Comments on the Recommendations 01/2020 of the European Data Protection Board

On 11 November 2020, the European Data Protection Board published its draft Recommendations 01/2020[1] *"on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"* (hereinafter referred to as Draft Recommendations). The Draft Recommendations are open for public consultation until 21 December 2020.

1. The Draft Recommendations were "inspired" by the so-called Schrems II judgement[2], in which the Court of Justice of the European Union (CJEU) introduced the concept of *"essentially equivalent"* level of protection of personal data by further tightening the conditions of international transfer of personal data. This judgement concerned two legal instruments:

a) Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield, which was declared invalid,
b) Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EU of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016, concerning which the CJEU held that
    a. the Decision itself (and the Standard Contractual Clauses themselves) is/are not invalid,[3]
    b. *"appropriate safeguards, enforceable rights and effective legal remedies"* must be ensured in the case of transfer of personal data *"pursuant to standard data protection clauses"*,[4]
    c. *"competent supervisory authority is required to suspend or prohibit a transfer of data to a third country* ***pursuant to standard data protection clauses*** *(emphasis added—Zs.B.) …, if … those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law"*.[5]

In the Schrems II judgement (including the operational part and the reasoning part), the CJEU does not make any statements on other tools of the transfer of personal data, except for Article 49 of the GDPR: *"the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third*

[1] See at the following link https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en
[2] Data Protection Commissioner v. Facebook Ireland LTD, Maximillian Schrems, Case C-311/18 of the Court of Justice of the European Union (CJEU) – hereinafter: Schrems II judgement
[3] Schrems II judgement, operational part point 4
[4] Schrems II judgement, operational part point 2
[5] Schrems II judgement, operational part point 3

countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR." [6] From the paragraph 202 of the Schrems II judgment one can conclude that

a) appropriate safeguards under Article 46, other than the standard contractual clauses, are likely required to meet the same requirements as in the case of the standard contractual clauses,
b) Article 49 has a special nature, but it is a bit different from what the EDPB understands.

2. Although it is understandable that the EDPB intends to give some guidance and recommendations on how to handle the post-Schrems II situation, this guidance and these recommendations show a high degree of naivety. This naivety comes from the idea that the extraterritorial scope of the GDPR is acknowledged, accepted, and the provisions of the GDPR are implemented by actors outside the EU. I am afraid this is not the case.

a) Countries are sovereign in determining the rules of the activities that happen in their territories, including the conditions under which *anything* may enter their territories; these conditions may include an obligation to provide access to data even if they are encrypted. Neither contractual clauses between the controller and the data processor (cf. paragraphs 58 and 61), nor the GDPR itself, nor any measures prescribed by regulatory authorities in the EU impose any obligation on public bodies, including ***law enforcement agencies*** (and especially on intelligence services), in countries outside the European Economic Area (cf. Article 23 of the GDPR). Therefore, public bodies, including *law enforcement agencies (including intelligence services)* will apply their own national rules (or international treaties if there are any concerning their tasks). Without any thorough and comprehensive analysis of the possibilities and authorities of the law enforcement agencies, including intelligence services, one can state (without high risk of error) that—in addition to that these law enforcement agencies will apply their own national rules –

- these public authorities can have access to any data that they consider necessary for their tasks,
- when they appear at a controller or a data processor, they (normally) have the authorisation necessary according to the national legislation or
- in urgent case, they might exercise their authorities without *prior* external authorisation,
- an entity (be it controller or data processor) that hinders the activities of the law enforcement agencies (including in such a way that, for example, the controller/data processor deletes some data after reception of a request from a law enforcement agency) may face sanctions.

[6] Schrems II judgement, reasoning part point 202: "the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence ofan adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR.

And a controller in the EU (data exporter) has a very little impact on this. In other words: **in case of data transfer (irrespective of what the data exporter chooses out of the tools in Article 46 or 49 of the GDPR) the opportunity of law enforcement agencies (including intelligence services) to access to transferred data will always exist and can never be excluded. Therefore, there is not any single country in the world that, in this regard, could meet the requirements of the Draft Recommendations.**

b) According to the Draft Recommendations (paragraph 38) *"the existence of … an independent data protection authority … may contribute to ensuring the proportionality of government interference".* The Recommendations 2/2020 on the European Essential Guarantees for surveillance measures,[7] under *Guarantee D – Effective remedies need to be available to the individual*, determine – essentially – two basic conditions for a legal remedy to be "effective":

- organisational requirements concerning the remedial body (independence, qualification, etc.)
- power of the said body to remedy the non-compliance. In this regard, the same Recommendations cite the Schrems II judgement which reiterated that *"data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data".*[8]

Regarding the second condition, one can find that even the EU legislation does not fully meet this criterion: According to Regulation (EU) 2018/1725 (EUDPR), in the case of "operational personal data"[9] the data subject can exercise some of his/her rights through the European Data Protection Supervisor, and as a result of the investigation of the latter *"the European Data Protection Supervisor shall at least inform the data subject that all necessary verifications or a review by him or her have taken place. The European Data Protection Supervisor shall also inform the data subject of his or her right to seek a judicial remedy before the Court of Justice",*[10] and the European Data Protection Supervisor may be obliged, *"in the exercise of his or her supervision powers, to take utmost account of the secrecy of judicial inquiries and criminal proceedings, in accordance*

[7] See at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

[8] Schrems II judgement, para. 194

[9] According to Article 3(2) of the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC "operational personal data" means all personal data processed by Union bodies, offices or agencies when carrying out activities which fall within the scope of judicial cooperation in criminal matters or police cooperation [Chapter 4 or Chapter 5 of Title V of Part Three TFEU] to meet the objectives and tasks laid down in the legal acts establishing those bodies, offices or agencies.

[10] Article 84(1) of EUDPR

with Union or Member State law".[11] And even if judicial remedy is available,[12] it is quite unlikely that the data subject will have a real right to have access to their data, etc. This approach cannot be considered as unique.[13] **These provisions—although they are justifiable from the point of view of the national security, criminal investigation etc.—make the legal remedy available for a person just a *formal* remedy rather than a real one. It is question of personal taste to name such solution as "effective" remedy.**

c) While the Recommendations propose the use of technical measures to protect the transfer of personal data, since, as thought, *"there will be situations where only technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes"* (paragraph 48), the Recommendations ignore the fact that even EU Member States declare that *"upholding the possibility for law enforcement and judicial authorities to lawfully access relevant data for legitimate, clearly defined purposes of fighting serious crimes, in the digital world, are extremely important"*.[14]

In sum, before imposing conditions of extraterritorial scope, it should be proved that the EU law provides higher protection for personal data processed by law enforcement agencies (including intelligence services)—taking also into account what one of my excellent colleagues said: the shortest book of the world would be "NOYB: Additional authorities of the American intelligence services compared to their European colleagues' authorities".

3. The Draft Recommendations, in paragraphs 24 to 27, just refer to the EDPB's Guidelines 2/2018 on derogations of Article 49 under Regulation (EU) 2016/679[15] as "exceptional" tool. It must be noted, however, that paragraph 202 of the Schrems II judgement considers this tool as a possible one (and the given case, in my reading, the only one) for the transfer of personal data to third countries, since *"the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR."*

In the light of the statements in the Schrems II judgment (cf. the need for additional safeguards), the question must be raised whether such additional safeguards as described in the Draft

[11] Article 95 of Regulation (EU) 2018/1725.
[12] Article 84 of Regulation (EU) 2018/1725.
[13] For example, according to the Hungarian legislation, a data subject as client is excluded from the case in which the legality of the processing of his/her personal data is investigated by the national data protection authority, i.e. the data subject is just informed by the national data protection authority of the result of the investigation and – since he/she is not client – he/she cannot challenge the decision of the national data protection authority before a court.
[14] See Draft Council Declaration on Encryption at https://www.statewatch.org/media/1434/eu-council-draft-declaration-against-encryption-12143-20.pdf
[15] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

Guidelines can be imposed in the case of the application of Article 49 or not. The answer should be "no".

No, since, otherwise, the transfer of personal data pursuant to Article 49 would (also) be impossible, and—due to the fact that other tools are not available *per se* as explained above—the transfer of personal data to third countries as such would be impossible. In other words: **unless the intention is to totally block not only the data flow from the EU to third countries but the commercial relations as well,**[16] **Article 49 must always be applicable even if the level of data protection in the third countries is not acceptable by EU regulatory authorities.**

In this regard, it must be noted that, in my view, the interpretation, by the EDPB, of Recital (111) and Article 49 of the GDPR[17] is legally erroneous: the EDPB made wrong conclusions from the text of the recital while the text of Article 49 does not support this. Article 49(1) is divided into two subparagraphs: the first subparagraph enlists six cases [from point (a) to (g)] with regard to which the introduction of the subparagraph specifies that "a transfer or a set of transfers" may take place, i.e. such transfer may be a single transfer or repetitive transfers. The latter is also supported by the text of the second subparagraph which specifies that "a" "non-repetitive" transfer may take place when the first subparagraph cannot be applied.

The next question to answer is how to interpret the points of the first subparagraph of Article 49(1), i.e. the potential cases, and especially the contractual cases.

Having a social media account means that the data subject concluded a contract with the controller (for an information society service) in line with the general terms of the latter and in accordance with the choices made by the data subject during the setting up or any time later. In this regard, again, the interpretation, by the EDPB,[18] of Article 49(1)(b) is legally erroneous, since the text of the subparagraph specifies that transfer may take place either in the form of a single transfer or a "set of transfers". **That latter allows multiple transfers as well, and the transfers examined in the Schrems II judgment meet this condition.**

---

[16] Since even a simple hotel and/or flight reservation by a tourist agent falls under Article 49.

[17] *"The EDPB notes that the term "occasional" is used in recital 111 and the term "not repetitive" is used in the "compelling legitimate interests" derogation under Article 49 par. 1 §2. These terms indicate that such transfers may happen more than once, but not regularly, and would occur outside the regular course of actions, for example, under random, unknown circumstances and within arbitrary time intervals. For example, a data transfer that occurs regularly within a stable relationship between the data exporter and a certain data importer can basically be deemed as systematic and repeated and can therefore not be considered occasional or not-repetitive. Besides, a transfer will for example generally be considered to be non-occasional or repetitive when the data importer is granted direct access to a database (e.g. via an interface to an IT-application) on a general basis.*
Recital 111 differentiates among the derogations by expressly stating that the "contract" and the "legal claims" derogations (Article 49 (1) subpar. 1 (b), (c) and (e)) shall be limited to "occasional" transfers, while such limitation is absent from the "explicit consent derogation", the "important reasons of public interest derogation", the "vital interests derogation" and the "register derogation" pursuant to Article 49 (1) subpar. 1 (a), (d), (f) and, respectively, (g)." – EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, pp. 4-5.

[18] EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p. 8

Since, as pointed out, the tools regulated by Article 46 cannot be considered really suitable tools, the EDPB should reconsider its position on Article 49(1)(c)[19] with regard to, for example, the outsourced activities or such activities as cloud services, which can also be considered as "set of transfers".

In line with Article 13 or 14, the data subject must be informed of the transfer to a third country. Funnily enough, information on the specific risks and safeguards of such transfer is required by the GDPR only in the case of transfer based on the consent of the data subject [cf. Article 49, first subparagraph point a)] and—in accordance with Article 13(1)(f) or Article 14(1)(f)—in the case of transfer based on "*second* subparagraph of Article 49(1)".[20] Of course, it is not unlawful if the controller informs the data subjects of the risks and safeguards but it is, by law, obligatory only in the cases falling under first subparagraph of Article 49.

* * *

In sum: despite the extraterritorial scope of the GDPR, the EU cannot overrule third countries' legal provisions, and cannot oblige controllers or data processors having seat in third countries to contravene the local rules that must be applied by them in favour of the GDPR. Further, third countries can always enact legal provisions that block the effect any recommendations suggested by the EDPB. Only (bilateral or multilateral) international agreements could achieve those what the Schrems II judgement aims at. Unless the CJEU invalidates them…

By Zsolt Bartfai

[19] *"The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person",* see the interpretation in EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p. 9

[20] See the same wording in Article 30(1)(e), (2)(c) - regarding the records of processing activities.