Cross-Border Data Transfer Tools v. Privacy Enhancing Technologies: a False Debate

Version 2.0

By Sophie Stalla-Bourdillon
Content:

Summary ............................................................................................................................................... 3

1. Introduction .................................................................................................................................... 5

2. Data-Transfer Restriction Patterns ............................................................................................... 6
   2.1 Restriction Pattern #1: “Bind the Intended Recipient” .............................................................. 6
   2.2 Restriction Pattern #2: “Bind the Intended Recipient and Shield against Third Parties” ............ 7

3. PETs as Supplementary Measures .................................................................................................. 9
   3.1 A PET typology .......................................................................................................................... 10
   3.1.1 Relevant PETs ...................................................................................................................... 10
   3.1.2 The Inference Model ............................................................................................................ 11
   3.1.3 Data Transfers and PETs ...................................................................................................... 14
   3.2 Fine-grained Data Transfer Assessment .................................................................................... 16
   3.3 Data Transfers, Trustworthiness, and PETs ............................................................................... 20

4. Conclusion ....................................................................................................................................... 21

The Brussels Privacy Hub publications are intended to circulate research in progress for comment and discussion. Available at https://brusselsprivacyhub.com/. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged.

DISCLAIMER

The opinions expressed in this paper are those of the author/s.
Summary

Privacy Enhancing Technologies (PETs)’ potential has been acknowledged in various jurisdictions by data protection supervisory authorities. PETs have thus been prototyped in various sectors, in particular finance and healthcare, with the intention of generating new data flows. It is not surprising, therefore, to see that global efforts to promote the free flow of data across borders include workstreams on PETs. A framework to assess PET achievement, in particular in the context of cross board data transfers (CBDT), is however still needed. This note aims to lay the foundations for the development of such a framework and thereby aims to inform the work done at the international level to reduce fragmentation of data transfer regimes, be it in the context of the G7, the OECD or the G20 initiatives.

CBDT tools are legal mechanisms of which primary purpose is to ensure that a pre-determined level of data protection (broadly defined) is maintained, once the data is handled by the data importer operating in a third country, such as Standard Contractual Clauses (SSCs), Biding Corporate Rules (BCRs) or certification. They are thus a means to produce evidence of trustworthiness: either institutional trustworthiness through the analysis of the legal framework applicable within the jurisdiction of the data importer, or relational trustworthiness through the assessment of the behavior of the data importer or the formulation of binding commitments.

CBDT tools can be associated with at least two different types of data-transfer restriction patterns. A cross-border data transfer restriction pattern refers to a repeatable set of limitations imposed on the cross-border transfer of data from a data exporter to a data importer, which, through the requirement to adopt a data transfer tool, typically aims at exporting a certain level of data protection when the data leaves the jurisdiction in which it was initially processed or when the data is accessed from a third country. Restriction Pattern #1 targets the intended recipient of the transfer and aims to directly impact its processing practices. Restriction Pattern #2 targets the intended recipient and situationally-relevant third parties, e.g., third parties who create additional risks to the fundamental rights of data subjects. This pattern aims to directly impact the processing practices of both groups. The best illustration of Restriction Pattern #2 is the solution that has emerged in the European Union (EU), following the Schrems II decision: whatever the CBDT tool at stake, either essential guarantees against abuses committed by public authorities when processing the personal data must exist or supplementary measures must be put in place to effectively mitigate against this threat.

A subset of PETs, called Confidentiality Enhancing Technologies (CETs), is an attempt to formalise the selection process of controls addressing confidentiality threats associated with unauthorized or unwanted access, which constitute the main threats to mitigate when considering situationally-relevant third parties under Restriction Pattern #2. CETs therefore, at least at first glance, appear particularly useful under Restriction Pattern #2. CET implementation implies adopting a fine-grained approach to data transfers, which is compatible with Restriction Pattern #2 and is not necessarily inconsistent with the EU model, for which there is leeway to move away from a one-size-fits-all approach. However, crucially, CETs do not eliminate tradeoffs. They thus require careful consideration.

The note includes a typology of CETs. It shows that each CET within this typology pursues a limited objective, and that CETs are not perfect substitutes in terms of the guarantee(s) they offer. Moreover, following the inference model, it shows that whatever the CET at stake, context controls (technical or organizational controls applied upon the environment of the data as opposed to the data itself) implemented within the data importer’s perimeter will always be needed to address the full range of inferences (identify inference, attribute inference, participation inference, relational inference). Going further, it argues that anonymisation is always a tradeoff, i.e. a decision to prioritise utility over confidentiality, even when the strongest CETs are in place.
From these findings, three consequences are drawn. First, the CET selection process should be made transparent, and assumptions related to the types of inference in scope and the threat model (where relevant) should be made explicit to allow oversight. Second, the full CET setting should be taken into account to assess the output, and in particular the legitimacy of the processing purpose once the data is in the hands of the data importer and the level of data subject or end user intervenability. This should hold true, even if a claim of legal anonymisation is successful, as the anonymization process remains within the scope of data protection law. Third, even in the presence of CETs, relational trustworthiness remains relevant and CBDT tools will be needed to generate evidence.
1. Introduction

Privacy Enhancing Technologies (PETs)’ potential has been acknowledged in various jurisdictions by data protection supervisory authorities, including the European Data Protection Board (EDPB)’s predecessor. PETs have thus been prototyped in various sectors, in particular finance and healthcare, with the intention of generating new data flows. It is not surprising therefore to see that global efforts to promote the free flow of data across borders include workstreams on PETs.

To facilitate convergences of approaches across regions while avoiding falling into the trap of “technological solutionism”, it is essential to carefully unpack the potential of PETs in such a context.

The purpose of this policy note is thus to lay the foundations for PET assessment in cross-border data transfer scenarios and include some recommendations for policy makers leading workstreams in the space. This brings us to introduce an intermediate category of PETs, to call for a fine-grained approach to data transfer, and stress that PETs should not be considered as mere substitutes to data transfer tools, i.e., legal mechanisms of which primary purpose is to ensure that a pre-determined level of data protection (broadly defined) is maintained once the data is handled by the data importer operating in a third country such as Standard Contractual Clauses (SSCs), Biding Corporate Rules (BCRs) or certification.

Cross-border transfer tools can be associated with at least two different types of data-transfer restriction patterns. A cross-border data transfer restriction pattern refers to a repeatable set of limitations imposed on the cross-border transfer of data from a data exporter to a data importer, which, through the requirement to adopt a data transfer tool, typically aims at exporting a certain level of data protection when the data leaves the jurisdiction in which it was initially processed or when the data is accessed from a third country. Restriction Pattern #1 targets the intended recipient of the transfer and aims to directly impact its processing practices. Restriction Pattern #2 targets the intended recipient and situationally-relevant third parties, e.g., third parties who create additional risks to the fundamental rights of data subjects, and aims to directly impact the processing practices of both groups.

