# Position Paper

## EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

21.12.2020



### Introduction and Overview

The European Data Protection Board ("EDPB") has released draft recommendations on supplementary measures for data transfer mechanisms and corresponding European Essential Guarantees (together, the "Recommendations"). The Recommendations provide suggested steps for companies transferring personal data outside of the European Economic Area ("EEA") to ensure that these transfers are afforded a level of protection that is essentially equivalent to what is provided in the EEA.

The Recommendations are in response to the Court of Justice of the European Union's ("CJEU") Schrems II decision, which invalidated the Privacy Shield as a valid data transfer mechanism in July 2020. In contrast, Schrems II upheld the validity of the standard contractual clauses, however, this is subject to the implementation of "supplementary measures" (where necessary) to ensure that transferring parties are in compliance with their respective obligations under European privacy law, particularly with respect to access requests from public authorities. The Recommendations are long-awaited and seek to define and clarify what those "supplementary measures" should be in light of these transfers.

Bitkom welcomes the opportunity to provide feedback regarding the European Data Protection Board's "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data". Clear, proportionate and stable rules for the international transfer of personal data are vital for EU-headquartered companies exporting goods and services.

In our view, the following general aspect need special attention: The EDPB should more expressly communicate the GDPR risk based model in the recommendations document, including considering specific subjective factors e.g. numbers of requests received. The expectation for these recommendations was that a 'toolbox' of measures would be provided to organisations impacted by Schrems II. However, Annex 2 to the draft document provides use cases but does not contain a clear and accessible list of legal, tech-

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

**Rebekka Weiß, LL.M.**
**Head of Trust & Security**
P +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

nical or organisational supplementary measures for organisations to consider. A table with exemplary measures or something similar to provide orientation would therefore be appreciated. The responsibilities in these recommendations are beyond what should be required of organisations. The exporter is made responsible for making complicated legal analysis (that takes the European Commission years to undertake in the form of adequacy decisions). Taking into account the time, costs and resources this will consume, this will be prohibitive for most companies, particularly SMEs.

The recommendations should be aligned with the new draft SCCs from the Commission. In particular it should be confirmed whether the terms of those new SCCs are sufficient to meet the requirement of additional legal supplementary measures that should be considered by an exporter so that only technical and organisational supplementary measures may be required in certain cases.

If not amended, we see some relevant risks to the development of the market and the global data economy:

The guidance in its current form does not reduce the legal risk for businesses that rely on non-European service providers to operate their business as the majority of these services will fall under the use cases 6 and 7 for which the EDPB could not identify effective supplementary measures. Likewise, European firms with operations in the US and elsewhere will find it difficult to maintain their global operations based on the recommendations for the same reasons.

For example, they will not be able to transfer HR data outside of the EU. Start-ups or SMEs that rely on widely used internet-based services to maintain or grow their business will struggle or fail to replace their existing service providers with appropriate alternatives because these services are in many cases the global standard in their respective categories. Small or fast growing services based in a third country might even have to stop offering their service in Europe because they cannot afford to essentially duplicate their infrastructure in the EU. The guidance therefore risks cementing current market imbalances. For consumers, the recommendations will probably result in less choice because new services and services that are free or only have small margins will not be able to operate in the EU. Many popular apps for example are built on a global cloud infrastructure and require data transfers for the provision of their service.

As Bitkom has always worked with its members and the Data Protection Authorities to further a common understanding, help implement the GDPR requirements and issued practical guidance, we have developed a concept to secure international data transfers in

the light of the Schrems II decision, which we would like to put up for discussion. You can find the current draft state of the concept in Annex 1 (Part B) to this Position Paper.

## A. Bitkom Position regarding EDPB Recommendations 01/2020

### 1. Key Aspects

#### 1.1. Securing Data Flows as Cornerstone of the Economy

Whether engaged into B2C or B2B business model, most of European companies undertake commercial activities around the world and rely on a worldwide footprint of affiliates and suppliers to this purpose. Common tools are deployed for various purposes: HR, marketing, communication, production etc. Significant data flows are generated in this context within this footprint.

The draft EDPB Guidance would require on top of transfers mapping, the businesses to assess the surveillance laws of the country in which they export the data against certain European Essential Standards as published by the EDPB in order to determine whether additional technical means are required. Very strict technical protection would be required for countries not meeting these standards.

This raises a number of very critical issues:

- The country assessment can't be reasonably expected from the businesses due to the nature of the work (high profile legal assessment of the importing country laws); on this ground, even the EU Commission has been sanctioned by the Court of Justice through the Privacy Shield invalidation.

- The volume of work that the Guidance would generate in term of mapping details, country assessment and technical protection implementation seems to be quite burdensome. All these combined would generate heavy legal and technical workloads generating huge costs for all companies and might overburden mid or small companies, which form the bulk of many supply chains.

- The systematic implementation of technical measures in countries not meeting the European Essential Guarantees will make the transfer not legally feasible where the data need to be available in the clear for the data importer. Under Use cases 6 and 7 the data shall remain encrypted and not be available in the clear. Most of intra-group transfers in the above countries would then be impacted while access in clear is needed for global company business continuity.

Finally, it seems that these requirements would apply whatever the data/processing sensitivity. Use cases 6 and 7 are indeed totally irrespective of the data sensitivity. The above requirements would then apply to names, e-mail addresses, which by nature are required just to be able to communicate. This is exchanging personal data at all which would be made almost impossible.

Finally due the above reasons, the Guidance as drafted would be a very serious obstacle for the management and the development of the European businesses around the world.

### 1.2. Balancing of rights

We invite the EDPB to expressly recognize that the right to data protection is not absolute, but that other fundamental rights, such as the freedom to conduct a business, as enshrined in Article 16 of the Charter of Fundamental Rights of the European Union, must also be taken into consideration when determining the exact scope of legal obligations in the context of international data transfers. The Recommendations should be updated to reflect this more clearly, and the consequences of this important principle should be clarified for data exporters and data importers.

Recital 4 of the GDPR recognizes that the right to data protection is not an absolute right and that it must be balanced against other fundamental rights, in accordance with the principle of proportionality.

"(4) 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. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

This principle has also been recognized in the case law of the Court of Justice of the European Union ("CJEU"), including in the "Schrems II" (Grand Chamber) judgment:

[172] "However, the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society (see, to that effect, judgments of 9 November 2010, Volker und Markus Schecke and Eifert, C-92/09 and C-93/09, EU:C:2010:662, paragraph 48 and the case-law cited, and of 17 October 2013,

Schwarz, C-291/12, EU:C:2013:670, paragraph 33 and the case-law cited; and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 136)."

Even more recently, the CJEU (Grand Chamber) has stated:

[49] "None of those three fundamental rights constitutes an unfettered prerogative, as each of them must be considered in relation to its function in society (see, regarding the right to an effective remedy, judgment of 18 March 2010, Alassini and Others, C-317/08 to C-320/08, EU:C:2010:146, paragraph 63 and the case-law cited, and, concerning the rights to respect for private life and the protection of personal data, judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 172 and the case-law cited)."

[50] "Thus, in a situation where several rights guaranteed by the Charter are involved in a given case and are liable to be at odds with each other, the necessary reconciliation of those rights, in order to ensure that a fair balance is struck between the protection attached to each of them, may lead to limitations being imposed on them (see, to that effect, judgments of 29 January 2008, Promusicae, C-275/06, EU:C:2008:54, paragraphs 63 to 65, and of 27 March 2014, UPC Telekabel Wien, C-314/12, EU:C:2014:192, paragraph 46)."

### 1.3. Individual circumstances of the transmission to be considered

We suggest confirming more clearly that all obligations of the GDPR, including the obligations regarding international transfers of personal data, must be interpreted in accordance with the principle of proportionality, and that this includes the recognition of the individual circumstances and whether such circumstances are likely to entail a threat to the rights and freedoms of the data subjects as introduced by Article 24(1) GDPR which confirms such concept to be applicable to all obligations in the GDPR including Art. 44 – 46 GDPR:

"Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

The approach laid out in the Recommendations stands in contrast to an approach based on proportionality that forms the basis of the GDPR and data protection laws globally. A risk assessment was critical to the Schrems II judgment and forms part of the newly-

released and updated standard contractual clauses. Schrems II requires a "case-by-case" analysis – as opposed to a "country-by-country" analysis – of the essential equivalence of third country laws. The key terms are "appropriate safeguards" or "adequate additional measures", and any appropriateness or adequacy requires an individual assessment of all relevant elements. The assessment of the likelihood of government access can be based on objective factors like the frequency of access requests in previous years. These are observable, objective metrics that should not be considered a 'subjective' factor to take into account.

