DIGITALEUROPE

21 DECEMBER 2020

Response to draft EDPB Recommendations on supplementary measures for personal data transfers

Executive summary

DIGITALEUROPE is deeply concerned about the draft Recommendations adopted by the European Data Protection Board (EDPB) with respect to supplementary measures for personal data transfers.[1]

In their current form, the draft Recommendations fundamentally misinterpret the requirements laid down in the *Schrems II* ruling[2] and would create unjustifiable disruption to economic activity. In mandating drastic measures for all data transfers, the draft Recommendations would impede or severely hamper the conduct of business inside and outside Europe, with no corresponding benefits in terms of data protection.

European companies operating internationally have achieved strong levels of integration across their businesses and affiliates around the world. They have design offices, assembly lines, suppliers, partners, training and maintenance centres located both inside and outside Europe. Such integration also relies on common tools used by affiliates across the globe for various purposes: human resources (HR) management, marketing and sales, information systems, engineering, operations, finance, etc.

Our recent survey about the use of standard contractual clauses (SCCs) shows that only 9 per cent of companies based in Europe do not transfer any data outside the EU, while 75 per cent of those that do are European companies.

[1] Draft Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

[2] C-311/18.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Three-quarters of companies using SCCs transfer data to more than one non-EU country simultaneously.[3]

It is essential that the final Recommendations recognise all the relevant nuances associated with data transfers and allow for a correct interpretation of companies' obligations.

Crucially, in line with the General Data Protection Regulation (GDPR) and the *Schrems II* ruling, the final Recommendations should allow for an assessment of all the circumstances surrounding a specific transfer, including the nature, scope, context and purposes of processing as well as the actual likelihood and severity of risk.

In our response we offer an in-depth assessment of the repercussions that the draft Recommendations would have, were they to be followed, and offer interpretations and requirements that are consistent with the ruling.

Given the importance of these issues, we urge the EDPB to allow for sufficient time to duly consider all stakeholder feedback received during the public consultation and to issue a revised set of Recommendations.

[3] *Schrems II impact survey report*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf.

Table of contents

Assessing adequacy

Step 3, devoted to the assessment of third-country law or practice, takes up most of the draft Recommendations. However, along with the accompanying European Essential Guarantees (EEGs),[4] it fails to provide concrete guidance for data exporters and importers.

This section of the draft Recommendations reiterates the *Schrems II* findings in relation to US law, while the EEGs for the most part concern rulings from the Court of Justice of the European Union (CJEU) relating to Member State laws.

It would be useful if the EDPB could provide more concrete guidance concerning at least those third countries, if any, where it deems that the EEG requirements are met. Absent this, exporters and importers as well as DPAs will continue to generate incoherent interpretations that only fuel legal uncertainty.

Section 702 of the US Foreign Intelligence Surveillance Act (FISA) is the only foreign law that is explicitly considered as inadequate in the draft Recommendations.[5] However, in considering only whether the data importer or any further recipient falls under FISA's overall scope, the draft Recommendations fail to consider the context of the data in scope, which is a significantly more limited dataset than all personal data processed by a covered data importer.[6] While these factors may not be conclusive to reach a general adequacy decision, they should be relevant when considering if and how third-country legislation applies to the transferred data in a specific situation.

Making data access 'impossible or ineffective'

The draft Recommendations offer a blanket statement that contractual and organisational measures will in themselves 'generally' not be sufficient and can only act as complements to technical measures in order to prevent access by third-country public authorities.[7]

Similarly, in assessing whether such public access is possible, the draft Recommendations stipulate that only 'relevant and objective factors' should be considered in addition to relevant legislation, excluding factors the draft

[4] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

[5] Paras 44 and 76 of the draft Recommendations.

[6] For example, an electronic communication service may process customer-generated data such as files or messages and their metadata, which are relevant under FISA 702. However, it may also process a limited set of personal data strictly for billing purposes that is not of relevance under FISA but is still subject to the same approach under the draft Recommendations simply because it is processed by the provider in question.

[7] See in particular paras 48 and 93 of the draft Recommendations.

Recommendations call 'subjective' such as the likelihood of actual access to the transferred data.[8]

This reasoning underscores the draft Recommendations' incorrect assumption that all transfers must equally make access to the transferred data 'impossible or ineffective,'[9] irrespective of the full circumstances surrounding the transfer, simply based on a theoretical possibility of unjustifiable interference by third-country public authorities.

In line with this reasoning, all the examples of effective supplementary measures in the draft Recommendations describe scenarios where the transferred data is made *completely illegible* in the destination country – not only by public authorities but also by the data importer itself.[10]

Is a data transfer a data transfer?