Although Restriction Pattern #2 is per definition more demanding than Restriction Pattern #1 in terms of the types of controls one would need to put in place to protect the data, this does not mean that Restriction Pattern #2 is inherently flawed and does not lend itself to a formalised risk-based assessment. A subset of PETs, called Confidentiality Enhancing Technologies (CETs), is an attempt to formalise the selection process of controls addressing confidentiality threats associated with unauthorized or unwanted access, which constitute the main threats to mitigate when considering situationally-relevant third parties under Restriction Pattern #2. Their implementation implies adopting a fine-grained approach to data transfers, which is compatible with Restriction Pattern #2. Crucially, however, implementing such CETs should not

---

1 Article 29 WP, Anonymisation Techniques, Opinion 05/2014 on Anonymisation Techniques, WP216, Adopted 10 April 2014. Guidelines on a similar topic have been produced in Canada, Singapore, Spain, the United Kingdom (UK). These guidelines however do not usually cover data transfer scenarios.


mean that the data exporter is given carte blanche to initiate the transfer and that there is no need to subject the data importer to any restriction.

A data transfer tool will still be needed at a minimum to ensure that context controls, i.e., controls applied upon the environment of the data such as purpose-based access control, have been put in place within the perimeter under the data importer’s responsibility. This is because, even if CETs, in some instances, would make it possible to achieve legal anonymisation, i.e., to reduce re-identification risks to an acceptable level, such a finding cannot be made upon the consideration of the data control applied on the data only, i.e., the data transformation technique applied on the data. Going further, as an anonymisation finding is always a tradeoff, i.e., a decision to preserve utility over confidentiality, such a tradeoff should always be validated at a minimum in the light of the legitimacy of the downstream processing purposes and the level of data-subject or end-user intervenability allowed by the CET setting. What is more, considering the CET setting holistically and bearing in mind that the anonymisation process remains governed by data protection law, the data exporter should select the CET setting that preserves the highest level of data subject intervenability.

This policy note is structured as follows. Section two introduces the two main data-transfer restriction patterns that are found in practice. Section three unpacks the potential of CETs in the context of data transfers and highlights their implications and limitations. Section four concludes.

2. Data-Transfer Restriction Patterns

Two main data transfer restriction patterns usually emerge when reviewing data transfer regimes.

2.1 Restriction Pattern #1: “Bind the Intended Recipient”.

The primary objective of a cross-border data transfer mechanism is to define a normative baseline with which the data importer must comply, i.e., to bind the intended recipient of the data when operating within its own jurisdiction to ensure a pre-determined level of data protection. This is what is called Restriction Pattern #1. The focus of this pattern is set upon the intended recipient: it is therefore (e.g., contractually) imposed a series of obligations such as obligations related to purpose limitation, data minimisation, record keeping, security (integrity and confidentiality) and breach notification, and individual right-related obligations.

The normative baseline can also include rights granted to third-party beneficiaries, who are thus empowered, at least as a matter of principle, to enforce their rights against the parties to the cross-border data transfer. Third party beneficiaries’ rights can be effective against a wide range of obligations imposed upon data importers, e.g., provisions that provide safeguards for the handling of personal data or ensure specific individual rights.\footnote{Unsurprisingly, the strength of the normative baseline embodied within cross-border data transfer mechanisms can vary greatly. To take the example of model clauses, the ASEAN model contract clauses, for example, have very little on third-party beneficiary rights, as they are designed to enforce safeguards mandated within the ASEAN Framework on Personal Data Protection of 2016. On the other hand, the Ibero-American Model Transfer Agreement aims to enable entities to meet the Personal Data Protection Standards for the Ibero-American States: it is therefore closer to the EU Standard Contractual Clauses (SCCs). Its goal is to ensure that “the level of protection of the personal data of the citizens of a country does not decrease or}

Unsurprisingly, the strength of the normative baseline embodied within cross-border data transfer mechanisms can vary greatly. To take the example of model clauses, the ASEAN model contract clauses, for example, have very little on third-party beneficiary rights, as they are designed to enforce safeguards mandated within the ASEAN Framework on Personal Data Protection of 2016. On the other hand, the Ibero-American Model Transfer Agreement aims to enable entities to meet the Personal Data Protection Standards for the Ibero-American States: it is therefore closer to the EU Standard Contractual Clauses (SCCs). Its goal is to ensure that “the level of protection of the personal data of the citizens of a country does not decrease or
disappear when exported or transferred to another country or countries.” Of note, although Brazil includes model clauses within its transfer toolbox, it has not yet endorsed this set of model clauses, as it is probably waiting to receive an adequacy finding from the EU first.

Importantly, and as mentioned above, when the restriction pattern at stake is Restriction Pattern #1, data handling obligations are usually imposed upon the data importer. Imposing data handling obligations upon the data importer should imply on the part of the data importer an obligation to implement controls to prevent confidentiality threats such as unauthorized access. As the intensity of the controls should be proportionate to the risks posed to data subjects, a risk assessment should be performed by the data importer even when Restriction Pattern #2 is not applicable. This does not mean however that the threat model that the data importer should be using to select appropriate controls and comply with its obligations will necessarily include public authorities. In fact, standard practice, as described by Data Protection Authorities, such as the UK Information Commissioner’s Office (ICO), excludes public authorities from the definition of a typical motivated intruder.

It is worth noting that Restriction Pattern #1 can emerge even in scenarios in which there is no express cross-border data transfer rules issued by the jurisdiction of the data exporter. Suffice it to identify a requirement to bind the data recipient even when data handling rules are not applicable to the latter as a covered entity. This is what happens with the California Consumer Privacy Act, as amended by the California Privacy Rights Act, since it includes a requirement to bind service providers through contract and specifies a minimum set of obligations to include within such a contract.

2.2 Restriction Pattern #2: “Bind the Intended Recipient and Shield against Third Parties”

Restriction Pattern #2 has a broader target than Restriction Pattern #1. It aims to impact both the practices of the intended recipient and third parties that are situationally relevant, such as public authorities.

Let’s take the example of a specific data transfer tool to better illustrate Restriction Pattern #2 and compare it with Restriction Pattern #1: the EU SCCs. The roots of Restriction Pattern 2 associated with the EU SCCs are to be found in two places. First of all, Article 44 of the General Data Protection Regulation (GDPR) states

---


7 “Threat modeling works to identify, communicate, and understand threats and mitigations within the context of protecting something of value,” e.g. data as OWASP explains. “A threat is a potential or actual undesirable event that may be malicious (such as DoS attack) or incidental (failure of a Storage Device).” OWASP, Threat Modelling, available at https://owasp.org/www-community/Threat_Modeling, accessed 28.01.24. An event is usually associated with a particular attacker, for whom a series of assumptions will be made to define its profile.