A number of the proposed measures in the Recommendations go far beyond what is proportionate to implement in response to the perceived threat of government access to data. We suggest that the Recommendations be amended to return to the proportionate approach that is typical of data protection law when determining which supplementary measures to implement in the light of disproportionate threats to the rights and freedoms of the data subject.

### 1.4. Definition and Scope of "Transfer"

We invite the EDPB to reconsider its Use Case 6 and to differentiate between a transfer of personal data where the data is ultimately stored outside the EU/EEA, and a transfer which consists of only granting a third party access to data stored in the EU.

In our view, these two situations differ substantially both from a technical and from a legal perspective. The Recommendations should reflect these differences, and respect that the legal framework for these two types of transfers in the GDPR is different.

Access to data stored in the EU can be granted in many forms, and most of these do not have a risk profile that would be remotely similar to the situation discussed in the CJEU's Schrems II decision. We respectfully submit that applying the Schrems II considerations to all forms of "transfer" is inappropriate, not proportionate and not required by the Charter of Fundamental Rights of the EU.

The Recommendations should clarify that merely granting access to data stored in the EU should be subject to a much "lighter" set of restrictions than other forms of transfers.

We ask the EDPB to clarify the relationship between Article 3 GDPR and Chapter V of the GDPR: Certain recipients of personal data outside the EU may be subject to the GDPR because of Article 3 GDPR. There are currently still uncertainties whether additional safeguards in the meaning of Article 46(1) GDPR are required when personal data is transferred to these kinds of recipients.

In this context, we would like to mention that the response to this question of very significant practical relevance for internal data transfers of EU/EEA-based controllers to e.g. branch offices and affiliates outside the EU/EEA.

We invite the EDPB to clarify that data transfers to a recipient in the EU are out of scope of the Recommendations, even if such recipient in the EU may have a parent company outside of the EU.

We respectfully submit that this situation is different from the scope of the Recommendations. Possible conflicts in situations where the parent company may request that the EU-based recipient makes available certain personal data to the non-EU parent should be examined in a different guidance document.

### 1.5. Country Assessment

Assessing whether local surveillance requirements or powers are limited to what is necessary and proportionate in a democratic society, is an extremely difficult appreciation/assessment, despite the European Essential Guarantees for Surveillance Measures, 10 November 2020 published by the EDPB. Especially for SME the task puts them at a disadvantage as it is clearly too extensive. Furthermore divergent results of the assessment are to be feared. In our view, assigning companies with the task contradicts Art. 46 GDPR as the adequacy assessment should be made by the EU Commission, not the controllers. From a controllers point of view an assessment should always be limited to what is strictly necessary to address actual risks that arise from a data transfer/processing for the data subject.

Requiring each business/company to undertake this comprehensive task in respect of its own processing will have adverse consequences:

- the assessment will probably not be done since it will require resources not available in many companies (competences, proper information availability, budget)
- if the assessment is done, it will lead to very inconsistent results across the players for similar countries and processing
- in all cases it will lead to a huge workload and heavy costs considering the numerous countries to cover for most businesses and the need to undertake/update the assessment for each transfer

- it will create obstacles to the competitiveness of the European players.

In addition, a requirement of an across-the-board assessment of the regulatory framework around law enforcement and surveillance may not appropriately address the threats for warranty objectives under the GDPR potentially leading to risks for the data subjects. As much as shortcomings in the legal protection of personal data within a given country (as may be the case) and a resulting overall lower adequacy rating may not have an impact on risks identified for a specific data transfer, the legal and regulatory assessments shall be limited to what is relevant for the protection of the warranty objective in question relevant for the specific data transfer activity.

The absence of clear reference regarding the countries critical in respect of personal data protection will also create a major legal security issue which combined with the possible several interpretation by the data authorities across Europe will not be manageable for businesses.

### 1.6. Specifications on certain services used worldwide

Exhaustive mapping of the international transfers in the context of the cloud providers very evolutive and complex supply chain is not feasible without such providers being addressed and made specifically responsible.

Similarly in this context, maintenance services may require in certain instances access to the data; the full protection of the data not being readable would require the services to be relocated in Europe, triggering a major renegotiation with the providers and requiring their consent. This would require that the cloud providers are legally and directly bound by the same obligations. The SCCs are helpful in this respect but will take time to be effective, and EDPB specific Recommendations would certainly help both the final result and the SCCs to signed/implemented quickly.

### 1.7. Accountability and Data Minimization Principle

Paragraph 3 states that "[c]ontrollers and processors must also be able to demonstrate these efforts to data subjects, the general public and data protection supervisory authorities". However, GDPR does not create any obligations of controllers and processors vis-a-vis the general public when it comes to the demonstration of internal accountability programs.

Paragraph 4 states that the principle of accountability "also applies to data transfers to third countries since they are a form of data processing in themselves". As mentioned

above, the recommendations should specify on which basis it concludes that the accountability principle is relevant in the context of international transfers. E.g., the lawfulness principle is only referring to Art 6 GDPR not to Art. 44 et seq and the other principles are even more removed from international transfers, so the accountability principles as enshrined in Art 5 (2), would have to be applied very loosely to make it relevant for international transfers. Generally, these recommendations apply the accountability principle very loosely, turning it into an amorphous concept, whereas, the language of Art 5 (2) very clearly limits that principle to the controller's compliance with the Art. 5 (1) principles.

Paragraph 8 states that data "you are fully aware of your transfers (know your transfers)". The recommendations need to add guidance on the types of transfers that are out of the scope of this exercise, because they are not attributable to the controller or processor conducting the exercise:

- Transfers to a data importer in a third country that is subject to the GDPR, e.g. by virtue of Art. 3 (2) or Art. 3 (3) should be out of scope, since the GDPR continues to apply at the point of destination of the transfer.

- Transfers that are attributable to the data subject. For example, in many cases, it is the data subjects themselves that initiate the transfer, such as by sending an EMail, publishing a post, sharing a document, traveling to a third country and taking remote access to data stored by their provider in the EEA etc. Those types of transfers are not attributable to the provider of the service and are therefore not in scope of his obligations under Chapter V of the GDPR.

- Transfers attributable to a third party. In many places the Recommendations refer to actions by third parties in third countries by which they gain unauthorised access to personal data, as if these actions would create obligations under Chapter V of the GDPR for the controllers or processors whose date security measures have been breached by those actions of that third party. However, if a breach of security leads to unauthorised access by a third party in a third country, such as in a case of hacking by that third party, any resulting transfers is not attributable to the entity operating the data processing operation that has been hacked. These types of scenarios will not even be "transfers" in many cases. In Footnote 14 of the Recommendations the EPDB makes reference to C-362/14 (Schrems I), paragraph 45 where a transfer is referred to as a "disclosure by transmission, dissemination or otherwise making available". However, controllers or processors storing data in their systems are not “disclosing” data to third parties that gain unauthorised access to such data.

Paragraph 11 refers to the principle of data minimisation and that it must be verified "that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country". As previously mentioned the data minimisation principle is misapplied here. The data minimisation principle puts the amount of data in relation to a processing purpose, but not in relation to every processing activity done for that purpose. If data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, the principle is being met, including for all processing done for that purpose. In conclusion, if a transfer is part of a processing operation undertaken for a specific purpose, there is no separate test under the purpose limitation principle that is focussed on that transfer.

### 1.8. Impact of the Recommendations on BCRs

There is uncertainty around the impact of these Recommendations on Binding Corporate Rules. Binding Corporate Rules ("BCRs") are company-specific, group-wide data protection policies approved by European data protection authorities to facilitate international transfers of EU personal data. BCRs are seen as the "gold standard" of transfer mechanisms because they are based on strict privacy principles and require intensive consultation with and approval by European data protection authorities. In Schrems II, the CJEU did not opine on the requirement to use "supplementary measures" for data transfers on the basis of BCRs. However, in the period since this judgment was handed down, a number of data protection authorities and the EDPB, in a separate FAQ, have suggested that the same requirements may also apply to the BCRs.