In this context, an interesting question is whether personal data transfers *are actually at play* in light of the type of effective supplementary measures identified in the draft Recommendations.

By requiring access to the data to be completely impossible for the third country's public authority as well as for the data importer – because the encryption keys or identifying data are retained solely under the control of the data exporter or other entities established in the European Economic Area (EEA) or adequate countries,[11] or because the data cannot be reconstructed[12] – the draft Recommendations seem on the contrary to be mandating a process whereby the data is *rendered anonymous* for the purposes of the transfer.

Because the draft Recommendations require encryption to be 'flawlessly implemented'[13] to counteract the means 'reasonably likely to be used to identify

---

[8] Para. 42, ibid. This language echos Recital 104 GDPR, which requires the Commission to 'take into account clear and objective criteria' for the purpose of adopting an adequacy decision. This is due to the fact that adequacy decisions have a general binding effect, as opposed to SCCs, which apply to each individual transfer. See, to this effect, para. 129, C-311/18.

[9] Para. 44 of the draft Recommendations.

[10] The only exception is use case 4, which involves transfers 'to a data importer in a third country specifically protected by that country's law, e.g., for the purpose to jointly provide medical treatment for a patient, or legal services to a client' (p. 25 of the draft Recommendations). We note that, because such exemption stems from the relevant third-country legislation applicable to the transferred data, this should result in a positive assessment of the third-country laws applicable to the transfer and that hence *no supplementary measures are needed*.

[11] Use cases 1-3, ibid.

[12] Use case 5, ibid.

[13] Paras 79 and 84, ibid.

the natural person,'[14] it must be concluded that the information, both in transit and at rest in the destination country, can genuinely be considered anonymous.

Irrespective of this interpretation, the draft Recommendations render controller-to-controller and processor-to-controller transfers *completely impossible*.[15] A controller in the destination country – for example, a non-EU subsidiary of an EU parent company – must be able to process the transferred data for its own purposes, but clearly cannot do so if it cannot access the data.

Precluding all access

The draft Recommendations specify that the supplementary measures 'aim to preclude potentially infringing access by preventing the authorities from identifying the data subjects, inferring information about them, singling them out in another context, or associating the transferred data with other datasets they may possess that may contain, among other data, online identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts.'[16]

Not only does this interpretation have no basis in the *Schrems II* ruling, but it sets a bar that may well be completely impossible to meet. The draft Recommendations do not consider that, even in the case of end-to-end encrypted services, at least some metadata needs to be unencrypted to achieve the transfer. This will include connection information, session state, IP addresses or basic subscriber data.

From this perspective, we submit that upon closer scrutiny not even the scenarios identified by the draft Recommendations as providing effective measures (use cases 1–5) would meet the draft Recommendations' standards.

Trade without personal data flows?

The draft Recommendations provide two examples that clearly illustrate the logical limitations and profound economic damage that would result from an incorrect interpretation of the *Schrems II* ruling.

What happens if we enforce the draft Recommendations

Use case 7 describes a mundane scenario in which data transfers are necessary for business purposes, be it within a multinational group of companies or

[14] Recital 26 GDPR.

[15] Again, the only exception being use case 4 of the draft Recommendations.

[16] Para. 74, ibid. See, to the same effect, paras 80–83.

between different companies engaged in mutual economic activities. The use case specifically calls out HR data and communications with customers, which are routine transfers for any company operating outside the EU.

In all these cases, the draft Recommendations stipulate that, simply because the data is available in the clear to the data importer, no effective technical measures exist and the transfer must hence not commence or be stopped.[17]

As evidenced by our recent survey, these scenarios represent a predominant part of all data transfers outside the EEA.[18] We estimate that 85 per cent of companies operating in Europe use SCCs, the vast majority (75 per cent) headquartered in the EU, and that 90 per cent of them are business-to-business (B2B) entities. Over 57 per cent transfer data to close business partners or non-EU subsidiaries using controller-to-controller SCCs. As seen above, controllers in the destination country *must* be able to access the transferred data lest the transfer be made completely pointless.

The draft Recommendations would force all these companies to stop their data transfers to non-adequate countries, with repercussions on their business that would be dire.

Use case: How does a German car get to China?

A major European carmaker has set up a joint venture in China, which is by far the main market for the company. The Chinese plant manufactures cars for the entire Asia-Pacific market. A Sino-German team must work together throughout the manufacturing design process. Vehicle designs, models and specifications need to flow from Europe to the Chinese entity, along with the HR information of the European employees.

