WHC/2019/031

WELSH HEALTH CIRCULAR

Llywodraeth Cymru
Welsh Government

Issue Date: 18th September 2019

STATUS: INFORMATION

CATEGORY: INFORMATION GOVERNANCE

Title: The Department of Culture, Media and Sport (DCMS) guidance for UK departments on mitigation options for risks to data flows

Date of Expiry / Review Our current assessment is that the likelihood of leaving the EU with no deal on 31 October subject to UK leaving the EU on 31 October

For Action by:
UHB/Trust CEO's
WAST
NWIS
PHW
Dentistry
Pharmacy
Social Services
HEIW

Action required by: As soon as possible
The Welsh Government has been working across the public sector to ensure that the risk of loss of access to required data following Brexit is understood and mitigated for. The DCMS has prepared guidance for UK departments on mitigation options for risks to data flows.

Sender:
Peter Jones, Deputy Director of Operations, Health and Social Services

HSSG Welsh Government Contact(s) :
Peter Jones, Deputy Director of Operations, Health and Social Services Peter.Lloyd.Jones@gov.wales
Jacalyn Lewis, Department Knowledge and Information Manager Jacalyn.lewis11@gov.wales

Enclosure(s): Please find enclosed a cover letter and guidance for all Welsh Public Sector Bodies

Grŵp Iechyd a Gwasanaethau Cymdeithasol
Health and Social Services Group

Llywodraeth Cymru
Welsh Government

Our ref/Ein cyf: WHC/2019/031

18 September 2019

Dear Colleague

You will be aware from previous communications that The Welsh Government has been working across the public sector to ensure that the risk of loss of access to required data following Brexit is understood and mitigated for. Our current assessment is that the likelihood of leaving the EU with no deal on 31 October is at least as great as any time so far.

By way of background, personal information has been able to flow freely between organisations in the UK and European Union due to the General Data Protection Regulation (GDPR) rules. The UK Government has indicated that at the point of exit from the EU, there will be no substantive change to the rules governing personal data as GDPR will be absorbed into UK law.

The two-way free flow of personal information will not be as straightforward however, if the UK leaves the EU without a withdrawal agreement that specifically provides for the continued flow of personal data. In such a case, transfers of personal information from the UK to EEA should not be affected, however data flow from EEA to the UK will be affected.

The UK will need to undergo an adequacy assessment of its data protection arrangements by the EU. However, the European Commission has stated repeatedly it will not commence its adequacy assessments of the UK until after the UK has left the EU. There would therefore be an “adequacy gap” immediately after a No Deal Exit, likely lasting for several years, until such time as the EU reaches a decision over whether the UK has adequate arrangements in place to allow for the free flow of personal data from the EEA to the UK. During this time the legal, free flow of personal data from the EEA will cease.

Grŵp Iechyd a Gwasanaethau Cymdeithasol
• Health and Social Services Group
Parc Cathays • Cathays Park
Caerdydd • Cardiff • CF10 3NQ

Canolfan Cyswllt Cyntaf
• First Point of Contact Centre:
E-bost • E-mail:
CustomerHelp@gov.wales
Ffôn • Tel: 0300 0604400

The purpose of this letter is to ensure that you have all the available guidance to enable you to mitigate the risk of any loss of data that you have identified.

Please find attached guidance that has been produced by the UK Government.

The Welsh Government is sharing this with all Welsh public sector bodies in order to help prepare for a “No Deal” BREXIT. The attached document brings together all of the latest available guidance on disruption to data flows and should be read in conjunction with the UK Information Commissioners Office (ICO) guidance which is regularly updated. https://ico.org.uk/for-organisations/data-protection-and-brexit/

Yours sincerely

Peter Jones
Deputy Director of Operations
Health and Social Services

Llywodraeth Cymru
Welsh Government

August 2019

Welsh Government Guidance for Welsh public sector bodies.

This guidance is designed to help Welsh public sector bodies mitigate the data protection risks associated with a no deal Brexit.

The following pages bring together all the latest available guidance and should be used in conjunction with the Information Commissioners Office (ICO) guidance which is regularly updated.

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 published a suite of no deal guidance on their website:

- FAQs
- Six steps
- Detailed guidance
- 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.

Llywodraeth Cymru
Welsh Government

Contents

Llywodraeth Cymru
Welsh Government

Using Standard Contractual Clauses to access data from the EEA in a no deal Brexit

This guidance is designed to help Welsh public sector bodies:

- decide whether they can use Standard Contractual Clauses (SCCs) to safeguard the international transfer of personal data from the European Economic Area (EEA) to the UK, in the event the UK leaves the EU without a deal; and
- practically implement SCCs into new or existing arrangements.

Flow of personal data in a no-deal Brexit

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

However, we do not expect the European Commission to have made an adequacy decision regarding the UK at the point of exit in October 2019. Therefore, for the purposes of the EU GDPR the UK will be treated as a third country without an adequacy decision. The transfer of personal data **from the EEA to the UK** will be restricted unless appropriate safeguards are in place, or the transfer benefits from one of the statutory exceptions (known as derogations for specific situations). Further information on international transfers, including a list of appropriate safeguards, is available from the Information Commissioner's Office (ICO).

Applicability and limitations

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

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

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

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

SCCs are valid for scenarios involving the receipt of personal data from an EEA organisation acting as a controller (i.e. where the EEA organisation is solely or jointly responsible for defining why and how personal data in the relevant database are to be used, collected and shared). 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 entity). In that case, please see guidance below on 'Working with data processors based in the EEA under a no deal Brexit'. 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, please read further guidance below on alternative transfer mechanisms and derogations.

Central approach – SCC implementation on behalf of Welsh Government
Welsh Government are aware that Cabinet Office's Crown Commercial Service (CCS) shall be writing to all suppliers on their G-cloud and Networks frameworks to ask them to put in place standard contract clauses. All new Frameworks will have these data-specific standard contractual clauses included as standard.

Welsh public sector bodies may wish to consider a similar approach. To this end, you can use the template SCC addendum contained in Appendix A to this guidance.

Actions to take
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 (for example HR, finance and front-line operations).

Step 2: For each business 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 contained in Appendix A to 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 a no deal Brexit. 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 ("Commission") of which there are currently three types:

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

Template SCCs and cover letter
Attached to this note at Appendix A is a template letter to suppliers and contract addendum to support you in implementing the SCCs in applicable contracts, including call-off and direct contracts.

