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

January, 31. 2022

Comments on 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 adopted on 18th of November 2021 EDPB

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 ("MD-T") welcomes the important clarifications brought by the Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers ("Guidelines"). In particular, the clarifications referring to the notion of data transfer and the application of Chapter V to data importers subject to GDPR.

However, MD-T believes that Guidelines missed the opportunity to clarify several aspects of the subject and provide additional means to achieve compliance with GDPR. Moreover, the examples described, although very interesting, appear oversimplified compared to real-life scenarios and do not help to understand how to comply in the absence of long-awaited tools (such as SCCs for transfer to the entities

under GDPR scope as per art 3.2) while EDPB itself points to this gap (to quote section 23, they "currently are only available in theory").

MD-T would like to emphasise that due to the absence of a practical and pragmatic approach to data transfers, the compliance with Chapter V of GDPR remains still the biggest bottleneck of the GDPR implementation. This is particularly true for a crucial sector, such as the clinical sector, where the exchange of personal data at the international level does not only constitutes the core business of the industry (whether drug or device or other), but is necessary and essential to guarantee the physical integrity of clinical study participants (for instance in the scope of pharmacovigilance) and is largely imposed by the international guidelines (such as ICH-GCP) and implemented in the law (including EU law and laws of EU member states). This is specifically relevant today, considering the challenges and needs brought by the current Covid-19 pandemic that require a joint international effort and a rapid response from the international scientific community. Indeed, incertitude related to the compliance and sometimes the pure impossibility to fully comply with the data transfers rules may limit the international data flows not only jeopardizing the research activities and the business continuity but endangering human lives.

More specifically, MD-T would like to emphasize to EDPB:

- ⇨ The urgent need to clearly allow the use of new SCCs in case of transfers to an entity under the scope of GDPR as per article 3.2, until the additional "lighter" set is available;
- ⇨ Clinical sector: the urgent need for EDPB and the Data Protection Authorities in all member states to take a clear position on the national templates (patient information and/or site contracts) that clinical trial sponsors frequently find not sufficiently compliant while not allowed to be modified in practice;
- ⇨ The need to provide more practical examples in relation to the measures to be described within intra-group agreements (i.e. is the reference to the solid GDPR compliance programme / list of procedures applicable enough?);
- ⇨ The need to further illustrate and clarify the notion of direct data flow (collection of data from individuals not qualifying as 'transfer');

⇨ The need to urgently address the inconsistencies in the approaches between the EDPB and the European Commission and to provide a clear consensus to the stakeholders.

We further develop this point of view and present more detailed comments further in this document.

Introduction and general considerations

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

- Recital (4) GDPR: "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality";
- 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 organisations, while ensuring a high level of the protection of personal data";
- EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, including the six-step methodology proposed by the EDPB;
- EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR adopted on the 7th of July 2020, with regard to intra-group data disclosures.

Specific comments

Example 1. Addressing the remaining gaps in the direct collection's approach

As per the example 1, data are disclosed directly and on the own initiative of the data subject to the recipient, such disclosure does not constitute a transfer under Chapter V since the data subject is neither a controller nor a processor.

This example is very helpful. However, it leaves some pending questions and points to the lack of clarity of the notion of the direct collection (versus indirect collection) and the difference between the direct collection and direct dissemination.

To understand properly when there is a direct data flow from individuals not qualifying as a 'transfer', MD-T considers there is a need to provide further explanations regarding the rationale behind this different treatment and the limits of this approach.

MD-T proposes clarifying and further illustrating the scope of this approach through different scenarios:

- Scenario I: direct collection without transfer. The data subject discloses its personal data by filling personally a form or by sending an e-mail. This form or e-mail is firstly conveyed by a Processor (i.e., cloud service provider or a message management web application provider…) prior to be received by the Controller. The processor does not structure or analyse the data but only transports and/or provide a support to the data.

  MyData-Trust suggests considering that in this scenario, there is indeed no transfer, but a disclosure of the data from a data subject to the data controller. MD-T also suggests to clarify that the above remains applicable where the dissemination is supported by a vendor that qualifies as an intermediary service provider in the sense of the article 12 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), and that the mere involvement of such a vendor does not create an instance of transfer.

- Scenario II: direct collection with transfer. The data subject provides, at the first place, its personal data to a call centre subcontracted by the data controller.