Under use case 7, in light of concerns about Chinese state and public security laws and the fact that the data must be available to the Chinese entity in the clear, the European company concludes that no effective technical measures exist and is forced to stop the Chinese manufacturing process. This costs the company close to €15 billion in revenue the first year alone.

Use case 6 tackles cloud processing as well as 'other processors which require access to data in the clear,' irrespective of any further details around the processed data, and makes it impossible for the processor to access the data although such access is necessary to perform the processing operation.[19]

---

[17] Paras 90-91, ibid.

[18] *Schrems II impact survey report*.

[19] Paras 88–89 of the draft Recommendations.

Use case: How do European industrial parts get from Mexico to the US?

A European manufacturing company has a factory in Mexico which manufactures parts for the US industrial market. In an effort to improve production, working with the chief technology officer's team in the European headquarters, the company deploys an IoT operating system (OS) using a US cloud service provider, which it has selected because it allows quick and scalable deployment. The company's customers and partners – which may be based in Europe, Mexico or the US – can access the OS through an application programming interface (API) in order to develop applications based on it; to this end, they also have direct access to the cloud provider's collaboration tools.

These operations involve access to data in the clear on the part both of the company's customers and partners and of the cloud service provider.

Because such data includes, among others, the personal data of the company's European employees, customers and partners, under use case 6, the company concludes that no effective technical measures exist and is forced to stop deployment of the solution, resulting in immediate loss of business for the coming year. The company is unsure whether it will be able to select another cloud provider that meets its business requirements during the following years, and may have to abandon the project and associated revenue indefinitely.

What if all my data is in Europe?

As the draft Recommendations explain, remote access from a third country is also considered a data transfer.[20]

This situation could involve a simple scenario whereby a French parent company uses a centralised HR service based in France that is shared with its US and Asian subsidiaries. Although the data is only stored in servers in France, these are still transfers under the GDPR. The French company and its subsidiaries each act as controllers for the independent purposes they pursue and the French HR service acts as processor for all of them.[21]

---

[20] Para. 13, ibid.

[21] To reflect this, the new draft SCCs published by the European Commission include Module Four (processor to controller) covering situations where an EU processor combines the personal data received from the third-country controller with personal data collected by the processor in the EU. See https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Cothefmmission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

Use case: An international strategy for data?

As part of the European Strategy for Data, the European Commission funds the establishment of an EU-wide interoperable manufacturing data space with the aim to ensure Europe's global competitiveness and data sovereignty. The data space enables value-added exchange or joint exploitation between data holders and data users via a platform containing mixed datasets. All the data is stored in Europe by an EU-headquartered provider of data sharing services.

A data user headquartered in Denmark would like to use some of the datasets for commercial purposes. To do so, its subsidiary in California, which is its global R&D competence centre for the relevant type of manufacturing data, must access the data. The US subsidiary will combine the transferred data with other datasets it owns in the context of a project it is conducting with a local university, which acts as processor. The personal and non-personal datasets are 'inextricably linked' and the transfer is therefore subject to the GDPR.[22]

Because of use cases 6 and 7, given that the data must be accessible in the clear both by the US subsidiary and the US university, the Danish data user concludes that no effective technical measures exist and aborts the R&D project. The service it had planned to develop proves impossible and the Danish data user decides to exit the data space.

This makes it evident that companies cannot solve issues identified in their assessments of third-country transfers simply by moving all data storage to the EEA – that is, unless they also accept the prospect of ending their underlying international operations, for which such transfers are necessary.

Full circumstances surrounding the transfer

This draconian approach runs counter to a basic tenet of the *Schrems II* ruling, which always refers to the need to consider each specific transfer 'in the light of all the circumstances of that transfer.'[23]

It also runs counter to the general GDPR rules pertaining to technical and organisational measures, which require due consideration for 'the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.'[24]

---

[22] See COM/2019/250 final.

[23] See notably paras 112, 113 and 121 of the draft Recommendations.

[24] Arts Art. 25(1) and 32(1) GDPR.

The draft Recommendations do recognise some such circumstances – including the nature of the data, the complexity of the data processing workflow and the possibility of onward transfers – yet proceed to only specify technical measures pertaining to one type of circumstance, i.e. the format of the transferred data (plain text, pseudonymised or anonymised).[25]

We submit that all these elements should be considered in the assessment of supplementary measures and note, in particular, that in direct contrast with the draft Recommendations, the GDPR specifically refers to the 'likelihood and severity' of risk.