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. The ICO advises that the Commission intends to update the existing SCCs for the GDPR but until those revised clauses are adopted existing contracts incorporating the current SCCs can continue to be used for transfers and should not be adjusted to accommodate the GDPR.

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 is best placed to complete this section as the data exporter 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 the UK following a no-deal UK exit. If they do not do this, they risk being in breach of the GDPR. The European Data Protection Board, (EDPB) and the ICO have both issued guidance on this position which you may find helpful to refer to when engaging with suppliers.

There are some limited cases where it may not be necessary for a supplier to enter into the SCCs in respect of a transfer of personal data outside of the EEA – for example if the supplier is established in the UK, but the underlying EU-UK data transfer is governed by an intra-group data transfer arrangement which incorporates the SCCs, or the supplier group benefits from Binding Corporate Rules. These are limited exceptions which should be carefully assessed.

Llywodraeth Cymru
Welsh Government

Llywodraeth Cymru
Welsh Government

Administrative Arrangements under Article 46 GDPR

This guidance is designed to help Welsh public sector bodies when considering entering into administrative arrangements for the transfer of personal data from organisations in the EEA to public authorities or bodies in the UK if the UK leaves the EU without an adequacy decision and where SCCs are **not** applicable.

Article 46(3)(b) refers to “provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights" (e.g. an MoU or policy).

This supports transfers between public authorities or bodies who cannot enter into a legally binding contract with each other.

Benefits

- They can be tailored to individual public authorities’ or bodies’ processing situations. Although the administrative arrangements 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’ 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 competent supervisory authority. The GDPR does not expressly require the supervisory authority to consult with the EDPB (see above) but the EDPB appear to think they should, as they have stated in their no deal guidance on data transfers that these arrangements are ‘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. Therefore it may not be feasible to get an administrative arrangement in place before 31 October 2019. Public authorities or bodies should consider short term mitigations including the possibility of using SCCs 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).

Template administrative arrangement and cover note

Attached to this guidance at Appendix B is a template administrative arrangement to support you in entering into administrative arrangements with EEA public authorities for the continued transfer of personal data. Please read the attached cover note which sets out handling advice and reiterates limitations that should be considered when determining whether an administrative arrangement is the most appropriate mitigation.

Llywodraeth Cymru
Welsh Government

Derogations for specific situations under Article 49 GDPR

This guidance is designed to help Welsh public sector bodies use derogations to transfer personal data from the European Economic Area (EEA) to the UK under Article 49 GDPR in the event the UK leaves the EU without a deal, in the absence of an adequacy decision or 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 - more details of which can be found in other sections of this guidance.

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.

How to Use Derogations

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. ● Explicit consent is a higher threshold than standard consent under GDPR. ○ Consent is defined in Article 4(11). 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." ○ 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 share this view and 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(s) 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 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	● 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.

performance of a contract concluded in the interest of the data subject	● Note that unlike the previous derogation 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 this 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 or codes of practice or in EU or member state caselaw. ● 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). ○ Note that 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. However, 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 doesn't 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, above. ● The supervisory authority must be informed of the transfer (but does not need to be authorised). ● 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.

Llywodraeth Cymru
Welsh Government

Working with data processors based in the EEA in a no deal Brexit

This guidance provides advice for Welsh public sector bodies concerned about the risk of disruption to the flow of personal data from processors based in the European Economic Area (EEA) in a no deal Brexit. This guidance provides our assessment of the risks of disruption to data flows between EEA data processors and data controllers in the UK, and an overview of action we have taken centrally to mitigate the risk.

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, including government departments, in the event of a no deal Brexit. No approved mechanism for repeated transfers currently exists.

The European Data Protection Board (EDPB) has not yet determined whether in its view these data flows are restricted international transfers under the EU General Data Protection Regulation (GDPR). The issue is unlikely to be resolved before 31 October.

Effect of no deal Brexit on transfers of data from EEA processors
We assess that the likelihood of significant disruption to transfers of personal data from processors in the EEA to controllers in the UK is very low.

● Data processors in the EEA are unlikely to consider the regulatory risk too high and stop sending data to the UK. This issue is not specific to Brexit and has been a current and ongoing risk for the past 20 years. 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 first bullet, though the timing of any decision may be some months away. We expect the EDPB to 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. You could take additional mitigation action during the litigation.

Central approach
To mitigate this risk, the following action was taken at UK level.

Discussions with key suppliers:
The Department of Culture, Media and Sport (DCMS) worked with the Cabinet Office to successfully secure letters of assurance from the 19 most critical strategic suppliers to government, from a personal data perspective, that they would continue to provide services in a no deal scenario. The letter was aimed at making the suppliers aware of the potential for data flows to be disrupted in a no deal EU exit scenario and outlined a set of contingency planning questions for them to consider. All 19 companies either signed the assurance letter or provided their own letter of assurance.

Service providers prioritised for Cabinet Office
Accenture
Atos
Amazon Web Services
BAE
BT
Capgemini
CGI
DXC
Fujitsu
Google
IBM
Microsoft
Motorola
Oracle
Salesforce
Sodexo
Sopra Steria
Virgin Media
Vodafone

The assurances given by suppliers relate to all central government departments and in some cases extend to Arm's Length Bodies (ALBs). In order to establish whether an ALB is covered by these assurances, the ALB will need to satisfy themselves that they can be defined as a UK 'public authority'. In the context of the GDPR, public authorities are defined in section 7 of the Data Protection Act 2018 (DPA) and

broadly comprise bodies subject to the Freedom of Information Act 2000 (although there are some exclusions).

Characteristics that suggest an ALB might be a public authority are:
● if its role is closely assimilated to or takes the place of government
● if it is linked to the government or its function could be described as governmental
● if it provides a public service
● if it is regulated, supervised and/or inspected by government
● if it is subject to judicial review or is publicly accountable for its actions
● if it has charitable objectives
● if it has enhanced statutory powers
● if its rights and responsibilities are found in public law rather than private law.

Actions

Identify and prioritise critical personal data and assess risks:
Identify and prioritise the personal data datasets which are critical to your work. Make an assessment of the risks to the continuation of critical service delivery should the flow of this personal data to your department 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.

After identifying and prioritising critical personal data as above,

Consider whether you are covered by the central assurances:

If you are covered by the above assurances consider whether this mitigation is enough for your own risk assessment.

If you are not covered or have *critical* personal data datasets with providers other than those listed, consider contacting the supplier to see what assurances they are willing to offer about the continuation of service if the UK becomes a non-adequate third country.

