![hse[v]]()

**Transfer Impact Assessment (TIA)**

**Template**

Version 1.0

**Introduction**

In July 2020, in its Schrems II judgement, the Court of Justice of the European Union (CJEU) decided that, while EU Standard Contractual Clauses (SCCs) remain a valid legal mechanism under Article 46 of the GDPR for transferring personal data outside the European Economic Area (EEA), there is also a need to assess, on a case-by-case basis, whether the personal data being transferred will be adequately protected. Where the level of protection provided by the SCCs would not be ‘essentially equivalent’ to the level found in the European Union, the parties must put in place supplementary measures to bring the level of protection up to that standard.

In practice, the decision by the CJEU means that organisations like the HSE (i.e. ‘data exporter’) who are using either SCCs or any other transfer mechanism under Article 46 of the GDPR, are legally required to carry out a Transfer Impact Assessment (aka Transfer Risk Assessment) before transferring personal data outside the EEA.

**What is a Transfer Impact Assessment (TIA)?**

A Transfer Impact Assessment (TIA) is a type of risk assessment that enables organisations like the HSE (i.e. ‘data exporter’) to determine if the SCCs or other mechanism under Article 46 of the GDPR, that they intend using for transferring personal data outside the EEA provides an adequate level of protection in the specific circumstances of that transfer.

The TIA must evaluate whether the laws and practices in the country outside the EEA (i.e. third country) where the personal data is being transferred to or accessed from, provides ‘essentially equivalent’ protection and does not impinge on the effectiveness of the SCCs or other mechanism under Article 46 of the GDPR used to facilitate the data transfer.

If the outcome of the TIA is that the laws and practices in the third country impinge on the effectiveness of the GDPR Article 46 mechanism, then the HSE (i.e. ‘data exporter) must identify and adopt supplementary measures to bring the level of protection for the transferred personal data up to the EU level of protection.

**When is a TIA Required?**

A TIA is only required when transferring personal data to a third country outside the EEA not covered by an European Commission adequacy decision. 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 are relied upon, no other GDPR transfer mechanism, such as appropriate safeguards under Article 46 noted above or a TIA, are required.

**Who in the HSE is responsible for undertaking the TIA?**

The TIA must be undertaken by HSE business units who are intending to transfer personal data to countries outside the EEA not covered by an EU adequacy decision. Whilst undertaking the TIA, the HSE business unit will need the assistance of the organisation (i.e.‘data importer’) in the country outside the EEA where the personal data is being transferred to. Local law advice may be required. The TIA must be made available to a supervisory authority, such as the Data Protection Commission, upon request. It is recommended that specialist legal advice is sought where the relevant HSE business unit has any legal difficulties or queries in relation to the interpretation, application or construction of any of the data transfer mechanisms or risk management measures arising from data protection legislation set out in the TIA (contact should be made with the HSE office of legal services to acquire any appropriate legal advice).

|  |
| --- |
| **Section A. Overview of Data Transfer** |
| **1.** | **Parties to the Data Transfer & TIA** |
| 1.1 | Data Exporter | *[Health Service Executive (“****HSE****”)]* |
| 1.2 | Status of the Data Exporter in relation to the data transfer | ☐ Controller☐ Joint Controller☐ Processor☐ Sub-processor |
| 1.3 | Data Importer |  |
| 1.4  | Country of Data Importer  |  |
| 1.5 | Status of the Data Importer in relation to the data transfer | ☐ Controller☐ Joint Controller☐ Processor☐ Sub-processor |
| 1.6 | Nature of Data Importer’s business/operations | ☐ Individual☐ Public sector organisation (e.g. a regulator, a government department, ☐ Private sector organisation☐ Non-governmental or civil society organisation☐ Other If ‘Other’ Provide details |
| 1.7 | Starting date of the data transfer |  |
| 1.8 | How often will the TIA be reviewed? (next date of review to be specified and recorded for follow up purposes) |  |
| 2. | **Receiving Jurisdiction / Third Country** |
| 2.1 | What country is the personal data being transferred to/accessed from? |  |
| 2.2 | What GDPR Article 46 transfer mechanism is used to facilitate the data transfer to the Data Importer? |  |
| 2.3 | Nature of Data Transfer | ☐ Personal data is hosted by HSE within the EEA,  the Data Importer does not have the ability to  download copies of the personal data, but the  Data Importer does have the ability to access the  personal data remotely from a country outside  the EEA not covered by a European Commission ‘adequacy decision’.☐ Personal data is hosted by HSE within the EEA,  the Data Importer has the ability to access the  personal data remotely from a country outside  the EEA not covered by an European Commission  ‘adequacy decision’, and if necessary to  download and store copies of the personal data  within the country outside the EEA not covered  by an European Commission ‘adequacy decision’,☐ The Data Importer hosts or stores the personal  data in a country outside the EEA not covered by an European Commission ‘adequacy decision’ |
| 2.4 | Will the Data Importer be transferring the personal data onwards to another party/parties (e.g. sub-contractors, sub-processors, etc.)? | ☐ Yes☐ NoIf ‘Yes’ identify all other parties involved, the parties’ location(s), purpose of the onward transfer(s) and mechanism(s) under Article 46 of the GDPR or European Commission ‘adequacy decisions’ used or relied upon to transfer data onwards. |
| 3. | **Details of the Data Transfer** |
| 3.1 | What is the context and purpose of the data transfer (e.g. IT support, storage, backup, research, analysis, marketing, compliance with legal obligation)? |  |
| 3.2 | What processing activities will the Data Importer undertake on the personal data onceit is transferred? |  |
| 3.3 | What categories of personal data are transferred (e.g. HR data, financial data, survey data, training data, audit data etc.)? |  |
| 3.4 | Will special categories of personal data be transferred? | ☐ Yes☐ NoIf ‘Yes’ specify types of special categories of personal data.☐ Racial or ethnic origin☐ Political opinions☐ Religious or philosophical beliefs☐ Trade union membership☐ Genetic data☐ Biometric data for the purpose of uniquely  identifying a natural person☐ Health data☐ Sex life or sexual orientation |
| 3.5 | Will personal data relating to criminal convictions and offences be transferred? | ☐ Yes☐ NoIf ‘Yes’ describe data involved |
| 3.6 | Who are the data subjects or classes of data subjects? | ☐ HSE employees & contractors☐ HSE patients and services users☐ HSE suppliers ☐ HSE funded agency employees & contractors☐ HSE funded agency patients and service users☐ HSE funded agency suppliers☐ Other If ‘Other’ describe data subjects |
| 3.7 | Will the personal data of children and/or vulnerable data subjects be transferred?  | ☐ Yes☐ NoIf ‘Yes’ Describe |
| 3.8 | Have the data subjects been notified of the nature of the transfer (e.g. privacy statement, etc.)? | ☐ Yes☐ NoIf ‘Yes’ Describe |
| 3.9 | What is the expected volume of personal data being transferred? |  |
| 3.10 | What is the HSE’s lawful basis for processing the personal data (by transferring it) under Article 6 of the GDPR? | ☐ Consent of the data subject(s)☐ Performance of a contract with the data subject or to take steps pre-contractual steps at the data subject’s request ☐ Compliance with a legal obligation☐ Protection of the vital interests of an individual☐ Performance of a task carried out in the public interest or in the exercise of official authority ☐ In the legitimate interests of the HSE (except where those interests are overridden by the interests or rights and freedoms of the data subject and never where processing is carried out in the performance of its tasks as a public authority) |
| 3.11 | Where the transfer includes specialcategory data or data concerningcriminal convictions or offences (see2.4 above), which condition(s) applyunder Articles 9 or 10 of the GDPRand/or, if applicable, Chapter 2, Part3 of the Data Protection Act 2018? |  |
| 4. | **Existing safeguards in place**  |
| 4.1 | In what format will the personal data be transferred? | ☐ Plain text/In the clear☐ Pseudonymised☐ Encrypted☐ Other If ‘Other’ Describe |
| 4.2 | How will personal data be transferred to the Data Importer? |  |
| 4.3  | What security measures does the Data Importer have in place to mitigate any risks associated with data transfers to countries outside the EEA which are not covered by an European Commission ‘adequacy decision’. | ☐ Only minimum data set transferred outside the  EEA☐ Data encrypted in transit☐ Data encrypted at rest☐ Role based access ☐ MFA / 2FA☐ 24/7 access monitoring☐ MFA / 2FA☐ OtherIf ‘Other’ Describe |
| 5. | **Possible Alternatives** |
| 5.1 | Can the HSE’s purposes be achieved without transferring the personal data to a country outside the EEA not covered by an European Commission ‘adequacy decision (e.g. using a supplier based within the EEA or a country outside the EEA covered by an European Commission ‘adequacy decision)? | ☐ Yes☐ No If ‘Yes’ explain why this option has not been taken |
| 5.2 | Can the HSE’s purposes be achieved with the transfer of anonymised data to the Data Importer, in place of personal data? | ☐ Yes☐ No |