Such a vendor does not qualify as an intermediary service provider, as per article 12 (1)(c), as it selects or modify the information contained in the transmission before transferring it to the Controller (for instance by analysing, structuring, pseudonymising the data etc..).

MyData-Trust suggests considering that scenario as a 'direct' collection with transfer. Pursuant to Article 13 GDPR, the data subject is directly involved into the collection of its personal data to the processor. However, by contrast to the scenario I, such scenario includes an 'indirect input' where the processor has firstly structured and filtered the data before transmitting it to the Controller. This indirect input implies a transfer of personal data to the Controller which must be framed as per Chapter V.

- Scenario III: indirect collection (with or without transfer outside EU).

  In our experience, the notion of direct/indirect collections are frequently confused with the notion of real-time versus differed collection. For example, where data subject consents to a blood test and provides the blood sample. This sample may be collected by the hospital and provided to the laboratory (vendor/processor) for analysis on behalf and for the purposes defined by the clinical trial sponsor. Personal data "extracted" from the sample were not, as such, provided by the data subject (while the sample and few data elements collected about it, such as that sample was taken at fast, are collected directly). In such case, the data subject does not really provide its personal data but its blood. The data subject is only aware of the sources from which its personal data are collected (from the blood) and, without appropriate information, would not even know the categories of data that will be generated through the analysis.

  MyData-Trust suggests considering that scenario as an 'indirect' collection to provide the most protective option for the data subjects.

MD-T deems useful to provide a definition or, at least, the elements to consider when assessing whether there is a direct collection or not. According to MD-T, those elements should be related to the awareness and the control of the data subject over its own personal data but also depending on the role that each processor exercises over the data. As a matter of fact, where collection is an

indirect collection, where flow crosses the EU limits, there will always be a transfer.

Those clarifications are even more relevant since, without them, the considerations of the example 1 could apply to the provision of sample scenario. This could lead to situations where companies will be tempted to rethink their flows to face fewer GDPR compliance issues while offering fewer rights and protection to the data subjects.

Example 3. Clarifying the notion and modalities of onward and backward transfers

Example 3 illustrates a situation where the EU processor sends data back to a non-EU controller. This example confirms the interpretation of GDPR which imposes on any EU entity (controller, processor or other) to fully apply GDPR and specifically its chapter V to any personal data, including data from non-EU data subjects, received from non-EU out of GDPR scope entities.

First, this example only confirms that the re-transmission back must be regarded as transfer but does not provide clarification on practical aspects of other consequences. For example, using SCC, the importer will be abided to grant the same data subjects rights (which data subjects may not have had otherwise, including in case where data controller would hire a non-EU processor).

Moreover, it may not be even possible in practice to grant some of these rights. Indeed, many regions do not have any data protection authority to complain to. Are EU data protection authorities ready to receive questions and complaints from non-EU data subjects? What about the language barrier?

MDT suggests EDPB to provide clear guidance on how data subjects' rights shall be guaranteed in this case and who's responsibility, accountability and liability is involved (processor versus controller).

Moreover, the example provided does not reflect the richness of this type of flows in practice and does not clearly explain the impact. In the scope of complex data flows terms of "onwards" and "backwards" transfers are frequently used. In the example 3 EDPB uses a new term: "retransmission back".

MDT thus concludes that the terms "onwards" and "backwards" are to be used for portions of flows outside the EU (not crossing the EU borders). However, there is no clear concise guidance on the extent to which chapter V applies to the data flow once data are out of the EU.

MD-T suggests the following two sub-examples to clarify when (i) an onward flow and/or (ii) a backward flow shall be considered as a data transfer subject to Chapter V GDPR and the modalities of performance of the Transfer Impact Assessment (TIA):

(i) Onward flow

Considering (A), the data controller outside EEA not subject to GDPR for its processing. Data (sent to and received back from the EU processor B) are sent subsequently by (A) to processor (C) outside EEA, then to Controller (E) outside EEA but not subject to GDPR under Article 3(2), then to Controller (F) outside EEA not subject to GDPR under Article 3(2).

MD-T suggests clarifying where the chain of data flow shall not be considered as a data transfer anymore, specifically by stating that there is a transfer between (A) and (D) because it is an onward transfer of (B) to (A); but there is no transfer between (E) and (F) since (E) is not subject to the GDPR for the new purpose of the processing. The chain is re-analyzed by the intervention of a new data controller.

