



PrivacyRules is the global alliance of data protection and cybersecurity experts

Feedback to The European Data Protection Board Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

(as accessible at https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en , last reviewed on 21 December 2020)

Contributing PrivacyRules members



RP Legal & Tax



Headquarters:

3491 Forestoak Court
Cincinnati, Ohio 45208, United States of America
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 53 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](#).



Headquarters:

3491 Forestoak Court
Cincinnati, Ohio 45208, United States of America
Website: www.privacyrules.com
Email: info@privacyrules.com

Copyright © PrivacyRules - All rights reserved 2016-2020

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 [Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data](#) (hereafter "*the Recommendations*"), 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 Recommendations or Use Cases being commented on
2. Comment/feedback to the high-level issue
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 drafted by 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 summarised as follows:

1. Fear of data localisation with adverse effects

There is a general fear that organisations will no longer transfer personal data to non-adequate jurisdictions outside the European Economic Area (hereinafter as EEA) just because:

- they don't want to take the risk of not being compliant; or,



- they prefer not going through the difficult and costly task of assessing foreign law and adopting supplementary measures.

If EEA-based organisations stop using service providers in non-adequate jurisdictions outside the EEA due to heavy legal restrictions in the EEA, cross-border economic activity will probably suffer and third countries are likely to impose similar requirements.

2. Need to keep a risk-based approach

The Recommendations should leave organisations with sufficient freedom to assess transfers on a case-by-case basis and adopt measures they deem appropriate based on the risks identified. This is especially important for small and medium enterprises (hereinafter as SMEs) engaged in less risky activities.

Only certain sectors where the risks related to data transfers are more substantial should or could be subject to stricter and hence also more burdensome and costly procedures.

The Recommendations should therefore provide more clarification on their degree of importance for specific sectors, the risks involved for such sectors and the measures to adopt for mitigation of such risks.

To the extent that individual data controllers can be deemed to have a role in the assessment of foreign law systems, they should be given more guidance and tools, such as official questionnaires that they can share with their business partners in non-adequate countries and which are limited to the information that should absolutely be obtained.

3. Need to keep a data-centric approach

The Recommendations could elaborate more on the fact that current data protection technologies such as encryption, are not sufficient to adequately protect data in transit or data stored in third countries, because foreign authorities can request encryption keys or could otherwise access the data.

Essential Guarantees should be reinforced by providing additional *Supplementary Measures* that are data-centric in their protective approach, such as continuous monitoring and full auditable security of the data, in combination with state of the art technology, such as ephemeral encryption keys.



Headquarters:

3491 Forestoak Court
Cincinnati, Ohio 45208, United States of America
Website: www.privacyrules.com
Email: info@privacyrules.com

Copyright © PrivacyRules - All rights reserved 2016-2020

PrivacyRules members' comments on the EDPB Recommendations 01/2020

- [EDPB Recommendations 01/2020](#) (on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data)
- [EDPB Recommendations 02/2020](#) (on the European Essential Guarantees for surveillance measures)

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>[datalex]</p> <p>Swiss legal expert</p>	<p>1. Data localization vs economy. Except under some exceptions, the EDPB recommendations indirectly create a data localization privacy framework within adequate countries.</p>	<p>Data localization seems to be contrary to the EU approach. Many assessments of data transfers occurring with a third country (such as the US or India) will lead to the conclusion that because the recommendations are so burdensome, the easiest way would be to localize the data in EU or stop working with the EU. The consequences of data localization could likely be the following:</p>	<p>Avoid data localization</p>



	<ul style="list-style-type: none"> • The free flow of information in a digital society will impair cross-border economy. • More than ever, US companies and other organisations in third countries may isolate from the EU • Third countries may impose counter measures to regulate in the sense of data localization in their own country. 	
<p>2. Impossible to implement the measures for SMEs. Excessive difficulty for small and mid-size multinationals companies, with a presence in a third country (such as the US) to implement additional safeguards.</p>	<p>The Recommendations are rendering HR data impossible to transfer to the US, even for intra-group data transfers. This means that US-based small to mid-size multinationals managing or accessing HR data from the US will have to cease deciding on salary bonuses, etc. either directly or via third party global vendors providing payroll or HR cloud-based solutions.</p> <p>Imposing such difficult measures to SMEs, in particular for less-risky activities may discourage them to comply with the recommendations.</p>	<p>We suggest to further clarify that the recommendation can apply differently depending on the company size and the nature of its services. Most SMEs will have no resources, skills nor budget to comply with the recommendations.</p>



