FAQs in relation to *Schrems II*, new SCCs and HSE compliance requirements
Last updated 6 December 2021

Q1. Do special rules or restrictions apply to international transfers of personal data?

The General Data Protection Regulation ('**GDPR**') applies a regime of data protection rules across the European Economic Area ('**EEA**'), which includes all EU countries and Iceland, Liechtenstein and Norway. Transfers of personal data transfers from inside this region to a destination outside the EEA (known as a '**third country**') are subject to restrictions and must use a transfer mechanism prescribed by the GDPR.

Chapter 5 of the GDPR sets out the permitted transfer mechanisms to transfer personal data, to or permit access to the data from, third countries such as adequacy decisions, appropriate safeguards (including standard contractual clauses), and in certain limited circumstances, exemptions to these restrictions (known as '**derogations**').

Q2. (a) What is *Schrems II* and (b) what are its implications for transfers of personal data outside the EEA?

(a) On 16 July 2020, the Court of Justice of the European Union gave judgment in Case C-311/18: Data *Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (known as '***Schrems II***')[1] which examined the validity of (i) a partial adequacy decision for transfers of personal data to the United States known as the EU-US Privacy Shield and (ii) the validity of standard contractual clauses as an appropriate safeguard.

(b) The Court found that the EU-US Privacy Shield was invalid and could no longer be relied upon as a lawful transfer mechanism of personal data to the United States. Thus, standard contractual clauses continued to be valid but only where the data exporter verifies (prior to any transfer taking place and taking into account the circumstances of the transfer) whether a level of protection applies to the personal data that is 'essentially equivalent' to that found in the European Union is respected in the third country concerned. This requires the data exporter with the data importer to assess if there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate safeguards being relied upon, taking into account the circumstances of the particular transfer. Where an impingement is identified, the parties must then look at whether any supplementary measures can be adopted that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence. This assessment is known as a transfer risk assessment or transfer impact assessment (a '**TIA**').

Q3. Where can I get more detailed information on *Schrems II*?

A more detailed legal FAQ on *Schrems II* can be requested via your regional consumer affairs department.

Q4. What are adequacy decisions?

An adequacy decision is a decision adopted by the European Commission where it has decided that a third country, a territory, one or more specified sectors (e.g. public or private) within a third country or an international organisation including its subordinate bodies (such as the United Nations and the World Health Organisation) ensures an adequate level of protection of personal data. Where adequacy decisions can be relied upon, no other GDPR transfer mechanism, such as appropriate safeguards or an associated TIA, are required.

[1] The judgment is full is available here: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11388612

Q5. For which countries has the European Commission adopted adequacy decisions?

The European Commission has adopted adequacy decisions for the following countries: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, United Kingdom and Uruguay.

The adequacy decisions on Canada and Japan are partial decisions that apply only to private entities subject to certain data protection laws in those countries.

Where adequacy decisions are in place, the data exporter is not required to implement any other appropriate safeguards or put any supplementary measures in place to validate the transfer.

Q6. Is there an adequacy decision for transfers to the United Kingdom?

Yes. The European Commission adopted an adequacy decision on 28 June 2021 for the United Kingdom so no further steps need to be taken in respect of personal data transfers to the UK where this adequacy decision applies (Transfers for the purposes of UK immigration control are excluded from the scope of the adequacy decision). This adequacy decision remains valid for four years (unless amended or revoked) until 27 June 2025.

From a general data protection perspective, relationships with any UK-based service providers or partners should consider whether any other formal arrangements are required such as a data processing agreement (as required by Article 28 of the GDPR) or a data sharing 'arrangement' (as required by Article 26 of the GDPR) with joint controllers.

Q7. Can the adequacy decisions be withdrawn?

Yes. Adequacy decisions should be reviewed carefully, as they can be limited in scope to certain territories or sectors and can be invalidated with immediate effect if a supervisory authority or data subject challenges them before national courts (as occurred in *Schrems II* in respect of the Privacy Shield) or if the European Commission withdraws or suspends the Adequacy Decision. Some Adequacy Decisions may also have expiration dates. For example, the Adequacy Decision for the United Kingdom is due to expire (unless renewed) on 27 June 2025.

Q8. What are appropriate safeguards?

Appropriate safeguards are a range of transfer tools, one of which is provided by a Controller or Processor such as standard contractual clauses ('**SCCs**'), binding corporate rules, certification mechanism or codes of conduct on condition that the data subjects concerned will have enforceable data subject rights and effective legal remedies in the destination third country.

Appropriate safeguards are required in all circumstances where personal data is being transferred outside the EEA and there is no adequacy decision in place and no derogation applies.

In response to *Schrems II*, the European Data Protection Board ('**EDPB**') has adopted final Recommendations 01/2020 on measures that supplement appropriate safeguards for international personal data transfers to ensure compliance with the EU level of protection of personal data (the '**Recommendations**').[2] The Recommendations set out a six step approach to compliance with Chapter 5 of the GDPR and *Schrems II*.

[2] The Recommendations are available here: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

The EDPB has also published Recommendations on European Essential Guarantees for surveillance measures[3] to guide data exporters in evaluating whether requirements to disclose personal data or measures authorising access by public authorities in a third country are "*limited to what is necessary and proportionate in a democratic society*".

Q9. What are the SCCs?

The SCCs are standard or model contractual clauses approved by European Commission which (i) implement contractual safeguards between the data exporter and the data importer (i.e. the relevant third party service provider, supplier or other entity as the case may be that is located in a third country); and (ii) ensure that any personal data leaving the EEA will be protected to the standard applicable in the EU under the GDPR read in light of the Charter of the Fundamental Rights of the European Union.

On 27 June 2021, new SCCs adopted by the European Commission came into effect (**2021 SCCs**). The 2021 SCCs replace three sets of SCCs (adopted pre-GDPR in 2001, 2004 and 2010) in order to update them to reflect GDPR requirements and modern business realities, as well as taking into account *Schrems II* requirements.

Q10. Can the pre-2021 SCCs still be relied upon?

Since 27 September 2021, it is no longer possible to conclude contracts incorporating any of the pre-2021 sets of SCCs.

Data exporters and data importers may continue to rely on those older sets of SCCs that were concluded before 27 September 2021 until 27 December 2022, provided the processing operations governed by the SCCs remain unchanged. From 27 December 2022, all transfers relying on SCCs must rely upon the 2021 SCCs.

Q11. Can SCCs be altered or amended?

No, the SCCs are non-negotiable and cannot be amended. The parties can however add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the SCCs or prejudice the fundamental rights or freedoms of data subjects. In practice, this means that parties can add clauses that are purely commercial in nature and do not impact upon the level of protection applicable to the personal data or the rights afforded to data subjects or supervisory authorities under the SCCs.

Q12. Can the SCCs be included as part of another contract such as Services Contract or Master Services Agreement?

Yes. The SCCs can operate as a stand-alone contract or can be incorporated in a wider contract, where required.

Q13. Can additional parties sign up to the SCCs at a later date?

Yes. It is possible for additional controllers and processors to accede to the 2021 SCCs as data exporters or data importers throughout the lifecycle of the relevant contract and an optional "docking clause" is included for this purpose.

[3] The European Essential Guarantees: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en

Q14. How do the SCCs work?

The 2021 SCCs follow a modular approach. There are four modules as follows depending on the relationship of the parties under the GDPR:

- Module 1 SCCs (Controller to Controller)
- Module 2 SCCs (Controller to Processor)
- Module 3 SCCs (Processor to Processor)
- Module 4 SCCs (Processor to Controller)

The relevant module of SCCs must be identified, populated and signed by the parties. Each category of personal data being transferred must be considered separately to determine the roles of the parties in respect of a particular dataset.

Q15. Where SCCs are in place, must a data processing agreement or a data sharing 'arrangement' also be put in place?

Under Article 26 of the GDPR, where a controller shares personal data with another controller and they jointly determine the purposes and means of processing, they are joint controllers and must put in place an arrangement to reflect their respective roles and relationships regarding the data subjects. Module 1 SCCs do not explicitly meet this requirement so data sharing arrangements where the parties are joint controllers should be considered in addition to the SCCs.

Under Article 28 of the GDPR, personal data sharing from controller to processor or processor to processor require certain mandatory contractual provisions to be put in place between the parties, i.e. a 'data processing agreement'. The 2021 SCCs state that where relying upon Module 2 SCCs or Module 3 SCCs, no additional data processing agreement is required to be put in place between the parties.