(ii) Backward flow

In the first sub(example), Controller (A) is still outside EEA but is subject to the GDPR via Art. 3(2) – having received data from data subjects located in EEA via a processor (0) established in EEA ("Flow 0")- and processor (B) is now outside EEA and subject to GDPR via Art. 3(2) when processing data received by (A). Controller (A) is sending data to (B) ("Flow 1") and then (B) is sending data back to (A) ("Flow 2").
In this example, Controller (A) is Sponsor of a clinical Study, Processor (0) is a European Hospital, (B) is a vendor performing analysis on health data for Sponsor.

MD-T suggests clarifying that in a situation of backward flow (meaning where personal data are flowing back to its original sender) the applicability of Chapter V and the modalities of the transfer impact assessment are based on **additional risks** of (Flow 2) with regards to precedents flows. Such additional risks may be inherent to the addition/production/inference of personal data/data subjects or the fact to send data to a recipient subject to new local laws.

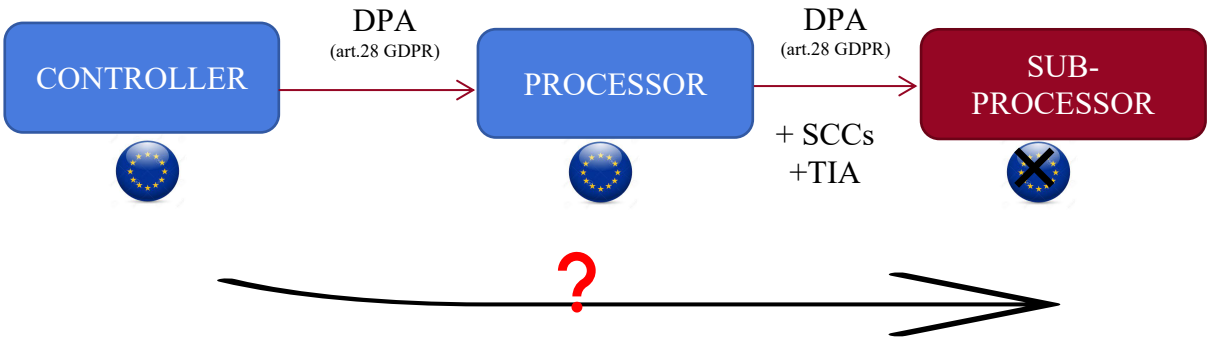
Hence, it is usual in a flow chain, that several parties outside EEA will exchange data between each other (via email, analysis, reports…). Data flows are rarely purely linear. It would mean that as soon as the Parties are not in EEA and that flows are subject to Chapter V GDPR, a double transfer mechanism shall be needed (for both direction).

In our example, if (B) is inferring new data, for instance genetic data, there is a need to have a data transfer mechanism and a TIA in place for "Flow 2" evaluating the additional risks of flow 2 with regards to flow 1, while it may not be necessary to have data transfer mechanism (and TIA) if (B) is a purely hosting company. As a reminder, "Flow 1" is covered from a Chapter V perspective.

Also, the insurance that processor (0) has already performed a TIA for Controller (A) in the context of flow (0) is an element that could be taken into consideration by (B) since (A) is already analyzed as a data importer by the sender making the first data transfer outside EEA. As the data controller, (A) shall receive data from a multitude of processors in and outside EEA that shall need to perform a TIA. This raises the question of the **interoperability** of TIA. This is even more relevant when Sponsor is working with dozens of EEA hospitals, with a lot of "Flow 0" in parallel to be analyzed with no additional risks.

