



PrivacyRules is the global alliance of data protection and cybersecurity experts

Feedback to The European Data Protection Board Guidelines 5/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR

(as accessible at https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en, last reviewed on 31 January 2022)

Contributing PrivacyRules members



Pearl Cohen Zedek Latzer Baratz



RP Legal & Tax

T I M E L E X



Headquarters:

PrivacyRules Ltd.
151 West 4th Street
Suite 200

Cincinnati, OH 45202, USA

Website: www.privacyrules.com

Email: info@privacyrules.com

Copyright © PrivacyRules - All rights reserved 2016-2020

Background

About PrivacyRules

PrivacyRules was formed in 2017 by a group of legal and tech experts across Europe and America (<https://www.privacyrules.com/>) to address the growing demand for data protection and cybersecurity services. Launched in 2018, PrivacyRules is the world's only leading professional alliance of data privacy experts from the legal and tech disciplines. We formed this alliance to provide *integrated and effective assistance and services* to multinational companies and institutions.

In our early age of only two years we have grown dramatically, now with members in almost 60 jurisdictions worldwide and a number of tech and cybersecurity companies within the alliance or cooperating with us. With our members we offer unique services combining legal and technical advice to avail multinational clients of implementable, holistic data privacy solutions in all continents.

In addition to organising webinars, podcasts, in person conferences and e-conferences, PrivacyRules disseminates independent information on data privacy matters via all its platforms. In this way, our alliance contributes to the global awareness about privacy and is an active contributor to the international dialogue on data protection and cybersecurity. PrivacyRules regularly meets institutional interlocutors, at national and international level.

To find out more about us, please visit our [website](#) or [LinkedIn](#).

About this document

PrivacyRules recognises the fundamental role of the European Data Protection Board (hereinafter as EDPB) for the consistent application of data protection rules throughout the European Union (hereinafter as EU), for the cooperation between the EU's Data Protection Authorities, and for its relevance at international level since the EU data privacy interpretation and application has impact at global level.

Further to the EDPB European [Data Protection Board Guidelines 5/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR](#) (hereafter "*the Guidelines*"), our members are therefore pleased to provide the below feedback structured on the following high-level issues:

1. Brief description of the high-level issue of the Guidelines or Use Cases being commented on
2. Comment/feedback to the high-level issue



Headquarters:

PrivacyRules Ltd.
151 West 4th Street
Suite 200

Cincinnati, OH 45202, USA

Website: www.privacyrules.com

Email: info@privacyrules.com

Copyright © PrivacyRules - All rights reserved 2016-2020

3. Proposed mitigation/solution/change to the issue

We are therefore pleased to submit this feedback with the aim of bringing to the EDPB's attention, for its consideration, not only observations on the Recommendations from EU legal practitioners, but also the ones issued by data privacy legal and technical experts from outside the EU.

This brief introduction of the given feedback has been developed by Janvier Parewyck under the supervision of Geert Somers, Chair of the PrivacyRules European Committee and Partner at [Timelex](#), a niche law firm matching law and innovation.

Executive Summary

The main concerns from the PrivacyRules members can be summarized as follows:

1. Fear of too broad applicability of Chapter V rules

It is a fact that the notion of "data transfer" has consistently been interpreted broadly by the Article 29 Working Party / the EDPB, as well as the CJEU, in order to maintain a high level of protection. The interpretation of the notion and the applicability of Chapter V GDPR should however not go beyond the legislator's intention to provide such a level.

The aim of Chapter V is to prevent a decrease in the level of protection granted as a result of the transfer of data outside the EU. However, when a data set originates from a third country, is processed by a European processor, and immediately sent back to their controller, the level of protection does not change since the data already comes from a third country.

This lack of appropriate interpretation for this type of processing unnecessarily complicates or prevents normal business operations in everyday life, and runs counter to an objective of the GDPR that is corollary to that of personal data protection: international trade and cooperation (Recital 101).

2. Fear of a (temporary) lack of available transfer tools for data exporters

The distinction between exporters already subject and not subject to the GDPR should not create unnecessary uncertainty as to the validity of the use of the current SCCs. Until the Commission adopts new SCCs for transfers to importers already subject to the GDPR, the guidelines should confirm, for the avoidance of doubt, that the use of current SCCs remains valid. This should be the case even once the new SCCs become available.



Headquarters:

PrivacyRules Ltd.
151 West 4th Street
Suite 200

Cincinnati, OH 45202, USA

Website: www.privacyrules.com

Email: info@privacyrules.com

Copyright © PrivacyRules - All rights reserved 2016-2020

3. Limited guidance on the requirements to consider a given transfer as *related* to a processing activity subject to the extraterritorial scope of the GDPR

According to the wording of Article 3(2), a processing activity “related” to the provision of goods or services to data subjects in the Union or the monitoring of their behavior is subject to the GDPR. It is however not clear to what extent the data transfer activity (such as, in the issue at hand, a data transfer) must be linked to those activities in order to fall under Article 3(2).

In an IT landscape where multiple intermediaries from all over the world are involved for a single end purpose, and where technological tools are used for multiple aspects related to the final delivery of the service or monitoring, it becomes difficult to know what should be considered as *related* to an activity covered by the extraterritorial scope of the GDPR. It is crucial, however, that exporters can assess with a satisfactory level of certainty not only the quality of their business partners for a given activity but also whether processing activities involving a transfer of data are sufficiently *related* to fall under Article 3(2). Without further clarification, exporters will have to try to find an answer to these questions at their own risk, which causes an undesirable economic disincentive not intended by the EU legislator in the GDPR.

4. Limited guidance in non-transfer situations where data is sent to a third country

The guidelines specifically address the case where data is transferred to a third country but does not constitute a transfer under Chapter V GDPR, recalling that such processing requires enhanced protection under Article 32 GDPR. To reach precise and exhaustive guidelines, clarifications would be welcome as to the type of measures to be adopted.

5. The long awaited definition of data transfers could be refined and made more useful.

These guidelines could be an opportunity to exclude from the notion of data transfer obvious cases where the EDPB has already declared that they are allowed under Chapter V because they offer high or even absolute guarantees, such as in a 'zero-knowledge' context. This would provide legal certainty and allow data sharing that is manifestly safe and consistent with the case law of the Court not to divert resources that might otherwise be allocated to transfers that require particular or innovative additional protections.



Headquarters:

PrivacyRules Ltd.
151 West 4th Street
Suite 200

Cincinnati, OH 45202, USA

Website: www.privacyrules.com

Email: info@privacyrules.com

Copyright © PrivacyRules - All rights reserved 2016-2020

PrivacyRules members' comments on the EDPB Guidelines 05/2021

- [EDPB Guidelines 5/2021](#) (on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR)

PrivacyRules member expert comment	Description of the high-level issue of the Recommendations or Use Cases being commented on	Comment/Feedback to the high-level issue	Proposed mitigation/solution/change to the issue
<p>TIMELEX</p> <p>Belgian legal expert</p>	<p>1. Transfers to importers subject to the GDPR under Article 3(2) should not be more difficult than transfers to importers that are not. The guidelines may be understood as preventing data exporters from relying on the existing SCCs 2021/914 when transferring data to a third party <i>subject</i> to the GDPR under Article 3(2), paradoxically making data transfers to importers subject to the GDPR more complicated than with those which are not.</p>	<p>According to the Guidelines, the sharing of personal data from a controller/processor to an organisation established in a third country falling under the extraterritorial scope of the GDPR (Article 3(2)) qualifies as a data transfer, and is therefore subject to Chapter V GDPR. The Guidelines however state that "safeguards need to be customized depending on the situation" and distinguish between the legal mechanisms and safeguards that can be used when the importer is <i>not subject</i> to the GDPR on the one hand, and when the importer <i>is subject</i> to the GDPR under Article 3(2) on the other.</p>	<p>Clearly state in the Guidelines that while new, less stringent, SCCs may be issued in the future and relied upon to transfer data to importers subject to the GDPR, the current SCCs may also be used for transfers to importers subject to the GDPR.</p>



Headquarters:
 PrivacyRules Ltd.
 151 West 4th Street
 Suite 200
 Cincinnati, OH 45202, USA
 Website: www.privacyrules.com
 Email: info@privacyrules.com

In this regard, the Guidelines acknowledge that in order to achieve an adequate level of protection in the latter situation, “less protection/safeguards are needed” than when the importer *is not subject* to the GDPR. The rationale behind this statement is in all likelihood that importers *subject* to the GDPR are already expected to comply with the GDPR and are prone to enforcement actions, thus reducing the safeguards required to “fill the gaps” and achieve an adequate level of protection.

The SCCs 2021/914 currently in force state, in their Article 1, that they are intended for use in a context where the importer is *not subject* to the GDPR. Concurrently, at the time of writing there are no SCCs available for situations where the data importer *is subject* to the GDPR. To avoid an unnecessary vacuum, the Guidelines should not be understood as preventing an exporter from using SCCs 2021/914 if the importer *is subject* to the GDPR. Since, according to the Guidelines' rationale, data transfers to importers *subject* to the GDPR require fewer safeguards, exporters should all the more benefit from the possibility of using the SCCs 2021/914, which in principle offer more guarantees than would hypothetical



Headquarters:

PrivacyRules Ltd.
151 West 4th Street
Suite 200

Cincinnati, OH 45202, USA

Website: www.privacyrules.com


Email: info@privacyrules.com

Copyright © PrivacyRules - All rights reserved 2016-2020

		SCCs specific to importers <i>subject</i> to the GDPR.	
	<p>2. An exporter of data should be able to assess whether the importer is already subject to the GDPR with regard to a given processing activity.</p>	<p>It is clear from the very wording of Article 2 and 3 of the GDPR, as well as from the consistent interpretation, both in previous guidelines (see e.g. Guidelines 3/2018 p. 14), and in the rulings of the Court of Justice (such as the Fashion ID case), that the rules of the GDPR may apply differently to each of the separate processing activities carried out by one and the same controller / processor.</p> <p>For a processing activity to fall within the scope of Article 3(2), it must itself <i>relate</i> to (i) the provision of goods or services to data subjects in the Union or (ii) the monitoring of their behaviour. An activity outside such a purpose falls outside Article 3(2). It is not clear from the guidelines when an activity can be "linked" to such a purpose. Should a controller who is subject to the GDPR because it provides services or monitors individuals be considered an "importer subject to the GDPR" when a company established in the EU transfers to it data which is not directly, but indirectly, used to provide the service or monitor behaviour, e.g. HR data?</p> <p>In other words, what is the "linkage" requirement between one of the two Article 3(2) activities pursued by the</p>	<p>Clarify in the guidelines what the linkage requirements are between the data transfer and the main processing activity already subject to the GDPR, and give concrete and more specific examples.</p>




Headquarters:
 PrivacyRules Ltd.
 151 West 4th Street
 Suite 200
 Cincinnati, OH 45202, USA
 Website: www.privacyrules.com
 Email: info@privacyrules.com

		<p>importer in a third country on the one hand, and the processing activity of transferring data to that same importer on the other? Without clearer guidelines on this issue, there will be a lack of legal certainty for exporters who will not know whether the importer should be considered as subject to the GDPR or not.</p> <p>This seems to revive the question, not really elucidated in the previous 3/2018 guidelines, of what kind of processing activity can be considered as sufficiently <i>related</i> to one of the purposes of Article 3(2).</p>	
 <p>RP Legal & Tax</p> <p>Italian legal expert</p>	<p>The Guidelines provide a use case describing an employee of a company, based in the EU, who travels to a third country on a business trip (use case no. 5). However, the Guidelines do not provide an analytical description of the extensive security measures needed to conduct the processing operations by such employee in the third country.</p>	<p>In the use case no. 5, the Guidelines state that we are not in a “transfer” situation, since the employee is an integral part of the controller, and thus the figure of the importer is absent.</p> <p>However, even if there is not a “transfer” situation, the Guidelines correctly require the controller/processor to implement extensive security measures in accordance with Article 32 GDPR. In this regard, the Guidelines, as the only example, recommend the controller/processor to prevent its employees from bringing their laptops to certain third countries.</p>	<p>Considering the increase of companies that have their employees working from non-European countries, the Guidelines may describe in more detail the extensive security measures needed to conduct the processing operations by employees in a third country, although there is no a “transfer” situation.</p>



Headquarters:
 PrivacyRules Ltd.
 151 West 4th Street
 Suite 200
 Cincinnati, OH 45202, USA
 Website: www.privacyrules.com
 Email: info@privacyrules.com

		<p>Although we agree with the approach of the Guidelines, we also believe that a deeper description of these extensive security measures is necessary in order to help the controllers/processors. Nowadays, in fact, it is increasingly common for companies to have their employees located in different countries, even for a long period of time, who need to access to the IT tools of their companies.</p> <p>Before allowing its employees to work remotely from a third country, the controller/processor should carry out an assessment of the level of data protection guaranteed by the third country and the relevant risks that may occur, taking into account for example the period of stay of the employee in that country, the amount and nature of data processed by the employee and the security measure already implemented by the company. Moreover, the controller/processor should provide for more detailed instructions for those employees who work from a third country (i.e. extensive instructions on how to use IT tools and process personal data).</p>	
 <small>Pearl Cohen Zedek Latzer Baratz</small>	<p>An EU-established processor should not be bound by Chapter V when it carries out processing on behalf of a non-EU</p>	<p>Consider Company A established in a third-country where Company A is also not subject to the GDPR under Article 3(2). A French Company B is processing personal data on behalf of Company A.</p>	<p>Clearly state in the Guidelines that in order to avoid a strictly technical, rather than substantive, interpretation of the transfer rules,</p>



Headquarters:
 PrivacyRules Ltd.
 151 West 4th Street
 Suite 200
 Cincinnati, OH 45202, USA
 Website: www.privacyrules.com
 Email: info@privacyrules.com

<p>Israeli legal expert</p>	<p>controller or processor not subject to the GDPR as per Article 3(2).</p> <p>The guidelines may be understood as restricting an EU-processor from performing a return-transfer of data back to a non-EU-established entity not subject to the GDPR.</p>	<p>Company A first transfers its non-GDPR covered data to company B for processing. This first leg of the data flow is rightfully not considered a 'transfer' according to the proposed guidelines because Company A is not subject to the GDPR.</p> <p>Company B, the French processor, processes the data for Company A and then re-transmits the processed data back to Company A. This return flow is considered a 'transfer' according to the proposed guidelines, because Company B is subject to the GDPR. Thus, Company B is restricted under Chapter V from sending the data back to the rightful controller.</p> <p>This leads to an absurd result whereby Company A is not able to seamlessly receive its data back, despite the GDPR's express intention not to restrict Company A's activities on account that the GDPR does not apply to Company A. The only way for Company A to receive its data back is to be coerced to become partially subject to the GDPR <i>de facto</i>, through Chapter V, the SCCs and supplementary data transfer measures. This is in contravention of the GDPR's intention of not having the GDPR apply to Company A, and is a <i>de facto</i> unintentional and undesired expansion</p>	<p>the roundtrip flow of data in which the first one-way segment is not deemed a 'transfer' subject to Chapter V, will in whole not be deemed a 'transfer' subject to Chapter V (or, at the very least and consistent with the instructions for MODULE FOUR of the SSCs, that this flow in whole is not deemed a 'transfer' subject to Chapter V where the EU processor <u>does not combine the personal data received from the third-country controller with personal data collected by the EU processor</u>).</p>
------------------------------------	--	--	--



Headquarters:

PrivacyRules Ltd.
151 West 4th Street
Suite 200

Cincinnati, OH 45202, USA

Website: www.privacyrules.com

Email: info@privacyrules.com

Copyright © PrivacyRules - All rights reserved 2016-2020

		of the GDPR's already broad extraterritorial reach.	
<p>TUCA ZBARCEA / ASOCIATII</p> <p>Romanian legal expert</p>	<p>Second criteria: <i>This controller or processor ("exporter") discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer") should entail supplementary clarifications on potential exemptions which may apply.</i></p>	<p>According to the Guidelines, any transmission or making available of the data to another third country entity/organisation represents a data transfer and is therefore subject to Chapter V GDPR.</p> <p>Consideration should be given however to exceptional cases where the transfer/making available of data per se do not value a transfer in the sense of GDPR and should not entail supplementary safeguards. E.g.: where the data is solely stored in an encrypted format and the key for decryption is held by the exporter only (the data importer having no possibility to decrypt de information) it should be emphasised whether same rules apply or if in such case, no transfer occur; where the data importer only accesses remotely via secured environment the data on exporters' servers/databases with no possibility of copying/exporting the information; where the data importer from a third country only accesses the data in exporters' premises without any data being in fact transferred/accessed from the third country;</p>	<p>Clearly state in the Guidelines the particulars and exemptions from the second criteria for a third country data transfer.</p>



Headquarters:
 PrivacyRules Ltd.
 151 West 4th Street
 Suite 200
 Cincinnati, OH 45202, USA
 Website: www.privacyrules.com
 Email: info@privacyrules.com

On behalf of PrivacyRules, we would like to express appreciation for the EDPB's openness to receiving feedback about its Guidelines from data privacy practitioners. We stand ready to provide additional clarifications regarding our comments if needed.

PrivacyRules and its members contributing to this feedback authorise the publication of the present document and of the content of the feedback provided therein, in full or in part, wishing that the authorship of these comments will be credited.

Coordinated by

Alessandro Di Mattia

Legal & Executive Officer, PrivacyRules Ltd.

E-mail: adimattia@privacyrules.com

Web: www.privacyrules.com



Headquarters:

PrivacyRules Ltd.
151 West 4th Street
Suite 200

Cincinnati, OH 45202, USA

Website: www.privacyrules.com

Email: info@privacyrules.com

Copyright © PrivacyRules - All rights reserved 2016-2020

Contributing PrivacyRules members

Belgium: Timelex attorneys

Geert Somers: geert.somers@timelex.eu

TIMELEX

Italy: RP Legal & Tax attorneys

Chiara Agostini: Chiara.Agostini@relegal.it



RP Legal & Tax

Israel: Pearl Cohen attorneys

Haim Ravia: HRavia@PearlCohen.com

PEARL COHEN

Pearl Cohen Zedek Latzer Baratz

Romania: Tuca Zbarcea Asociatii

Ciprian Timofte: ciprian.timofte@tuca.ro

**TUCA ZBARCEA
ASOCIATII**

END of the comment of the [PrivacyRules](#) feedback to the European Data Protection Board Guidelines 05/2021 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.



Headquarters:

PrivacyRules Ltd.
151 West 4th Street
Suite 200

Cincinnati, OH 45202, USA

Website: www.privacyrules.com

Email: info@privacyrules.com

Copyright © PrivacyRules - All rights reserved 2016-2020