice Services (RM3786)
- Finance and Complex Legal Services (RM3787)
- Contingent Labour ONE (RM960)
- Non Medical Non Clinical (RM971)
- Occupational Health Services, Employee Assistance Programmes and Eye Care Services (RM3795)
- Managed Learning Service (RM3822)
- Apprenticeship Training and Related Services (RM382)

This list includes frameworks which CCS identified as potentially involving the supplier acting as data controller and therefore SCCs may be applicable. Devolved Administrations may wish to consider a similar approach. Variation to the framework contracts will **not** affect existing call-off contracts or direct contracts held by public sector organisations. This means contracting authorities **will** still need to put in place SCCs for affected call-off contracts under these frameworks contracts where applicable. To this end, you can use the template SCC addendum published alongside this guidance.

Administrative Arrangements under Article 46 GDPR

This section is designed to help you if you are considering entering into administrative arrangements for the transfer of personal data from organisations in the EEA to public authorities or bodies in the UK, where SCCs are **not** applicable.

Administrative arrangements support transfers between public authorities or bodies who cannot enter into a legally binding contract with each other. Provisions can be “inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights" (e.g. an MoU or policy (Article 46(3)(b) GDPR).

Benefits

- Administrative arrangements can be tailored to reflect specific transfers between public authorities or bodies. Although they must be authorised in advance by a supervisory authority, there is no express requirement for the supervisory authority to consult with the European Data Protection Board (EDPB) before authorising provisions to be inserted in administrative arrangements under Article 46(3)(b) (but see “Limitations” below). Accordingly, this process may be quicker than the process under Article 46(3)(a) (custom contractual clauses), outlined in the ‘Alternative Transfer Mechanisms under Article 46 GDPR: legally binding instruments and custom contractual clauses’ section of this guidance. The supervisory authority should however notify other supervisory authorities first and these other supervisory authorities may request the matter is considered by the EDPB.

Limitations

- The administrative arrangement must be authorised in advance by the lead competent supervisory authority for the EU organisation sending the data. The GDPR does not expressly require the supervisory authority to consult with the EDPB. However, guidance published by EDPB has indicated that these arrangements should be ‘subject to an authorisation by the competent national supervisory authority, following an opinion of the EDPB.’ This may influence the approach of supervisory authorities seeking to comply with the consistency mechanism as required by Article 46(4) GDPR and therefore lengthen the time frame for finalising an administrative arrangement. Public authorities or bodies should consider short term mitigations including the possibility of using SCCs (if appropriate) or relying on derogations, even if an administrative arrangement is the appropriate longer-term solution.
- They can only be used for arrangements between public authorities or bodies (i.e. this is not an appropriate safeguard if one of the parties is a private body).

Alternative Transfer Mechanisms under Article 46 GDPR: legally binding instruments and custom contractual clauses

SCCs and administrative arrangements are likely to provide the most easily implemented and appropriate options for mitigating the risks to public sector EU - UK data flows. However, in the event that neither of these options is appropriate, public bodies may also rely on legally binding instruments and custom contractual clauses as alternative legal bases for transfers of personal data.

You may be aware that there are other appropriate safeguards for transferring personal data under Article 46, such as binding corporate rules (BCRs), codes of conduct and certification schemes. These mechanisms are unlikely to be useful in the context of safeguarding EU - UK flows in a 'no adequacy' scenario and so have not been covered in this guidance.

Legally Binding Instruments:

Article 46(2)(a) GDPR refers to "a legally binding and enforceable instrument between public authorities or bodies."

This can allow a data controller to transfer personal data outside of the UK where there are arrangements, governed by a contract, treaty or other legally binding instrument between public authorities or bodies, which (1) provide appropriate safeguards to protect the privacy of data subjects, and (2) include a mechanism to support enforceable data subject rights and legal remedies for data subjects. Note that a memorandum of understanding (MoU) or similar administrative arrangement will generally not be sufficient for the purposes of Article 46(2)(a) as the relevant instrument has to be legally enforceable. However, an MoU may form the basis of an administrative arrangement (see section above on 'Administrative Arrangements under Article 46 GDPR' for further information).