While such factors may not be central to the theoretical assessment of the third-country law and practice, they should be considered as part of the assessment of the supplementary measures. In other words, if the data is of limited real-world interest to public authorities – for example business contact information or other low-risk personal data – this should have a bearing on the type of supplementary measures that are required. Experience companies have had with these types of requests in the past should also be factored in.

All the above is correctly reflected in the new draft SCCs published by the European Commission, with which we urge full alignment. The new draft SCCs include due consideration for 'the content and duration of the contract; the scale and regularity of transfers; the length of the processing chain, the number of actors involved and the transmission channels used; the type of recipient; the purpose of processing; the nature of the personal data transferred; any relevant practical experience with prior instances, or the absence of requests for disclosure from public authorities received by the data importer for the type of data transferred.'[26]

From this perspective, the final Recommendations should provide a more balanced toolbox of supplementary measures that data exporters can rely on based on their assessment of the full circumstances surrounding the specific transfer at hand.

Improper application of GDPR principles

Accountability

The draft Recommendations frame the entire process of third-country transfers as a specific application of the principle of accountability.

[25] Para. 49 of the draft Recommendations.

[26] Clause 2(b)(i), Section II.

Accountability is indeed a central tenet of the GDPR. However, its application has a general nature that merely states that '[t]he controller shall be responsible for, and be able to demonstrate compliance with,' the other six general principles for the processing of personal data.[27] We note that this responsibility lies only with the controller.[28]

We therefore do not believe that interpreting third-country transfers primarily through the accountability principle is at all useful. Rather, the general principle for third-country transfers is laid out in Art. 44, which provides that controllers and processors must comply with the conditions laid down in Chapter V GDPR in order not to undermine the GDPR's level of protection.

Data minimisation

The draft Recommendations also extend the data minimisation principle to require that third-country transfers be limited to what is 'adequate, relevant and limited to what is necessary in relation to the purposes for which [the data] is transferred to and processed in the third country.'[29] This appears to imply that the GDPR imposes a duty to minimise transfers themselves, as opposed to the *overall* data processing.

This interpretation has no basis in the GDPR. The data minimisation principle applies in relation to each processing *purpose*, but not in relation to every *processing activity* undertaken within such purpose, which may include third-country transfers.

It is Chapter V GDPR alone that stipulates the conditions for transferring personal data to third countries. Such specific conditions do not include any reference to minimisation applied specifically to transfers. This is also made clear by the fact that where Chapter V requires transfers to be occasional and not repetitive, which are specific examples of minimisation, it does so explicitly.[30]

---

[27] Art. 5(2) GDPR.

[28] By contrast, the draft Recommendations expand the general accountability principle to both controllers and processors, who must 'be able to demonstrate these efforts to data subjects, the general public and data protection supervisory authorities' (para. 3). We are also unsure about footnote 11 referring to joined cases C-92/09 and C-93/09, which relate to the financing of the EU's common agricultural policy and only refer to accountability in a democratic system in relation to the principle of transparency as stated in Arts 1 and 10 TEU and Art. 15 TFEU, not with respect to the GDPR.

[29] Para. 11 of the draft Recommendations.

[30] Notably with respect to derogations. The term 'occasional' (closely linked to the term 'necessary,' which is used in Art. 49(1)(b), (c), (d), (e) and (f)) is used in Recital 111 in relation to the contract and legal claim derogations; similarly, the term 'not repetitive' is used in Art. 49(1)(2) specifically in relation to the compelling legitimate interest derogation. From this perspective, para. 25 should be amended to clarify that not all derogations require transfers to be occasional and non-repetitive.

Binding corporate rules and ad hoc clauses

The draft Recommendations repeat that the *Schrems II* ruling also applies to binding corporate rules (BCRs) and ad hoc contractual clauses, stating however that 'the precise impact … is still under discussion.'[31]

We would like to stress that both BCRs and ad hoc clauses are adopted by the competent data protection authority (DPA), satisfying DPAs that their contractual safeguards can be complied with. As such, we urge the EDPB to provide clearer reassurance as to their continued validity and that no further reassessment of adequacy is necessary.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

See our response to the Article 29 Working Party draft guidelines on Article 49 of Regulation 2016/679, available at https://www.digitaleurope.org/wp/wp-content/uploads/2019/01/DIGITALEUROPE%20response%20to%20public%20consultation%20on%20Guidelines%20on%20Article%2049%20of%20Regulation%202016679%20(wp262)%5B1%5D.pdf.

[31] Paras 59 and 61 of the draft Recommendations.

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK