Some comments on EDPS Guidelines on the concepts of controller, processer and joint controllership

The document is informative and clear on most topics. There are some subjects though that are not so clear that maybe should be reconsidered or at least better explained.

"Natural or legal person, public authority, agency or other body"

There is need to clarify the blue parts of para 17. Can these categories be processors and risk sanctions (article 83). In which situations?

> 17. The first building block relates to the type of entity that can be a controller. Under the GDPR, a controller can be "*a natural or legal person, public authority, agency or other body*". This means that, in principle, there is no limitation as to the type of entity that may assume the role of a controller. It might be an organisation, but it might also be an individual or a group of individuals.[7] In practice, however, it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller within the meaning of the GDPR. As far as data processing within a company group is concerned, special attention must be paid to the question of whether an establishment acts as a controller or processor, e.g. when processing data on behalf of the parent company.

Obligations under article 26

In the guideline you can read the following:

> 163. In this perspective, the compliance measures and related obligations joint controllers should consider when determining their respective responsibilities, in addition to those specifically referred in Article
> 26(1), include amongst others without limitation:
> - Implementation of general data protection principles (Article 5)
> - Legal basis of the processing[56] (Article 6)
> - Security measures (Article 32)
> - Notification of a personal data breach to the supervisory authority and to the data subject[5] (Articles 33 and 34)
> - Data Protection Impact Assessments (Articles 35 and 36)
> - The use of a processor (Article 28)
> - Transfers of data to third countries (Chapter V)
> - Organisation of contact with data subjects and supervisory authorities

Although I can see the point for this in some relationships it will be a lot of joint controlling situations where this will be complicated (and not add any extra value to the data subjects). The blue colored points above are not clear when you read the wording of the Article (it looks more like Article 28 demands to me). You have a lot of examples in the guideline; is all this really necessary to consider all this in all the example situations? Note that there might not be a contract between parties that are joint controllers. I think this part could be a recommendation, but the wording "should" goes further than the wording of Article 26 of GDPR (it will also be a problem when you apply Article 83). Some of the bullet points above is not suitable to inform data subjects about (security issues) and since Article 26 mentions Article 13-14 and not Article 28 this is a bit strange.

Example: Travel agency

I have a question about this example:

> A travel agency sends personal data of its customers to the airline and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. Each of the actors processes the data for carrying out their own activities and using their own means. In this case, the travel agency, the airline and the hotel are three different data controllers processing the data for their own purposes and there is no joint controllership.
>
> The travel agency, the hotel chain and the airline then decide to participate jointly in setting up an internet-based common platform for the common purpose of providing package travel deals. They agree on the essential means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out joint marketing actions. In this case, the travel agency, the airline and the hotel chain, jointly determine why and how personal data of their respective customers are processed and will therefore be joint controllers with regard to the processing operations relating to the common internet-based booking platform and the joint marketing actions. However, each of them would still retain sole control with regard to other processing activities outside the internetbased common platform.

Why is it not a convergent decision in the first paragraph above? They have a joint purpose: to make arrangement from a travel package which they all profit from. I guess that they use the same way to communicate about the arrangements, probably e-mails (which is a mean I guess?). Maybe the three parties have not agreed formally on this but they all have used e-mails for communications for years. If you compare to some of the CJEU-cases there were no formal agreement about methods to process data (means) but the court still said that there were Article 26-situations? Note that you in para 54 say: "*For example, in Jehovah's Witnesses, the CJEU considered that a religious community must be considered a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching. The CJEU considered that it was not necessary that the community had access to the data in question, or to establish that that community had given its members written guidelines or* instructions in relation to the data processing." The cooperation in this case seem to be much more vague than the cooperation between the travel agencies?