Pridatect

TRANSFER IMPACT ASSESSMENT

Pridatect

CONTENTS

Following the Court of Justice of the European Union's decision in Schrems II, European Union organisations that rely on article 46 GDPR mechanisms to transfer personal data must assess, on a case-by-case, whether the laws of the territory into which personal data is being transferred guarantee data subjects a level of data protection essentially equivalent to that required under European Union law.

The European Data Protection Board (EDPB) in '*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*' put forward the following steps in relation to accountability for transfers:

1. Know your transfers;
2. Identify the transfer tools you are relying upon;
3. **Assess whether the transfer tool you are relying upon is effective for all circumstances of the transfer;**
4. Adopt supplementary measures if necessary;
5. Procedural steps if supplementary measures are necessary;
6. Re-evaluate at appropriate intervals.

The purpose of this template is to provide a framework and means of recording the assessment in relation to step number 3 of the EDPB Recommendations 01/2020.

NOTE: If there are more than one destination country or relevant onward transfer, you should perform a separate Transfer Impact Assessment for each step in the data lifecycle

1	**Describe the transfer**
1.1	**Identification of the data exporter**
	e.g. Legal and business name, registration details, exporter country or countries.
1.2	**Identification of the data importer**
	e.g. Legal and business name, registration details, type of recipient (e.g., private company, public authority), recipient country, is it subject to any rules of professional conduct?
1.3	**Context of the transfer**
	e.g. Nature of relationship between the parties (e.g., parent company), purpose(s) of the transfer, means of the transfer (e.g., email, secure file transfer protocol, remote access), how often will it occur, what will be the importer doing with the data.
1.4	**Categories, amount & format of personal data involved**
	e.g. Identification details, nationality, applicants' CVs, payment details, etc. [Special relevance of any sensitive personal data]. *e.g. number of files/records* *e.g. plain text, pseudonymized, encrypted, etc.*
1.5	**Level of risk of harm to data subjects in cases**
	e.g. Based on the above information, do you expect this data transfer to result in a high, medium or low level of risk of harm to the data subjects involved: this can be an estimate, though do attempt to justify. This will be re-evaluated in the conclusion of this Impact Assessment.

1.6	**Duration of the transfer**
	e.g. Indefinite basis, 1 year, etc.

2	**Alternatives**
2.1	**Are there any feasible processor/supplier alternatives you could use that are located within the EEA/EU or another "adequate" country according to article 45 GDPR?**
	e.g. It may be the case that you can find a processor that fulfils the same purpose that is located in Europe, and as such is not as much of a potential risk to data subjects. If this is not possible financially, technologically or organisationally explain why.
2.2	**Can you rely on any of the article 49 GDPR exceptions for this transfer?**
	e.g. The data subject has explicitly consented to the proposed transfer, after being informed of the possible risks due to the absence of an adequacy decision and safeguards as stated in article 49 (1) (a). *e.g. Transfer is necessary for performance of contract between data subject and controller or for implementation of pre contractual measures taken at the data subject's request per article 49 (1) (b).* *e.g. Transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person per article 49 (1) (c).* *e.g. Transfer necessary for important reasons of public interest per article 49 (1) (d).* *e.g. Transfer is necessary for the establishment, exercise or defence of legal claims per article 49 (1) (e).* *e.g. Transfer is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent per article 49 (1) (f).* *e.g. Transfer made from a public register per article 49 (1) (g) and 49 (2).*

3	**Describe the importer's country legal regime**

3.1	**Does the importer's country legislation offer a level of data protection essentially equivalent to that guaranteed within the EU/EEA by the GDPR?**
	e.g. Relevant factors when making this assessment include the rule of law; respect for human rights and fundamental freedoms; relevant legislation; access by public authorities to personal data; the existence of independent supervisory authorities; effective data subject rights and effective redress for data subjects whose personal data is transferred. *Further factors indicating concern there could be: non recognition or enforcement of foreign judgments or arbitration awards, country not being party to international conventions (e.g. human rights), limited access to justice for overseas litigants, non-independent or non-impartial authorities, widespread levels of corruption, etc.*
3.2	**Are there any specific laws in the destination country that may impinge the enforceability of the selected Article 46 GDPR transfer tool?**
	e.g. any applicable laws on intelligence and access by competent public authorities, sectoral legislation applicable to the particularities of the transfer (e.g. on health data, financial data, human resources data, etc.) *e.g. US Legislation Section 702 FISA and Executive Order 12 333.* *e.g. Russia's SORM system (Система оперативно-разыскных мероприятий, lit. 'System for Operative Investigative Activities, as stated in the ECHR in case Zakharov v. Russian Federation, no. 47143/06, ECHR 2009-X, paragraph 302)*
3.3	**If so, Does the data importer fall under the scope of said laws?**
	e.g. You use a Human Resource Management tool that is domiciled in the United States so are conducting this assessment, but FISA + EO 12.333 does not target - for example - HR data. This is confirmed by a report of the Privacy and Civil Liberty Oversight Board (PCLOB) (here) as well as the decisions of the Foreign Intelligence Surveillance Court (FISC) when granting access in FISA cases (here).

	These sources contain no indication that such data has ever been the target of searches under Section 702 FISA or EO 12.333. Also, Section 702 FISA is only about communications services provided to the targets of the searches, and not to others or applications such as the present one. Therefore, you would state here that you believe that the probability that the parent company has or will receive a surveillance order with respect to your data during the period under consideration is very low. *This can only be justified insofar as there is public information available.*
3.4	**Can the request be made with a lack of judicial review?**
	e.g. There is no mandatory requirement for judicial oversight through a judge. For example, in the US National Security Letters (NSLs) do not require a Judge to sign off before the gag order / access request is executed. Though the requests themselves may be hidden to all except the recipient, data about the number of requests made by the public authority in a time period will likely be publicly available.
3.5	**Does the law provide the data importer any mechanisms to challenge the application of said laws to the personal data?**
	e.g. With non-judicial mechanisms this is unlikely. An example of a challenge could be legal action before the competent court with the aim to stop or control access of authorities to personal data.
3.6	**Does the law provide for mandated technical measures which make public authorities' access to personal data possible?**
	e.g. Mandated backdoors in software that will be used in the processing of data.
3.7	**Does the law provide for access to the data in transfer?**

	e.g. Is there a record of access to telecommunications providers in the importer country that could affect your data prior to the importer receiving it?

4	**Describe likelihood of legislation application to your transfer of personal data**
4.1	**Have public authorities previously requested access to personal data held by the data importer?**
	e.g. Collaborate with the importer to find out if they have received any access requests.
4.2	**Have public authorities successfully obtained access to personal data held by the data importer in the past?**
	e.g. Have any requests been successful?
4.3	**Has the data importer successfully caused the public authority to give up its request of data in the past?**
	e.g. Certain countries where challenging requests is encouraged may result in refusal. This is a consideration: if the importer receives a request, is there a good chance that they can force the authority to forfeit the access request?
4.4	**Have public authorities previously requested access to data from the same category of company that you are aware of?**
	e.g. Though the importer may not have received any requests, or be under an order prohibiting their disclosure of such, it can be helpful to look at other companies in this sector. Data is usually publicly available from larger providers.
4.5	**Does the data importer's country have any systems in place to prohibit disclosure of access requests?**

	e.g. Certain public authorities will include gag orders / NDAs with their access requests which will mean the data importer may have received requests but cannot share this information with you.
4.6	**Are you aware if your data potentially contains any specific "selectors", or identifying attributes, that may be of interest to the public authorities of the importer country?**
	e.g. Is it likely that your data contains something related to a name, email, etc that could be flagged for additional surveillance or access? This could be a hard selector (email of a person of interest) or a soft selector (geographic location or specific node known for criminal activity). Further examples and detail can be found in the Director of National Intelligence infographic here.

5	**Safeguards**
5.1	**Is clear text transmission necessary in the transmission of this transfer?**
	e.g. Certain processing activities require that the data is transmitted in clear text (non-encrypted) format.
5.2	**Is clear text processing necessary upon the receipt of the personal data?**
	e.g. Certain processing activities require that the data is received in clear text (non-encrypted) format. For example, HR data for the purpose of entry into a HRM system - if it is encrypted it is essentially useless, as it will not fit the entry fields.
5.3	**Is the recipient contractually required to defend the personal data at issue against access requests?**
	e.g. Within the EU, importers have a general duty of care that requires you to defend the personal data of citizens. This is not always the case in other countries.

5.4	**Have you implemented any additional encryption access controls aiming to minimise the likelihood of a breach occurring or reducing risk of harm to data subject if a breach does occur?**
	e.g. In at-rest encryption you will encrypt the data prior to transfer using an appropriate encryption solution (i.e. storage encryption) and you will implement suitable key management procedures. A superior solution would be to encrypt data prior to transfer using appropriate encryption solutions and then splitting the encrypted datasets between multiple parties.
5.5	**Have you applied the data minimisation principle?**
	e.g. You minimise the data transferred to the minimum required to conduct the processing activity. This could also include pseudonymisation techniques prior to transfer, with the importer not having access to the additional information. A superior solution would be to split pseudonymised data sets between multiple entities, so there is a minimal risk that any one party could identify a data subject.
5.6	**Has the data importer set any organisational access control measures?**
	e.g. This could include role-based access profiles, third-party access protocols or a policy to handle legal orders for third-party data access.
5.7	**Has the data importer/data exporter set in place a process to handle data subject complaints that includes a compensation scheme?**
	e.g. Not strictly necessary, and only available to larger organisations with substantial financial resources,
5.8	**Have you set in place any contractual rights for data subjects to bring a claim against the exporter if the importer fails to comply with its obligations?**

	e.g. A policy could be in place to ensure that these cases are dealt with effectively. Contractual rights could be included in main service agreements.
5.9	**Is there any data protection authority with active powers of oversight over the data importer and/or exporter?**
	e.g. Certain countries may have a more active data protection authority that can provide protections that can be relied upon. This is likely to safeguard the rights of data subjects and is a positive for the transfer's success.
5.10	**Have you any review procedure in place to ensure the descriptions contained herein continue to be accurate?**
	e.g. It is important to ensure that you have a review procedure in place. Data collected from public sources within this impact assessment may become outdated in a matter of months, or years. Periodic review ensures that data subjects are not put at risk.

Conclusion	
Permitted	*Not Permitted*

(Remove colour from box that does not apply above)

Your transfer should be permitted once you have completed the above assessment and believing that the answers indicate that you are:

- *Meeting the wider EU GDPR compliance requirements*
- *Confirming that the transfer is not high risk or complex*
- *Assessing and recording details of the restricted transfer (Sections 1-2)*
- *Confirming that the contractual rights set out in your transfer tool are likely to be enforceable in the target country (Sections 3-4), and where there are concerns the risk of harm to data subjects is low or can be reduced to low by additional steps and measures such as encryption, pseudonymisation etc (Section 5)*
- *Confirm that one of the following applies in the context of your restricted transfer:*
    1. *the destination regime provides appropriate protections for third party*

access to data (including surveillance).

2. *the likelihood of third party access (including surveillance) taking place is minimal or becomes minimal once you apply any extra steps or protections.*
3. *if concerning third party access to data takes place, the risk of harm to data subjects is low or becomes low once you apply any extra steps or protections.*

When justifying the conclusion in this section please refer to your answers in Sections 1-5.