9 See California Civil Code section 1798.100(d).

10 On 4 June 2021, the EU Commission adopted the latest version of SCCs through it Implementing Decision (EU) 2021/914 and thereby replaced the set of clauses adopted under the Data Protection Directive and before the CJEU’s Schrems I and II rulings. By doing so, it introduced four modules to govern four different types of relationships: transfers from data controller to data controller, data controller to data processor, data processor to data processor, and data processor to data controller. All transfer tools should be associated with the same restriction pattern. 11 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) OJ L 119, 4.5.2016, p. 1–88.
that “[a]ll provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.”\textsuperscript{12} Article 44 must be read in the light of Article 46(1)\textsuperscript{13} and Article 46(2).\textsuperscript{14} There are at least two ways to interpret these provisions together: either the use of SCCs creates the presumption that data subjects have been granted effective rights on the condition that the rights are enforceable under the law of the contract,\textsuperscript{15} or the SCCs do not create any conditional presumption. Excluding the first interpretation would clearly undermine the raison d’être of EU SCCs. As of today, there is no reason to exclude this interpretation. The EC’s 2021 decision acknowledges that with these new international transfer SCCs, the parties can freely choose the EU Member State law that will govern their SCCs, on the condition that the Member State’s laws allow for third-party beneficiary rights.\textsuperscript{16} The Court of Justice of the European Union (CJEU) in Schrems II made it clear that appropriate safeguards are able to be provided by the SCCs adopted by the Commission.\textsuperscript{17}

The second locus of Restriction Pattern #2, as embodied in EU SCCs, is to be found in the Charter of Fundamental Rights of the European Union (Articles 7, 8, 47 and 52). This has been confirmed by the CJEU, and in particular in its Schrems II decision specifically examining the validity of SCCs.\textsuperscript{18} This led the CJEU to state that “the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.”\textsuperscript{19}

What the CJEU is thus suggesting in Schrems II is that in certain cases public authorities should be considered as situationally-relevant attackers. To determine whether the public authorities of the third country should be considered situationally-relevant attackers, an assessment of the legal system of the third country is considered to be necessary by the CJEU. More specifically, both a legal analysis and a factual analysis appear to be in scope, as the CJEU refers to relevant aspects of the legal system of the third country.\textsuperscript{20} This is because access by public authorities is dependent upon the scope of interception powers and powers to request access to data held by private parties as well as the practice of these powers.

\textsuperscript{12} GDPR, Article 44.

\textsuperscript{13} Article 46(1) provides that: “In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.”

\textsuperscript{14} Article 46(2) provides that: “The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:...(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).”

\textsuperscript{15} In order to achieve effective enforcement, the data importer through the SCCS agrees to submit itself to the jurisdiction of the competent supervisory authority (usually the competent supervisory authority of the EU Member State in which the data exporter is established), to cooperate with such authority and comply with any binding decision under the applicable EU or Member State law, including decisions rendered by an EU Member State’s court. Data subjects also get a right to access SCCs.

\textsuperscript{16} Ireland had been the only member state that did not allow for third-party beneficiary rights as the law had required strict privity of contract. Despite some commentary about data subjects being able to use a theory of agency to enforce their rights, the Irish Department of Justice issued a statutory instrument to amend the Irish Data Protection Act 2018.

\textsuperscript{17} CJEU Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, 16 July 2020, ECLI:EU:C:2020:559 (hereafter Schrems II), para. 2.

\textsuperscript{18} Schrems II, para. 105.

\textsuperscript{19} Schrems II, para. 105.

\textsuperscript{20} Schrems II, para. 126.
The CJEU goes further, however, when it imposes upon data controllers an obligation “*to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned.*”\(^{21}\) Following its Advocate General, the CJEU holds that “*the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority.*”\(^{22}\) Although such a stance could appear harsh to data exporters at first glance, the presumption of responsibility imposed upon the data controller is a general underpinning of the GDPR, as illustrated by Article 82(2), which aims at ensuring that data subjects are granted an effective right to compensation. Importantly, such a stance does not preclude Supervisory Authorities, the European Data Protection Board (EDPB), nor the European Commission, to become more proactive and produce their own legal assessment with a view to alleviate the burden imposed upon data controllers.

In an attempt to offer detailed guidance to data exporters, the EDPB produced a set of recommendations on supplementary measures which includes an assessment method.\(^{23}\) This method comprises a requirement for data exporters to produce a legal analysis, as well as an analysis of public authorities’ practices. The upshot of such an analysis should in theory help data controllers determine whether supplementary measures are needed, i.e., measures reasonably likely to mitigate against confidentiality threats posed by public authorities.

Given the powers and means of public authorities, it is reasonable to assume that context controls, including technical controls affecting the environment as opposed to the data itself, such as access controls, cannot suffice. Data controls such as de-identification and anonymisation techniques thus appear to be key controls in this context. This explains the focus upon PETs, or at the very least, a subcategory of PETs.

### 3. PETs as Supplementary Measures

The EDPB has made it clear that PETs could be useful measures in the context of cross-border data transfers to help justify the lawfulness of the transfer.\(^{24}\) Commentators have however been very severe with the EDPB’s recommendations on supplementary measures even if the second version of the recommendations appears less restrictive than the first one. Rubinstein and Margulies write for example that “[w]hile the Final Recommendations identify risk-based factors for evaluating foreign law and the effectiveness of supplementary measures, in the end these factors reduce to the binary decision of whether or not the essential equivalency standards are satisfied.”\(^{25}\) For the purposes of this note, the difficulty stems from the fact that it is confusing to acknowledge the relevance of PETs without clearly unpacking a risk-assessment method. Yet, the EDPB does not specify a risk-assessment method that could be leveraged for the selection of PETs.

To lay the foundations for such a risk-assessment method, it is important to build a PET typology, organising PETs by objective and limitation. Once this is done, it becomes clearer that PET selection implies a fine-grained approach to data transfer and that PETs cannot act as substitute for data transfer tools.

---

\(^{21}\) Schrems II, para. 142.

\(^{22}\) Schrems II, para. 134.

\(^{23}\) EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the level of protection of personal data, version 2.0, Adopted on 18 June 2021.

\(^{24}\) EDPB, Ibid.

3.1 A PET typology

3.1.1 Relevant PETs

The ICO defines PETs as “technologies that embody fundamental data protection principles by minimising personal data use, maximising data security, and/or empowering individuals. Data protection law does not define PETs. The concept covers many different technologies and techniques.”

The European Union Agency for Cybersecurity (ENISA) refers to PETs as: “software and hardware solutions, ie systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.”

What these definitions do not make clear is that PETs can be of relevance for any type of confidential data, be it personal or not. This is the reason why the concept of CETs is introduced. CETs, a subset of PETs, are an attempt to formalise the selection of controls for a given (and limited) type of threats, i.e., confidentiality-related threats associated with unauthorized or unwanted access. CETs, just like PETs in general, are not a means to address all data protection goals at once. In fact, their implementation usually embed a variety of tradeoffs between competing data protection goals (usually determined in the light of business interests pursued), e.g., typically between confidentiality and transparency, or even between confidentiality and fairness. Such tradeoffs, it is suggested, should always be made explicit when a CET is selected for a particular use case, bearing in mind that duties to preserve data-subject or end-user intervenability through appropriate design are starting to emerge more clearly. These duties are all the more relevant that any personal data transformation process is subject to data protection law, including anonymisation processes.

Importantly, CET settings can vary greatly. In some cases, they will rely upon a trusted intermediary, in others they make it possible to bypass trusted intermediaries. In some cases, they are set up directly between the data subject and the intended recipient of the data, in others they are set up between a controller and a processor or a covered entity and a service provider or contractor.

---

26 ICO, Draft Chapter 5: Privacy Enhancing Technologies, September 2022, p. 3.
29 There is a long history of using PETs to engineer data protection requirements within IT systems. PETs is usually understood broadly and span a variety of coded safeguards, including consent management processes or cookie banners.
30 Engineers often reduces data protection or privacy to confidentiality. See e.g., S. Gürses, Can You Engineer Privacy? (2014) 57 Communications of the ACM 20.
31 See e.g., e.g. M. Veale, Denied by Design? Data Access Rights in Encrypted Infrastructures, 2023, July 27, available at https://doi.org/10.31235/osf.io/94y6r, accessed 28.01.24. (“Designing privacy into complex informational infrastructures requires the navigation of trade-offs that do not have an intuitive or obvious balance.”)
32 See e.g. Recital 20 of the EU Data Act in relation to data access by users of connected products (“It is therefore necessary to ensure that connected products are designed and manufactured, and related services are designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, including for the purpose of retrieving, using or sharing them, are always easily and securely accessible to a user, free of charge, in a comprehensive, structured, commonly used and machine-readable format.”)
In the context of Restriction Pattern #2, when situationally-relevant third parties are in scope, one is concerned with a specific confidentiality threat, which should be mitigated through the prevention of unwanted access.

The list of potentially relevant CETs in such a context is represented in Table 1:

<table>
<thead>
<tr>
<th>CET</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Differential Privacy (GDP)</td>
<td>GDP ensures that an attacker querying the data set cannot reliably infer whether a particular individual’s data is included within the data set, even with access to every record in the data set, except for that specific individual’s data.</td>
</tr>
<tr>
<td>Local Differential Privacy (LDP)</td>
<td>LDP ensures that an attacker querying the data set cannot reliably infer whether a particular attribute is associated with a particular individual whose data is included within the data set, even with access to every record in the data set, except for that specific individual’s data.</td>
</tr>
<tr>
<td>K-anonymisation (K-anon)</td>
<td>K-anonymisation ensures that an attacker with access to the data cannot single out a particular individual within the data set beyond a minimum k number of records</td>
</tr>
<tr>
<td>Homomorphic Encryption (HE)</td>
<td>HE ensures that an attacker, including a malicious processor, cannot access the input data it computes over and the results it generates form the computation</td>
</tr>
<tr>
<td>Trusted Executive Environment (TEE)</td>
<td>TEEs ensures that an attacker, including a malicious processor, cannot access the input data it stores</td>
</tr>
<tr>
<td>Federated Learning (FL)</td>
<td>FL ensures that a Machine Learning (ML) architecture processes user-level training data locally and send model outputs only to a centralised server</td>
</tr>
<tr>
<td>Secure Multi-Party Computation (SMC)</td>
<td>SMC ensures that a participant to the scheme cannot access the raw data held by other participants to the scheme</td>
</tr>
<tr>
<td>Zero Knowledge Proof of Knowledge (ZKPK)</td>
<td>ZKPK is a special case of SMC, that allows a user to prove an assertion without revealing any confidential information related to the assertion</td>
</tr>
<tr>
<td>Synthetic Data</td>
<td>Synthetic data is drawn from a model which has been trained on real data and which outputs data such that it is considered to be consistent with the training data.</td>
</tr>
</tbody>
</table>

Table 1. CET goals

3.1.2 The Inference Model

There are different ways confidentiality threats can be mitigated and the choice of controls should ultimately depend upon the type of inference to prevent.

The inference model is a formalised method developed to inform confidentiality-related risk assessment.\(^{33}\)

In an inference model, there are four types of inferences an attacker could try to make:

- Identity inference: inference that a record corresponds to an individual.
- Attribute inference: an inferred value for a particular attribute within an individual record.
- Participation inference: an inference that the data of a particular individual is included within a data set.

- Relational inference: an inference that two records correspond to the same individual.

Because CETs are built to achieve a very limited objective, it is hard to compare them. It is however possible to distinguish between the following five objectives, which should inform the choice of the best-suited CET for a given use case:

1. To offer a guarantee of deniability to the participant to a data set. In other words, once the CET is applied it will be possible to argue that a particular data subject or data point has never been included in the data set and therefore data associated with the data subject or data point could not have contributed to the query results.
2. To offer a guarantee of deniability as to the value of particularly sensitive attributes. In other words, once the CET is applied it will be possible to argue that a participant to the data set has never been associated with a particular sensitive value or that a particular event or product has never been associated with a particular sensitive value.
3. To offer the guarantee that the raw data has never been accessed by a particular stakeholder, which is different from stating that no inference has ever been derived from the raw data.
4. To offer the guarantee that it is not possible to single out an individual, an event or a product within a particular data set, which is different from arguing that it is not possible to infer any attribute, including a sensitive attribute, about a particular individual or product or service.
5. To offer the guarantee that an untrusted processor cannot read the protected data, which is different from stating that the data holder cannot compute over the protected data, although the processor will not be able to read the results of the computation either.

Each CET usually addresses one of these objectives. Some CETs offer formal guarantees, others do not.

Crucially, CETs should not be examined in isolation but should be assessed within their settings. A CET setting has three main components: data (input and output data), stakeholders (at a minimum a data exporter and a data importer), and infrastructure (technical and organizational structures that make processing by the data importer possible). CETs, irrespective of the formal guarantee they offer, always require the implementation of context controls once the broader picture of the CET setting is taken into consideration.

Given the limited guarantee they offer, it may make sense to combine them.

In a non-data transfer scenario, where public authorities are not arguably in scope, a situationally-relevant attacker is usually defined in terms of a motivated intruder who does not have prior knowledge and does not necessarily possess expert technical skills.