Benefits

- Does not require any specific authorisation by a supervisory authority.
- Possibly more flexible than an SCC because the form of arrangement is not limited to a contract - safeguards could be met by using a different form of legally binding agreement (e.g. a treaty).

Limitations

- Requires a legally enforceable instrument to be put in place, which would likely involve a lengthy and resource intensive process.
- Can only be used for agreements between public authorities or bodies.

Custom Contractual Clauses:

Article 46(3)(a) refers to "contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation."

This anticipates the adoption of custom contractual clauses that can either operate on a standalone basis or can be inserted into an existing contract.

Benefits

- Can be tailored to individual public authorities' or bodies' processing situation.
- Article 46(3)(a) (custom contractual clauses) are not limited to transfers only between public authorities or bodies and so can be used to enable transfers between public and private bodies.

Limitations

- There are potential procedural hurdles. These safeguards require specific authorisation by the supervisory authority in the country (or countries) from which the restricted transfer is being made. Before granting an authorisation for contractual clauses under Article 46(3)(a), the relevant supervisory authority to whom the application for approval is made must consult with the EDPB through the consistency mechanism under Article 63. This approval process is likely to be lengthy, resource intensive and incur considerable expense.

Derogations for specific situations under Article 49 GDPR

This section is designed to help you use derogations to transfer personal data from the European Economic Area (EEA) to the UK under Article 49 GDPR in the absence of an adequacy decision or other appropriate safeguards.

Where an adequacy decision is not available, appropriate safeguards should always be the first option for public authorities or bodies engaging in international transfers of personal data. For this reason, please consider the applicability of standard contractual clauses or other transfer mechanisms under Article 46 GDPR in the first instance.

Existing Guidance: In May 2018 the European Data Protection Board (EDPB) published guidance on the derogations under Article 49. The ICO has also provided its own detailed analysis of the derogations (referred to as "exceptions"). If you are considering using any derogations under Article 49, you may find it useful to refer to these links.

This guidance covers:

1. Key overarching points to consider when using any derogation under Article 49 GDPR; and
2. Key points to consider for each of the derogations in Article 49.

Actions for organisations

When using derogations under Article 49 GDPR it may be helpful to remember that:

- The EDPB view is that derogations should be treated strictly as exceptions to the general rule prohibiting international transfers in the absence of an adequacy decision or appropriate safeguards; in other words, that they should only be relied on in specific situations and not routinely.
- Use of the derogations should never lead to a situation where fundamental rights under GDPR might be breached.
- The derogations listed under Article 49(1) GDPR are qualified by Article 49 in its entirety and also by the interpretations suggested in recitals 111-115 GDPR (although these recitals do not have legal effect). You should consider the whole of Article 49 when looking at whether you can rely on a particular derogation.
- If none of the derogations in Articles 49(1)(a)-(g) are applicable, Article 49(1) subparagraph 2 allows for an ad-hoc transfer to be relied upon in limited circumstances, based on the "compelling legitimate interests" of the controller.
- The derogations available are for the benefit of the party ***transferring*** the personal data

(i.e. the data exporter). It is that organisation (rather than the recipient of the data / data importer) who must meet the relevant requirements in Article 49. For example, the first three derogations in Article 49(1) **cannot be relied on by** public authorities (see Article 49(3)). However, this would not prevent a private body in the EEA relying on these derogations to transfer personal data to a public authority or body in the UK.

● Where a data subject in the EEA is transferring their own personal data directly to an organisation located outside the EEA, this is not a restricted transfer and no derogation (or appropriate safeguard) is required.

Application of individual derogations in Article 49 GDPR

The table below provides an indication of how the derogations may be applied in practice. Note however that member states may have their own interpretations of these principles so the local position should always be checked before relying on a particular derogation.

Derogation	**Interpretation**
Article 49(1)(a) GDPR: Transfers based on explicit **consent**	● Explicit consent must be obtained from the data subject for the specific restricted transfer / set of transfers in hand. General consent for restricted transfers will not be sufficient. ● Consent must be "freely given, specific, informed" and must be accompanied by an "unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action" (Article 4(11) GDPR). ● The threshold for explicit consent is higher than this requiring something more than "clear affirmative action" to confirm approval – typically showing some form of express confirmation in words. ● Depending on the circumstances, explicit consent may require a written statement explaining the transfer, supported by an express indication of approval by the individual – for example a signature or written confirmation. Pre-ticked boxes will not be valid. ● The statement should inform the data subject about the nature of the transfer, including the possible risks arising from the transfer (see the ICO's guidance, as above). ● The data subject should be able to withdraw consent at any time following which the organisation would be required to cease the transfer.

	● The derogation cannot be relied on by public authorities exercising their public powers as stated in Article 49(3).
Article 49(1)(b) GDPR: Transfers that are necessary for the **performance of a contract** between the data subject and the data controller	● This can include implementation of pre-contractual measures at the request of the data subject. ● Recital 111 suggests data transfers in reliance on this derogation may only take place where the transfer is occasional. ● The transfers can happen more than once, but not regularly. The EDPB note that whether a transfer is occasional can only be determined on a case-by-case basis. Occasional might be interpreted as occurring outside the regular course of actions, for example, under random, unknown circumstances and within arbitrary time intervals. An existing framework of stable cooperation involving systematic and repeated data transfers between the data controller and receiver of the personal data would not be deemed occasional. ● The transfer must be necessary for performing the contract. ● EDPB and ICO guidance outlines a high threshold for this necessity test. ● This will typically only be met if the core purpose of the contract or the core purpose of the steps needed to enter into the contract cannot be performed without making the restricted transfer. ● There must be a close and substantial connection between the data transfer and the purposes of the contract - just because the desired data flow would be more cost effective or efficient doesn't mean that it is necessary. ● Only personal data that is essential to the performance of the contract should be transferred. The derogation cannot be relied on by public authorities exercising their public powers as stated in Article 49(3).
Article 49(1)(c) GDPR: Transfers that are necessary for the conclusion or performance of a contract concluded in the interest of the data subject	● This derogation closely follows the derogation above and so is subject to the same limitations in relation to occasional use and necessity of the transfer. In this case, where necessity is to meet a need that is in the interest of the data subject. ● This exception does not allow for transfers that take place prior to entering into the relevant contract.

	● The derogation cannot be relied on by public authorities exercising their public powers as stated in Article 49(3).
Article 49(1)(d) GDPR: Transfers necessary for important reasons of public interest	● The transfer must be necessary for important reasons of public interest. ● Article 49(4) sets out that the public interest being relied on must be recognised in EU law, or the law of the controller's member state. A narrow interpretation of these criteria would require as a basis something that is expressly recognised as a public interest in legislation of a national parliament. A broader interpretation may consider as a basis something recognised as public interest in statutory/authoritative guidance, codes of practice or in EU or member state case law. ● When considering what is in the public interest, it is important to consider this from the perspective of the EU or the controller's member state. ● The relevant assessment is whether the transfer is in the public interest of the relevant EU exporting country, rather than the interests of the recipient third party country (even if the intended use in the third country is for a purpose recognised as being in the public interest within the EU). ● The public interest may well be satisfied if the data transfer is linked to an arrangement where there is an element of reciprocity and international cooperation (e.g. an international agreement or convention that recognises certain objectives and provides for international co-operation). ● Recital 112 gives various examples of what the term public interest could mean including for social security matters, or public health. ● EDPB and the ICO do not expect transfers under this derogation to be used for large scale or systematic transfers.
Article 49(1)(e) GDPR: Transfers necessary to establish, exercise or defend a legal claim	● Recital 111 suggests that this derogation can only be relied on for occasional transfers - it can happen more than once, but not regularly. The EDPB note that whether a transfer is occasional can only be determined on a case-by-case basis. Occasional might be interpreted as occurring outside the regular course

