

MyData-TRUST S.A. Boulevard Initialis 7, Bte 3 7000 Mons www.mydata-trust.com

30/09/2022

Comments on Guidelines 07/2020 on certification as a tool for transfers (Version 1.0) adopted on 14 June 2022.

Comments from:

MyData-TRUST

When DATA PROTECTION Meets Life Sciences

MyData-TRUST provides DATA PROTECTION services in the LIFE SCIENCE sector (such as privacy risk assessments, external DPO as a service, etc.). Active since 2017, it is registered under Belgian Laws. Its Multi-Disciplinary Team relies on Data Privacy Lawyers, IT Security Specialists and Clinical Experts. Our clients include among others Pharmaceutical, Biotech and Medical Device companies, Contract Research Organisations (CROs), Healthcare providers and associations.



Key messages

MyData-TRUST (hereinafter referred as "**MD-T**" or "**we**") welcomes the clarifications brought by the Guidelines 07/2020 on certification as a tool for transfers adopted on 14 June 2022 ("**Guidelines**"). In particular, the clarifications on the object of the certification, on the certification criteria but also on the obligations up to the exporter when relying on such transfer tool.

While the Standard Contractual Clauses ("**SCCs**") have been quite challenged following the Schrems saga, the release of the first practical guidance on certification seems to come at the right time and gives some alternative through another transfer mechanism not really used in practice until now.

Even though the Guidelines bring new light on data transfers mechanisms, MD-T believes the Guidelines missed the opportunity to clarify several aspects which were currently not yet settled for other tools as SCCs and provide additional means to achieve compliance with Chapter V of the GDPR.

More specifically, MD-T would like to emphasize:

- → The need to provide a harmonized approach with regards to the importer's role in the performance of the Transfer Impact Assessment ("TIA") (1).
- → The need to rethink the supplementary measures to enable more efficient safeguards, especially against intrusive access of third country's authorities (2).
- → The need to create relevance and incentives to rely on certification by opening its scope to importer already subject to GDPR (3).

We further develop these different points of view and present more detailed comments further in this document.

Introduction and general considerations

This feedback document and reasoning were built with the essence of the GDPR in mind and considering notably:

Recital 6 GDPR: "Technology has transformed both the economy and social life and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organizations, while ensuring a high level of the protection of personal data";



- EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation (Version 3.0) adopted on 4 June 2019;
- EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) adopted on 18 June 2021.

Specific comments

WHO IS LIABLE FOR WHAT IN THE TIA? FOCUS ON THE IMPORTER'S ROLE (1)

As highlighted by paragraph 1.5 of the Guidelines, the responsibility for data processing compliance but also the compliance of all provisions of Chapter V remain with the data exporter, which includes the performance of the TIA.

Besides, the Guidelines go deeper than previously and set forth further obligations on the importer. As requirement included in the certification's criteria, each importer is supposed to perform an assessment of the third country relevant legal framework and provide (and where appropriate, request) supplementary measures to the exporter.

MD-T deems this clarification on the importer's role for the performance of the TIA is a real added value, especially when in practice most of the importers tend to offload any TIA's obligations to put it on the head of the sole exporter.

- **Imbalance of powers**. Such trends are especially present face to large companies (mostly US-based) such as multinational technology company and corporation which tend, due to their position on the market, to disclaim any liability.
- **Minimization concerns**. Furthermore, some of them use to include all their worldwide affiliates as importer to put the whole liability up to the exporter regardless the relevance of the involvement of such affiliates in the specific transfer.
- **Conflict of interests**. Finally, when considering the role of the importers, it is also worth considering the contradictory position in which they are regarding the TIA. As further developed on Point 2, while the importers are subject to third country's legislations, they concurrently want to be the most competitive on the market. Then, put on their head more responsibilities on the determination of the supplementary measures for instance could be somewhat tricky.



In view of the foregoing, most of the time, the exporter is alone to perform the whole TIA while the importer remains the best placed person to support him on this task. Then, the further importer's obligations provided in the Guidelines bring more clarity and set forth a real shared-responsibility - which was not reached so far.

However, even if this clarification brings some light on what the exporter may expect from the importer, it creates at the same time confusion compared to the previous EDPB Recommendations 01/2020¹ ("**Recommendations**"). In its executive summary, the Recommendations seem rather to consider that the responsible for the performance of the TIA is the exporter only, while the importer must solely support exporter as part of its collaboration's duty. Further, the exporter seems to be the only one supposed to identify and implement the supplementary measures.

MD-T suggests EDPB to adopt a harmonized approach regarding the role of importer in the performance of the TIA regardless the transfer mechanism used in the specific context.

Then, in line with this approach, the previous Recommendations should be amended accordingly. Further, we suggest EDPB to include a table to split properly the role and responsibilities of each Party with a particular focus on the collaboration's duty and the liability of the importer, while taking into due account the conflict of interests faced by the importer.