In a non-data transfer scenario, the inference model leads to a risk-based assessment centered around the following questions:

1. Is it reasonable to assume that the main inference to mitigate against is identity inference? (Note that identity inference is usually associated with objective 4)
2. Given the sensitivity of some attributes at stake, would it make sense, as a matter of precautionary measure, to mitigate against attribute inference as well? (Note that attribute inference is usually associated with objective 2)
3. Given the sensitivity of group membership-related information, would it make sense, as a matter of precautionary measure, to mitigate against membership inference as well? (Note that group membership inference is usually associated with objective 1)

---

34 A formal guarantee is a guarantee that can be demonstrated mathematically.
35 S. Stalla-Bourdillon & A. Rossi, n(33).
36 S. Stalla-Bourdillon & A. Rossi, n(33).
37 See ICO, Code of Practice on Anonymisation n(8), and the 2022 draft chapters (8).
4. Given the data environment at stake, does it make sense as a precautionary measure to also mitigate against the linking of certain types of data sets?

Often, in practice, the answer to the first question is positive. On occasions, some additional data controls are put in place to mitigate against sensitive attribute inference or group membership inference as well. Relational inference may be of relevance, for example, when data is combined in such a way that it would very easily jeopardize mitigation against identity inference.

Crucially, it is not possible to completely eliminate re-identification risks and even when identity inference risks are mitigated to a satisfactory level, other types of confidentiality-related risks can persist.\(^{38}\)

Going further, unless one implements a data transformation method that is indifferent to the attacker’s prior knowledge or one precisely determines the extent of an attacker’s prior knowledge, it is simply impossible to rule out inference attacks in the absolute sense.\(^{39}\) It follows that simplistic oppositions drawn between individual-level data and aggregated data are misleading.\(^{40}\) It is just wrong to claim that relying upon aggregated data never raises privacy concerns. A better formulation would be to state that anonymization can be pursued through the aggregation but is likely to require more than aggregation to mitigate re-identification risks.

Basically, a controller is thus left with two options: either to minimise the amount of information transmitted to a potential attacker regardless of the background knowledge of the attacker through the formalisation and implementation of global differential privacy-based controls (option 1) or to formalise an attack model (i.e., drawing a realistic profile of the situationally-relevant attacker) and implement relevant controls arguing that either it is reasonable to assume that any attacker successful in reaching the data is unlikely to possess relevant background information, or that when such an event occurs, individual impact is limited by the applied controls (option 2). To be truly indifferent to the background knowledge of the attacker, option 1 requires implementing a privacy budget for each data consumer, which when exhausted, will mean that the data consumer will not be able to query the data further. What this means is that access control, i.e., a context control, is essential for the success of option 1.

As a result, anonymisation always remains a tradeoff, i.e., a decision to prioritise utility over confidentiality. Therefore, anonymisation should always be coupled with safeguards applicable to downstream uses: in particular, it is essential to make sure that the purpose for which the data is anonymised is legitimate and to consider whether some level of data-subject or end-user intervenability is preserved. Interestingly, the recently-adopted Quebec Law 25, which amends the Act respecting the protection of personal information in the private sector,\(^{41}\) acknowledges the importance of purpose legitimacy clearly. What is more, it is possible in practice to set up CETs in such a way that data lineage, and therefore capabilities to object, are preserved, even if data is transformed to reduce re-identifiability risks for a particular use case.

**Recommendation:**

Consider showcasing CET settings that are able to preserve data-subject and end-user intervenability

---

\(^{38}\) In particular, when the attacker has some prior knowledge.

\(^{39}\) C. Dwork, Differential Privacy, Lecture Notes in Computer science book series, LNTCS, volume 4052.

\(^{40}\) See e.g., the European Commission’s statement in the EU-US 2023 adequacy decision: "Statistical reporting relying on aggregate employment data and containing no personal data or the use of anonymized data does not raise privacy concerns."

\(^{41}\) chapter P-39.1, Section 23 ("Where the purposes for which personal information was collected or used are achieved, the person carrying on an enterprise must destroy the information, or anonymize it to use it for serious and legitimate purposes, subject to any preservation period provided for by an Act").
To be sure, even if anonymisation is fundamentally a tradeoff, resorting to threat modelling techniques is not pointless. It is actually quite the opposite: these techniques forces the data controller to make its assumptions explicit. Yet, we suggest that both assumptions related to the types of inference in scope and the applied threat model should be made explicit to allow oversight.

**Recommendation:**

*Consider producing guidance on threat modelling techniques*

### 3.1.3 Data Transfers and PETs

In the context of data transfers, public authorities comprising intelligence services and law enforcement agencies representing situationally-relevant attackers should be assumed to have prior knowledge and expert technical skills: global differentially-private methods (i.e., option 1) thus appear more attractive. However, when this option is not available due to utility constraints, an attack model will need to be formalised (i.e., option 2), which will imply making assumptions about the degree to which the data would be of interest to the situationally-relevant attackers or would otherwise already be available to them, and the types of individual impact (e.g., which could be a physical or psychological harm or even a human-right violation) a successful attack could generate.

The strongest CETs or combination of CETs in cross-border data transfer context appear to be:

<table>
<thead>
<tr>
<th>CET</th>
<th>Guarantee (under a suitable attack model)</th>
<th>Effect</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDP</td>
<td>Formal deniability against participation</td>
<td>Prevents an attacker from learning more than a limited amount of additional information about an individual record (the amount is controlled by E)</td>
<td>The mathematical value Epsilon (often named privacy budget) is set properly</td>
</tr>
<tr>
<td>K-anon</td>
<td>Formal guarantee against singling out</td>
<td>Prevents an attacker from attributing a record to an individual</td>
<td>Both the mathematical values Epsilon (often named privacy budget) and K (the number of individuals sharing identical attributes within a data set) are set properly</td>
</tr>
<tr>
<td>+ LDP</td>
<td>Formal deniability against sensitive attribute disclosure</td>
<td>Prevents an attacker from learning more than a limited amount of additional information about an individual’s attribute</td>
<td></td>
</tr>
<tr>
<td>HE</td>
<td>Formal practical impossibility to read the input data and the results</td>
<td>Prevents an attacker from learning non-negligibly more than the message length in practice</td>
<td>Decrypting without the key is computationally infeasible</td>
</tr>
<tr>
<td>TEE</td>
<td>Formal practical impossibility to read the input data (no guarantee for the results unless other protective measures are put in place)</td>
<td>Prevents an attacker from learning non-negligibly more than the message length in practice</td>
<td>The hardware manufacturer is trusted, the hardware is bug free and not under physical surveillance, and the PKI is trusted</td>
</tr>
</tbody>
</table>
SMC: Formal practical impossibility to read the input data of other party members (but no guarantee for the results unless other protective measures are put in place)

Prevents an attacker from accessing the data when jointly processing the data (but the attacker could learn anything inferable from the size of the input together with the results)

Decrypting without the key is (at least) computationally infeasible

Note on FL:
There is no guarantee as FL is an ML architecture which has the effect of minimising the amount of data processed by the global model with no guarantee that the global model cannot memorize the training data. However, FL can be coupled with differentially private techniques.