In the Recommendations, the EDPB notes that the same reasoning set forth with respect to the standard contractual clauses also applies to BCRs on the basis that they are of a contractual nature, so the guarantees within them cannot bind public authorities and their access rights. The Recommendations continue to say that "[t]he precise impact of the Schrems II judgment on BCRs is still under discussion. The EDPB will provide more details as soon as possible as to whether any additional commitments may need to be included".

It is not clear from the Recommendations which aspects of the Recommendations will be applicable to the BCRs and what new provisions, if any, will be required to be added to the BCRs. As a matter of standard practice, BCRs currently require wording to address government access requests (i.e. as provided in the Article 29 Working Party Group guidance on Processor Binding Corporate Rules).

### 1.9. Technical Measures

Articles 24 and 25 of the GDPR refer to technical and organisational measures taking into account the nature, volume and risks of the data for the data subjects. State of the art and costs are also to be taken in the context of Privacy by Design. The data controller is responsible to apply a protection proportionate to the data at stake (nature, volume, purposes etc.).

Imposing technical measures such as encryption for all transfers to countries not meeting the EEGs goes therefore beyond the terms of the GDPR requirements. This would raise a legal issue. Arguably only a GDPR amendment could come to this result. Despite the fact that the Guidance would not be directly enforceable, it is clear that all GDPR data protection authorities will rely and apply the Guidance in their legal assessment and decisions and that this Guidance would in therefore have in practice a legal effects although indirect.

Imposing technical measures such as encryption in particular for the transfers to countries not meeting the EEGs would also disregard a fundamental principle of data protection and the GDPR: the protection should be proportionate to the risks. This proportionality is expressed in all articles related to the protection of the data: article 23, 24 and 25 of the GDPR. The Guidance can't just ignore this concept. Nature, volume and risk triggered by the data is only considered in the Guidance for the country assessment while taken into account in the EU Commission SCC draft.

Applying technical protection under such strict conditions as defined in the Guidance (Use Case 6 and 7: data not to be available in the clear at all in the importing country) would make a multitude of transfers with no purpose any longer. Why exchanging the data, if the data cannot be read on the other side ? Intra-group transfers are immediately impacted as well as any exchange which would be necessary for business operations. Even intra-group intranet platforms for transnational communication with the employees would be hardly operable. Article 49 cannot obviously offer a reliable alternative channel for communication.

The Guidance and the SCCs draft as issued by the EU Commission do not match, creating a dilemma for the data controllers/processors. The new SCC draft, provides that technical protection shall be "considered ... where it does not prevent fulfilling the purpose of the processing" suggesting that other means are possible and that the availability of the data in the clear may be needed and satisfied. Shall the various businesses apply the Guidance or the SCC approach when considering their transfers?

We would suggest that the EDPB aligns with the EU Commission approach. Contractual and organizational measures alone may not suffice to safeguard data transfers - specific technical measures appear to be prescribed in certain circumstances. The EDPB states that in certain instances, contractual and organizational measures may not be enough to restrict access to personal data by public authorities and that only technical measures can render that access ineffective, particularly in instances of surveillance.

For example, the EDPB repeatedly notes that encryption keys should be held by the data exporter in instances where data is transferred to a country whose laws allow disproportionate access to data by public authorities. This effectively produces a de facto requirement for companies wishing to transfer data to the U.S. or similar jurisdictions with expansive surveillance laws to hold the encryption keys out of jurisdiction.

Requiring specific technical measures goes against the spirit of the GDPR, which is intended to be a "technology neutral" piece of legislation that avoids dictating technical requirements in order to allow companies of all sizes to assess their security requirements in line with the risks. It is designed to be flexible and adaptable to new technologies. In addition, the mandatory implementation of certain technical measures is expensive and may have a substantial operational impact on a company's operations.

As part of its Schrems II ruling, the CJEU only required "adequate additional measures" without limiting these to technical measures or excluding organizational and contractual measures or a combination of all. Since the CJEU dealt with US surveillance laws FISA 702 and E.O. 12333 in the decision, it would have been easy for the CJEU to clarify its view that only a certain category of measures (i.e. technical or organizational) would be adequate. Instead it chose not to opine on such measures. In its Recommendations, the EDPB's interpretation incorrectly narrows the scope of interpretation conferred by the CJEU to the controller when choosing the adequate supplementary measures.

We feel as though many service providers currently meet and should be able to continue to meet the required standard for safeguarding data through a combination of comprehensive contractual and organizational measures with some flexibility as to the technical measures that are put in place.

The Recommendations should therefore propose technical measures that are workable in practice, a non-exhaustive list of technical measures that data exporters can use to supplement the safeguards in the SCCs. Unfortunately, the Recommendations' case studies on the use of these measures reflect an unworkable and unrealistic view of how these measures operate in practice.

For instance, the Recommendations suggest that organisations can rely on encryption as a safeguard in most cases only if the data never appears in an unencrypted form in the third country and if the decryption keys are held only within the EU (or an adequate jurisdiction) (see, e.g., paras 79(6), 89(2-3), 84(11)). They also suggest that encryption almost never provides sufficient protection where data is accessible "in the clear" in the third country, including where an EU organisation uses an online service that may process the data in the third country (paras 88-89), or where employees or others in the third country can access the data on a shared IT system (e.g., human resources data) (paras 90-91).

Moreover, because the Recommendations state that even remote access by an entity in a third country to data stored in the EU constitutes a "transfer" (e.g., footnote 22, para 13), organizations in many cases would need to apply these technical safeguards to EU-stored data as well. This fact underscores the impracticality of the Recommendations and their incompatibility with other important EU interests, such as promoting open global trade and research necessary to protect vital interests (for instance in the context of the COVID-19 pandemic). At a time when policymakers across the world, including in Europe, are pressing companies to provide greater access to encrypted communications in order to help governments more effectively fight terrorism and other threats, the proposed Recommendations would appear to penalize companies for making such access possible.

More pragmatically, the Recommendations' positions on technical measures would render the SCCs virtually worthless as a transfer mechanism. In the vast majority of cases, the reason companies transfer data to third countries is to communicate and share information with people in those countries. If those people cannot access the information—as the Recommendations would require—there is no point to the transfer. Similarly, many online services that EU businesses rely on today must be able to process the information in unencrypted form in order to work properly; given the nature of the Internet and the global economy, this might entail some processing that occurs outside the EU, irrespective of where the data controller or data processor is based. The Recommendations would prohibit EU organizations from engaging in these commonplace and essential business activities.

In reality, most EU organizations would not be able to cease these activities entirely while still remaining economically competitive. Instead, many would likely turn to other legal mechanisms, such as the derogations set out in Article 49 of the GDPR. Because organizations adopting this approach might transfer data to non-adequate jurisdictions without even adopting SCCs (to say nothing of additional safeguards), this outcome would leave EU data subjects worse off, because their data would be subject to fewer protections than they are today. However, the EDPB also noted that such derogations (which would include

data subject consent) must be interpreted restrictively and mainly relate to processing activities that are occasional and non-repetitive.

To avoid these consequences, the EDPB should revise the Recommendations to ensure that the proposed technical measures are workable in practice, and should leave it to data exporters to determine whether any particular measure adequately protects the transferred data. The Recommendations should not prohibit all access to data in the third country; doing so will discourage organizations from adopting technical measures, such as encryption, that in fact provide meaningful safeguards against unauthorized access.

### 1.10. Contractual measures

Although the Recommendations propose a non-exhaustive list of contractual measures that can offer additional safeguards, they also include language suggesting that contractual or organizational measures on their own (i.e., without additional technical measures) cannot provide the level of data protection that EU law requires (para 48). This position appears to be based on the assumption that the mere theoretical possibility of access by third-country authorities—even if the practical risk of such access is vanishingly small—renders a transfer unlawful.

This position adopts an overly restrictive reading of the Schrems II judgement. The Court in Schrems II held that transfers of data to third countries should be prohibited only "in the event of the breach of [the SCCs] or it being impossible to honor them" (para 137). This language, and similar passages elsewhere in the judgement, suggest that, so long as the data importer does not in fact disclose data to third-country authorities (or, if it does make such a disclosure, that it notifies the data exporter accordingly), then the parties may rely on the SCCs (para 139). Under this reading, it is clear that contractual measures alone can provide the additional safeguards needed to safely transfer data to a non-adequate jurisdiction.