FAQs
Are these assurances legally binding?
● These assurances are not legally binding. Legally binding assurances cannot be given as the personal flows operate in an area of regulatory ambiguity that precedes and goes beyond Brexit

Will you be sending further letters to these suppliers?
● The assurances were not time limited - they were assurances that flows of data would continue to flow should the UK leave the EU without a deal.

● Welsh Government has received these assurances and supporting guidance from DCMS.

How did you identify these suppliers?

● Cabinet Office and DCMS worked together to identify suppliers which provide critical services or are used by a large number of public sector organisations - those that were identified were either ones that represent over £100 million government spend and/or provide goods or services to multiple government departments.

Do these assurances extend to the subsidiaries of the suppliers?

● The commitments made in the letter are intended to cover the activities of the relevant strategic supplier on an organisational / group wide basis.

● Whilst there is no express reference to affiliates etc within the letter itself, we would expect the scope to be clearly understood as extending across the wider supplier organisation.

Llywodraeth Cymru
Welsh Government

Access to EU systems, networks and databases in a no deal Brexit

This guidance is designed to help Welsh public sector bodies factor in data protection legislation when considering options to mitigate losing access to EU systems, networks and databases in a no deal Brexit.

Transfer of personal data in a no deal Brexit

The UK will transitionally recognise the EEA as though they have been subject to an affirmative adequacy decision by the UK at the point of exit in a no deal scenario. This means that, for example, personal data can continue to flow freely **from the UK to the EEA**.

However, we do not expect the European Commission to have made a data adequacy decision regarding the UK at the point of exit in October 2019. Therefore, for the purposes of the EU GDPR the UK will be treated as a third country without an adequacy decision on exit.

The transfer of personal data **from the EEA to the UK** will therefore be restricted unless appropriate safeguards are in place, or the transfer benefits from one of the statutory exceptions (known as derogations for specific situations). Further information on international transfers, including a list of appropriate safeguards, is available from the Information Commissioner's Office (ICO).

Access to EU systems, networks and databases
For the purpose of this guidance, 'EU systems, networks and databases' are defined as databases or other data-related infrastructure or services held by an EEA institution that your organisation currently has access to. Your access may be prevented as a result of the UK leaving the EEA.

Data protection aspects of access to EU systems, networks and databases

When data protection law is one of the reasons you will be prevented access: If restrictions on personal data transfers from the EEA to the UK are one of the factors that will limit access to EU systems, networks and databases post EU-Exit, your department (involving the data protection officers and departmental lawyers) should look at implementing appropriate safeguards. Guidance on GDPR appropriate safeguards and LED appropriate safeguards can be found on the Information Commissioner's Office (ICO) website and in above guidance on 'Using Standard Contractual Clauses to access data from the EU in a no deal Brexit', 'Administrative Agreements under Article 46 GDPR', and 'Alternative Transfer Mechanisms under Article 46 GDPR'.

When access will be prevented by factors other than compliance with data protection law: If continued access to EU systems, networks and databases is not possible due to legal or other factors beyond data protection and your organisation is considering other options of retaining the data, then you will still want to ensure that you comply with relevant data protection legislation as it applies to the particular processing in question.

Example Case 1

Negotiating an agreement with the EU organisation to continue access to systems, networks and databases

In some instances, setting up an agreement with an EU organisation to maintain a formal relationship post EU-Exit could allow for continuing access to an EU systems, networks and databases. If this database contains personal data, your department (in consultation with lawyers and the data protection officer) should consult guidance on which appropriate safeguards to consider. For instance:

● If you are able to enter into a contract with the EU organisation holding the database, refer to DCMS guidance on Standard Contractual Clauses.

● If you or the EEA controller of the database cannot enter into a contract, alternative options are available. See separate DCMS guidance on 'Administrative Arrangements under Article 46 GDPR', 'Alternative Transfer Mechanisms under Article 46 GDPR' and 'Derogations for specific situations under Article 49 GDPRs'.

Example Case 2

When an agreement is not possible

If your organisation is not in a position to retain continued access the EU system, network or database and you are considering alternative options, you should first engage with your data protection officer and lawyers to ensure you continue to comply with data protection law.

Roles and responsibilities
Public sector bodies retain overall responsibility for their assessment of loss of access, data management and risk mitigations.

In some cases, public sector bodies may choose to recognise and accept the unmitigated impact or be able to mitigate through alternative actions. In some discrete cases, there may be a need to copy or repatriate data (which is a decision to be taken on the bodies' own risk profile), to reconfigure a system or build a replacement.

DExEU and BEIS have also issued guidance to regulators on implementing contingency plans in a no-deal scenario to continue accessing regulatory data that is currently available to UK regulators in the form of an EU database or on an EU server.

Llywodraeth Cymru
Welsh Government

Data protection compliance in a no deal Brexit

This guidance considers data protection compliance issues in a no deal scenario **other than** in relation to the impact on international transfers which is covered in other sections of this guidance.

Data protection law post-Brexit
Once the UK leaves the EU, the EU GDPR will be adopted into UK law by section 3 of 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.

This means that, post-Brexit, 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 UK GDPR compliance when making no deal related changes to data
Organisations may be considering making changes to the way in which data processing is carried out as part of their no deal 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.

It is important to take a holistic view of the GDPR when no deal planning and ensure any compliance actions are identified and applied.

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 Brexit, including to record transfers to EEA countries as international transfers.

○ Privacy notices: Articles 13 and 14 UK GDPR requires 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 Brexit.

● 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 is taking place, the location of the data, references to relevant data protection laws, or other regulatory responsibilities resulting from Brexit. 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 should take a risk-based and proportionate approach to updating contracts (for example in a scenario of having to make relatively minor changes to a large number of contracts). Organisations could take a risk-based decision to prioritise a review of contractual language going forward to ensure it aligns with the UK GDPR.

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

<u>The requirement to comply with the EU GDPR:</u>
Organisations should be aware that they may have liability under EU GDPR in two situations:

● 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.

Given the very close alignment between UK and EU GDPR we do not anticipate significant differences to the obligations on UK organisations under the UK and EU regime at the point of Exit. 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 we recommend 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 allows data controllers and processors to liaise with one lead supervisory authority where the data processing takes place on a cross-border basis within the EEA, or if 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.