Note on Synthetic Data:
There is no guarantee as Synthetic Data is simply the product of a model that is trained to reproduce the characteristics and structure of the original data with no guarantee that the generative model cannot memorise the training data. However, data synthetisation can be coupled with differentially private techniques.

Table 2. CETs that may be relevant in a cross-border data transfer context

Again, as it is not possible to eliminate all re-identification risks, anonymisation in the context of data transfers remains a tradeoff, despite the absolutist language used by the EDPB who seems to ignore that the absolute impossibility to attribute the information to an individual can only be based upon the information available within the data set under GDPR Article 4(5). Yet, once both publicly-available information and prior knowledge are in scope, it becomes impossible to ensure such an absolute impossibility! This therefore means that the processing purpose should remain a key component of the assessment, as well as the level of data-subject or end-user intervenability preserved, and that there may be an argument to loosen restrictions when transfer is in the public interest.

Pushing the analysis further, the difference in the range of situationally-relevant attackers between a non-transfer scenario and a transfer scenario means that data that is considered anonymised within the EU should not necessarily be authorised to travel to third countries, as additional checks may be needed to ascertain whether the data should be considered appealing to a wider range of situationally-relevant attackers, i.e., intelligence services and law enforcement agencies, and whether sensitive information has been protected to an acceptable level. One way to eliminate this double standard would be to assume that in a data transfer context, the output data remains at most pseudonymised. This would make it possible to govern onwards...
transfer while not necessarily ruling out data transfers. Note that the ICO is of the view that it is possible to achieve anonymisation in the hands of the data importer.45

As it is becoming clear from this analysis, implementing CETs implies a tradeoff and can be resource intensive. One way to reduce uncertainty would be for a competent authority, e.g., the EDPB at the EU level, to produce clear guidance about the types of legitimate use cases CETs could enable in a data transfer context. This would not necessarily relieve data exporters from their risk assessment obligations however, as they would focus the analysis upon the particular implementation of the CET within a pre-determined setting and assess the limitations of the CET in this context.

When assessing CET use cases to select legitimate ones, it is essential that CETs’ implications in terms of data and infrastructure monopoly be seriously taken into account to avoid strengthening monopolies through CET promotion,46 which explains why imposing a blanket obligation to use hard PETs47 on the ground of a data protection-by design obligation only, such as GDPR Article 25, remains problematic.48 At most, an obligation to consider the implementation of CETs could be imposed.

Recommendation:
Consider producing a list of recommended PET use cases starting with use cases that are in the public interest considering a wide range of dimensions of concern

3.2 Fine-grained Data Transfer Assessment

To be able to formalise an attack model, a fine-grained assessment of the data transfer at hand is necessary. A fine-grained data transfer assessment implies distinguishing between different types of processing activities on the basis of the level of data sensitivity, data availability, anticipated individual impact if situationally-relevant attacks succeed, the legitimacy of processing purposes and the level of data subject or end-user intervenability. Such an approach, however, does not align well with the one-size-fits all approach adopted by some EU data protection authorities, which quite understandably have been wary of data exporters’ attempt to perform risk assessments in this context.49 This said, these authorities have more leeway than they think.

45 ICO, Annex to the Transfer Risk Assessment Tool, available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/international-data-transfer-agreement-and-guidance/transfer-risk-assessments/#TRA-tool, accessed 28.01.24. (“Note: You should also consider anonymisation techniques. If the personal information is effectively anonymised in the hands of a receiver so that it is no longer personal information, the UK GDPR transfer”).
47 an expression sometimes used to refer to CETs or a subpart of CETs.
48 See e.g., I. Rubinstein and N. Good, The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default (September 30, 2019). International Data Privacy Law (2020) doi: 10.1093/idpl/ipz019, who argue that “In order to advance data protection in its own right rather than merely reinforce the general principles of the GDPR, Article 25 must be interpreted as requiring the implementation of privacy engineering and hard PETs. A bold way to achieve this is by mandating that data controllers use available hard PETs for data minimisation.”
49 For a critique of these decisions see Lokke Moerel, What happened to the Risk Based Approach to Data Transfers? How the EDPB is rewriting the GDPR, (Future of Privacy Forum blog, 2022). This author, however, does not unpack the concept of a risk-based approach. See also on a risk-based approach to data transfer
One concerned usually raised when a fine-grained approach to data transfer is presented relates to the subjectivity of the assessment, which may undermine the Schrems II holding.50 There are however ways to address such a concern. The most effective way would probably be for a competent authority sitting within the jurisdiction of the data exporter to expressly acknowledge that public authorities, i.e., intelligence services and law enforcement agencies are not interested in all types of data, and exclude low-risk data, starting with data that could easily be accessed through other means, unless the scope of the database would be such that it would offer an added-value to the third-party attacker, e.g., a social media data base. The US Government 2020 White Paper for example states that “[c]ompanies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data.”51 While more granularity would be preferable, it is probably fair to infer from this statement that business-to-business personal data or personal data collected in the context of business-to-business relationships, which usually comprises names, job titles, and contact details, (that is to say a reduced set of demographic data) and is information that is usually publicly available on a variety of platforms, be it social media or businesses’ own websites, should be considered low risk in a data transfer context.

Telemetry data is another category of data that is often discussed in the context of cross-border data transfers.52 Telemetry data usually includes sessions, events, logs that are generated by an application. There are however two types of telemetry data that are worth distinguishing: system telemetry data, which is often used for security purposes, and is first and foremost interested in the behaviour of an application. Some items of personal data could nonetheless be present in the logs generated by the application such as IP addresses, emails and/or account names, permission and/or access grants... User telemetry data, which tends to be used for product and service improvement, concerns the way users use the services. It usually comprises user ids, which could be randomised or at the very least obfuscated, device information, clicks within the product or service, and other actions. There is often no need to process directly identifying user telemetry data, but user telemetry data could potentially encompass a wide range of activities, in particular when joined across products and services before being aggregated at some later point in time. Notably, in an AI context, user telemetry is likely to include prompts or input data. There are good arguments for compromising on the flow of system telemetry data. They comprise a limited set of personal data that is

50 This seems to have worried the EDPB in particular who in its first version of its recommendations had stated that data exporters shall “not rely on subjective [factors] such as the likelihood of public authorities’ access to your data in a manner not in line with EU standards.” EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 1.0, Adopted on 10 November 2020, para. 42.


shared with the service provider running the application for a legitimate internal purpose: to guarantee that the application is secure.\textsuperscript{53}

Interestingly, the European Commission itself in its adequacy decision concerning the US indirectly acknowledges that certain types of human resources data are less risky than other types of data, or said otherwise, tries to find a compromise for data processed for occasional employment-related operational needs.\textsuperscript{54} This solution should also be seen in the light of the EDPB guidance on the definition of restricted transfers within the meaning of Chapter V, which excludes from its remit data flows between individual employees and their employer subject to the GDPR.\textsuperscript{55} Interestingly, in its newly-released draft Rules, which are expected to be adopted by the end of November, China is attempting to facilitate transfers of employee personal information by exempting it if such data is necessary to perform human resource functions or to administer collective employee agreements, assuming processing practices comply with China labor law requirements.\textsuperscript{56}

For other types of more sensitive data, like key-coded research data, similar compromises could perhaps also be considered assuming reasonable steps are taken to confirm that such data should not be deemed of interest to public authorities, which could very well be a reasonable assumption to make in several instances. Interestingly, China has recently attempted to soften its stance for data generated in international trade, academic cooperation, multinational manufacturing and marketing activities that do not contain personal information and important data.\textsuperscript{57} It remains to be seen whether China will agree to find that individual-level personal data could be transformed into anonymised data without necessarily aggregating the data.

On the basis of the UK GDPR, the ICO has developed a transfer risk assessment tool that is based upon the classification of personal data in relation to risk levels.\textsuperscript{58} It is clearly stated within the tool that when categories of personal information are associated with low-harm risks, it is possible to proceed with the transfer, no matter what the response might be to the next questions, which relate to human rights and enforceability risks. The ICO is thus trying to set forth a fine-grained approach to data transfers on the basis of the UK GDPR, which would suggest that there is no reason why the EDPB could not pursue a similar

\begin{itemize}
  \item \textsuperscript{53} See also P. Swire et al., Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics and Procedures, Draft June 1, 2023, available at \url{https://ssrn.com/abstract=4466479}, accessed 28.01.24, who argue on the basis of the EDPB’s guidance on breach notification that “in most contexts the data elements used in cybersecurity, such as IP address, MAC address, or email address, are low risk – not requiring a breach notice even when they are seized illegally by hackers and transferred to a third country.” The position taken in this paper is however slightly different from P. Swire et al, as when defender techniques are user focused as opposed to application focused and consist in systematically profiling users to eventually impact upon their legal interests to public authorities, which could ver
  \item \textsuperscript{54} See Annex I, III Supplementary Principles, para. 9.(e)(i) "For occasional employment-related operational needs of the participating organization with respect to personal data transferred under the EU-U.S. DPF, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees can take place to controllers without application of the Access Principle or entering into a contract with the third-party controller, as otherwise required under the Accountability for Onward Transfer Principle, provided that the participating organization has complied with the Notice and Choice Principles.”
  \item \textsuperscript{55} EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, version 2.0, Adopted on 14 February 2023 (“the second criterion implies that the concept of “transfer of personal data to a third country or to an international organisation” only applies to disclosures of personal data where two different (separate) parties (each of them a controller, joint controller or processor) are involved.”)
  \item \textsuperscript{56} See the new draft on “Regulation and facilitation of cross-border flow of data”.
  \item \textsuperscript{57} See the new draft on “Regulation and facilitation of cross-border flow of data”.
  \item \textsuperscript{58} ICO, Transfer Risk Assessment Tool, n(45). The ICO explains that there are two ways to comply with chapter 5 of UK GDPR.
\end{itemize}
objective, as long as it is clear that it is the likelihood of human right violation that should be used to set the threshold as harm is not a prerequisite to the protection of human rights. With this said, the harm classification produced by the ICO raises questions. It is not clear, for example, why habits should be classified as low risk when these are the basis of intrusive profiling. Besides, one should look beyond the data and take into account the purpose of the data flows and the level of data-subject intervenability to strike a more legitimate compromise.

Another way to explain the reluctance of EU supervisory authorities to endorse a fine-grained approach could be found in the view that the Schrems II decision necessarily endorses a one-size-fits-all approach that makes it impossible to refine the profile of the attacker in the light of the circumstances of the case at hand. It is unclear whether the CJEU ever went that far however.

In addition, a one-size-fits-all approach is hard to reconcile with a definition of restricted transfers that is also a compromise. The EDPB definition for example, which builds upon the CJEU case law, 59 excludes data flows between data subjects and entities acting as controllers or processors of personal data, thereby requiring an interaction between two types of covered entities. 60 The EU definition of data transfers is thus the fruit of a compromise between the will to ensure a high level of data protection and the acknowledgement of the realities of cross-border data exchanges enabled by the Internet. Since 2018, this compromise is reached with the implementation of a safety valve: Article 3(2) of the GDPR. 61 In other words, even if data flows departing from data subjects are not deemed restricted transfers within the meaning of Chapter V, it is very likely that the data importer will be subject to the GDPR anyway. There is no reason why such a safety valve should not be used for low-risk data or better low-risk processing activities between covered entities, as data flows between data subjects and covered entities could very well lead to situations of high risks for the fundamental rights and freedoms of individuals.

What is more, an adequacy decision is always a compromise. 62 Take the example of New Zealand, which has received an adequacy decision prior to the GDPR, and of which validity has been confirmed post GDPR a few months ago by the European Commission. 63 Data originating from the EU could leave New Zealand, on the

---

59 See CJEU Case C-101/01 Bodil Lindqvist 6 November 2003 ECLI:EU:C:2003:596.

60 This approach is peculiar to the EU as Convention 108+ adopts a different approach and defines restricted transfer as access by a recipient that is not a party to Convention 108+, making the role of the parties to the data flow irrelevant (see Article 14 read in the light of the Explanatory Report). The same approach has been adopted by China, but as mentioned above, this country is now considering loosening its approach. Of note, Brazil also seems to go down a similar path by distinguishing between data transfer and data collection and excluding the latter from the remit of transfer restrictions.

61 This begs the question why not using this safety valve for all types of transfer in an attempt to simplify the regulatory burden. There are good reasons not to go in this direction though, in particular if the goal is to force data importers to shield themselves from local public authorities. In addition, Kuner makes it clear that “data transfer rules also provide more enforcement possibilities than does extraterritorial application of the GDPR, since many transfer rules can also be enforced against the data exporter in the EU.” Christopher Kuner, Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU’s Ambition of Borderless Data Protection, Paper no. 20/2021, April 2021, Legal Studies Research Paper Series, University of Cambridge, p. 25. Besides, he also observes that “the appointment of a representative as a way to improve enforcement of the GDPR against non-EU parties has thus far proven largely toothless.” Ibid, p. 12.

62 One compromise that has often been criticised is the adequacy decision issued in favour of Japan, despite clear evidence that the level of enforcement was rather weak. The same is true with the adequacy decision issued in favour of Israel that has been recently confirmed following the review process of 11 pre-GDPR adequacy decisions.

basis of Principle 12 of the Privacy Act 2020\footnote{Privacy Act 2020, Section 22, Information Privacy Principle 12(1)(b).}, without any restriction when the data importer is subject to the Act.

A compromise is also implicitly set forth when capabilities to access protected data from third countries (in the absence of actual data flows) are not considered sufficient to trigger the applicability of GDPR Chapter 5.\footnote{See e.g., EDPS, Decision on the CJEU's use of Cisco Webex video and conferencing tools, 13 July 2023, available at \url{https://edps.europa.eu/data-protection/our-work/publications/authorisation-decisions-transfers/2023-07-13-edps-cjeus-use-cisco-webex-video-and-conferencing-tools_en#-text=In%20its%20Decision%20published%20on%20%20July%202023%2C%20bodies%20and%20agencies%20accessed%2028.01.24, para. 35 ("The EDPS considers that transfers resulting from unauthorised access by third country entities, which are merely potential and in no way foreseeable in light of the content or purpose of a contract or another stable relationship between the parties, do not fall under the scope of Chapter V of the Regulation"). There does not seem to be perfect consensus on the matter however.}

\begin{center}
\textbf{Recommendation:}
\end{center}
\begin{quote}
Consider developing a fine-grained data transfer assessment method
\end{quote}

### 3.3 Data Transfers, Trustworthiness, and PETs

Despite recent references to trust\footnote{See the Data Free Flow with Trust initiative promoted at the Group 7 (G7) and Organisation for Economic Co-operation and Development (OECD) levels. See e.g., Japan Digital Agency, Data Free Flow with Trust, available at \url{https://www.digital.go.jp/en/dfit-en}, accessed 28.01.24; OECD, Moving forward on data free flow with trust: New evidence and analysis of business experiences, OECD Digital Economy Paper, n°353, available at \url{https://www.oecd.org/sti/moving-forward-on-data-free-flow-with-trust-1afab147-en.htm}, accessed 28.01.24.}, governing cross-border data transfers is fundamentally about forcing the production of trustworthiness evidence. Trust and trustworthiness are two different, even if related concepts. While trust is an attitude, trustworthiness is a property.\footnote{There are many conceptualisations of trust stemming from different disciplines, including economics, sociology, psychology and law. The trustor's willingness to be vulnerable is central to most conceptions of trust. On the other hand, when trustworthiness is distinguished from trust, it is usually described as a property of the trustee that can ground a trustor's expectations, when trust is conceived as the expression of a rational choice (i.e., cognitive trust as opposed to affective trust). Trust and trustworthiness are, however, often wrongly conflated with each other. See e.g., M. Greenwood & H. Buren, Trust and Stakeholder Theory: Trustworthiness in the Organisation-Stakeholder Relationship, 95 (2010), 425-438; H. Sekhon, C. Ennew, C., H. Kharouf, & J. Devlin, Trustworthiness and trust: influences and implications, Journal of Marketing Management, 30(3-4) (2014), 409-430.} Said otherwise, trust is a leap-faith on which to base a decision, it implies accepting risk and vulnerability. Trustworthiness, on the other hand, is a set of qualities considered to be sufficient to elicit reliance. Therefore, it is a means to reduce risk and vulnerability. The starting point in the context of a commercial relationship is trustworthiness. A party to a commercial relationship relinquishing control over governed data should thus require from the other party or other authoritative sources evidence of trustworthiness.

Trustworthiness in a cross-border data transfer context can be established at two levels: at the jurisdictional level and/or at the entity level. As a result, two types of trustworthiness evidence are distinguished. When the evidence focuses upon the regulatory framework of the jurisdiction in which the data importer operates, it relates to \textit{institutional trustworthiness}, while when it focuses upon the commitments and/or behaviour of the data importer itself, it relates to \textit{relational trustworthiness}.
CBDT tools are thus a means to produce evidence of trustworthiness: either institutional trustworthiness, e.g., with adequacy decisions, or relational trustworthiness, e.g., through SCCs, BCRs or certification.

Importantly, even when CETs are implemented to mitigate against the absence of institutional trustworthiness, which is problematic when Restriction Pattern #2 is applicable, evidence of relational trustworthiness is still relevant. It often makes sense to subject data importers to contractual obligations to make sure appropriate context controls are put in place, e.g., obligation to implement strict access control, to comply with purpose limitation, or not to collude with other data sharing scheme participants. Even if a claim of legal anonymisation is asserted, context controls remain relevant even when the strongest CETs are implemented (e.g., through global differentially-private methods) and enforcement assurances should be sought through appropriate CBDT tools.

What is more, when a CET setting aims to preserve some level of data subject intervenability, which should facilitated by a query setting, it may make sense to impose upon data importers an obligation to assist the data exporter when responding to data subject requests.

What this shows is that data transfer tools such as SCCs, BCRs or certification, of which primary purpose is to evidence relational trustworthiness, will still be needed and CETs should only be conceived as complements to such tools.

**Recommendation:**

**Consider closely intertwining PETs and a cross-border data transfer tools workstreams**

### 4. Conclusion

Incentivising the free flow of data through PET promotion requires carefully thought-through nuances. First, such an effort implies creating a consensus upon a fine-grained approach to data transfer, which on occasions has been welcomed with suspicion by regulators as it is challenging to draw distinctions between processing activities on the basis of individual impact. Second, it requires formalising a contextual risk-assessment method to help assess the legitimacy of the tradeoff reached between two competing goals, utility and confidentiality. This method should comprise at least two steps:

1. A relatively narrower step during which the types of inferences addressed by the CET setting are explicitly identified and mapped against relevant controls
2. A broader step during which other data protection goals than confidentiality are taken into account, such as purpose limitation and data subject/end user intervenability.

Third, it requires acknowledging the ongoing relevance of CBDT tools. This is because in many instances claims of legal anonymisation should be made dependent upon downstream controls set by the data importer. Conceiving CBDT tools and PETs as alternatives is thus inherently flawed.

This policy note includes recommendations for policy makers interested in setting or contributing to PET workstreams and who are engaged in actions to reduce the fragmentation of data flow regimes at the global level. The note has shown that CETs on their own are implemented to pursue very limited objectives. In addition, it has made clear that while some of these CETs are very powerful in the light of the particular objective they aim to pursue, they always imply a tradeoff, i.e., a decision to prioritise utility over confidentiality. Therefore, this note suggests that CET selection and implementation should be use-case specific and take into account a wide range of dimensions of concern, including the legitimacy of processing purposes, the level of data-subject or end-user intervenability, as well as eventual broader implications, such as implications in terms of data and infrastructure monopoly.
Acknowledgements:

The author would like to thank Graham Greenleaf, Alex Joel, Eric Lachaud, Theresa Stadler and Olivier Blazy for their insightful comments upon earlier drafts. All mistakes are hers.

This research has been funded by Cerre, Brussels, Belgium.