In addition, MD-T deems the following alternatives could be considered:

- Additional enforcement to prevent any misuses. To avoid the concerns described above as the data minimization concerns, MD-T believes the importer should provide the full data flows with only the accurate affiliates. Otherwise, in the case where the importer tries to impose affiliates to the exporter which do not appear relevant for the specific transfer, the exporter should no longer be considered as primary liable for these onwards transfers

¹ EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0) adopted on 18 June 2021, p. 3.

[&]quot;To help **exporters** (be they controllers or processors, private entities or public bodies, processing personal data within the scope of application of the GDPR) with the complex task of assessing third countries and identifying appropriate supplementary measures where needed, the European Data Protection Board (EDPB) has adopted these recommendations. These recommendations provide **exporters** with a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place".



but the importer. To this extent, a contractual clause in that direction could be included in the main agreement between exporter and importer. However, to prevent on a broader scale such misuses from importer, we consider additional enforcement measures should be put in place.

- **Further transparency through a passive way**. While considering the conflict of interests faced by importers, MD-T deems the "*warrant canary*" method could constitute a fair alternative. Such method consists of the commitment of the importer to regularly publish (e.g., at least every 24 hours) a cryptographically signed message informing the exporter that, as of a certain date and time, it has received no request to disclose personal data. Otherwise, the absence of an update of this notification will indicate to the exporter that the importer may have received a request to disclose / make available such data. In principle, even though the importer is subject to the third country's laws, it will not prevent importer to issue this form of passive notification to the exporter.



WHAT ARE THE REAL AND EFFICIENT SAFEGUARDS AGAINST PROBLEMATIC ACCESS FROM THIRD COUNTRY'S AUTHORITIES? (2)

The Annexes of the Guidelines provide some examples of supplementary measures in line with those in Annex II of the EDPB Recommendations 01/2020. On the one hand, the Annex A covers the measures to be implemented by the importer and on the other hand, the Annex B covers the measures to be implemented by the exporter.

- Use Case 2: pseudonymization's loophole

Among the supplementary measures, the pseudonymization has been provided as per the Use Case 2 of the Guidelines. This echoes the former Recommendations which pointed out the 4 cumulative criteria of the pseudonymization to be considered as providing effective measure.

Despite the fact we truly consider the pseudonymization is a key measure to implement, especially in the life sciences' sector, we believe the criteria to meet are not realistic in our modern society. This especially applies for the fourth criteria. Even if the 3 first seem reasonable, the fourth one appears problematic and even unrealistic in practice since the risk "zero" does not exist, especially with the digital era, where a lot of personal data is easily available through social media and public websites making unwanted identification a possible risk through chain reaction. Furthermore, it is worth noting the new technologies render increasingly easy for hackers to break the pseudonymization.

In view of the foregoing, the mosaic effect suggests that even anonymized data, which may seem innocuous in isolation, may become vulnerable to re-identification if enough datasets containing similar or complementary information are released.

Then, we strongly believe the pseudonymization is an effective measure only in the case where those who rely on it, use it fairly and properly. The pseudonymization is not impossible to achieve but is far from easy to implement. Plus, the boundaries of the pseudonymization remain blur. It is difficult to determine whether the pseudonymization should prevent the risk of re-identification following legitimate actions only or both legitimate and illegitimate actions – which is a different matter.

- Use Case 3: encryption's loophole



Like the previous Recommendations, the encryption has been provided. It constitutes one of the foundational principles of Privacy by Design.

Encryption is useful for storing backups of data but when it comes to processing data using cloud services, encryption is not sufficient. In accordance with the Use Case 6 from the Recommendations, in the case where "unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys". Until fully homomorphic encryption becomes practical and supported by mainstream cloud services, it remains mostly academic at this point. Third country-based cloud providers cannot be used for the parts that are covered by GDPR. For the moment, exporters should still be looking at cloud native tools.

Further, it is worth noting that, in the clinical sector, the encryption appears not feasible and most of the time cannot be even considered since the personal data need to be processed in the clear. Encryption appears then useless for a large proportion of the companies developing drugs – either for sponsors or service providers.

In view of the foregoing, pseudonymization and encryption appear poor. Plus, they do not constitute *one-size-fits-all* measures, especially face to the problematic access of personal data from third country's authorities.

- US Surveillance Laws. US-owned "electronic communication service providers" (e.g., AT&T, Amazon (AWS), Apple, Cloudflare, Dropbox, Facebook, Google, Microsoft, Verizon Media (former Oath & Yahoo), and Verizon) should no longer be used to process EU personal data, "due to Section 702 of the US Foreign Intelligence Surveillance Act (FISA 702) and US Executive Order 12333 (EO 12333), which specifically require "electronic communication service providers" to comply with US surveillance requests regardless of where data processing occurs - in the US, the EU, or anywhere. Even with anonymized, pseudonymized or encrypted data, EU personal data is still subject to potential surveillance when they are processed by US "electronic communication service providers" and because the US government has vast powers to break those measures.