|  |
| --- |
| **Section B. The enforceability of appropriate safeguards, e.g. Standard Contractual Clauses (“SCCS”) (article 46 GDPR)** |
| **1.**  | **Data protection law or practice in recipient third country**  |
| **Question (Complete these Sections B(1) and (2) for all jurisdictions identified in Section A 2.1 – 2.4 (inclusive)** | **Yes/No** | **Information provided by data importer** | **Information from the HSE’s own enquiries (incl. source)** |
| 1.1 | **Data Protection Regime**  |
|  | Does the country have a dedicated data protection law? |  |  |  |
|  | Is that data protection law based on any international instruments on privacy or data protection? |  |  |  |
|  | Is the Data Importer subject to the data protection law(s) described at section 1.1.1? |  |  |  |
|  | Do individuals have substantive data protection or privacy rights, e.g. right to access their personal data, right to remedy for breach of their rights? |  |  |  |
|  | Are there any specific restrictions on the disclosure of personal data by the data importer to third parties? |  |  |  |
|  | Is there a distinction under data protection or privacy law between citizens or residents and non-citizens or non-residents? |  |  |  |
|  | Is there an independent data protection regulator with powers of oversight and enforcement? |  |  |  |
|  | Can individuals exercise their data protection rights through the judicial system or data protection regulator? |  |  |  |
|  | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties?  |  |  |  |
|  | Is there a legal requirement that any restrictions to fundamental rights and freedoms be necessary and proportionate (e.g. that restrictions are for justified and limited in purpose such as for law enforcement, national security or safeguarding public health)? |  |  |  |
|  | Is there evidence that the law(s) identified above at 1.1.1 are applied in practice? |  |  |  |
|  | **Access to Personal Data by Public Authorities**  |
| 1.2.1 | Is the Data Importer aware of any applicable laws or practices (e.g. criminal law enforcement, national security intelligence and surveillance, regulatory compliance etc.) within the recipient third country that could constitute an obstacle to its ability to comply with appropriate safeguards (i.e. SCC’s) pursuant to the GDPR? If so, please explain in the detail what these laws or practices are and how these could impact the Data Importer’s ability to comply. |  |  |  |
| 1.2.2 | Do national intelligence or security services within the recipient third country, operate surveillance programmes? |  |  |  |
| 1.2.3 | Can public authorities (e.g. intelligence, law enforcement, defence services, regulatory agencies or other government agencies) within the recipient third country, access or compel disclosure of personal data from the Data Importer?  |  |  |  |
| 1.2.4 | What personal data can public authorities require an organisation (e.g. the Data Importer) to provide and in what circumstances, e.g. under:1. Any applicable security surveillance regime?
2. In the course of a criminal or regulatory investigation?
 |  |  |  |
| 1.2.5 | Is any public authority access described above in 1.2.2 to 1.2.4 inclusive provided for in law? If so, is the Data Importer within the scope of this law? |  |  |  |
| 1.2.6 | Does the access noted in 1.2.4 include personal data that the Data Exporter (i.e. the ‘HSE’) will transfer to the Data Importer? If so, what risks are posed to the security of personal data which the Data Exporter (i.e. the ‘HSE’) transfers to the Data Importer? |  |  |  |
| 1.2.7 | What limitations in law and/or practice are imposed on such requests by public authorities? |  |  |  |
| 1.2.8 | Is there evidence of surveillance authorities in the third country accessing large volumes of personal data? |  |  |  |
| 1.2.9 | Are surveillance operations / operators in the third country subject to audit or oversight for compliance?  |  |  |  |
| 1.2.10 | Can individuals challenge, before a judicial or other independent tribunal, access to their personal data by public authorities, including for surveillance measures? |  |  |  |
| 1.2.11 | Has the Data Importer ever been subject to a request (including by request, court order or other form of access) from public authorities within the recipient third country for access to EEA personal data? If so, how often and by whom? [*Documented evidence (e.g. records of public authority requests) should be provided by the data importer where available*] |  |  |  |
| 1.2.12 | Could the Data Importer be subject to a request from public authorities within the recipient third country, for access to data held within the EEA by the Data Importer? |  |  |  |
| 1.2.13 | Does the Data Importer have a documented public authority access policy? If so, provide a copy of the policy. |  |  |  |
| 1.2.14 | Does the Data Importer refuse access requests from public authorities within the recipient third country, unless the request is a mandatory compulsion order or where the Data Exporter has provided their written consent? |  |  |  |