<p>3. No more privacy risk-based approach. Organizations should have the ability to keep a risk-based approach for data transfers.</p>	<p>One of the successes of the GDPR relates to its risk-based approach. Organizations can conduct a risk assessment in order to evaluate what activity requires less or more privacy and security controls.</p>	<p>We suggest that the Recommendations keep some degree of risk-based approach to data transfers in order to avoid the risk that many industries will not have the ability to conduct this complex legal and privacy assessment per transfer.</p>
<p>4. The Recommendations are industries agnostic. The recommendations should remain sector-specific, and/or emphasize that certain industries may be less impacted by national surveillance activities than others.</p>	<p>The Recommendations do not take into account the reality of certain industries that should not be subject to disproportionate access to personal data of individuals located in the EU. Certain industries, in particular giant tech, banks, social media companies, should be more in the focus of the recommendations than other industries, such as hospitals, hairdressers, or discos.</p>	<p>This comment is related to the reduction or the absence of a risk-based approach.</p> <p>The recommendations should acknowledge or further clarify what industries could be more impacted by the recommendations for assessing the likeliness of certain requests from third countries' governments to access EU personal data. We suggest adding clarification for sector specific organizations and other case studies or examples how less-risky industries could navigate with those guidelines.</p> <p><u>Example 1:</u> A multicentric clinical study, or scientific research conducted on global + EU patients</p>



			<p>is very unlikely to interest foreign third country intelligence services, although the data would qualify as sensitive.</p> <p><u>Example 2:</u> OTT services, social media, banks (money laundering suspicions), bitcoins and other e-currency platforms, could more likely be subject to a request from foreign government to access EU data.</p>
<p> SHAKESPEARE MARTINEAU Legal advice for life and business</p> <p>UK legal expert</p>	<p>No scope under the Recommendations to take a risk-based approach</p>	<p>As is well known, the GDPR is built around broad principles and not prescriptive rules. This ensures it is adaptable, flexible and workable in all kinds of situations, and for businesses of all sizes and in many different sectors. It accordingly allows for implementation by businesses based on proportionality and appropriateness (“appropriate technical and organisational measures”, “appropriate safeguards”, etc.) considering the particular circumstances.</p> <p>The Recommendations appear to take an “all or nothing” approach.</p>	<p>The Recommendations should allow for an element of risk assessment, considering criteria laid down in the Recommendations (for example those set out in paragraph 33), and adding in other factors proposed by EDPB which may help companies whose data is unlikely to be at risk from national legislation to legitimately decide that the full due diligence is unwarranted for particular transfers to particular destinations.</p> <p>Assistance should also be provided so that companies which do need</p>

		<p>All businesses regardless of size, business sector, the type of data involved and so on must carry out the assessment. Furthermore, if national legislation is deemed vague, the exporter is even at this stage not permitted to take account of the reality of the likelihood of the authorities accessing the data (para 42).</p> <p>A risk of taking such a rigid position is that businesses will either decide they have to ignore the legal requirements and not carry out the risk assessment, or they will be forced to localise their data, to the detriment of cross-border commerce.</p>	<p>to carry out due diligence are provided with an approved methodology and, especially in the case of jurisdictions where transfers are likely to be frequent (such as to the US), clear and simple explanations of the risks involved for various types of businesses arising out of the national legislation concerned (FISA 1978, Cloud Act 2018, etc.) and the best way businesses can mitigate those particular risks. This will help minimise the complexity and costs for business in carrying out the due diligence.</p>
 <p>RP Legal & Tax</p> <p>Italian legal expert</p>	<p>The third step of the Recommendations imposes to data controllers to assess if there is anything in the law or practice of the third country to which the data should be transfer that may impinge on the effectiveness of the appropriate safeguards of the transfer itself. For evaluating the elements to be taken into account, the data controller should carefully consider when the legislation of</p>	<p>This step of the Recommendations imposes an excessive level of accountability on data controllers, without considering the dimension of most of the operators that will be required to implement them. For example, in Italy the majority of active businesses are SMEs; it would be extremely difficult and expensive for such small businesses to conduct</p>	<p>1) We suggest that the Recommendations indicate more reasonable ways for data controllers to carry out a privacy assessment on the legislation of third countries; according to this approach the EU institutions could take charge of such due diligence activities, thus avoiding leaving it exclusively to data controllers to conduct it.</p>

	<p>the third country governing the access to data by public authorities is ambiguous or not publicly available. According to this step, the data controller should conduct an assessment with due diligence on the third country legislation and document it thoroughly, as the data controller will be held accountable to the decision it may take on that basis.</p>	<p>a due diligence assessment on the legislation of the country to which they want or have to transfer data. This assessment activity would be even more difficult if the data transfer is to be made to federal states, as it would be necessary to assess both federal and single member state legislation. A significant risk of such approach is that data controllers may stop any extra-EU data transfer, to avoid any critical issue, or that they may refrain from complying with these requirements because they consider them too burdensome, thus exposing the data they process to high risks.</p>	<p>2) Alternatively, the EDPB could draw up an official model questionnaire to be sent by data controllers to their suppliers operating outside the EU, in which should be included all the information that, according to the Recommendations, needs to be obtained in order to assess the level of security of the third country's legislation. This would avoid the need for data controllers to examine the entire privacy legislation of a non-EU country in order to independently assess its compliance with the Recommendations.</p>
<p>PEARL COHEN <small>Pearl Cohen Zedek Latzer Baratz</small></p> <p>Israeli legal expert</p>	<p>A Case by Case objective evaluation of the law in the third country.</p>	<p>This requirement shifts the burden from the EU institutions to each organization that transfers data from the EU, amounting to a privatized "mini adequacy" decision.</p> <p>It is not realistic to expect this feat from small and medium-sized organizations. Even large</p>	<p>A subjective or a risk based approach (taking into account the nature of the data, the relevant industry, the specific receiver of data and the likelihood of access by authorities) is more realistic.</p>

		<p>organizations will struggle with this requirement when they transfer data from the EU on a regular basis. It cannot be reconciled with the fast pace of present business reality.</p> <p>Since this requirement applies only to countries that were not recognized as “adequate” by the EU Commission, in most cases an objective evaluation will raise issues that impinge on the effectiveness of the SCC.</p> <p>Moreover, the updated SCC draft published by the EU Commission specifically refers to a subjective evaluation.</p>	
	<p>Most of the proposed supplementary measures are not effective where the issue is the authorities’ access to personal data.</p>	<p>The only supplementary measure that can be considered to be effective in such cases is a technological one, namely encryption. Regrettably, this solution is applicable only under specific circumstances, when there is no need to access the data for processing in the third country. In other words, processing personal</p>	



		<p>data in a third country would be subject to a flat ban.</p> <p>There should be another mechanism that will facilitate transfer of data, otherwise, it will be almost impossible to transfer unencrypted data to the U.S. for processing, for example.</p>	
 <p>US tech expert</p>	<p>Data Transfer Technology Current data protection technologies such as encryption, encryption control systems, including key and certificate management are no longer sufficient to protect, adequately, personal data of EU persons while the data are in transit.</p>	<p>Essential Guarantees recommendations provide legal frameworks governing access to personal data by public authorities in a third country. These Guarantees are strengthened when examining the underlying data loss protection technologies for their adherence to the underlying purposes of the Guarantees.</p> <p>Current data loss protection vulnerabilities are well characterized. Third country nation state actors are increasingly gaining sufficient skill and tradecraft to access cryptographic secrets such as</p>	<p>Reinforce the Essential Guarantees by providing for additional Supplementary Measures that are data centric protection in nature. State of the art data centric security technologies exist today.</p> <p>Add compensating data security controls based on the following core data protection principles:</p> <ol style="list-style-type: none"> 1. All data exporters and importers must provide for full and continuous monitoring of personal data to and from any third country or cloud service,

encryption keys, certificates and other identity, authorization and access management tools. The EDPB is aware of these threats to the sanctity of personal data in cross border transfers and while data transit or are processed in third countries.

Techniques employed by third country nation state actors include but are not limited to:

1. Availability of stored and static encryption keys upon request by third country authorities.
2. Compromise of data loss protection tools such as;
 - a. Attacks against key management systems.
 - b. Acquisition of stored or static encryption keys.
 - c. Phishing campaigns to acquire trusted and validated security credentials including

location of the data centre or service notwithstanding.

2. All data exporters and importers must provide for fully **auditable security** of personal data to and from any third country or cloud service, location of the data centre or service notwithstanding.
3. All data exporters and importers must provide for **immediate threat detection** (without the need to decrypt the data in transit for inspection) of personal data to and from any third country or cloud service, location of the data centre or service notwithstanding.
4. Use a data encryption or data loss protection technology that provides only warrant and judicial remedy access for data-in-transit to and from a third country. This prevents unauthorized and



Headquarters:

3491 Forestoak Court
Cincinnati, Ohio 45208, United States of America
Website: www.privacyrules.com
Email: info@privacyrules.com

		<p>but not limited to login ID's, passwords and MFA information.</p> <ol style="list-style-type: none"> 3. Capture or scanning of personal data-in-transit by a third country without the data exporter's or data importer's knowledge. 4. Capture or scanning of personal data transiting a third country without the data exporter's or data importer's knowledge. 5. Leveraging the inability of data exporters and importers to have meaningful custodial knowledge of the full lifecycle of personal data transit to and from third countries. 	<p>unwarranted access by a third country.</p> <ol style="list-style-type: none"> 5. Use a data encryption or data loss protection technology that provides only warrant and judicial remedy access for data transiting a third country. This prevents unauthorized and unwarranted access by a third country. 6. Use data loss protection solutions that employ ephemeral encryption key technology where the key only exists in the location and for the length of time to achieve the purpose of encrypting personal data. 7. Use data loss protection that employs the equivalent of a "digital one time pad."
<p>TIMELEX Belgian legal expert</p>	<p>User case 7: Scenario with a data exporter making personal data available to entities in a third country to be used for shared business purposes. Stating that there are no ways to add effective security measures in such a broad and general manner may</p>	<p>This is a very common scenario for international companies. The data that they exchange is relatively of low sensitivity (e.g. basic work data for workforce management, basic client contact data etc.). Moreover,</p>	<p>We suggest that these examples are more nuanced and industry specific, rather than generic, as it is now.</p>



have a real and damaging effect for their business as they may need to stop the transfers which are vital for their ongoing projects	the GDPR recognizes the need to exchange such data within a group of companies (although in the context of legitimate interest – recital 48). Such data is typically of no interest to the surveillance agencies or is even beyond what these agencies may be able to access.	
--	---	--

On behalf of PrivacyRules, I would like to express appreciation for the EDPB's openness to receive feedback about its Recommendations 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.

Sincerely,

Andrea Chmieliński Bigazzi

CEO, PrivacyRules Ltd.

E-mail: ceo@privacyrules.com

Web: www.privacyrules.com



Headquarters:

3491 Forestoak Court
Cincinnati, Ohio 45208, United States of America
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

Israel: Pearl Cohen attorneys

Haim Ravia: HRavia@PearlCohen.com

PEARL COHEN

Pearl Cohen Zedek Latzer Baratz

Italy: RP Legal & Tax attorneys

Chiara Agostini:
Chiara.Agostini@replegal.it

Agostini:



RP Legal & Tax

Switzerland: datalex attorneys

Gabriel Avigdor:
gabriel.avigdor@datalex.ch

Avigdor:

[datalex]

United Kingdom: Shakespearen Martineau Kim Walker: kim.walker@shma.co.uk
attorneys

SHAKESPEAREMARTINEAU
Legal advice for life and business

United States of America: KnectIQ cybersecurity company Kenneth Morris: kmorris@knectiq.com



END of the comment of the [PrivacyRules](#) feedback to The European Data Protection Board Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.



Headquarters:
3491 Forestoak Court
Cincinnati, Ohio 45208, United States of America
Website: www.privacyrules.com
Email: info@privacyrules.com
Copyright © PrivacyRules - All rights reserved 2016-2020