MD-T acknowledges the technical measures remain the ones to especially consider where the law of the third country is capable of impinging on the contractual guarantee of the essential equivalent level of protection against access by the foreign authorities. However, we believe this is a missed opportunity to EDPB not to have further offer practical advice on the approach to adopt when relying on such measures. To be truly effective, we consider the measures should be sector-specific and especially, adapted to the risks at stake.

Further, MD-T deems the approach that both exporter and importer should be involved in the implementation of the safeguards is fair. However, **MD-T suggests** EDPB to consider a right balance between their respective responsibilities, especially regarding the conflict of interests we may face to in practice. Indeed, while the importers are subject to third country's legislations, sometimes deemed as problematic, they concurrently want to be the most competitive on the market.

As a result, putting too much responsibility on the importer's side could lead to partial and 'opportunist' decisions from the importer which may impact the effectiveness of safeguards in place. On the other side, it could also lead to unwanted reactions from foreign authorities to counteract measures put in place by importers. For instance, if importers, established in a third country, would decide to store all they encryption keys in trusted party established in the EU only, foreign authorities could see this in a bad light.

Then, to avoid such conflict, MD-T suggests EDPB to proceed in two distinct phases when implementing the safeguards – the first one would be carried out by the importer, the second one by the exporter.

- **Phase 1: importer's liability**. First, we deem the obligations up to the importer could be clarified by introducing a strong transparency measure. This measure could take the form of a "*whitepaper*" provided by the importer itself. It should be made available publicly through its website for instance and kept up to date. In this whitepaper, the importer would indicate:
- \checkmark The applicable third country's laws that might be of interest for the exporter.
- \checkmark The assessment of the 'generic' risks at place regarding such laws.
- ✓ The technical and organizational measures implemented by the importer to address such risks.



This on-line disclaimer would help the exporter to better understand the risks implied by a transfer of personal data in the specific third country. It will constitute the first step for legal certainty.

- Phase 2: exporter's liability. Secondly, it would be up to the exporter to review such information with regards the specific transfer at stake and, where appropriate, adopt the safeguards that seem the most appropriate for the case considered. So, the measures would be implemented by the exporter who, unlike the importer, has no other interest than to protect the personal data.

Further, when we think of certification as a tool for transfers we can try to find out ways of implementing supplementary measures through an approach which could be offering a "grading" to the type of transfer (low, medium, or high risk), making it so that after having the exporter assessment done, the later could choose their data importer according to the level of risk or it can only offer a limited range of services, in correlation with the risk level of the transfer.



WHAT IS THE RELEVANCE AND INCENTIVE TO RELY ON CERTIFICATION INSTEAD OF OTHER TRANSFER TOOLS AS STANDARDS CONTRACTUAL CLAUSES? (3)

The essence of the certification as a tool for transfers consists in demonstrating existence of appropriate safeguards as per Article 42 (2) GDPR. Then, the transfer of personal data will be carried out to the certified importer, as trusted party.

Although the certification offers a new alternative to frame the transfers of personal data, it covers the same scope than the SCCs - namely the transfers to importer non subject to GDPR. Knowing that SCCs are the most used tool for transfers (even though they are quite challenged so far), MD-T believes that the Guidelines are a missing opportunity that could have been used to fill the current gaps by framing the transfers not already covered by SCCs.

In view of the foregoing, since the importer already subject to GDPR seem to be excluded from the transfer tools under Article 46 GDPR, **MD-T suggests** EDPB to provide a clear statement about what is expected to implement in case of such transfers. It would be welcomed to get some clarifications on which concrete tool are we supposed to rely on to frame a transfer to an importer already subject to GDPR (other appropriate safeguards / derogation / nothing at all?).

Finally, MD-T deems that reversing the trends by completely rethinking the scope of the certification could be the solution to address the gaps pointed out by the SCCs while creating incentives and relevance for the certification as a transfer tools. That way, the certification would cover transfers to importer already subject to GDPR which are not already covered by other tools as SCCs and at the same time, could imply less obligations (e.g., a light TIA²) since the transfer is carried to a trusted importer which is already GDPR-compliant. Hence, it will incentivize the use of the certification as a valuable tool thanks to the competitive advantage for companies by having less burden obligations while getting more legal certitude when they invest in GDPR's compliance.

² A TIA could be lighted in terms of laws. Because rights will be already enforced through the GDPR's compliance of the importer, the gaps related to the third country's laws will no longer be relevant. Hence, the TIA should only focus on the foreign surveillance laws while not analyzing the foreign data protection laws.



Conclusion

MD-T calls to EDPB to provide pragmatic solutions to the issues and uncertainties occurring in the context of international data transfers to especially address:

- The blurriness which remains around the role of importer
- The lack of practical advice and guidance on the adoption of measures
- The lack of incentive and relevance of the certification as a transfer tool

Those clarifications would benefit all sectors combined but also would support the companies specialised in clinical trials which must handle, as integral part of their activities, the transfer of personal data at the international level.

MD-T is committed to share its expertise in the field and we remain at your disposal should you require further information or clarifications.