When the UK exits the EU, 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. 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

The requirement to appoint an EU representative**: Public authorities are exempt from the Article 27 EU GDPR requirement to appoint an EU representative when processing EEA resident data**. However, any department that is concerned

that organisations they are responsible for may be within the scope of Article 27 (ie because they are not a public authority) may wish to discuss this further with DCMS.

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 the relevant lead Government department as in some cases the implementing legislation may create a shortfall which will impact the original lawful basis. (We are not aware of any specific cases where this is an issue).

Llywodraeth Cymru
Welsh Government

Alternative Transfer Mechanisms under Article 46 GDPR

This guidance is designed to help Welsh public sector bodies consider implementing appropriate safeguards for the transfer of personal data from organisations in the EEA to public authorities or bodies in the UK if the UK leaves the EU without an adequacy decision and where SCCs and administrative arrangements are **not** applicable. It will focus on the implementation of the following appropriate safeguards under Article 46 GDPR: legally binding instruments and custom contractual clauses.

Please note, it is highly unlikely that custom contractual clauses could be put in place before 31 October 2019 due to the approval process required. To mitigate the day-one risks of a no deal EU Exit you should consider, perhaps as a short term mitigation, whether SCCs could in fact be used, or whether it is possible to rely on derogations in Article 49 GDPR. See sections of this guidance that cover SCCs and derogations for more information.

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 safeguards do not form the substance of this guidance. Further information can be found in the “Key Questions and Answers” section, below.

Legally Binding Instruments
Article 46(2)(a) 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 guidance 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.
● It is only applicable between public authorities or bodies, not between public bodies and private companies.

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
● 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 and is very unlikely to be completed before 31 October 2019.

Key Questions and Answers

Can BCRs be used by public authorities?
No, BCRs are designed to allow multinational companies to transfer personal data intra-group from EEA affiliates to their affiliates located outside of the EEA. BCRs can be either specifically for data controller to data controller personal data transfers (Controller BCRs), or for data transfers involving data processors (Processor BCRs). BCRs are therefore not relevant to the public sector.

Will EU supervisory authorities be promoting certification schemes or codes of conduct?
To enable a transfer from the EU to a UK organisation in a no deal, the UK organisation would need to be signed up to an EU approved code or be certified under an EU certification scheme. At this time, there are no codes of conduct or certification mechanisms that could be used if we have a no deal in October, and

creating such codes or mechanisms in order to facilitate transfers from the EU to the UK is not within the UK's gift.

Accordingly, at this stage, these safeguards should not be considered for use.

FAQ

Are Standard Contractual Clauses (SCCs) still the preferred option for safeguarding the transfer of personal data from the European Economic Area (EEA) to the UK, in the event of a no deal EU-exit?

- SCCs are a well-known safeguard and we recommend 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.
- 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 exit date 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.

What is the risk of SCCs being struck down by the CJEU in the Schrems II case?

- The court case is ongoing and it is difficult to predict what the outcome will be. A preliminary (AG) opinion will be issued in December 2019, with a final judgment expected in March 2020 (based on usual timeframes).
- The UK government considers SCCs fit for purpose and they are the preferred option at this time. We have submitted our observations on the Schrems II case to the CJEU in support of the decisions taken by the European Commission, which underpin SCCs.
- This is not an EU exit issue and the decision may have much wider ranging implications for all international transfers between the EU and third countries. DCMS will continue to monitor the impact of developments and put out further advice as necessary.

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 in to your risk assessment.

Were the letters of assurance from the 18 key suppliers to government, from a personal data perspective, time limited?

- The assurances were not time limited - they were assurances that flows of data would continue to flow should the UK leave the EU without a deal.
- Departments/devolved authorities have received these assurances and supporting guidance from DCMS. Depending on their own risk tolerances they may seek to take further measures to address this risk, however that must be balanced against other operational risks.

APPENDIX A - TEMPLATE SUPPLIER LETTER & SCC ADDENDUM

[Insert Contracting Authority letterhead]
[Supplier Contract Manager Name
Supplier Name
Street name
Town
County/Country
Postcode]

[00 Month] 2019

Dear **[Name of Supplier Contract Manager]**

Re: SCC Addendum to reflect the impact of the UK exiting the EU and the ongoing receipt of personal data from the EEA

It is in everyone's interests that the exchange of personal data between the European Economic Area (" **EEA** ") and the UK continues in the event of 'no deal' Brexit.

You may have already been contacted by the Crown Commercial Service advising you that you should expect to hear from Contracting Authorities about entering into the Standard Contractual Clauses (" **SCCs** ") in respect of transfers made under existing call-off contracts under frameworks or contracts you hold directly with departments. This letter is a request from us, as a Contracting Authority, to enter into the SCCs in respect of the following contract:

[Insert Contract Name/Date/Reference]

Action Required - by [DATE]

We ask you to review the SCCs in Annex 1 to this letter. If you are happy that they accurately reflect EEA to UK personal data transfers made from you as Supplier to us as Contracting Authority under the above contract, then you should complete any missing details, finalise Annex B: description of transfer and execute the SCCs where indicated.

The SCCs shall only be effective once signed by the Parties from the date that the United Kingdom leaves the European Union, and where:

- no adequacy decision has been made by the European Commission concerning the UK under Article 45 of the GDPR; and

- the UK is not subject to a legal transition period under which it is treated by the European Union as a Member State for the purposes of European Union law (such as the one created by Article 126 of the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, as

endorsed by leaders at a special meeting of the European Council on 25 November 2018).

Cost of Compliance

The SCCs will sit alongside our contract to support the data flows made under that contract and are a separate agreement. They do not constitute a variation to the terms of the existing contract. Further, we do not, in any case, expect organisations to incur any cost in relation to the adoption of standard contractual clauses. However, if any costs are incurred we would expect them to be attributable to cost of conducting business in the EU, and not to the supply of services to the UK public sector.

We further note that the legislative change Clause [insert clause number or remove this paragraph if you do not have clauses dealing with change in law] under the contract says that a Supplier is not entitled to relief of obligations or increase in prices as a result of a General Change of Law.

Annex 1: Controller to Controller Standard Contractual Clauses

[Note : To be populated in collaboration Parties respective Data Protection Officers]

CONTROLLER TO CONTROLLER STANDARD CONTRACTUAL CLAUSES

Data transfer agreement

between
…… (name)

…… (address and country of establishment) [TO BE COMPLETED]

hereinafter " **data exporter** ")
and
…… (name)

…… (address and country of establishment) [TO BE COMPLETED]

hereinafter " **data importer** "

each a " **party** "; together " **the parties** ".