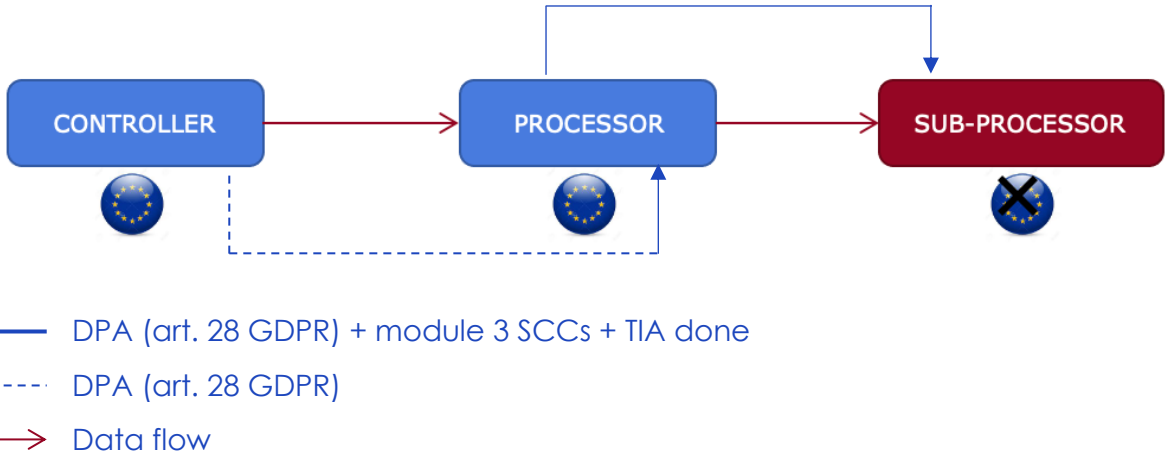
In the example 3 of EDPB, data are sent to (A) in a country and to a type of entity already holding the data (so to local laws) to which data subjects were already subject and this shall not be taken as an additional risk in the TIA.

Example 4. Clarifying the limits and the scope of a direct transfer between an EU controller and a sub-processor located out of the EU



As per the example 4, when data comes from Processor established in the EU and are transferred to a sub-processor established in a third country, Chapter V of the GDPR applies because it is a transfer of personal data to a third country or to an international organization. However, the question arises as to disclosures of personal data involving two different (separate) parties – each of which is a controller, a joint controller, or a processor.

MD-T suggests clarifying the meaning and scope (including limitations) of this approach by allowing a Controller, located in EEA, to be able to directly transfer data to Sub-processor based on the safeguards provided in a chain of contracts: contract between controller and processor and contract between the Processor and the Sub-processor. The analysis of this case highlights that there is a controller/processor relationship within the EEA. Transfers are freely allowed. Then, the Processor shall use Module 3 with its Sub-processor.



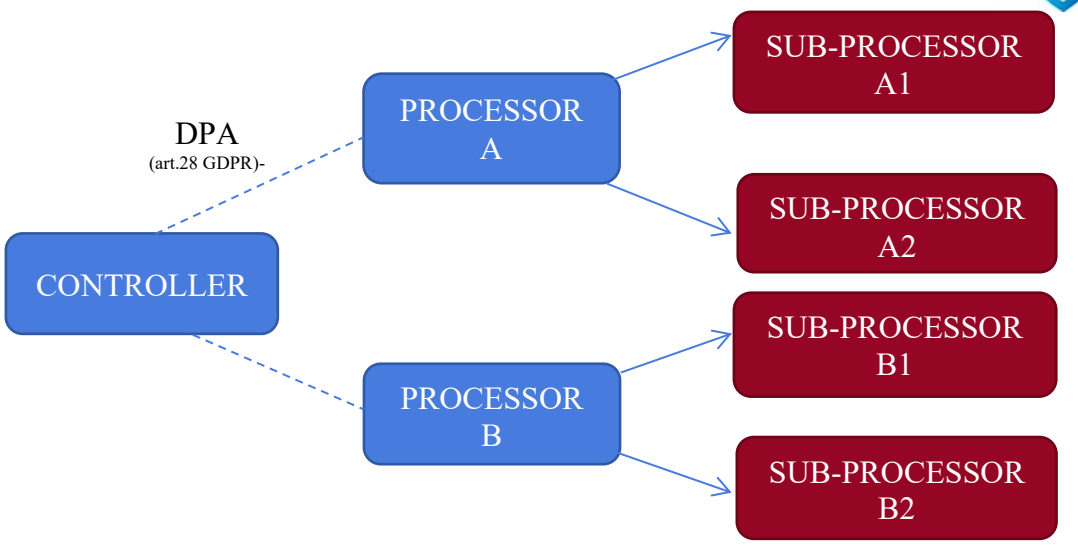
In this chain of contracts three elements will ensure data subject protection and compliance with GDPR:

1. A **Data Protection Agreement** (DPA) in the contract between the controller and the processor, which beyond the requirements of the articles 28 and 32, strengthens the measures by including Articles 9, 14 and 15 of the GDPR, to take into account the Schrems II ruling;
2. The **Module 3** (P2P) **of SCCs** between the European processor and the non-EAA sub-processor. We refer to the module 2 of SCCs to make use of clauses 8.8 and 9, they will allow the Controller to safely transfer the data to the Sub-processor; the requirements for the onward transfer are fulfilled by the transfer. We refer to this SCCs module to account for sub-processing contracts, where the transfer of data outside of the EU is not made by the controller itself, but by a first processor who wishes to use another processor;
3. The realization of a **Transfer Impact Assessment** (TIA), following the need highlighted by the EDPB to carry out a TIA in order to assess the Article 46 transfer tool in light of the legal framework and practical application of the law in the destination country.

These three elements allow a transfer between the processor and sub-processor. To allow a direct transfer between the controller and the sub-processor, **MD-T suggests that the controller co-signs as exporter the same contract signed between the processor and the sub-processor**.

Transfers between the controller and the sub-processor are possible when the scope is limited to a specific project defined in the contract between the processor and the sub-processor.

For law firms, the chain of contracts will be sufficient for GDPR accountability. They will not feel the need to clarify the situation, other companies will instead favor the physical flow.



DPA (art. 28 GDPR) + module 3 SCCs + TIA done

DPA (art. 28 GDPR)

A concrete example is the situation presented above. With one controller, two processors and four sub-processors, to allow data transfer, we would have to set up 10 contracts, as opposed to 6 contracts if we did not have to set up any between the controller and the 4 sub-processors.

This solution avoids the debate about the discrepancies between the contractual flow and the physical flow. However, this scenario is only possible when the sub-processor is hired specifically for the activities of that processor. In this way, the sub-processor will not require the controller to set up an additional direct contact with the sub-processor

Example 6. A missing opportunity to clarify how to frame intra-group disclosures.

As recalled by section 16 of the EDPB's Guidelines, legal entities belonging to the same corporate group may qualify as separate controllers or processors, and intra-group data disclosures may indeed constitute an international transfer of personal data.

This notion is not new. It was already stated by section 4 (75) of the Guidelines 07/2020 on the concepts of controller and processor in the GDPR adopted on 02 September 2020 by the EDPB ("Within a group of companies, one company can be a processor to another company acting as controller, as both companies are separate entities").

MD-T deems very useful to have recalled this concept further and confirmed a coherent approach to the matter.

However, compared to the above-mentioned Guidelines 07/2020 which provided clear and concrete examples to clarify and qualify the role of the different legal entities belonging to the same corporate group (for instance, under section 69 and 87), the example nr. 6 proposed by the EDPB's Guidelines doesn't provide the same degree of clarity.

Although MD-T deems that it is a very interesting example as it describes a standard data transfers scenario, occurring often in the practise, between a subsidiary located in the EU (controller) and its parent company (processor) located in a third country, it addresses only the surface of the challenges brought by such a complex scenario. Indeed, the EDPB does not clarify what measures should be implemented by a corporate group to have in place a solid GDPR compliance programme to frame intra-group disclosures and what the best practises are. In particular, it could have been a great opportunity to recommend:

a) Which transfer tools could be used to protect the personal data; and

b) What kind of organizational and security measures are expected to be implemented to protect the data transferred among several jurisdictions, some of which may not guarantee the same level of protection established by the European Union.

Regarding section a), MD-T believes that this a missing opportunity as the Guidelines do not offer any practical advice on the approach to be taken to frame intra-group data disclosures, and on which transfer tool rely among those listed under article 46 GDPR, namely with regard to Binding Corporate Rules ("BCRs") and SCCs.

Although due to their binding nature, BCRs can be used as a fundamental mechanism to document the accountability of organizations, also with regard to data transfers, MD-T believes that it is difficult for this tool to find widespread use for the following reasons:

- BCRs are complex to design and implement within an organization, especially for small and medium-sized enterprises (SMEs);

- BCRs require great efforts and resources that are usually the exclusive prerogative of large corporations.

Therefore, **MD-T suggests the use of SCCs as the primary tool for intra-group disclosures** and believes, once again, that the Guidelines are a missing opportunity that could have been used to clarify what would be the best approach to take among the use of a light or a full version of the SCCs.