To align with the Schrems II judgement, the Recommendations should remove all language suggesting that contractual measures alone are insufficient safeguards to satisfy EU law. The Recommendations should instead articulate several possible contractual measures that EU organizations may consider when transferring data to a non-adequate jurisdiction, then leave it to data exporters and importers to evaluate which measures are appropriate in context and "in the light of all the circumstances of that transfer" (Schrems II, paras 121, 146).

### 1.11. Practical examples and Use Cases

We suggest including additional Use Cases into the Recommendations with clarifications for day-to-day situations that do not involve cloud-type services. This includes clarifications of the scope of applicability of Use Case 7.

From the perspective of EU/EEA-based companies that does business in countries outside of the EU, the current wording of the Recommendations may raise questions whether, in the view of the EDPB, there is a legal basis for e.g. the following activities:

- An employee based in the EU/EEA sending an email with an offer for certain goods to a potential customer outside the EU/EEA
- Informing an employee in a country outside the EU/EEA about the name and telephone number of a superior who is based in the EU/EEA
- Operating a website which contains provider information identifying the name and further information about one or several natural persons, as required by Article 5 of Directive 2000/31, and (if the controller is a natural person) Article 13/14 of the GDPR
- Travel of EU/EEA employees to a country outside the EU/EEA with technical devices or paperwork that contain e.g. names and email addresses of colleagues, and/or preparatory notes with names and email addresses of contacts in the country of destination

We respectfully submit that the legal framework described in the Recommendations, especially Use Case 7 is not an appropriate approach to deal with these kinds of routine everyday transfers, that a one-size-fits-all approach will not work in practice and is not required under GDPR, and that a framework for these kinds of use cases must take into consideration the risk-based approach and the principle of proportionality.

## 2. Comments on specific paragraphs of the Recommendations

### 2.1. Para 3 (page 7)

Under Article 5(2), the controller is responsible for, and must be able to demonstrate compliance (accountability). In these recommendations, the principle of accountability is expanding significantly onto the processor. A28.3 (h) GDPR explicitly requires the processor only to provide the information demonstrating compliance to the controller and to the

auditor engaged by the processor. In this case the sentence: "Controllers and processors must be able to demonstrate these efforts to data subjects, the general public and the data protection supervisory authorities" is adding new obligations on processors and blurring the line between controllers and processors. This is not required under GDPR or the Schrems II ruling.

### 2.2. Para 6 (page 8)

The request that the data exporter, irrespective of being a controller or processor now has to put in place supplementary measures ("in order to find out if you (the data exporter) need to put in place supplementary measures to be able to legally transfer data outside the EEA") unnecessarily overlaps with the obligations of the controller according to Art. 5 f GDPR.

### 2.3. Para 7 (page 8)

The reference made here to Art. 5 (2) and Art. 24 (1) GDPR are responsibilities related to the controller only and confirm that the expansion of accountability beyond the text of GDPR, which should not be the case.

### 2.4. Para 9 (page 8/9)

Art. 13.1. and 14.1. GDPR are explicitly related to the controller and not a processor.

### 2.5. Para 42 (page 14)

*"In the absence of legislation governing the circumstances in which public authorities may access personal data, if you still wish to proceed with the transfer, you should look into other relevant and objective factors, and not rely on subjective factors such as the likelihood of public authorities' access to your data in a manner not in line with EU standards."*

In our view, subjective aspects can also be relevant and important for assessment. Organizations should be able to take into account subjective matters. This is specifically included in the new draft SCCs in the implementing decision (para 20) and the Clauses (Clause 2(b)(i)). The SCCs consider 'practical experience' of requests received by the importer to be relevant.

### 2.6. Para 46 (page 15)

It is not clear how this requirement is different from the existing requirements of Art. 24(1) and Art. 32 of the GDPR.

### 2.7. Para 52

There seems to be a contradiction in this paragraph: The EDPB recommendations are not in line with current European Legislation. The recommendations state that if encryption is prohibited in a country the transfer may not happen but the EU is on its way to loosen the application of encryption (in case of messengers) (see Council of the European Union - Draft Council Declaration on Encryption - Security through encryption and security despite encryption No. 12143/20.).

### 2.8. Para 56/57 (page 17)

The meaning of additional clauses here is unclear. Is the mindset that organisations can add additional clauses to the SCCs unless they change or contradict them? Does this mean organisations could add the additional clauses directly to the SCCs or is it intended that organisations would have a data privacy section in the main contract and then separately add the SCCs? It seems from the new SCCs that they will cover the requirements of Art. 28(3) and (4) GDPR also so it would seem that additional sections should not be necessary.

### 2.9. Para 59 (page 18)

The value of binding corporate rules (which are expensive and difficult to get and maintain) will be diminished significantly where onerous additional commitments are added. BCRs are already at a higher standard to other transfer mechanisms given they are approved by regulators and require significant work to maintain.

### 2.10. Para 69 (page 21)

*"Selecting and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires."* More clarity would be welcome here as to the effectiveness of the suggested supplementary measures. Given the complexity of the recommendations and requirements therein, adding caveats of this nature is unhelpful. The Schrems II case is extremely complex so organisations require more certainty.

2.11. Para 79 (2) (page 22)

In terms of expecting organisations to have insights into the resources and technical capabilities available to public authorities we would like clarifications on how the organisations and businesses should make that kind of determination. What level of research and analysis would be expected to fulfil the requirements?

2.12. Para 79 (3) (page 22)

*"The strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved"*- propose that this statement is more clearly communicated – not clear what this means from a technical perspective.

2.13. Para 79 (4) (page 23)

The term flawlessly' needs explanations and clarifications as this seems to be a higher standard than GDPR requires. The requirement should be in line with the requirements of Article 32 GDPR.

2.14. Para 79 (6) (page 23)

Regarding the phrase *"the keys are retained solely under the control of the data exporter"* we ask the EDPB in which situations organisations could use cloud native encryption solutions. In that scenario keys are retained by the cloud provider and stored on their platform but CSPs do not have access to the keys, they are controlled by the organisation, including control over the algorithm responsible for de-encryption. This should, in our view, be a sufficient technical measure.

2.15. Para 80 (1) (page 23)

Regarding the phrase *"...without the use of additional information"* we ask for clarifications what is considered as "additional information"? We would like to request that this is enhanced with an example.

2.16. Para 80 (3) (page 23)

*"ensured that the data export retains sole control of the algorithm or repository that enables re-identification..."*

The EDPB should also include practical examples such as organisations using cloud native encryption solutions. Keys are retained by the cloud provider and stored on their platform in that scenario. Cloud Service Providers do not have access to the keys, however the organisation controls them – including control over the algorithm responsible for de-encryption.

2.17. Para 83 (page 24)

Paragraph 83 seems to require an impossible task and consideration from the businesses: How shall the exporter be able to identify what data the public authorities may already possess in order to re-identify an individual. The paragraph should therefore be amended.

2.18. Para 84 – Use Case 3 (10) (page 24/25)

Routing through the internet is generally no point-to point communication. In order to sustain desired speeds, Internet Network Providers route the traffic where it is fastest at the moment. Internet traffic can go through many countries. The user generally does not have control over this. All of the data packets contain personal data (IP address of the sender and the receiver, the user and the host). Even where host and user are in one country traffic could be routed through other countries. Either the internet is going to be regulated to allow control over this. Or this chapter would make non-encrypted transfers only possible for individuals that can afford dedicated connections. If this chapter is to be interpreted strictly, it would require the creation of a EU-internet that is separate from the internet that we know. It would also prohibit any email communication that is not encrypted and there is no way to initiate such encrypted communication through internet communication.

2.19. Para 86(5) (page 26)

The standard of security of the algorithm should be in line with the requirements of Article 32 GDPR.

2.20. Use Case 6 (Para 88, page 26)

Regarding the transfer to cloud services providers or other processors which require access to data in the clear, the EDPB states that they are "incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights." And "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." We ask the EDPB to offer advise on other security measures aside from encryption or contractual or organizational measures that may be available in this case. Or if a risk based approach may be taken (for example, where the data is business contact data versus special categories of personal data).

### 2.21. Para 118/119 (page 34)

It should be clarified that the duty to inform the data subject only exists to the extent that access is actually (i.e., not only potentially) targeted at a specific person.

If, for example, access to minimized/pseudonymized data is granted for technical support and this data is then to become the subject of sovereign access, it is in principle possible to re-identify and inform the data subject.

As a result, however, this will often mean an even greater encroachment on the rights of the data subject, because it is only through re-identification (possibly involving other clients in a chain) that the link between the seized minimized data and the data subject is established.

In addition, there are the corresponding efforts that are necessary for re-identification.

Ex: For service purposes, we receive an erroneous X-ray image (data set) from a hospital, the data set is pseudonymized (patient name etc. are removed). However, for error analysis, the dataset needs to be sent to a third country expert for the system. The data set is not anonymous because re-identification is possible via the pixels in the data set and parameters still present, at least with the involvement of the hospital.

If this data set now becomes the subject of a monitoring measure and the data subject is to be informed about this, this would be possible after re-identification, but until this re-identification, at least we did not know who the patient is. As a result, this also increases the risk that the authority can identify the patient.

### 2.22. Use Case 7 (Para 90/91)

It appears this only relates to importers using the data 'for its own purpose' i.e. becoming a separate and independent controller. Can the EDPB please clarify that if the importer is acting on the instruction of the exporter that this is permissible (where technical and organisational supplementary measures are implemented, where needed).

Where the EDPB considers no technical measures are available, can the EDPB consider other security measures aside from encryption or otherwise contractual or organizational measures that may be available in this case? For example, using TLS or a dedicated channel using VPN to access the data where it is stored

Annex 1 Definitions - should provide a definition of "data in the clear". It should also provide a definition of 'public authority' that is limited to law enforcement authorities, which is the focus of the Schrems II case

## 3. Conclusion and Proposal

The Guidance needs to better and more realistically reflect a risk approach orientation regarding determination of the protection additional to the BCRs and SCCs. In the current form, the Guidance appear as not proportionate as it would jeopardize the possibility to exchange personal data at all in certain countries and thus the business continuity. The risk based approach orientation would better align the Guidance recommendations with the spirit and letter of the GDPR and of the EU Court of Justice Schrems 2 judgment. This would also reconcile the Guidance and the new SCCs.

Clearer top down determination of critical countries is also needed since the EEGs alone would create an absence of security and the situation would not be manageable for the European companies.

A specific guidance should be set out with respect of cloud services, where transfer mapping are by definition very difficult to implement.

Finally the Recommendations in their current form would generate a heavy and costly workload resulting from the combination of exhaustive and detailed transfer mapping, countries assessment and the technical protection implementation. This would as a minimum require a grace period of one year.

Seeing the current difficulties that arise from the Recommendations and as Bitkom has always worked with its members and the Data Protection Authorities to further a common understanding, help implement the GDPR requirements and issued practical guidance, we would like to put the following concept (in its current draft version) up for discussion.

## B. Bitkom Concept (Annex 1)

### Assessment for Third Country Data Transfers - taking into account the individual circumstances of the transfers

(Draft version) 21.12.2020

### 1. Introduction

The legal situation brought about by the judgment of the European Court of Justice ("CJEU") of July 16, 2020, Case No. C-311/18 ("Schrems II Judgment") has caused perplexity and uncertainty within the industry on how to deal with international data transfers. The uncertainty relates less to the aspect of the ineffectiveness of the Privacy Shield. Rather, it concerns the more subtle consequences for international data transfers in general. According to the ruling, even in the case of the use of standard contractual clauses within the meaning of Article 46(2)(d) of the GDPR, there are further requirements both for companies[1] and for supervisory authorities[2] on the question of the necessity of supplementary measures for the protection of the rights and freedoms of data subjects in the case of third-country transfers. The CJEU did not make any clear statements on the subsequent questions regarding the triggers for the necessity of additional measures and the nature of the measures themselves, so that this vacuum must be filled by practitioners.

The existing vacuum is unacceptable from Bitkom member companies´ point of view, because it causes legal uncertainty and planning insecurities. Across all industry sectors and internal company processes, certain reliable practices have been established for years in reliance on the existing legal situation (see B.). These practices may be confronted with changes that could have disruptive consequences if the Schrems II ruling is implemented without restrictions.[3]

These concerns, that have been voiced by many stakeholders, associations and companies EU-wide, have not led to an improvement with regard to giving companies legal certainty yet. Neither the European Data Protection Board nor the German supervisory authorities have so far presented any convincing concepts. This applies both to the FAQs issued immediately after the ruling and to the corresponding press releases. For this reason, Bitkom has been addressing this challenge since August 2020 within the framework of a working group and has developed this concept (see C.I.).

The concept also explains the legal basis (see C.II.). These explanations are all the more relevant because the most recent statements by the European Data Protection Board suggest a less flexible interpretation of the legal situation by the supervisory authorities. Accordingly, German data protection supervisory authorities are also cautious or critical of the approach favoured by Bitkom.

[1] See CJEU, Schrems-II decision, para 132.
[2] See CJEU, Schrems-II decision, para 146.
[3] See CJEU, Schrems-II decision, para. 135 sentence 1.

## 2. Current situation

A practice of international data flows has long been established within Bitkom' s member companies. International data transfers are intrinsic to a globalized economy. Companies of all sizes and in all sectors and industries rely on (digital) services that are associated with the international availability of data, especially in the USA. The focus on U.S. companies is neither coincidental nor intended as an end in itself, but unavoidable due to the lack of alternatives. This is because powerful, standardized and established solutions or components for such solutions can only be identified on international markets. These components support or supplement the corporate portfolio of companies within the framework of their own value chains or simply to support internal processes. And after the USA has been a strategic partner of the German and European economy for decades, strategic partnerships have been established in particular with companies based in the USA. It is no coincidence that around half of the data flows in Europe can be traced back to data exchange with the USA.[4]

Going beyond transferring data into third countries such as the US, the integration of editorial content, human expertise, technical components, and procedural value creation is complex and far-reaching:

- *Integration of external content:* Existing processes and resources in companies are being supplemented. Personal data plays a subordinate role and is solely a means to the end of making it available. Corresponding potentially affected personal data hardly goes beyond organization-related data (digital identity within the company, contact data, organizational affiliation, rights granted). Examples: LinkedIn Learning; integration of YouTube or other video players on the company website.
- *Integration of technical components:* If and if only the integration of technical components operated by third parties (abroad) and the potentially associated exposure of personal data makes corporate processes possible in the first place, a higher level of integration has been achieved. This is accompanied by a corresponding loss of direct control. The relevance for the protection of personal data is highly dependent on the business process involved and can be quite distinct. Nevertheless, in these cases, outsourcing is not aimed at working with personal data, but at most at its technical management. Examples: Travel planning and expense reporting applications, data and application hosting, outsourcing of infrastructure and higher layers of the technical enterprise architecture to the cloud (IaaS, PaaS, Saas with all difficulties regarding delimitation of processes*)*.
- (Partial) business process outsourcing: Where processes are outsourced as a whole or partially, overall (legal) responsibility is not externalized, but a corresponding degree of operational responsibility and thus control is. The associated loss of control also includes the handling of personal data at the process level. This is even more true if and because these processes are operationalized on infrastructure that the legally responsible party cannot actually control. The dependency thus established and the possibil-

[4] see *Weiß*, ZD 2020, 485.

ities for influencing personal data and the rights and freedoms of the data subjects suggest the theoretically highest risk and require very far-reaching safeguards. Examples: Outsourcing of customer service, outsourcing of payroll, outsourcing of the travel process, outsourcing of logistics services, outsourcing of IT operations, 24/7 IT support, server maintenance.

- *Data transfer within the group:* All of the above facets can be found within (international) group structures, including those of companies headquartered in Europe, especially in Germany. They depend on international data flows to make internal technical resources available in a globally scalable form, to maintain uniform processes, and to ensure the development, operation, and maintenance of a rational technology landscape. In other words, for international companies with subsidiaries or branches abroad, international data flows are a prerequisite for their very existence. However, risks to personal data can be managed far better via uniform company policies and procedures as well as control and reporting systems than with respect to third parties. Examples: Pooling of IT services, operation of a global active directory, central personnel management, global intranet.

## 3. Concept of an assessment based on the risk of the transfer

### Summary

This concept explains the required test of a data transfer and also describes the content of the components relevant for this test. Bitkom has identified the following steps and components:

- **Examination of the circumstances of the data transfer:** Bitkom considers it necessary to examine the characteristics of the data transfer independently of the third country concerned first. According to these individual circumstances, threats to the relevant protection goals of the GDPR can be derived. Based on the reasoning of the CJEU in the Schrems II ruling, these can be condensed to the objectives of transparency, confidentiality, integrity, availability and intervenability anchored in the standard data protection model[5] ("SDM"). This, in turn, allows risks to be derived that arise from data processing, or more precisely, from a data transfer as such. This is because the transfer of data is accompanied by a reduction of control over personal data. However, the extent of this loss of control and the resulting threats to the rights and freedoms of the data subjects do not arise automatically, but rather depend on the technical characteristics of the data transfer and the data itself. For this reason, the determination and weighting of these individual circumstances is the starting point of every data transfer assessment and is included as an input variable in an overall assessment.

[5] Data Protection Conference of the Independent Federal and State Data Protection Supervisory Authorities, The Standard Data Protection Model, A Method for Data Protection Advice and Auditing Based on Uniform Performance Objectives, version. 2.0 b, April 17, 2020, available at https://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/Standard-Datenschutzmodell.pdf;jsessionid=2BC564F660D1A026686B730CF3F54E50.1_cid344?__blob=publicationFile&v=2 (last accessed Dec. 17, 2020).

- **Examination of the level of data protection in the third country:** After the CJEU in its ruling required companies[6] [...] to examine the level of data protection in the third country, Bitkom has developed a catalogue of criteria that can be traced back to the relevant objectives of the SDM and which two parties cannot address or can only address incompletely within the framework of the contractual design of the transfer relationship. In this context, Bitkom stresses that in the constellation of Art. 46 GDPR, companies cannot - and not even to a certain extent - be expected to conduct the depth of review of an adequacy decision within the meaning of Art. 45 (2) GDPR. First of all, this is the task of the European Commission. Furthermore, this is not necessary because the use of standard contractual clauses is already an instrument which, according to Article 46(2)(d) GDPR, should be sufficient for normative reasons alone to ensure the level of data protection. For that reason, the depth of the additionally required assessment must be kept within limits and may also refer solely to the scope of the (mass) data accesses problematized by the CJEU. Therefore, it is essential to include the specific processing and the associated risk for the data subjects in the overall evaluation. The level of data protection that is assessed with that in mind is expressed in a quantitative or qualitative value and related to the transmission risk identified in the first step. This relation is considered to have been established if the threat to the SDM objective identified in the first assessment step meets with a deficit within the third country's regulatory framework precisely with regard to this specific SDM objective.
- **Supplementary measures:** The requirement for supplementary measures is easily constructed. However, such measures must be linked to specific individual circumstances of the transfer, from which threats to the rights and freedoms of data subjects[7] arise, if and to the extent that these circumstances negatively contribute to identified risks to the SDM's objectives. Therefore, the relevant factor and starting point for the assessment cannot be the level of data protection in the third country, because these are circumstances not at the disposition of the contracting parties. Supplementary measures to be agreed between the parties can be procedural, organizational or technical and can potentially affect all aspects of the risk of the data transfer. Supplementary measures are not always required in all scenarios, nor can the risks to the rights and freedoms of the data subjects be sufficiently mitigated by additional measures in all cases.

[6] See CJEU, Schrems-II decision, para 132.
[7] Cf. also Conseil d'Etat, Urt. v. 13.10.2020, Az. 444937, Rn. 11-14 (German translation available at https://datenrecht.ch/wp-content/uploads/444937-CNLL-et-autres-DE.pdf, last accessed on 15.12.2020), which is why the focus of the examination is precisely not the level of data protection in the third country, but the associated or deepened risks to the rights and freedoms of the data subjects, if any.

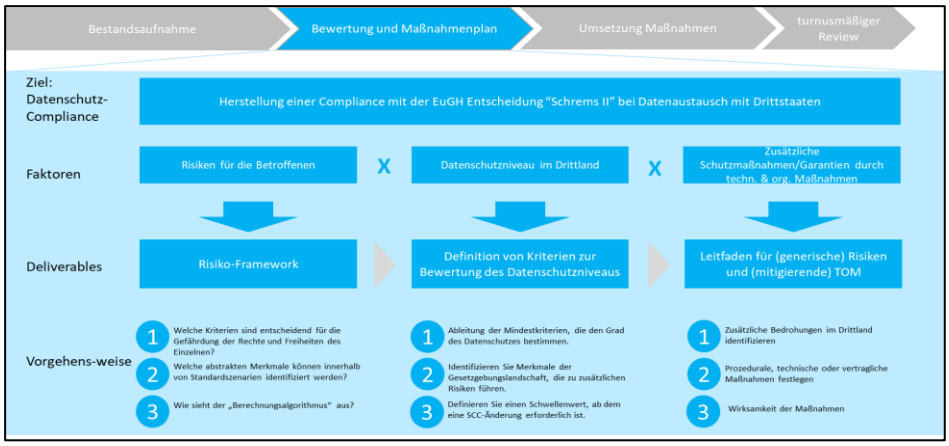


Table 1: Risk-Management-Process for the Data Transfer

- **Overall result of data transfer risk**: The result of the assessment is the lowest possible risk in the context of the data transfer from the perspective of the data subject. If and as long as this "net risk" lies on the "acceptable" side of the threshold, the data transfer can be carried out. Bitkom is aware that even and especially after such an examination, there may be data processing that cannot take place or cannot take place in its originally planned form.

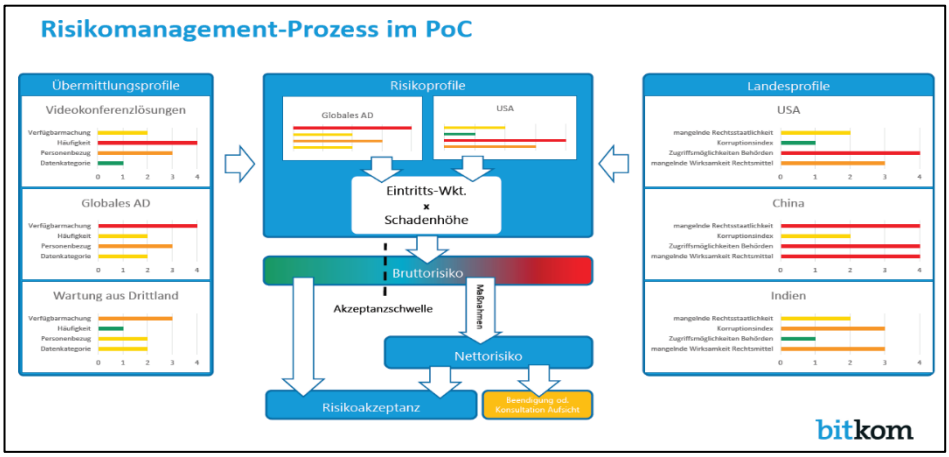


Table 2: Component of the risk of data transfer

### 4. Legal assessment

It goes without saying that the requirements formulated by the Schrems II ruling to protect the rights and freedoms of the data subject must be implemented. Bitkom meets this challenge with the concept presented here. While in the public discussion, also on the part of the supervisory authorities, the third country concerned seems to be the sole yardstick for the necessity of additional measures, including changes in data processing, Bitkom advocates a stronger focus on the individual aspects of data processing (see above under C.I.) and bases the consideration of these transfer parameters on the following legal aspects, in addition to the data protection level in the third country:

- First of all, it must be taken into account that the approach advocated here is relevant in scenarios of Art. 46 GDPR, where an adequacy decision of the EU Commission pursuant to Art. 45 (3) GDPR is missing. It is therefore impossible to expect companies to conduct in-depth legal and factual investigations, which may then turn out differently for different companies. If companies rely on standard contractual clauses in their respective version, a very significant part of the basis for the data transfer is already in place. The higher the requirements for additional measures, on the other hand, the more likely this is to contradict Article 46 (2) of the GDPR, which contains and allows sufficient contractual guarantees. Against this background, Bitkom calls for more flexibility in determining the need for supplementary measures (which is not to be understood as rejecting the data protection level of the GDPR).
- The wording of the GDPR itself leaves no doubt that the decision on the lawfulness of data transfer to third countries is to be made precisely in accordance with the circumstances of the individual case relevant to the data transfer.
    - The approach introduced by Art. 24 (1) sentence 1, 32 (1), (2) and Art. 35 as well as Art. 5 (1) GDPR to take into account risks to the rights and freedoms of data subjects requires the determination of concrete circumstances of the individual case to derive corresponding risks. These circumstances include, among other things, the data categories, the purposes, quantity structures, existing protective measures, etc. [8] While not all aspects may be relevant to the specific risk associated with the transfer, this illustrates the multitude of variables that must form the basis of an assessment.
    - According to Recital 108, the processing (and thus the individual aspects that characterize it) must be the focus for adequate protection and not (merely) the third country framework. Moreover, Recital 108 clarifies that the protection must be adequate, i.e. it does not apply absolutely.[9]
    - Since Article 44 (1) sentence 1 GDPR refers to the specific provisions of Chapter 5 of the GDPR as well as to the other provisions of the GDPR, Articles 24, 32, 35 and 5 of the GDPR naturally also apply to data transfers. A focus of the consideration

[8] See Recital 75 GDPR.
[9] See regarding the relevance of Recital 108 also: CJEU, Schrems-II decision, para 95, 131.

of the data transfer to the single element of the third country is therefore not evident.

- Art. 46 GDPR refers to "appropriate" safeguards in the absence of an adequacy decision. The criterion of "adequacy" is open to evaluation and thus to application in individual cases. The yardstick of this adequacy is the protection of the data subject.[10] In order to determine the need for protection of the data subject in context of an international data transfer and, if necessary, to derive appropriate measures, Art. 5 (1) (f) GDPR, the risk for data subjects must first be determined. Otherwise, no valid statement can be made about their effectiveness. In this respect, the assessment of a data transfer to a third country pursuant to Art. 44 et seq. GDPR must also be based on the concept of considering the individual aspects of a data transfer.
- According to the draft version of 13.11.2020 on the implementation of new standard data protection clauses of the European Commission, the European Commission also considers it necessary that data importer and data exporter consider the individual circumstances of a data transfer in order to ensure the required level of data protection in the third country. Thus, in Recital 20, but also in the standard contractual clauses themselves under clause 2 (b) (i), the document refers in a non-exhaustive catalogue to the need to examine parameters such as the categories of data or the categories of recipients. However, such a case-by-case examination only makes sense if and to the extent that it has an influence on additional measures. This is to be assumed in any case if the characteristics of such variables determine the amount of damage or the probability of occurrence of a risk.
- Also according to statements by the European Data Protection Board ("EDPB"), the level of data protection in the third country is not generally or even solely relevant, but must be differentiated according to the details of the data transfer. For example, the EDPB focuses on the roles of parties involved in the data transfer and discusses necessary technical measures depending on the applicability of specific legal acts granting access, such as Section 702 FISA. Only if and to the extent that the respective importer or other recipients in the U.S. fall within its scope of application at all, does the EDPB conclude that regulatory access must be completely precluded or rendered ineffective by technical measures.[11] In this respect, the characteristic of the recipient must be able to find its way into the examination as one parameter (of several). Even in the case of the applicability of certain legal norms that enable access, the EDPB looks at the respective risk, in particular the (concrete) probability of access by the authorities. This means that even at the level of applicable legal norms, a blanket approach is not sufficient, but opens the way to a differentiated examination.[12] Furthermore, the EDPB points out that supplementary measures for data protection and data security must be implemented

[10] See Recital 108 sentence 1 GDPR.
[11] EDPB Recommendations 1/2020, para 44.
[12] EDPB Recommendations 1/2020, para 135.

on the basis of risks: For example, with regard to the application of specific security requirements, it refers to risks that exist for transferred categories of personal data.[13] Bitkom also focuses on the need to examine precisely these details. Finally, references to the consideration of the specific circumstances of the individual transfer run through the entire EDPB Recommendations.[14] In this respect, one can only conclude that this is a concept that supports the EDPB´s Recommendations.

- The rights to privacy and data protection protected in Articles 7 and 8 of the EU Charta do not preclude a differentiated approach. oth do not apply per se and without restriction. Rather, they are subject to limitations inherent in fundamental rights or statutory limits, which permit and also require a more precise consideration of the individual circumstances of the data transfer:
  - The right to privacy ends at the limit of its scope of protection. In this respect, the Federal Constitutional Court, in its decision on secret tape recordings[15], differentiated according to the sphere theory it developed for the right to informational self-determination according to different degrees of personal involvement, namely according to intimate, private and social spheres.[16] In this respect, differentiating justification requirements or toleration obligations apply. Since Art. 7 EU Charta even explicitly mentions the private sphere, the home, family life and (private) communication as objects of protection, the sphere theory is to a certain extent already anchored at the level of fundamental rights. Accordingly, on the basis of Article 7 EU Charta, there is no or a low need for protection outside its explicit scope of protection. Accordingly, the context of the personal data must first be determined and weighted (against the background of Art. 7 EU Charta). This, initially, has no relation to a framework of a third country.
  - The right to protection of personal data under Article 8 of the EU Charta guarantees the institution of data protection as the subject of secondary legislation at EU level.[17] Accordingly, its scope of protection is not conclusively determined, but the right refers in this respect to the regulations that formulate it, Art. 8 (2) EU Charta. These regulations give life to the right referred to in Art. 8 EU Charta and align and balance it with other fundamental freedoms.[18] In this respect, the determination of any existing need for protection of personal data, taking into account the individual circumstances of their transfer, is not a question of conflict with Article 8 EU Charta, but is to be measured solely against the standard of the GDPR.[19]
- Finally, the CJEU itself suggests an individual examination of the individual case in its Schrems II ruling.[20]

[13] EDPB Recommendations 01/2020, para 135.
[14] EDPB Recommendations 01/2020, para 77, 93, 97, 122.
[15] BVerGE 34, 238 sqq.
[16] See BVerfGE 34, 238 (245).
[17] Buchholtz/Stenzel, in: Gierschmann et al, DSGVO Komm., Art. 1 para 32.
[18] See Recital 4 sentence 2 GDPR.
[19] And the GDPR does not grant absolute protection, but only adequate protection in the light of the processing, Recital 108.
[20] See above, footnote 5.

- Thus, supervisory authorities shall examine data transfers on the basis of agreed standard contractual clauses on a case-by-case basis "in the light of all the circumstances of the transfer" as to whether "the protection required by Union law" can be ensured[21] and, if necessary, suspend or prohibit such transfers by applying Article 58(2)(f) GDPR. This is particularly noteworthy because the CJEU - in addition to the wording of Article 58(2)(f) GDPR - explicitly considers all circumstances of the transfer to be relevant.[22]
- The CJEU also imposes the same standard as for supervisory authorities on the companies themselves.[23]
- In summary, it can be stated that, in the opinion of the CJEU, the variables of the processing or transfer must be examined and weighted in order to determine the additional need for protection resulting from this and against the background of the situation in the third country and to derive additional measures based on this.

A differentiated consideration of the (transfer) circumstances in the individual case is therefore not only permitted and reasonable, but also required. Consideration of the individual parameters of the data transfer is an essential component of the risk management process for (international) data transfers proposed by Bitkom.

## 5. Risk Assessment Model

**Phase 1 – Risk Identification**

1. Determination of a scenario
2. Identification of a risk in the scenario (reference: data protection principles)
3. Identification of a risk source (recurring/standardizable for the purpose of this concept)
4. Description of a risk (recurring/standardizable for the purpose of this concept)

**Phase 2 – Assessment of Damages**

5. Description of potential actual damages
6. Allocation of damage categories (standardizable in accordance with Recital 75 GDPR)
7. Allocation of the probability of occurrence (standardizable in accordance with ISO/IEC 29134)
8. Quantification of the amount of damage (standardizable in accordance with Bitkom Guidelines, „Risk Assessment & Datenschutz-Folgenabschätzung“[24], p. 50 ff.)

[21] CJEU, Schrems-II decision, para 146.
[22] CJEU, Schrems-II decision, para 146.
[23] CJEU, Schrems-II decision, para 132.