The parties agree that the clauses are entered into in respect of transfers of personal data made under the following contract: **[name of contract] [reference number] [date].**

The parties further agree that the clauses shall come into effect in the event that the United Kingdom leaves the European Union and where: (i) no adequacy decision has been made by the European Commission concerning the UK under Article 45 of the GDPR; and (ii) the United Kingdom is not subject to a legal transition period under which it is treated by the European Union as a Member State for the purposes of European Union law (such as the one created by Article 126 of the Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community, as endorsed by leaders at a special meeting of the European Council on 25 November 2018).

Definitions

For the purposes of the clauses:

> "**personal data**", "**special categories of data/sensitive data**", "**process/processing**", "**controller**", "**processor**", "**data subject**", and " **supervisory authority/authority** " shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby the "**authority**" shall mean the competent data protection authority in the territory in which the data exporter is established);
>
> "**clauses**" shall mean these contractual clauses which are a free standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements;

"**data exporter**" shall mean the controller who transfers the personal data; and

"**data importer**" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

1. Obligations of the data exporter

The data exporter warrants and undertakes that:

1.1 personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter;

1.2 it has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses;

1.3 it will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established;

1.4 it will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time; and

1.5 it will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause 3, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

2. Obligations of the data importer

The data importer warrants and undertakes that:

2.1 it will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of

security appropriate to the risk represented by the processing and the nature of the data to be protected;

2.2 it will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data;

2.3 it has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws;

2.4 it will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses;

2.5 it will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed the data importer will assume responsibility for compliance with the provisions of clause 1.5;

2.6 at the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause 3 (which may include insurance coverage);

2.7 upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion;

2.8 it will process the personal data, at its option, in accordance with:

2.8.1 the data protection laws of the country in which the data exporter is established; or

2.8.2 the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data imported complies with the relevant provisions of such an authorisation or decision and is based in

a country to which such authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data; or

2.8.3 the data processing principles set forth in Annex A:

2.8.3.1 Data importer to indicate which option it selects: 2.8.3

2.8.3.2 Initials of data importer deemed included

2.9 It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer;
and

2.9.1 the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection; or

2.9.2 the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU; or

2.9.3 data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards; or

2.9.4 with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

3. Liability and third party rights

3.1 Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (ie damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

3.2 The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses 1.2, 1.4, 1.5, 2.1, 2.3, 2.4, 2.5, 2.8, 2.9, 3.1, 5, 6.4 and 7 against the data importer or the data exporter, for their respective breach of their contractual obligations with regard to his personal data and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by that data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer, if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data

exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

4. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause 2.8 which shall apply only if so selected by the data importer under that clause.

5. Resolution of disputes with data subjects or the authority

5.1 In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

5.2 The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

5.3 Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

6. Termination

6.1 In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

6.2 In the event that:

6.2.1 the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph 6.1;

6.2.2 compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligation in the country of import;

6.2.3 The data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

6.2.4 a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter;

6.2.5 a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs;

6.2.6 then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by 6.2.1, 6.2.2 or 6.2.5 above the data importer may also terminate these clauses.

6.3 Either party may terminate these clauses if:

6.3.1 any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer; or

6.3.2 Directive (95/46/EC (or any superseding text) becomes directly applicable in such country.

6.4 The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause 6.3) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

7. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

8. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause 1.5. The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required.
Annex B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A: DATA PROCESSING PRINCIPLES

1. **Purpose limitation:** Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. **Data quality and proportionality**: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. **Transparency:** Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. **Security and confidentiality:** Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. **Rights of access, rectification, deletion and objection:** As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. **Sensitive data:** The data importer shall take such additional measures (eg relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause 2.

7. **Data used for marketing purposes:** Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt out" from having his data used for such purposes.

8. **Automated decisions:** For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

8.1 (i) such decisions are made by the data importer in entering into or performing a contract with the data subject; and

(ii) the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties; or

8.2 where otherwise provided by the law of the data exporter.

ANNEX B: DESCRIPTION OF THE TRANSFER

[*To be completed by the parties*]
Data subjects
The personal data transferred concern the following categories of data subjects:
[employees, candidates for jobs, consultants, agents, retirees]

Purpose of the transfer(s)
The transfer is made for the following purposes: [_]

Categories of data
The personal data transferred concern the following categories of data: [e.g. name, email address, postal address, national / social security insurance number, employee number]

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients: [e.g. to other group companies as required for the purposes of the transfer and to third party companies which are contracted to provide relevant services under instruction of the data importer.]

Sensitive data (if appropriate)
The personal data transferred concern the following categories of sensitive data:
[e.g. health data, trade union membership details, criminal convictions and offences]

Data processing registration information of the data exporter (where applicable)

Additional useful information (storage limits and other relevant information)

Contact points for data protection enquiries

DATA IMPORTER

…… ……

DATA EXPORTER

…… ……

APPENDIX B - TEMPLATE ADMINISTRATIVE ARRANGEMENT & COVER NOTE

Cover Note Template: Administrative Arrangement for the transfer of personal data

This template is designed to help when considering entering into an administrative arrangement with an EEA public authority under Article 46(3)(b) of the General Data Protection Regulation (GDPR).

This template is intended to be used for bilateral arrangements, however, you may consider tailoring this for multilateral arrangements if appropriate.

In the event that the UK leaves the EU without a deal or an adequacy decision, UK and EEA public authorities or bodies could use administrative arrangements to enable the continued transfer of personal data between them. Further information about administrative arrangements can be found at the ICO's website, or in the above guidance.

Limitations
Standard contractual clauses (SCCs) are generally the **preferable** alternative transfer mechanism and should be considered before administrative arrangements where they are possible to implement. SCCs are a well-known safeguard and can be implemented more quickly and easily (for further information about SCCs please see the guidance on 'Using Standard Contractual Clauses to access data from the EEA in a no deal Brexit').

Whilst the GDPR only expressly requires that administrative arrangements are authorised by the competent supervisory authority, it is highly likely that the European Data Protection Board (EDPB) will want to approve arrangements and may not begin this process until after the UK has exited the EU. This may influence the approach of supervisory authorities seeking to comply with the consistency mechanism as required by Article 46(4) GDPR. Therefore, it is important that EEA public authorities engage with the competent supervisory authority at an early stage to fully understand timing implications.