| 1.2.15 | Will the Data Importer notify the Data Exporter about any requests from Public authorities within the recipient third country for access to data which they received from the Data Exporter, unless legally prohibited to do so? |  |  |  |
| 1.2.16 | Does the Data Importer publish any transparency reports that set out the number of access requests or demands for data disclosure it has received from public authorities? |  |  |  |
| 1.2.17 | Is there evidence of other operators in the Data Importer’s sector in the recipient third country receiving requests for access or disclosure from public authorities? |  |  |  |
| 1.2.18  | In relation to surveillance measures allowing access to personal data by public authorities (e.g. national security agencies or law enforcement authorities), are **all four** European Essential Guarantees ([Click for European Data Protection Board Guidance](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en)) present in the recipient country by reference to the responses entered above? | Tick each European Essential Guarantee identified:☐ 1. Processing is based on clear, precise and accessible rules☐ 2. Necessity and proportionality regarding the legitimate  objectives pursued is demonstrated☐ 3. An independent oversight mechanism exists☐ 4. Effective remedies are available for data subjects |
| **Assessment of level of protection provided in third country** |
| **Taking account of the circumstances of the transfer detailed in section A and the responses at section B(1) above, is the HSE satisfied that the law or practice of the recipient third country will not impinge on the effectiveness of the safeguards provided by the SCCs, i.e. that the level of protection in the recipient third country is essentially equivalent to that guaranteed in the EU (by the GDPR read in light of the Charter of Fundamental Rights)?** | ☐ Yes [*summarise reasons and proceed to section C]*☐ No *Continue to section B(2)*☐ Not satisfied or unsure *continue to section B(2)*  |
| **2.** | **Supplementary measures to appropriate safeguards.** |
| 2.1 | **Potential supplementary measure****(**[**Click for European Data Protection Board Recommendations**](https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en)**)** | **Supplementary measure deployed (Describe measures that apply during transmission and/or to the processing in the recipient country)** |
| 2.1.1 | Pseudonymisation | ☐ Yes☐ NoIf ‘Yes’ provide details of the pseudonymisation process |
| 2.1.2 | Encryption | ☐ Yes☐ NoIf ‘Yes’ provide the following details:1. When is the data encrypted – before it is transferred or after it is transferred?
2. Details of encryption algorithms and protocols used.
3. Encryption products used
4. Is data encrypted at rest (i.e. on disk / storage)?
5. Is data encrypted in transit?
6. Who manages the encryption keys and where are the encryption keys stored
 |
| 2.1.3 | Protected recipient(s)  | ☐ Yes☐ No |
| 2.1.4 | Other technical measure(s) | *[Please provide details]* |
| 2.1.5 | Further binding contractual clauses to theSCCs(***NB:*** *the SCCs can be supplemented but not amended. Any contractual measure that might conflict with the SCCs must be notified to the Data Protection Commission*) | ☐ Yes☐ No[If yes, summarise the supplementary measure deployed] [If no, state why this supplementary measure is not appropriate or required]  |
| 2.1.6 | Organisational measures | ☐ Yes☐ No[If ‘Yes’, summarise the supplementary measure deployed] [If ‘No’, state why this supplementary measure is not appropriate or required]  |
| 2.2 | **Assessment of supplementary measures to appropriate safeguards** |
| 2.2.1 | Is the HSE satisfied that the supplementary measures identified at section B(2) will provide a level of protection for data subjects essentially equivalent to that found in the EU (by the GDPR read in light of the Charter of Fundamental Rights)? | ☐ Yes [*if Yes, continue to 2.2.2 below*]☐ No SCCs cannot be relied upon so the transfer cannot proceed (a limited exception under GDPR may apply but legal advice should be obtained prior to reliance upon such an exemption). |
| 2.2.2 | Is the HSE satisfied that the law of the third country does **not** prohibit or otherwise prevent the effectiveness of these supplementary measures? | ☐ Yes [*state reasons*]☐ No SCCs cannot be relied upon so the transfer cannot proceed (a limited exemption under GDPR may apply but legal advice should be obtained prior to reliance upon such an exemption). |
| **Section C. Transfer Risk Assessment Approval**  |
| **Date of next review:** | *[Insert proposed review date or state recommended frequency of review]* |
| ***Data exporter\* (HSE Business Lead/ Owner responsible for dataset or system)*** | ***Data importer*** |
| **Approved by:** **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***[Print name and role]* | **Approved by:** **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***[Print name and role]* |
| **Date of approval:** | **Date of approval:** |