**Phase 3 – Risk Assessment**

9. Offsetting damage amount and probability of occurrence („pure" calculation)
10. Mapping the risk on a heat-map to determine the risk-tolerance (corresponding to the acceptance threshold; to be agreed with supervisory authorities if necessary)

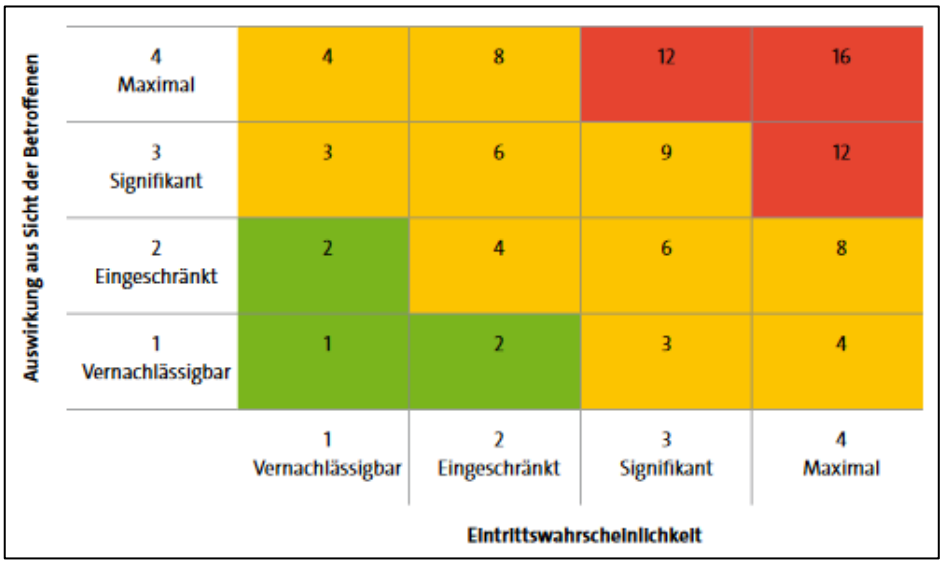


Table 3: Visualization of the transfer risk

### Modelling the level of data protection in the third country

The assessment of the level of data protection in the third country must always be within a framework that is reasonable and affordable for the company doing the assessment. The requirements must also not lead to distortions of competition between large companies with their own legal department and small and medium-sized companies that do not have the necessary resources for an in-depth assessment. It is therefore even more important that an assessment is carried out according to clear criteria and compiled into a country risk profile. For each country, threats to the data subject that could result from access to data by the authorities (e.g., discrimination, entry bans, political persecution) are considered, as are probabilities of occurrence based on the legal hurdles for accessing such data.

[24] See here: https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Datenschutz-Folgenabschaetzung.html

### Selection and control of supplementary measures

The selection of measures to mitigate the identified risks is an important basis for the permissibility of the transfer in the final result. If, based on the framework conditions of the transfer ("transfer profile" and "country profile"), the risk ("gross risk") is above the risk acceptance threshold, a transfer to the third country without additional safeguards is considered unacceptable and can thus be prohibited by supervisory authorities.

Any identified threats to performance objectives under SDM, which may be exacerbated by the legal situation in the third country, impact the necessary additional measures, which ultimately work in favour of the rights and interests of the data subjects. When selecting the measures, care should be taken to already ensure that the respective measure also has an effect on aspects of the probability of occurrence or the potential for harm from the perspective of the data subject and in this respect positively changes the risk.

Taking into account the corresponding measures ("risk treatment"), the risk must be reassessed ("net risk"). Only if the net risk is below the risk acceptance threshold and thus is not likely to lead to an unacceptable risk to the rights and freedoms of natural persons, an adequate level of protection can be assumed for the data transfer to the third country. In this respect, it should be noted that - unlike in enterprise risk management - risk acceptance beyond the acceptance threshold is excluded. The acceptance threshold must be based on the general standards in data protection and may objectively be below the level of a high risk.

The data exporter should ensure appropriate and comprehensible documentation of the assumptions and decisions made in order to meet the accountability requirements under Article 5(2) of the GDPR.

## 6. Outlook

### Data Protection Safeguard-Profiles as reference profiles

Initially, the data protection safeguard profiles created individually in accordance with the process described in C.III. to C.V. allow an assessment about the underlying scenario in each case. However, they can serve as a reference for the evaluation of other situations beyond the specific situation described. The creation of individual data protection safeguard profiles already achieves a certain degree of scalability. The more data protection safeguard profiles are created, the greater the scalability. This is because, since the decisive factor will always be whether other circumstances are characterized by the same manifestation of the variables relevant to data protection with regard to their relevance under data protection law, a greater number of data protection safeguard profiles will result in an exponentially growing number of reference constellations.

### Safeguard-Profiles vs. parameterization

The goal of Bitkom's activities in connection with international data transfers is the development of a technical procedure for standardized and automated testing of data transfers ("the product"). This is because the depth of integration of technical components and third-party services in the business processes of member companies means that, in addition to the need for standardization, the criterion of a fast audit protocol that can also be implemented by non-lawyers or data protection experts must also be met. The product is intended to lead companies to legally defensible audit results and handling instructions on the basis of the procedure documented here. Together with the documentation for the product, which is to be continued accordingly, and the documentation resulting from individual audits, the companies also fulfil their accountability obligations of Article 5 (2) GDPR.

The approach taken by Bitkom is based on the recognition that the variables relevant for the transmission risk, but also their characteristics, are not infinitely extensive or different. For this reason, the test can also be largely decoupled from concrete scenarios underlying a data protection profile. Instead, the test can be fully parameterized. All individual components are mapped into variables, which then can be characterized by a number of predefined values. The variables are technically linked to each other (after possibly different weighting) where logical dependencies exist. This applies to the elements of transmission risk as well as to the additional measures under consideration. Examples: Linking of data transmission parameters to make statements about the amount of damage or probability of occurrence, linking of measures with one or more values of one or more transmission variables to fix the 1:n relationship between measures and risk variables.

Bitkom is aware of the challenge that the parameters must not only be initially complete in order to adequately and comprehensively reflect the risks. It is also necessary to keep the respective entries up-to-date with regard to the respective current factual and legal situation. In addition, the components of the assessment model must be flexible and adaptable. Bitkom is convinced of the necessity and usefulness of such an approach and is therefore continuing to drive this development forward.

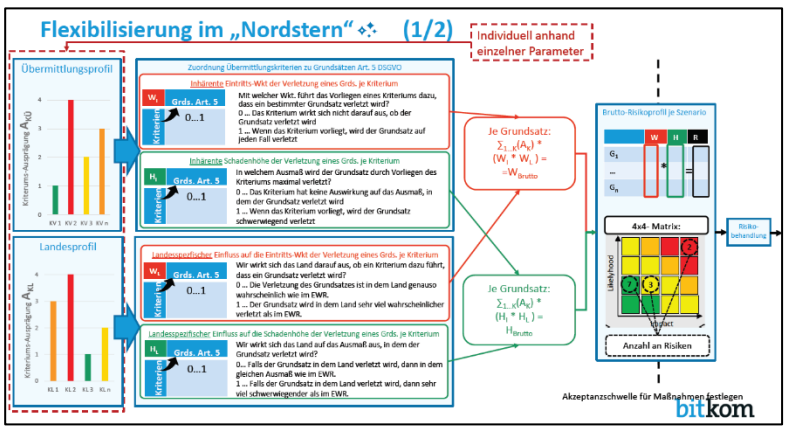


table 4: Parameterization of transmission and third country component

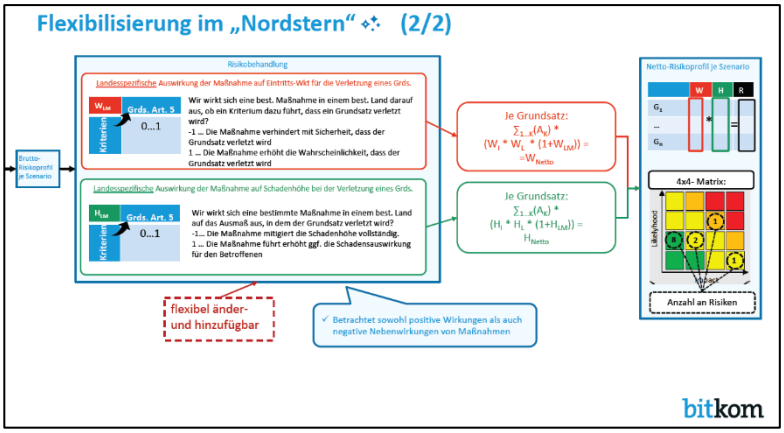

Table 5: Transfer to "classic" components of risk assessment