Moreover, due to the peculiar nature of intra-group disclosures, MD-T believes that the **adoption of a new tailored tool** for this specific scenario (such as, SCCs for intra-group disclosures) would be very welcomed.

Regarding section b), in intra-group data transfers the biggest source of risk of malicious or accidental disclosure of personal data resides with the group's employees. Therefore, **MD-T suggests that group-level organisational measures are implemented which reduce the risk**. Such measures could include:

- Group-level risk analysis of all data transfers executed within the context of a common risk framework;
- Group-level data protection policies which explicitly instruct employees on the risks of data transfers between entities and the measures needed to mitigate those risks;
- Group-level procedures for encryption with the recommended use of Public Key Infrastructures (asymmetric encryption) where key management costs are an important factor;
- Group-level policies regarding the use of cloud computing providers, in particular when those CSP solutions are used to execute the transfers;
- Group-level policies requiring awareness training on the risks and measures to be implemented needed when there are data transfers between entities;

- Common standards for human resource evaluation and discipline which encompass data protection and intra-company data transfers.

Regarding potential technical measures that could be used, the Guidelines do not recommend solutions that would assist groups who face the need for intra-group transfers.

What are the potential solutions?

As according to the fundamental principles of Privacy by Design and by Default established by article 25 GDPR, any action an organization undertakes that involves processing personal data must be done with data protection and privacy in mind, **MD-T deems that:**

1) **EDPB should recommend organizations to adopt a high-level internal policy** describing all the measures implemented in a transversal way across the company group to frame intra-group data disclosures (for instance, referring to measures such as encryption or ISO certifications). This approach would be particularly appreciated in the clinical sector where a large amount of sensitive data is processed on a daily basis and it would demonstrate not only a high degree of awareness and maturity regarding privacy and data protection issues, but it would also constitute a very effective way to demonstrate GDPR compliance and increase an organization's reputation in the marketplace. This approach would also facilitate the interaction with third parties, as rather than listing all the specific measures used to protect the personal data in a contract (which may require constant time-consuming contractual changes to keep the measures up to date), an organization could directly refer to its company policy;

2) organizations should also ensure that, by default, privacy is built into the internal system and procedures and appropriate measures are implemented to secure and protect the data. To meet this legal requirement, an organization must determine whether the chosen measures are proportionate to the risks arising from the processing activities, especially when the object of the processing

refers to sensitive data, such as health data. This aspect is particularly crucial for SMEs and fast-growing companies (such as start-ups) operating in the clinical trial sector that usually need guidance in the implementation of a solid GDPR compliance programme. Therefore, **MD-T suggests EDPB to provide organizations with an initial toolkit** to clarify which the minimum requirements are to ensure not only the safety of information systems from breaches, but also to protect individuals from the implications of these events. MD-T believes that the guidelines provided by the French Data Protection Authority - CNIL - may be an excellent reference to develop such a toolkit aimed to reassure SMEs on the security measures to be implemented and to keep spreading the culture of privacy and data protection within the European Union and globally.

Example 7. While an additional "lighter" set of SCCs is under consideration, additional uncertainties arise.

As per EDPB's Guidelines, when the importer is subject to the GDPR in respect of the given processing, Chapter V applies. The example 7 illustrates such situation where a transfer is carried out from an exporter subject to Art. 3 (1) GDPR to an importer subject to Art. 3 (2) GDPR.

In such case, EDPB considers that a 'lighter' set of SCCs should be implemented to avoid duplicating the GDPR obligations in order to address only the missing elements with regards to the risks related to conflicting local laws (e.g., government access, redress mechanisms…). The Guidelines create new complexity for organizations by creating a need for a "customized" transfer tool and the European Commission already committed to the development of a new set of SCCs for transfers to importers subject to Article 3 (2) GDPR.

Although the Guidelines clarified the controversial scope of the new SCCs released last June, it still does not address certain concerns that we describe hereunder.

a) The scope of use of the "full" set of SCCs

Since Chapter V applies regardless whether or not the importer is subject to GDPR in respect of the given processing activity, it is still unclear if the 'full' sets

of SCCs can be implemented even though out of its scope – when both parties are subject to GDPR (Recital 7 of the Implementing Decision).
Considering the Implementing Decision, the "full" sets of SCCs are not supposed to be used out of scope, and the "**lighter" version of SCCs appears therefore the best tool to use**.

b) What transfer tool to adopt in the meantime?

