**Guidelines 07/2020 on the concepts of controller and processor in the GDPR**

**Version 1.01**

| *Feedback number* | **Paragraph number** | **Feedback** |
|---|---|---|
| *1* | 17 | The useful recall that natural persons can also be controller should be better reflected across the whole guidelines. May be using the term "company" should be avoided and replaced by a broader term (any legal or natural person? Any individual or organisation?) |
| *2* | 22 and subs, Example boxes. | Examples contained in the various boxes are very useful. Having more and complex examples addressing AML/KYC or anti-tax evasion matters would be of great help for individuals and organisations considering the scope of application of these legislations, their critical nature and the numerous personal data that are therefore collected, processed, stored and even shared and the fact that support from external service providers (software providers, banks…) is often required or put in place to assist individuals and organisations having to comply therewith. As an example, a challenge that often occurs relates to the fact that identification documents from some jurisdictions contain sensitive data such as the religion (not needed for AML/KYC purposes) and one could argue that altering the document to hide these data be forgery |
| *3* | 27 | This clarification is welcome and worth stressing in these guidelines, considering negotiation process of GPRD related contractual provisions |
| *4* | 38 and 53 | The choice of software (or a SAS model) can have significant consequences on so-called "essential means" of the processing and may lead to a significant number of scenarii where the SAS/software providers and the user end up being joint controllers. Providing some guidance in this respect would be useful in light, for example, of the European Digital pack.<br>Section of the guidance relating to joint controllers could also contain more examples, some of them focussing on the digitalisation and software/IT developments and implications and being aligned with EU current initiatives in this area. |
| *5* | 61to 66 | As mentioned just above, practionners would appreciate clarifications or examples showing how the concept of joint controllers can apply in the world of software or platforms development, hosting and licensing… |
| *6* | 70 | Considering the high likelihood nowadays of having several chains of operations, a significant and practical challenge is to determine how far to go in detailing a chain of operations and processing while trying to have a right balance in place between the right to privacy and data protection and the right to still be able to do business. It would be very useful if the EDPB could provide guidance in this respect. |

| | | |
|---|---|---|
| *7* | 78 | As the concept of "delegation " is to be interpreted by reference to European legal terminology and in the absence of definition of this term in GDPR, it would be useful if the EDPD could make here reference to the European legal definition of the term "delegation" it is referring to here (this would facilitate shared European understanding of this concept and therefore compliance). |
| *8* | 79 | Considering the increased use of artificial intelligence and the challenges associated to their use of various types of data (often for marketing or political campaigns), it would be useful to give an example reflecting on the GDPR implications of the use by marketing companies/promotional platforms or software providers of the personal data they collect from clients/users |
| *9* | 82 | Having an example referring to cloud service provider is useful. It could also be useful to broaden the approach to capture clouds, software providers and users, as this is the case for various IT tools (https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html) and to make a distinction between customisable tools or non-customisable IT tools in order to raise awareness as to the need to ensure proper technical set up of any such tool. |
| *10* | 86 | This clarification is welcome and should be extended to capture cases where the controller is a natural person and has nevertheless someone under his/her authority: for example, a doctor or dentist who has an assistant with an employment contract. |
| *12* | 93 | This clarification is useful. By using a terminology frequently used in other sectors and especially in the financial and banking related regulations and guidance (i.e. performance of initial and ongoing due diligence on processors), it may be even clearer for practionners. |
| *13* | 103 | Useful proposal especially for small to medium size companies |
| *14* | 107 | Unfortunately, imbalance of powers between the parties can often not be sorted out by opting for a different service provider due to the lack of fully GDPR compliant options available on the market and the need for European companies to remain alive and competitive. It would therefore be appreciated if the EDPB could offer some guidance to address cases where no alternative options are available, leading to a conflict between fundamental rights and European principles so as to also enable fair competition and the need to perform proper risk assessment and checks of technical safeguards to be added.<br><br>Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services recently which recently enter into force could probably be mentioned here. |

| | | |
|---|---|---|
| *15* | 113 and subs. | EDPB clarifications and details are welcome. They could further take into account the fact that GDPR provisions will often be part of a more global agreement and some general clauses of this agreement may also be relevant to data protection matters, especially with regards to the process in place for providing instructions to the co-contractor, and be sufficient as long as general principles on hierarchy between conflicting legal provisions are kept in mind. |
| *16* | 120 | It could be useful to also clarify here the status of legal representatives/proxyholder whose mandate may also enable them to process personal data |
| *17* | 123 and 124 | While a controller must retain adequate control and oversight here, opting for a detailed approach may be counterproductive considering potential imbalance in terms of IT expertise here, especially with respect to outsourcing of cybersecurity, infrastructure or software…as well as regular evolution in terms of security standards and good practice. In addition, appendix to an agreement should not be the only option. Service level agreement and key performance indicators could also be used. |
| *18* | 158 and subs. | Some guidance and examples to address cases where there are case several joint controllers would be useful (may be again examples from the IT world such as software development). |
| *19* | 177 to 179 | Providing an illustrative example could be useful here |