Q16. What obligations do the SCCs impose on data importers?

The 2021 SCCs primarily impose GDPR-like obligations upon the data importer such as:

- adhering to purpose limitation, accuracy, minimisation, retention, and destruction requirements;
- documenting the processing activities it performs on the transferred data;
- submitting to the jurisdiction of and cooperating with the Data Protection Commission in relation to the transfer;
- notifying the data exporter if it is unable to comply with the SCCs;
- returning or securely destroying the transferred data at the end of the contract;
- applying additional safeguards to "sensitive data" which is special category data (such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data (where used for identification purposes); data concerning health, a person's sex life or a person's sexual orientation) or data relating to criminal convictions or prosecutions;
- notifying the exporter and data subject if it receives a legally binding request from a public authority to access the transferred data, if permitted; and
- challenging a public authority access request if it reasonably believes the request is unlawful.

Q17. (a) When is a TIA required and does it follow a prescribed format? (b) What does a TIA assess?

(a) The format of the TIA is not prescribed, although it must be documented and should meet the requirements of the Recommendations. Supplementary measures may also be required, depending on the outcome of the TIA. Both the Recommendations and the 2021 SCCs recommend that the TIA must primarily be based on objective sources of information. The 2021 SCCs require the data exporter and the data importer to warrant that there is no reason to believe local laws of the third country will prevent the data importer from complying with its obligations under the SCCs.

(b) However, before this warranty can be given, the TIA must assess:

- the facts and circumstances of the particular transfer (such as the nature of the data, economic sector in which the importer operates, the duration of transfer, purpose for processing, storage location of the data, intended onward transfers);
- the relevant laws and practices of the destination third country (including the existence or absence of public authority requests for access to the personal data); and
- any reasonable safeguards designed to supplement the protections of the SCCs that apply to the data in transit and during processing in the third country.

Q18. Is there an obligation to review the TIA following their completion?

The Recommendations provide that the TIA should be re-evaluated periodically in order to ensure the level of protection afforded to the personal data being transferred to or accessed from the third country is maintained or to identify any changes to the position.

Q19. I am a health researcher – where can I get the documentation I need for my clinical trial /study?

Please contact your local Research Ethics Committee (**REC**) office or the National Research Office (ResearchandDevelopment@hse.ie).

Q20. I am launching a new IT system under the governance of OCIO – how do I get access to the required documentation for international data transfers?

Please contact the OCIO (OoCIO.NationalServiceDesk@hse.ie).

Q21. How do I get access to the SCC module documents, guidance notes and the HSE TIA?

These can be requested via your regional consumer affairs offices.

Q22. What record keeping obligations does the HSE have in relation to SCCs and TIAs?

Each of the various business units within the HSE will be responsible for preparing their own transfer impact assessments (TIAs) and ensuring that the decisions arising from those TIAs are documented. The TIAs must be safely stored and easily accessible in order that they can be readily produced, for example, for audit purposes or where requested by the Data Protection Commission or any other supervisory or regulatory authority.

***To request copy of detailed legal FAQ on Schrems compliance and a copy of the HSE Transfer Impact Assessment (TIA) Form, please see relevant departmental details below*.**

Relevant contact details:

For OCIO International data transfer queries:

- Chris Meehan, OCIO Research and evidence office – Chris.Meehan@hse.ie
- OCIO Helpdesk - OoCIO.NationalServiceDesk@hse.ie

For Regional queries (for projects or data processing involving international data transfers not under governance of OCIO):

- West - Deputy Data Protection Officer - ddpo.west@hse.ie
- Dublin North-East - Deputy Data Protection Officer - ddpo.dne@hse.ie
- Dublin mid-Leinster - Deputy Data Protection Officer - ddpo.dml@hse.ie
- South - Deputy Data Protection Officer - ddpo.south@hse.ie
- National – DPO and Head of Data Protection – dpo@hse.ie

For Health Research queries on International data transfers (for ethically-approved studies):

- Research and Development - ResearchandDevelopment@hse.ie
- Research Ethics Committee - Hse.rec@hse.ie

For any legal issues/legal queries arising in relation to completion of Transfer Impact Assessment, Please contact Office of Legal Services for assistance: ols@hse.ie