If it is not possible to have an administrative arrangement approved from day one post-exit then departments should consider whether there are other short term mitigations that could be relied upon, for example, Article 49 GDPR derogations.

Handling advice

1. To consult with EEA public authority about preferred appropriate safeguard under Article 46 of the GDPR;

2. Template can be used to help authorities draft an administrative arrangement;

3. Administrative arrangement must then be authorised in advance by the competent EEA supervisory authority (please note that the ICO **does not** need to review arrangements as transfers from the UK to the EU will be covered by transitional adequacy provisions). The EEA public authority should engage the supervisory authority and attempt to have the arrangement reviewed (please note that it may not be possible to have the arrangement approved prior to the UK exiting the EU as there are no grounds for having an administrative arrangement between two EEA organisations).

Draft administrative arrangement for the transfer of personal data between

EEA public authority

And

UK public authority

each an " **Authority** ", together the " **Authorities** ",

acting in good faith, will apply the safeguards specified in this administrative arrangement (" **Arrangement** ") to the transfer of Relevant Personal Data between them,

recognizing the importance of the protection of Personal Data and of having robust data protection regimes in place,

having regard to Article 46(3)(b) of the GDPR and the UK GDPR,

having regard to Applicable Legal Requirements and in particular the incorporation of Regulation (EU) 2016/679 into UK domestic law,

having regard to the competence of the UK's data protection supervisory authority to handle complaints from EEA data subjects about controllers and processors in relation to

Processing by them regulated by the UK GDPR,

having regard to the jurisdiction of [UK courts] to adjudicate proceedings brought by EEA data subjects against controllers and processors in relation to Processing by them regulated by the UK GDPR,

[NOTE: Depending on the laws of the EEA state it may be possible to mirror the above two paragraphs in relation to the rights of UK data subjects before an EEA data protection supervisory authority or EEA court. However, you will need to first check this with the EEA public authority.]

acknowledging the importance of regular dialogue between the Authorities and their national data protection supervisory authorities,

having regard to the need to Process Personal Data to carry out the public mandate and exercise of official authority vested in the Authorities, and

having regard to the need to ensure efficient international cooperation between the Authorities acting in accordance with their mandates as defined by applicable laws to [insert relevant public function of Authorities],

have reached the following understanding:

I. Purpose and Scope

This Arrangement is limited to transfers of Relevant Personal Data between [EEA public authority] and [UK public authority], in their capacity as public authorities.

The Authorities are committed to having in place appropriate safeguards for the Processing of such Relevant Personal Data in the exercise of their respective responsibilities.

Each Authority confirms that it can and will act consistent with this Arrangement and that it has no reason to believe that existing Applicable Legal Requirements prevent it from doing so.

[NOTE: to be included if relevant] This Arrangement is intended to supplement existing information sharing arrangements or memoranda that may exist between [EEA public authority] and [UK public authority], and to be applicable in different contexts, including information that may be shared for supervisory or enforcement related purposes.

Effective and enforceable Data Subject Rights are available under Applicable Legal Requirements in the jurisdiction of each Authority, however this Arrangement does not create any legally binding obligations, confer any legally binding rights, nor supersede domestic law. The Authorities have implemented, within their respective jurisdictions, the safeguards set out in Section III of this Arrangement in a manner consistent with Applicable Legal Requirements. The Authorities provide safeguards to protect Relevant Personal Data through a combination of laws, regulations and their internal policies and procedures.

II. Definitions

For the purposes of this Arrangement:

(a) **"Applicable Legal Requirements"** means the relevant legal framework for the protection of Relevant Personal Data applicable to each Authority;

(b) " **Data Subject Rights"** means rights of Data Subjects under the GDPR and UK GDPR, including:

i. **the right not to be subject to automated decisions, including Profiling** : a Data Subject's right not to be subject to legal decisions being made concerning him or her based solely on automated Processing;

ii. **the right of access** : a Data Subject's right to obtain from an Authority confirmation as to whether or not Personal Data concerning him or her are being Processed, and where that is the case, to access the Personal Data;

iii. **the right of erasure** : a Data Subject's right to have his or her Personal Data erased by an Authority where the Personal Data are no longer necessary for the purposes for which they were collected or otherwise Processed, or where the data have been unlawfully collected or otherwise Processed;

iv. **the right of information** : a Data Subject's right to receive information on the Processing of Personal Data relating to him or her in a concise, transparent, intelligible and easily accessible form;

v. **the right of objection** : a Data Subject's right to object, on grounds relating to his or her particular situation, at any time to Processing of Personal Data concerning him or her by an Authority, except in cases where there are compelling legitimate grounds for the Processing that override the grounds put forward by the Data Subject or for the establishment, exercise or defence of legal claims;

vi. **the right of rectification** : a Data Subject's right to have his or her inaccurate Personal Data corrected or completed by an Authority without undue delay;

vii. **the right of restriction of Processing** : a Data Subject's right to restrict the Processing of his or her Personal Data where the Personal Data are inaccurate, where the Processing is unlawful, where the Authority no longer needs the Personal Data for the Purposes for which they were collected or where the Personal Data cannot be deleted;

(c) **"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

(d) **"Onward Transfer"** means the transfer, other than the Sharing of Relevant Personal Data, of Relevant Personal Data by the Receiving Authority to a third party in another country;

(e) " **Personal Data"** means any information relating to an identified or identifiable natural person (" **Data Subject** ") within the scope of this Arrangement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(f) **"Processing"** means any operation or set of operations performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(g) " **Professional Secrecy** " means the general legal obligation of an Authority not to disclose non-public information received in an official capacity;

(h) " **Profiling** " means automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a Data Subject;

(i) " **Purpose** " means the legitimate and specific purpose of assisting the Receiving Authority to fulfil its responsibilities as set out in this Agreement;

(j) " **Relevant Data Subject** " means a Data Subject of the Relevant Personal Data.

(k) " **Relevant Personal Data** " means Personal Data transferred from one Authority (**"Transferring Authority"**) to the other Authority (**"Receiving Authority"**) under this Arrangement;

(l) " **Relevant Personal Data Breach"** means a breach of data security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Relevant Personal Data transmitted, stored or otherwise processed;

(m) **"Sharing of Relevant Personal Data"** means the sharing of Relevant Personal Data by the Receiving Authority:

i. with a third party in its country;

ii. in the case of [the EEA public authority] , with a third party within the EEA; or

iii. with a third party in another country when that transfer is covered by an adequacy decision in accordance with the Applicable Legal Requirements of the Transferring Authority; and

(n) **"UK GDPR"** means the GDPR as it is has the meaning in section 3(10) of the UK Data Protection Act 2018.

NOTE: further definitions may be required depending on the nature of the transfer

III. Personal Data protection safeguards

1. Purpose limitation: The Authorities have responsibilities which include [to be completed as relevant]. Relevant Personal Data are transferred between the Authorities to support these responsibilities and are not transferred for other purposes such as for marketing or commercial reasons.

The Transferring Authority will transfer Relevant Personal Data only for the Purpose. The Receiving Authority will not further Process the Relevant Personal Data in a manner that is incompatible with the Purpose, nor with the purpose that may be set out in any request for the information.

2. Data quality and proportionality: The Transferring Authority will only transfer Personal Data that are adequate, relevant and limited to what is necessary for the Purpose.

The Transferring Authority will ensure that to the best of its knowledge the Personal Data that it transfers are accurate and, where necessary, up to date. Where an Authority becomes aware that Personal Data it has transferred to, or received from, the other Authority is incorrect, it will advise the other Authority about the incorrect data. The Authorities will, having regard to the Purpose for which the Relevant Personal Data have been transferred and further Processed, supplement, erase, block, correct or otherwise rectify the Relevant Personal Data, as appropriate.

3. Transparency: In addition to complying with its transparency obligations under the Applicable Legal Requirements, each Authority will provide a general notice to Relevant Data Subjects about: (a) how and why it may Process and transfer Personal Data pursuant to the Arrangement; (b) the details of the other Authority to which such data may be transferred; (c) the rights available to Relevant Data Subjects under the Applicable Legal Requirements, including how to exercise those rights; (d) information about any applicable delay or restrictions on the exercise of such rights, including restrictions that apply in the case of cross-border transfers of Personal Data; and (e) contact details for submitting a dispute or claim.

This notice will be effected by the publishing of this information by each Authority on its website along with this Arrangement or by making the notice and Arrangement available to individuals upon request (with a notice on its website to that effect).

4. Security and confidentiality: The Receiving Authority will have in place appropriate technical and organisational measures to protect Relevant Personal Data against accidental or unlawful access, destruction, loss, alteration, or unauthorised disclosure. Such measures will include appropriate administrative, technical and physical security measures. These measures may include, for example, marking information as Personal Data, restricting who has access to Personal Data, providing secure storage of Personal Data, or implementing policies designed to ensure Personal Data are kept secure and confidential.

In the case where the Receiving Authority becomes aware of a Relevant Personal Data Breach, it will inform the Transferring Authority as soon as possible and use reasonable and appropriate means to remedy the Relevant Personal Data Breach and minimize the potential adverse effects.

5. Safeguards Relating to Data Subject Rights
The Authorities will apply the following safeguards to Relevant Personal Data:

The Authorities will have in place appropriate measures which they will follow, such that, upon request from a Relevant Data Subject, an Authority will (1) identify any Relevant Personal Data it has received from the other Authority pursuant to this Arrangement; (2) provide general information, including on an Authority's website, about safeguards applicable to transfers to the other Authority, which may include the notice required by Section III (3) of this Arrangement (Transparency); and (3) provide access to the Relevant Personal Data and confirm that the Relevant Personal Data are complete, accurate and, if applicable, up to date.

The Receiving Authority will allow a Data Subject who believes that his or her Relevant Personal Data are incomplete, inaccurate, outdated or Processed in a manner that is not in accordance with the Applicable Legal Requirements or consistent with the safeguards set out in this Arrangement, to make a request directly to the Receiving Authority for any rectification, erasure, restriction of Processing, or blocking of the Relevant Personal Data.

The Receiving Authority, in accordance with the Applicable Legal Requirements, will address in a reasonable and timely manner a request from a Relevant Data Subject concerning the rectification, erasure, restriction of Processing or objection to Processing of his or her Relevant Personal Data. The Receiving Authority may take

appropriate steps, such as charging reasonable fees to cover administrative costs or declining to act on a request, where a Relevant Data Subject's requests are manifestly unfounded or excessive.

Each Authority may use automated means to more effectively fulfil its mandate. However, no Receiving Authority will take a decision which produces legal effects concerning a Data Subject or significantly affecting him or her based solely on automated Processing of the Relevant Personal Data, including Profiling, without human involvement.

Safeguards relating to Data Subject Rights are subject to an Authority's legal obligation not to disclose confidential information pursuant to Professional Secrecy or other legal obligations. These safeguards may be restricted to prevent prejudice or harm to supervisory or enforcement functions of the Authorities acting in the exercise of the official authority vested in them, such as for the monitoring or assessment of compliance with applicable laws or prevention or investigation of suspected offences; for important objectives of general public interest, as recognised in the jurisdiction of the Receiving Authority and, where necessary under the Applicable Legal Requirements, of the Transferring Authority, including in the spirit of reciprocity of international cooperation; or for the supervision of regulated individuals and entities. The restriction should be necessary and provided by law, and will continue only for as long as the reason for the restriction continues to exist.

6. Onward Transfers and Sharing of Relevant Personal Data:

6.1 Onward Transfer of Relevant Personal Data
The Receiving Authority will only Onward Transfer Relevant Personal Data with the prior written consent of the Transferring Authority, and if the third party provides appropriate assurances that are consistent with the safeguards in this Arrangement.

6.2 Sharing of Relevant Personal Data
(1) Sharing of Relevant Personal Data pursuant to this Arrangement will only take place with the prior written consent of the Transferring Authority, and if the third party provides appropriate assurances that are consistent with the safeguards in this Arrangement.

(2) Where assurances contemplated under the first paragraph cannot be provided by the third party, the Relevant Personal Data may be shared with the third party in exceptional cases if Sharing the Relevant Personal Data is for important reasons of public interest, as recognised in the jurisdiction of the Receiving Authority and, where necessary under the Applicable Legal Requirements, of the Transferring Authority, including in the spirit of reciprocity of international cooperation, or if the Sharing of Relevant Personal Data is necessary for the establishment, exercise or defence of legal claims.

(3) Where Sharing of Relevant Personal Data is for the purpose of conducting a civil or administrative enforcement proceeding, assisting in a self-regulatory organisation's surveillance or enforcement activities, assisting in a criminal prosecution, protecting the vital interests of the Relevant Data Subject or of another individual, or conducting any investigation for any general charge applicable to the violation of the provision specified in the request where such general charge pertains to a violation of the laws and regulations administered by the Receiving Authority,

including enforcement proceedings which are public, the Receiving Authority may Share Relevant Personal Data with a third party (such as public bodies, courts, [self-regulatory organisations] and participants in enforcement proceedings) without requesting consent from the Transferring Authority, nor obtaining assurances, if the Sharing of Relevant Personal Data is for purposes that are consistent with the Purpose or with the general framework of the use stated in the request, and is necessary to fulfil the responsibilities of the Receiving Authority and/or the third party. [NOTE: Optional if relevant] [When Sharing Relevant Personal Data received under this Arrangement with a self-regulatory organisation, the Receiving Authority will ensure that the self-regulatory organisation is able and will comply on an ongoing basis with the security and confidentiality protections set out in Section III (4) of this Arrangement].

(4) The Receiving Authority may Share Relevant Personal Data with a third party without requesting consent from the Transferring Authority, nor obtaining assurances, in a situation where the Sharing of Relevant Personal Data follows a legally enforceable demand or is required by law. The Receiving Authority will notify the Transferring Authority prior to the Sharing of Relevant Personal Data and include information about the data requested, the requesting body and the legal basis for Sharing the Relevant Personal Data. The Receiving Authority will use its best efforts to limit the Sharing of Relevant Personal Data, in particular through the assertion of all applicable legal exemptions and privileges.

7. Limited data retention period: The Receiving Authority will retain Relevant Personal Data for no longer than is necessary and appropriate for the Purpose. Such retention period will comply with the applicable laws, rules and/or regulations governing the retention of such data in the jurisdiction of the Receiving Authority.

8. Redress: Each Authority acknowledges that a Relevant Data Subject who believes that the Receiving Authority has failed to comply with the safeguards set out in this Arrangement, or who believes that his or her Relevant Personal Data have been subject to a Relevant Personal Data Breach, may seek redress against that Authority to the extent permitted by Applicable Legal Requirements. This redress may be exercised before any competent body, which may include a court, in accordance with the Applicable Legal Requirements of the jurisdiction where the alleged non-compliance with the safeguards in this Arrangement occurred. Such redress may include monetary compensation for damages.

In the event of a dispute or claim brought by a Relevant Data Subject concerning the Processing of the Relevant Data Subject's Relevant Personal Data against the Transferring Authority, the Receiving Authority, or both Authorities, the Authorities will inform each other about any such disputes or claims, and will use best efforts to cooperate and resolve the dispute or claim amicably. The Receiving Authority commits to put in place a mechanism to effectively handle and resolve complaints from Relevant Data Subjects regarding this Arrangement and complaints must be dealt with without undue delay, and in any event in accordance with the timings and requirements set out in Article 12(3) of the GDPR and the UK GDPR. The complaints must be dealt with by a clearly identified department or person with an appropriate level of independence in the exercise of his/her functions. The application form must explain how data subjects will be informed about the practical steps of the complaint system, in particular: where to complain, in what form, delays for the reply on the complaint, consequences in case of rejection of the complaint, consequences in

case the complaint is considered as justified, and consequences if the data subject is not satisfied by the replies (the right to lodge a claim before the Court and a complaint before the Supervisory Authority).

If an Authority or the Authorities are not able to resolve the matter with the Relevant Data Subject, the Authorities will use other methods by which the dispute could be resolved, unless the Relevant Data Subject's requests are manifestly unfounded or excessive. Such methods will include participation in non-binding mediation or other non-binding dispute resolution mechanisms, which may be done remotely (such as by telephone or other electronic means).

In the event that the Receiving Authority is not willing or able to implement the outcome of the non-binding mediation or other non-binding dispute resolution proceeding referred to in Section III (8) of this Arrangement, it will promptly inform the Transferring Authority and its competent data protection supervisory authority.

Where both Authorities agree to not implement the outcome of the non-binding mediation or alternative dispute resolution mechanism, the Authority that is the primary contact point for the Relevant Data Subject thereof shall inform him or her of (1) the decision to not implement the outcome of the non-binding mediation or alternative dispute resolution mechanism and reasons for not doing so; and (2) his or her right to lodge a complaint with the data protection supervisory authorities respectively competent for the Transferring Authority and the Receiving Authority, and how to make that complaint in practice.

If the Transferring Authority believes that the Receiving Authority is failing to comply with the safeguards set out in this Arrangement, the Transferring Authority will suspend the transfer of Relevant Personal Data to the Receiving Authority until the Transferring Authority is satisfied that the Receiving Authority has addressed those concerns, and will inform without undue delay the Relevant Data Subject, as well as the data protection supervisory authorities respectively competent for the Transferring Authority and the Receiving Authority.

IV. Ongoing relationship

1. Each Authority will conduct periodic reviews of its own policies and procedures that implement this Arrangement and of their effectiveness. If there is any change to policies or procedures that will impact this Arrangement, or if any policies or procedures relating to this Arrangement are found to be ineffective in the context of a periodic review, each Authority should promptly inform the other Authority, as well as its competent data protection supervisory authority. Upon reasonable request by the Transferring Authority, the Receiving Authority will review its Personal Data Processing policies and procedures to ascertain and confirm that the safeguards in this Arrangement are being implemented effectively. The results of the review will be communicated to the Transferring Authority.

2. Each Authority will promptly notify the other Authority of any change to the Applicable Legal Requirements that will impact this Arrangement, and in particular any of the safeguards and protections provided by it.

3. In the event that the Receiving Authority is unable to effectively implement the safeguards in this Arrangement for any reason, it will promptly inform the

Transferring Authority and its competent data protection supervisory authority, in which case the Transferring Authority will temporarily suspend the transfer of Relevant Personal Data to the Receiving Authority until such time as the Receiving Authority informs the Transferring Authority that it is again able to act consistent with the safeguards.

V. Revision and discontinuation

1. The Authorities may consult and revise by mutual consent the terms of this Arrangement in the event of substantial change in the laws, regulations or practices affecting the operation of this Arrangement.

2. An Authority may discontinue its participation in this Arrangement, vis-à-vis the other Authority, at any time. It should endeavour to provide 30 days' written notice to the other Authority of its intent to do so. Any Relevant Personal Data already transferred will continue to be treated consistent with the safeguards provided in this Arrangement.

3. The competent data protection supervisory authorities in the respective countries of the Authorities, will be notified by the Authorities of any proposed material revisions to, or discontinuation of, this Arrangement.

Date: