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

The document is informative and clear on many topics. There are some subjects though that that maybe should be reconsidered or at least better explained (a broader perspective with analysis of some other court cases may be very useful). Schrems II has had an enormous impact, so it is very important to clarify as much as possible to make it easier for controllers to act in a correct way.

The Principle of Proportionality

I think it can be very useful to describe how EDPB considers the principle of proportionality since the recommendation has a broader scope than the Schrems II case, see the recitals (I have highlighted some interesting parts with blue colour):

> 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.

Today a lot of business depends on American systems (the same goes for NGO: s and the public sector). The recommendations are therefore very complicated to comply with at least in a short perspective. Therefore, it is important to study the Schrems II ruling very carefully. The Court was very clear in its statements, but I think EPDB must consider what kind of facts and circumstances the Court investigated. The recommendation has a wider scope than the judgment; it also has a bigger impact on other rights (see the blue marked words above). I will give some examples in this paper that I hope you will consider. It would be very useful if EPDB describes its view on the principle of proportionality (a good starting point for the recommendation).

The Bodil Lindqvist Case[1]

One court case that should be analysed in the recommendation is the Bodil Lindqvist case. The following part is very interesting:

> 67. Chapter IV of Directive 95/46 contains no provision concerning use of the internet. In particular, it does not lay down criteria for deciding whether operations carried out by hosting providers should be deemed to occur in the place of establishment of the service or at its business address or in the place where the computer or computers constituting the service's infrastructure are located.
>
> 68. Given, first, the state of development of the internet at the time Directive 95/46 was drawn up and, second, the absence, in Chapter IV, of criteria applicable to use of the internet, one cannot presume that the Community legislature intended the expression 'transfer [of data] to a third country' to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them.
>
> 69. If Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet.
>
> 70. Accordingly, it must be concluded that Article 25 of Directive 95/46 is to be interpreted as meaning that operations such as those carried out by Mrs Lindqvist do not as such constitute a 'transfer [of data] to a third country'. It is thus unnecessary to investigate whether an individual from a third country has accessed the internet page concerned or whether the server of that hosting service is physically in a third country.

The Schrems II decision do not discuss the Bodil Lindqvist case and it is not mentioned in the recommendations. I guess we must consider that NBA, CIA and FBI, as well as other such services all over the world, often use public data from internet when they make profiles. Still, this is not considered to be a transfer of personal data to the USA if the servers are in Europe. The Bodil Lindqvist case shows how the principle of proportionality works. If we think that this Court case is still valid, then we also must consider that there exists a good access to personal data for different kind of agencies in third countries today. That is something we must live with, if we think that "freedom of expression and information" is important (se recital 4 cited above). It would be very interesting if the recommendation also dealt with different aspects of the Bodil Lindqvist case.

What the Court investigated

The Court investigated a very special transfer, i.e., '"bulk" collection of data:

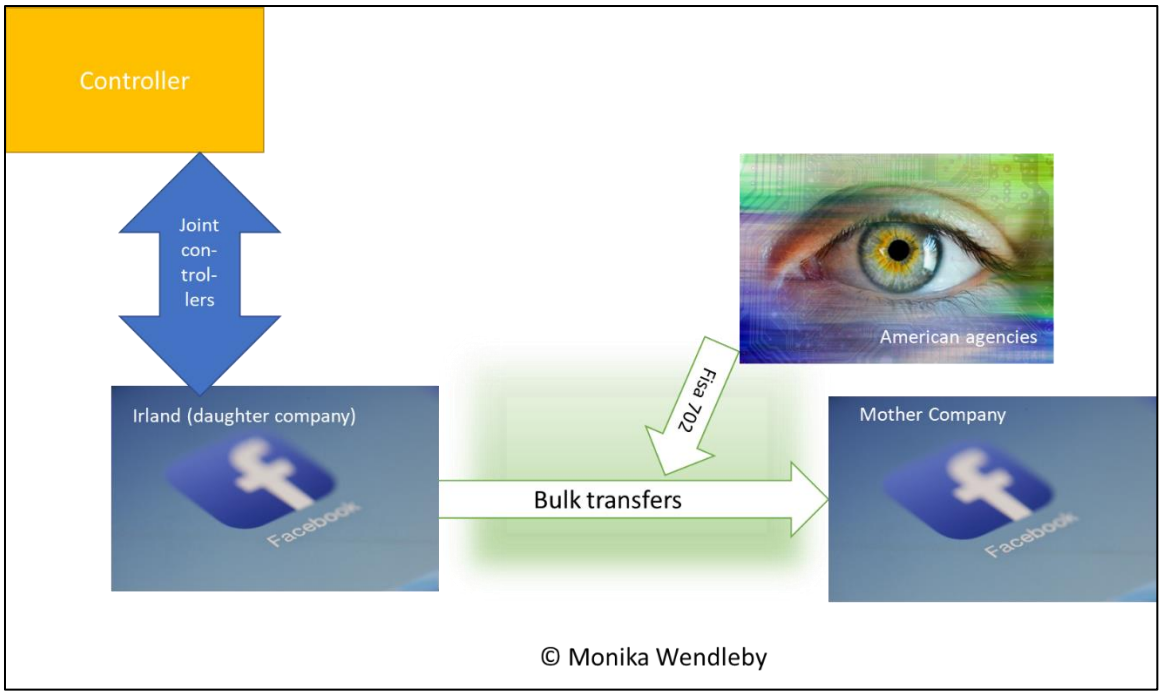
[1] Case C-101/01,

> 183. It should be added that PPD-28… allows for '"bulk" collection … of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target … to focus the collection', as stated in a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision. That possibility, which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data.
>
> 184. It follows therefore that neither Section 702 of the FISA, nor E.O. 12333, read in conjunction with PPD-28, correlates to the minimum safeguards resulting, under EU law, from the principle of proportionality, with the consequence that the surveillance programmes based on those provisions cannot be regarded as limited to what is strictly necessary.
>
> 185. In those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter.

The Court has not tried other handling of American agencies than the "bulk transfers". It has not addressed the question of a more targeted collection, for example collection after an American Agency gets data after an American Court has ruled in a specific case concerned a described individuals' criminal behaviour and issued a warrant (warrant situations). In the bulk transfer situation, there is an overwhelming risk that a lot of data concerning "innocent" people is collected and there are no real judicial safeguards when it comes to protection of individuals. In the "warrant situations" on the other hand the safeguards are better. In the "bulk-situations" a very large group of individuals are affected, in the "warrant situation" it is probably only a few individuals that are affected. I guess that the Court will consider all this (the risk for the individuals in a "warrant-situation" case) when it tests the principle of proportionality. It would be very useful if the "warrant situation" also could be commented in the recommendation (how the EDPB has considered the principle of proportionality). None of us know today how a "warrant situation" would be handled by the Court. Therefore, maybe there is a need to be more careful of what is recommended. It would also be extremely useful to get information of when EPDB considers it can be a question of "bulk transfers": which types of services must obey to FISA 702, E.O. 12333 and PPD-28?

Joint controllers

The Schrems II ruling deals with transfers between two Facebook-companies (a mother and a daughter company). Therefore, it is of course interesting to investigate the boundaries of joint controllership since the recommendation puts a lot of burden on controllers in such situations. The situation could be illustrated in the following way:



Here, I think it would be very useful if the EDPB analyses the situation from different Court Cases dealing with joint controllership (and identifies in which situations a controller, see the yellow figure in the picture, has a responsibility). The transfer the Court investigated took place in the green area in the picture, but the recommendation deals with relations outside this area. I think we all must bear in mind that the case only dealt with two kind of controllers (the Facebook-companies and the American agencies), but the recommendation is much wider.

In the Fashion ID case[2] the Court stated (I highlighted interesting parts in blue colour):

> 76. In view of that information, it should be pointed out that the operations involving the processing of personal data in respect of which Fashion ID is capable of determining, jointly with Facebook Ireland, the purposes and means are, for the purposes of the definition of the concept of 'processing of personal data' in Article 2(b) of Directive 95/46, the collection and disclosure by transmission of the personal data of visitors to its website. By contrast, in the light of that information, it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, meaning that Fashion ID cannot be considered to be a controller in respect of those operations within the meaning of Article 2(d).
>
> 77. With regard to the means used for the purposes of the collection and disclosure by transmission of certain personal data of visitors to its website, it is apparent from paragraph 75 above that Fashion ID appears to have embedded on its website the Facebook 'Like' button made available to website operators by Facebook Ireland while fully aware of the fact that it serves as a tool for the collection and disclosure by transmission of the personal data of visitors to that website, regardless of whether or not the visitors are members of the social network Facebook.

[2] Case C-40/17.

> 78 Moreover, by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without that plugin.
>
> 79 In these circumstances, and subject to the investigations that it is for the referring court to carry out in this respect, it must be concluded that Facebook Ireland and Fashion ID determine jointly the means at the origin of the operations involving the collection and disclosure by transmission of the personal data of visitors to Fashion ID's website.

I would be useful if the EPPB can clarify if (and if so how) a joint controller (like Fashion ID) can be responsible for the transfer of data that Facebook Ireland does to its mother company. Maybe, you could say that a controller in the yellow figure in the picture (like Fashion ID) that interacts with Facebook in the way that is described in the case must know that it will lead to a bulk transfer that may give American agencies (other controllers) information. Since this is a longer chain (a chain leading to a controller that uses a "like button" provided by Facebook also will be in a joint controller relationship with American agencies) than the Court tried in the Schrems II case is it important to understand the arguments. If I compare with the EDPB: s own analysis in another document[3] is it not easy to see that the analysis are uniform:

> 48. Article 26 GDPR, which reflects the definition in Article 4 (7) GDPR, provides that "[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers." In broad terms, joint controllership exists with regard to a specific processing activity when different parties determine jointly the purpose and means of this processing activity. Therefore, assessing the existence of joint controllers requires examining whether the determination of purposes and means that characterize a controller are decided by more than one party. "Jointly" must be interpreted as meaning "together with" or "not alone", in different forms and combinations, as explained below.
>
> 49. The assessment of joint controllership should be carried out on a factual, rather than a formal, analysis of the actual influence on the purposes and means of the processing. All existing or envisaged arrangements should be checked against the factual circumstances regarding the relationship between the parties. A merely formal criterion would not be sufficient for at least two reasons: in some cases, the formal appointment of a joint controller - laid down for example by law or in a contract - would be absent; in other cases, it may be that the formal appointment does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to "determine" the purposes and means of the processing.
>
> 50. Not all processing operations involving several entities give rise to joint controllership. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. More specifically, joint participation needs to include the determination of purposes on the one hand and the determination of means on the

[3] Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0 Adopted on 02 September 2020

> other hand. If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue.

Here is it also interesting to note what the Court said in the Wirtshaftsakademie case[4]:

> 35. While the mere fact of making use of a social network such as Facebook does not make a Facebook user a controller jointly responsible for the processing of personal data by that network, it must be stated, on the other hand, that the administrator of a fan page hosted on Facebook, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page, whether or not that person has a Facebook account.
>
> ---
>
> 43. However, it should be pointed out, as the Advocate General observes in points 75 and 76 of his Opinion, that the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.

The problem to define a processor

It is not easy always to decide if it is a question of joint controllership or a controller-processor situation. In the recommendations there is a lot written about cloud providers. I often hear that this is a controller-processor relationship. Though, it is not uncommon that the provider has its own purposes and means (for example Microsoft states that it is a controller when it comes to Bing but a processor in other relations). Can an actor (like Microsoft) be both a controller and processor in the same relationship? It would be very useful to get an analysis of this considering the questions I have raised above.

The problem with analysis of country information

In the recommendation a heavy burden is put on the processors: they must investigate the legal situation in different third countries and make correct assessments of that information. To assess other countries legal systems has a lot of methodological problems (how do you know that a source describes the whole area and that the source is updated). I think it could be useful if EDPB learned some about this from another agency, European Asylum Support Office, who has dealt with similar questions for a long time. It would also be useful if the EPDB created a country information portal. Ministries of foreign affairs often have a good knowledge about the situation from reports written by their Embassies (especially if the embassies understand that it is important to report back on such matters). Such information together with the sources EDPB mentions in the draft could be parts of such a portal.

[4] Case C-210/16.