	of actions, for example, under random, unknown circumstances and within arbitrary time intervals. An existing framework of stable cooperation involving systematic and repeated data transfers between the data controller and receiver of the personal data would not be deemed occasional. ● It also provides for quite a broad interpretation of a legal claim "regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies." ● EDPB view that the relevant procedure must have a basis in law and a legally defined process. ● There must be a real prospect of proceedings or a claim being brought, i.e. the exception cannot be relied upon if there is only the mere possibility that proceedings or a claim may be brought in the future. ● The transfer should be limited to personal data that is necessary for the purpose - there must be a close connection between the need for the transfer and the relevant legal claim.
Article 49(1)(f) GDPR: Transfers necessary to protect the **vital interests** of data subjects, or of other persons	● EDPB view this derogation to be relevant only where there is a present and immediate threat to an individual (e.g. a data subject is unconscious and in need of urgent medical care). ● It can only be applied where the data subject is physically and legally incapable of giving consent. ● EDPB view that legal incapability can extend to cases involving minors (as long as this doesn't prejudice national representation mechanisms). ● The derogation can support transfers in the aftermath of natural disasters for the purpose of rescue and retrieval as it is considered that data subjects are unable to provide their consent. ● The ICO frames this derogation solely in the context of medical emergencies. ● The derogation cannot be relied on to carry out general medical research.
Article 49(1)(g) GDPR: Transfers made from a **public register**	● The derogation applies to only those registers which are established under EU or member state law to provide information to the public. Local country rules should be checked as the types of registers which are

	public will vary between member states. ● Just because a register is public does not mean that the data within it may be processed freely. In many cases where a register has been established in law for a particular purpose, public access may be restricted to those eligible to use the data for a specific legitimate purpose. Before extracting data from a public register, a risk assessment should always be undertaken to validate the lawful basis for processing. Any adverse impact of the processing on the rights of the individuals whose personal data is to be transferred should also be carried out. This should include consideration of the risk posed by the personal data being held in a country outside the EEA. ● This derogation does not apply to registers run by private companies - e.g. credit reference databases. ● A transfer under this derogation is limited to ad hoc extracts only – the derogation cannot be relied on to support downloads of the entirety of the personal data or entire categories of the personal data contained in the register.
Article 49(1) subparagraph 2 GDPR: Transfers necessary for **compelling legitimate interests**	● The exporting controller must be able to demonstrate that they have considered the appropriate safeguards and the other derogations under Article 49(1) and have determined that it would not be possible to use them for the restricted transfer. This means the derogation should only be used in exceptional circumstances. ● The ICO guidance outlines that controllers should assure themselves of the above even if it involves significant investment. ● The derogation may not be relied on for routine transfers. The transfer may happen more than once, but not regularly. ● The derogation cannot be relied on by public authorities exercising their public powers as stated in Article 49(3). ● The compelling legitimate interests is a higher threshold than “legitimate interests” under Article 6(1)(f). ● The controller's compelling legitimate interests must outweigh the rights and freedoms of the individuals.

	This assessment and the suitable safeguards adopted should be documented as set out in Articles 49(6) and 30(1)(e). ● The personal data must only relate to a limited number of individuals. There is no absolute threshold for this. The number of individuals involved should be part of the balancing exercise (please see bullet above). ● The supervisory authority must be informed of the transfer (but does not need to provide authorisation). ● The data subjects must be informed of the transfer and of the compelling legitimate interests pursued. ● Recital 113 states that where scientific or historical research is sought, the aim of increasing knowledge should be taken into consideration with this derogation.

Working with data processors based in the EEA

This section provides advice about the risk of disruption to the flow of personal data from processors (particularly cloud storage suppliers) based in the EEA to data controllers in the UK in a non-adequacy scenario.

Legal status of data flows from EEA processors to UK organisations:

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 non-adequacy scenario. No approved mechanism for reverse transfers currently exists. The EDPB has not yet determined whether in its view these data flows are restricted international transfers under the EU GDPR. The issue is unlikely to be resolved before the end of the transition period.

Level of risk:

Central government assesses that the likelihood of significant disruption to transfers of personal data from processors in the EEA to controllers in the UK is very low. This is because:

- Data processors in the EEA are unlikely to consider the regulatory risk too high so as to stop sending data to the UK. This issue is not specific to the end of transition period preparedness and is an ongoing risk. 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 is more likely than the scenario where EEA data processors unilaterally choose to stop sending data to the UK (see the above bullet), though the timing of any decision may be some months away. It is expected that the EDPB will manage any change to allow for an orderly transition and thus not disrupt existing data flows.

- A data protection authority may receive a complaint from an individual or campaign group that leads to enforcement action: significant enforcement action of this type can take a long time to process with the potential for prolonged litigation. Organisations could take additional mitigation action during the litigation.

Actions for organisations

1. Identify and prioritise your personal datasets stored offshore in the EEA which are critical to your work.

2. Make an assessment of the risks to the continuation of critical service delivery should the flow of this personal data be disrupted. This will inform decisions about what, if any, mitigating actions should be taken in the event that the risk of disruption is considered too high.

3. Engage with your data storage suppliers based in the EEA and ask for written assurances that they will continue to flow data back to the UK following the end of the transition period.

Application of the Withdrawal Agreement Provisions

This section considers the data provisions in the Withdrawal Agreement, which are something that you will need to consider and prepare for in addition to what you did last year.

Part III, Title VII of the Withdrawal Agreement contains provisions that apply EU data protection law ('frozen' at the end of the transition period) to certain 'legacy' personal data if the UK has not been granted full adequacy decisions. 'Legacy data' includes data transferred to the UK prior to the end of the transition period, or subsequently on the basis of the Withdrawal Agreement.

At the end of the transition period, the UK will incorporate EU data protection law (with some technical amendments to ensure it is operable in the UK) into domestic law. This means that protections for 'legacy' personal data will not be any different to protections for other personal data, and UK organisations should not need to do anything differently immediately to accommodate the Withdrawal Agreement changes in practice.

It may be worth noting that technically some personal data you hold will be subject to UK domestic law, and some data subject to frozen EU data law under the Withdrawal Agreement. However, differences in UK and frozen EU data law are likely to come about over time. This may mean that UK organisations need to be able to distinguish between different categories of data so that they can treat different sets or items of data under different rules: some under UK domestic law, and some under frozen EU data law. Public bodies may need to introduce new systems or compliance models to remain compliant once any substantive differences emerge between these regimes.

HMG departments are currently working to develop an approach to these Withdrawal Agreement provisions that minimises the impact on public bodies, businesses, and other UK organisations whilst ensuring the obligations set out in the Withdrawal Agreement are met. Supplementary guidance on this will be issued in due course.

Actions for organisations

You should take the following steps to help minimise future costs, risks, or burdens related to the application of these provisions. These are all data protection principles that responsible organisations should be applying regardless, but that they should pay particular attention to in preparation for the end of the transition period. These steps are:

- **Audit personal data.** Ensure all personal data held is fully audited and accounted for, and relevant meta-data is held; including about its origin (including the jurisdiction in which it was collected), legal basis for collection and transfer, and from whom it was

transferred.

- **Erase unnecessary personal data.** Ensure that personal data held is relevant and limited to what is necessary for the purposes for which they are processed. Obsolete, unnecessary, or superfluous personal data should be erased.

- **Keep personal data accurate and up to date.** Where feasible, organisations should plan to refresh any datasets they hold from EU sources on or shortly after 1 January 2021, especially where the UK has not secured adequacy decisions. In doing so, they should ensure that appropriate safeguards are adopted in line with Article 46 GDPR for the legitimate transfer of such data.

Data protection compliance

This section considers the additional data protection compliance issues at the end of the transition period **other than** in relation to the impact on transfers from the EU/EEA, which is covered above. The issues raised in this section apply regardless of whether an adequacy decision is secured.

Data protection law post-transition period

Once the UK leaves the EU, the EU GDPR will be adopted into UK law by section 3 of the EU Withdrawal Act 2018 (**EUWA 2018**) and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (**Implementing Regulations**). Organisations based in the UK will need to comply with this version of the GDPR (**UK GDPR**) when processing personal data.

The UK GDPR largely follows the EU GDPR (save to make sense of the fact that the UK will no longer be a Member State of the EU). This means that, post-transition period under the new UK GDPR there will be no immediate change to the UK's data protection standards.

In some circumstances, organisations will also be required to comply with the EU GDPR - for example when processing data in relation to EEA residents. This guidance explains when the EU GDPR may apply and highlights some of the additional actions required to secure compliance with this parallel legal regime.

Ensuring compliance with UK GDPR

Organisations based in the UK will need to comply with UK GDPR. Organisations may be considering making changes to the way in which data processing is carried out as part of their post-transition period planning, for example by adopting new operating processes or making changes to existing technology infrastructure. The effect of this may be that organisations process personal data in a different way or hold data in a different location.

Actions for organisations

Actions may be required in the following areas:

- Ensuring the changes do not impact the ability to manage data subjects' rights (this may be an issue if for example the organisation makes changes to the provider of data services);
- Ensuring data subjects are aware of any changes to processing activity, and where applicable secure appropriate consents;
- Updating documentation, including:

    - Records of processing activities: Article 30 UK GDPR requires organisations to maintain a record of their processing activities. The record may need to be reviewed in order to reflect changes in processing activities which have been made as a result of the end of the transition period, including to record transfers to EEA countries as international transfers.
    - Privacy notices: Articles 13 and 14 UK GDPR require organisations to provide privacy information to data subjects. By way of example, Article 13(1)(f) UK GDPR creates an obligation to notify data subjects about transfers to third countries, which will include EEA countries once the UK leaves the EU. Organisations may need to review references to the lawful bases or conditions for processing if they refer to "Union law" or other terminology which is impacted by the end of the transition period.
- Conducting a Data Protection Impact Assessment (DPIA). The ICO advises that existing assessments may need to be reviewed (for example, in the context of international transfers which on exit date become "restricted");
- Updating contracts and other agreements which relate to the processing activity. For example contracts with third party controllers or processors may need to be updated to reflect changes in the processing activity that are taking place, the location of the data, references to relevant data protection laws, or other regulatory responsibilities resulting from the end of the transition period. Examples of technical changes required could include changes to the definition of “data protection laws” to include specific reference to the UK GDPR; or changes to the international transfer provisions. Organisations may take a risk-based and proportionate approach to updating contracts which could take account of the significance and extent of the changes; risk profile of the contracts / nature of data in scope; and the volume of contracts. Organisations could also consider, rather than amending existing contracts, to prioritise a review of contractual language for future contracts going forward to ensure they align with the UK GDPR.

UK organisations that have an EEA establishment or that process the personal data of EEA residents:

Organisations may find themselves having to comply with both UK GDPR and EU GDPR.

- If a UK organisation has an establishment (e.g. a branch or an office) in the EEA, the EEA establishment will need to comply with the EU GDPR in relation to the activities of that establishment (see Article 3(1) EU GDPR).
- Where the UK organisation has no establishment in the EEA, the EU GDPR will still apply if the organisation is offering goods or services to EEA residents, or monitoring the behaviour of EEA residents (insofar as that behaviour takes place in the EEA) (see Article 3(2) EU GDPR). “Monitoring behaviour” could include services which involve tracking or monitoring British citizens resident in the EU. In respect of “offering goods and services”, organisations should be aware that this could apply to non-commercial activities undertaken by government, for example the offering of visas. If this applies, organisations (but not public authorities) must take extra steps to appoint an EU representative pursuant

to Article 27 GDPR. (Please see guidance on Article 27 Representatives).

Given that UK GDPR will require UK organisations to meet the same standard as afforded under EU GDPR immediately post transition period, it is not anticipated that there will be significant differences to the obligations on UK organisations under the UK and EU regime. However, organisations should be aware that in some situations they may have liability under the EU GDPR as well as the UK GDPR.

This is a technical and nuanced area and it is recommended that UK organisations consult the European Data Protection Board (EDPB) territorial scope guidance, which can be accessed: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf.

Effects of other EU laws and EEA Member States' laws on processing: Organisations that have an EEA establishment or that process the personal data of EEA residents should also be mindful of any Member State laws that supplement the EU GDPR in technical areas (similar to how the Data Protection Act 2018 supplements the UK GDPR). For instance, Member State laws may provide special rules on managing data subject rights, or the processing of "special categories of personal data".

Dealing with other EU and EEA Supervisory Authorities: The One-Stop-Shop and lead supervisory authority arrangements in the EU GDPR allow data controllers and processors to liaise with one lead supervisory authority where either:

i. the data processing takes place on a cross-border basis within the EEA, or
ii. the controller or processor is based in one Member State, but the processing of personal data is likely to substantially affect individuals in any other EEA state.

At the end of the transition period, these arrangements will no longer apply to the UK. This means that UK based organisations that are involved in processing EEA resident data may have to deal with both the ICO and supervisory authorities in other relevant EEA states. In the event of non-compliance, the organisation could also be exposed to the risk of multiple enforcement action and/or sanctions from more than one supervisory authority. If this situation arises, please engage with the ICO at the earliest opportunity.

For further information, the EDPB's guidance on lead supervisory authorities can be accessed at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

Processing that has a legal basis in Union law: The EUWA 2018 brings EU law into domestic UK law as it stands at the moment of exit. This means that where an organisation has been relying on EU law as the lawful basis for processing personal data (e.g. under Article 6(1)) it is likely that the relevant law should now be carried forward into UK law. However, organisations should check this with their lawyers as in some cases implementing the legislation may create a shortfall which will impact the original lawful basis.

Scenario in which the UK Secures Adequacy Decisions

This section is designed to help you prepare for scenarios where adequacy decisions come into

effect by the end of the transition period.

Article 27 Representatives - where UK organisations are processing personal data of EU/EEA residents (pursuant to Article 3(2) GDPR)

Regardless of whether the UK secures adequacy decisions by the end of the transition period, some UK data controllers and processors may need to appoint EU-based representatives from 1st January 2021.

This could apply to businesses and other organisations based outside the EU/EEA which target data subjects in the EU/EEA by offering them goods or services or monitoring their behaviour.

Public authorities are exempt from the Article 27 EU GDPR requirement to appoint an EU representative when processing EEA resident data. However, it may be the case that organisations you are responsible for may be within the scope of Article 27 (i.e. because they are not a public authority).

Do I need to appoint a European representative?

Article 27 of the GDPR requires organisations (controllers and processors) not established in the EEA but that either (i) offer goods or services to individuals in the EEA, or (ii) monitor the behaviour of individuals in the EEA, to appoint an EEA-based representative.

This representative will act as your local point of contact with individuals and data protection authorities in the EEA and therefore should be based in an EU or EEA state where some of the individuals are located. This is separate from 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 representative can either be an individual or exercised based on a service contract concluded with an individual or an organisation (such as law firms, consultancies, private companies, etc.). One representative can also act on behalf of several non-EEA controllers and processors. They must be appointed in writing to act on your behalf in dealing with data protection authorities and individuals and their appointment should be made available to both individuals and data protection authorities – e.g. by publishing their details on your website privacy notice. It is important to note that the appointment of a representative does not affect your own liability under GDPR.
The EDPB published final guidelines dated 7 January 2020 outlining the role and obligations of these representatives, and you can find a summary of this on the ICO website.

UK domestic law also places a requirement on EEA organisations to appoint a representative. Controllers or processors located outside of the UK will need to appoint a UK representative if they either:

(i) offer goods or services to individuals in the UK; or
(ii) monitor the behaviour of individuals in the UK.

FAQs

1. Are SCCs still the preferred option for safeguarding the transfer of personal data from the EEA to the UK, in the event of a 'no adequacy decision'?

- SCCs are a well-known safeguard and it is recommended that these are considered ahead of other transfer mechanisms in the absence of adequacy decisions. Where they can be used, they are likely to be quicker, easier and cheaper to implement.
- The Schrems II judgment upheld SCCs as an alternative transfer mechanism to non-adequate third countries, but only where they provide "appropriate safeguards" as required by the GDPR. If the European Commission publishes an opinion that UK laws are not compatible with these safeguards, this may impact on the viability of SCCs and other alternative transfer mechanisms for EU-UK transfers. Further guidance will be issued in this case.
- Where SCCs cannot be implemented, public sector bodies should consider whether they could enter into an administrative arrangement, or whether another alternative transfer mechanism under Article 46 GDPR can be relied upon.
- If it is not possible to put in place an appropriate safeguard prior to the end of the transition period you should consider whether a derogation under Article 49 GDPR can be relied upon as a stop-gap option. However, derogations are designed to be treated as exceptions and should not be relied upon routinely.
- More detailed information can be found in the section of the guidance on 'Using Standard Contractual Clauses to access data from the EEA in a 'no adequacy' scenario'.

2. Could data be localised in order to mitigate the risk of disruption to critical data flows?

- It is likely that in most cases, **localising data would not be a proportionate action** for all but the most critical data sets given the risks associated with moving data, including security, cost, lead times, and technical capability.
- Localising data could conflict with the government's data and trade policies of removing barriers to data flows, principally by tackling unjustified data localisation. This conflict should be factored into your risk assessment.

3. Can I still send personal data unrestricted to countries in receipt of EU adequacy decisions after the end of the transition period?

- The UK has recognised the adequacy of all existing countries (and Gibraltar) that the EU has assessed as 'adequate'.
- The UK has allowed for the continued free flow of personal data from the UK to the EU.
- The UK will conduct assessments of the EU and wider EEA States and other countries under an independent international transfer regime.

4. Will I still be able to receive data from countries in receipt of EU adequacy decisions after the end of the transition period?

- Under current arrangements, flows of personal data to the UK after the end of the transition period will continue from 10 of the 13 third countries deemed adequate by the EU. Central government are working with the remaining 3 - Andorra, Guernsey, and Jersey - to maintain existing arrangements. Further information can be found on the ICO's website.

5. How do I send data to non-adequate third countries after the end of the transition period?

- At the end of the transition period, the domestic framework that will govern general processing of personal data, including rules on transfers to third countries, will be the UK GDPR.
- The UK GDPR broadly retains the same rules on international transfers that are in the EU GDPR. Alternative transfer mechanisms under Article 46 (such as administrative arrangements) and the derogations for specific situations in Article 49 will provide a legal basis for transfers of UK personal data to non-adequate third countries. Further advice on the application of these mechanisms is included above.

Definitions

In this guidance the terms "personal data", "controller" and "processor" are afforded the definitions provided by Article 4 of the General Data Protection Regulation ("GDPR").

"Personal data" 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).[1]

Further information

The ICO has also published a suite of guidance on their website:

- Data protection and the end of the transition period landing page
- FAQs
- Detailed guidance
    - Large businesses
    - SMEs
    - Police forces and other law enforcement authorities
- SCC guidance and tool

[1] Definitions for “controller” and “processor” as well as other related terms can be found in this ICO document: *https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.* Also see Articles 4(1), (7) and (8), GDPR respectively.