Considering that the "lighter" version of SCCs is "currently only available in theory" (to quote section 23 of the Guidelines) and EDPB does not provide further recommendations regarding what to do in the meantime, **MD-T suggests organizations to use the full version of SCCs while waiting the release of the new set**. However, while an additional "lighter" set of SCCs is considered, during this transitional period additional uncertainties arise:

(1) organizations could implement another transfer tool, such as the derogations established by article 49 GDPR. The derogations would be considered as a temporary solution in line with the exceptionality of their use and would be replaced afterwards once the new set of SCCs is adopted. Considering that we have already experienced the invalidation of international transfers agreements (such as the Privacy Shield) and we have witnessed the changes brought by the decision issued by the Court of Justice of the European Union in the context of the Schrems II ruling, and as we might envisage the invalidation of new transfer tools in the future, the derogations could be the best temporary available solution;

(2) Section 23 of the Guidelines clarifies that for « a transfer of personal data to a controller in a third country less protection/safeguards are needed if such controller is already subject to the GDPR for the given processing ». This implies that a controller has already implemented the necessary technical and organizational measures and operates in a GDPR environment. Therefore, based on this assumption and as alternative approach, we could deem that the measures implemented by an organization already operating in a GDPR environment are sufficient to frame international data transfers in compliance with GDPR for a transitory period until the new "lighter" version of the SCCs will be eventually adopted;

(3) Finally, as established by the recital 4 of GDPR, "the right to the protection of personal data is not an absolute right but it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality". This provision is aligned with articles 8 of European Convention on Human Rights and the article 52 of the Charter of fundamental rights of the European Union ("Charter") which state the conditions allowing the limitations to the right to the protection of personal data developed by the case law of the European Court of Human Rights and the Court of Justice of the European Union. Under both frameworks, any interference to this right is permitted and assessed based on a balancing test between the rights at stake. Hence, while waiting for the release of the new set of SCCs, organizations could take a pragmatic approach performing such a balancing test and documenting the non-compliance to Chapter V GDPR to prevent the risk of suspension or termination of the data transfers. Such an approach is particularly crucial for the clinical sector where other fundamental rights usually come into play (such as the right of freedom of research and right of access to health and to benefit from medical treatment, as established respectively by articles 13 and 35 of the Charter) and a balancing test between the clinical trial requirements and rights of data subjects is often needed. Moreover, as already mentioned, the exchange of personal data at the international level is essential to protect the physical integrity of clinical study participants. This is specifically relevant today considering the challenges and needs brought by the current Covid-19 pandemic. Indeed, the incertitude related to the compliance and sometimes the pure impossibility to fully comply with the data transfers rules may limit the international data flows not only jeopardizing the research activities and the business continuity but endangering human lives.

c) What are the appropriate safeguards available to the exporter while considering the difficulties that arise in practice, especially in the clinical sector?

As regards to the technical measures, it appears that the encryption may not fit with the transfer scenarios since the data are required "in clear" (at least the

data in use). Moreover, the efficiency of pseudonymization has been recently challenged by the CNIL and specifically its fourth criteria in the scope of capacity of authorities to use other sources to re-identify.

As regards to the clinical sector, additional challenges must be considered in the light of the appropriate safeguards. While the SCCs (light version) are considered as the tool to implement in the example 7, most of the clinical sites do not agree to sign these clauses but push for the derogation of consent (Art. 49 (1)(a) GDPR). Lastly, in some EU countries, the use of national clinical trials templates may constitute an obstacle to ensure compliance with GDPR as they are imposed by national Sites and the negotiation of the data protection language is often rejected (e.g., French Site due to the "Convention Unique").

Therefore, given the many questions that currently remain unanswered, **MD-T suggests EDPB to issue a dedicated opinion** to allow the use of SCCs including for organizations under the scope of GDPR as per article 3(2) until the light set of SCCs is released.

Conclusion

MD-T calls to EDPB to urgently provide pragmatic solutions to the issues and uncertainties occurring in the context of international data transfers, especially regarding a crucial sector, such as the clinical sector, where the exchange of big data at the international level is an integral part of the activities of the industry and taking into consideration the challenges brought by the current Covid-19 pandemic.

Despite the fact that the clinical trial sector is expecting to benefit this year from two codes of conduct, one for processors and another for controllers, the clarifications above would benefit other research and life science domains.

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