1. The obligation for data exporters and importers to assess whether surveillance measures allowing access to personal data by public authorities in a third country can be regarded as a justifiable interference or not is for most companies impossible to comply with. They don't have the legal knowledge, time or budget for outside counsel advice. The EU Commission must conduct and publish the results of these assessments for the key trading partners of the EU that don't have an adequacy decision yet, such as the US, China, Russia and Turkey. Such an assessment is more limited than a review whether the data protection laws of a third country provide "adequate protection", meaning this task can be accomplished in the next few months.

2. Recommendations para. 42: it is unclear why experience in the past relating to access to personal data by public authorities (or the fact that this over a period of years never took place) can't be accepted as an element for assessing the risks of a data transfer to a country that does not provide essentially equivalent protection. In practice certain US based service providers for processing employee data may not have received any access requests of US public authorities in the last five years. Why can't this be taken into account?

3. Recommendations para. 49: the nature of the data may influence what supplementary measures must be taken. The EDPB should in that regard provide some examples. Can indeed data exporters make a distinction between the level of sensitivity of the personal data that is transferred when requiring additional security measures? For example, transferring contact details of 100 European employees to an HR service provider in the US or transferring critical health information of a large group of patients. In that regard, article 32 of the GDPR takes a realistic approach: "Taking into account the state of the art, the costs of implementation and 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, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (…)".

4. Recommendations para. 88-91: the use cases 6 and 7 describe a cloud services provider or a group of companies that may need to access personal data in a readable format. In these scenarios the EDPB is of the opinion that no data transfers can take place. This conclusion is excessive and does not factor in the sensitivity of the personal data and any detriment an access request by public authorities could cause to the data subjects. Most service providers will (exceptionally) need to access personal data in readable format for technical support or for trouble shooting. Prohibiting the use of such service providers when the encryption is not completely under the control of the data exporter, will cause huge practical challenges for many business processes that rely on such services. EU companies could no longer use the services of US companies like Amazon, Google or Microsoft. For many use cases there are no EU service providers that provide competing services. When EU companies don't have an alternative, this would lead to the risk that EU companies would ignore the Recommendations altogether.