DIGITALEUROPE

19 OCTOBER 2020

Response to EDPB consultation on draft Guidelines on the concepts of controller and processor

Executive summary

The concepts of controller and processor are central to a correct application of the General Data Protection Regulation (GDPR).[1] In efficiently allocating responsibilities along the personal data processing value chain, these concepts can ensure effective protection for data subjects' rights.

We welcome the European Data Protection Board's (EDPB) draft Guidelines on these foundational GDPR notions. In particular, we appreciate the EDPB's process of stakeholder engagement well ahead of publication as well as the draft Guidelines' reference to existing case law and abundance of examples.

The question as to what extent an entity can be considered a controller or processor remains one of the key issues that still arise in the real world, leaving practitioners often unsure about their determinations. The importance of these foundational concepts, therefore, might require more examples than currently provided.

In our submission, we highlight:

- The need to better delineate the distinction between essential and non-essential means of processing;
- The importance of contracts in allocating roles and responsibilities, which includes the use of standard terms and flexibility in determining changes to security measures or sub-processors;
- The need to improve the final Guidelines with respect to group relationships;

[1] Regulation (EU) 2016/679

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

- The unclear characterisation of joint controllership as opposed to separate controllership or controller-processor relationships; and
- The need to expand the guidance to cover what controller obligations can be triggered in relation to the processor's legal obligations.

Table of contents

Broad vs functional interpretation

The draft Guidelines' general observations conclude stating that 'the concept of "controller" [and arguably that of "joint controller"] should be interpreted in a sufficiently broad way so as to ensure full effect of EU data protection law, to avoid lacunae and to prevent possible circumvention of the rules.'[2] This reflects the previous Opinion from the Article 29 Working Party (WP29), whose main goal seems to have been that of allocating responsibility so that compliance with data protection law could 'be sufficiently ensured in practice.'[3]

We note that the need to determine separate or joint control was stronger under Directive 95/46/EC, as such finding was necessary for enforcement. However, the GDPR has altered the context for such need largely as a function of the additional responsibilities and liability placed on processors.

We therefore suggest that the reference to a 'broad' interpretation of controllership is somewhat misguided and might be ineffective from the point of view of the actual protection of data subjects. Rather, as highlighted elsewhere in the draft Guidelines, the concepts of 'controller' and 'processor' should be interpreted in a strictly functional manner.

Controller-processor relationship

Essential vs non-essential means

The final Guidelines could contemplate a more realistic assessment of what can count as 'non-essential' means of processing.

For example, the accountants example at para. 39 lists 'how long the data shall be kept and what technical means to use' as essential elements pertaining to the controller's determination.[4] However, retention periods and essential technical means such as security measures can often be off-the-shelf elements of a processor service. This, in turn, does not necessarily imply that the controller cannot be qualified as such or that the processor must be qualified as joint or separate controller in its own right just because of these elements.[5]

Similarly, the example of hosting services in the same para., stating that the controller must provide instructions as to 'which technical and organisational

[2] Para. 14, p. 9 of the draft Guidelines.

[3] P. 1, WP29 Opinion 1/2010 on the concepts of 'controller' and 'processor.'

[4] P. 14 of the draft Guidelines.

[5] This is in line with para. 107, p. 32 ibid.

security measures are required,'[6] seems to contradict para. 124 of the draft Guidelines, which states that 'the controller may describe the minimum security objectives to be achieved, while requesting the processor to propose implementation of specific security measures.'[7]

Among the reasons why controllers may elect to outsource processing to a processor is precisely the processor's technical and security capabilities. In practice, standard security measures offered by processors may suffice to meet most controllers' processing needs, and might hence not qualify as an 'essential' means in determining controllership. Again, this does not turn the processor into a joint or separate controller.

We note that Art. 32 GDPR refers to both the controller and the processor as to the implementation of appropriate technical and organisational measures, suggesting that the delineation of such responsibility can be left to the parties, without this modifying their respective roles, so long as the substantive obligation is met in line with the stipulations under contract or other legal act pursuant to Art. 28(3)(c) GDPR.

Contracts

The draft Guidelines find that the 'GDPR imposes direct obligations upon processors, including the duty to assist the controller in ensuring compliance.'[8] However, it is important to note that Art. 28(3) GDPR does not create statutory obligations but rather makes the processor's obligations subject to a contract to be concluded with the controller or to a legal act. We urge the EDPB to better reflect this in the final Guidelines.

Compared to Directive 95/46/EC, the GDPR has largely shifted towards incentivising the parties themselves to lay out their respective roles and responsibilities in contracts. We believe that in most circumstances such contractual arrangements will reflect the factual circumstances around the processing at hand and serve as an essential tool to ensure both compliance on the part of controllers/processors and effective protection for data subjects. From this perspective, the final Guidelines could expand on what circumstances might lead DPAs to override the contractual arrangements thus reached.

Contract negotiations centrally revolve around defining clear tasks of the parties, as separate or joint controllers or processors; as in any other contract, such tasks determine responsibilities and liability. Because of the cost potentially associated

[6] P. 15, ibid.

[7] P. 35 ibid.

[8] Para. 91, p. 29 ibid.

with liability in relation to data subject rights and particularly data breaches, we observe the following two trends in contracting practices:

- Parties often try to pass on liability by negotiating a role (as processor or separate/joint controller) and subsequently attaching tasks or responsibilities to such role that may not actually fall within it; and
- The concept of joint controllership is rarely used because of the negotiations required to allocate responsibilities. Moreover, our experience indicates that parties only rarely determine the purposes and means of processing jointly.

Standard terms

A key aspect of the controller-processor relationship is to what extent the controller has to oversee the processor. While the draft Guidelines suggest in many instances heavy obligations in this respect, many companies – in particular SMEs – are in practice not willing nor able to implement complex supervision mechanisms such as audits, for which they may have to hire third-party providers. Standard terms play an important role in this respect and it is therefore important that their use not be unduly restricted.

We welcome para. 107 of the draft Guidelines, which clarifies that standard contractual terms or 'imbalances' of contractual power do not in themselves impact the controller-processor classification.

In line with this, we believe the requirement in the draft Guidelines for controllers 'to be able to request changes if necessary'[9] appears to unnecessarily limit controllers' ability to rely on off-the-shelf processor services, for which accommodating change requests from multiple individual controllers would be overly burdensome or expensive, if not outright impossible. In addition, it must be considered that renegotiating the relevant contract following the controller's requested changes could in essence change the scope of the processing service provided, requiring the processor to assess the request's technical and economic viability, which in turn may lead to a necessary price adjustment.

Similarly, processors may need autonomy to change standard elements of the service, which should be allowed as long as the scope of the processing service provided does not change and the controller chooses to accept those terms. For example, processors should be able to change security measures and other standard terms as long as the controller has given permission in the agreement and the changes are compliant with the general instructions under the agreement and the applicable laws. It should also be considered that such changes may

[9] Paras 28 and 82 ibid. We note that para. 28 uses 'and,' while para. 82 provides more flexibility by using 'and/or.'

consist in security updates that the controller will expect and may not always require the controller's approval, provided that they do not result in the degradation of the overall security of the service. From this perspective, the general requirement in para. 123 of the draft Guidelines to obtain the controller's approval before any changes to security measures appears to go beyond the requirements in Art. 28(3)(c).

More broadly, where a controller has agreed through the contract that a processor may update or modify certain aspects of the processing activities, then it should be possible for processors to publish changes to data protection terms as long as controllers are properly notified, e.g. via an internal portal or other similar channels. In addition, it should be clear that the controller's silence can be interpreted as approval.

Finally, para 137 of the draft Guidelines provides that controllers should always be able to reverse the option to have the data deleted or returned upon termination so long as such choice is made before the processing service provision ends. Again, such requirement appears to go beyond Art. 28(3)(g). A choice may not always be feasible in the case of off-the-shelf processor services. This, however, does not preclude the controller from making an informed choice.

Sub-processors

The final Guidelines could provide more clarity on the requirement to actively inform controllers about new sub-processors. For instance, it should be possible for processors to notify controllers by updating a list of sub-processors as long as the changes are clearly identified in the document. We believe that footnote 46 could be included in the body of the final Guidelines. Alternatively, we believe the final Guidelines could clarify that processors can inform controllers of such updates via an internal portal or similar channels.

The requirement in para. 152 of the draft Guidelines to include a list of sub-processors in general-authorisation contracts should instead be restricted to specific authorisation. In case of general authorisation, the criteria to guide the processor's choice of sub-processors should suffice.

Contracts and other mechanisms

Para. 111 of the draft Guidelines requires the contract to set out the controller's obligation 'to provide and document, in writing, any instruction bearing on the processing of data by the processor.'[10]

[10] Pp. 33-34 ibid. See also para. 115 to the same effect ('any written form').

We urge the EDPB to acknowledge in the final Guidelines that instructions need not necessarily be put in a human-readable text or words. On the contrary, controllers – much like data subjects – may use technical signals, such as user interfaces or APIs, to instruct the processor to process data in a certain way. Those instructions are normally documented through a digital log entry or other similar mechanisms.

Groups

We believe the final Guidelines could expand on data processing activities within company groups. Determining the different roles in a group context is particularly challenging, and more concrete guidance would be welcome.

For example, employing entities within a group that are each using a shared system for employment-related data may be acting, depending on the relevant processing purposes, as separate controllers, joint controllers or processors on behalf of each other. Similarly, contrary to what the draft Guidelines suggest,[11] matters such as retention are likely to be decided at group level rather than at the level of each company in a group, in particular if data is managed in centralised databases.

Joint controllers

Although we appreciate the draft Guidelines' effort to reference past case law,[12] we find the analysis of joint controllership to be overall unclear.

The draft Guidelines, in particular, outline the concept of 'converging decisions' to arrive at a determination of joint controllership.[13] Such concept is ambiguous and may lead to situations where entities that are mutually unaware of, and have not coordinated, each other's purposes can be found to be joint controllers and hence be liable for not meeting the specific legal obligations related to such relationship, i.e. drafting an arrangement concerning their respective responsibilities pursuant to Art. 26 GDPR.

In addition, a controller and processor working together will more likely than not have common business interests that will have an impact on the way the processing is carried out. This does not necessarily indicate that decisions on the purposes of processing are made jointly or 'converging.'

---

[11] Para. 69, p. 23 ibid.

[12] Notably cases C-210/16, C-25/17 and C-40/17.

[13] See in particular para. 53 of the draft Guidelines.

Similarly, paras 62-63 of the draft Guidelines appear to imply that a controller's selection of 'platforms, standardised tools or other infrastructure' as processor more likely than not makes the latter a joint controller. The use of a tool should not be the central element to assess the existence of joint controllership. Instead, the final Guidelines should provide more clarity as to how and to what extent purposes and means are jointly determined.[14]

Furthermore, there are numerous scenarios where independent controllers process the same data still requiring an intervention from other parties. APIs are one such example, whereby a controller can pull data from another. For this to happen, the latter controller must make the API available, thus making performance of the other controller's processing incumbent upon its intervention.[15]

The benefit of referring to joint controllership based on unclearly defined 'converging decisions' or the existence of standardised tools such as APIs is not evident compared to a possible alternative finding of separate controllership or controller-processor relationship, in particular when the latter can be established with respect to other processing operations.[16]

Arrangements

Section 2.1 of the draft Guidelines draws from the use of the words 'in particular' in Art. 26(1) the consequence that other necessary elements must be covered in the arrangement between joint controllers. We believe the EDPB's intention is to highlight elements that parties may want to consider including in such agreement, and would appreciate it if it was made clearer in the final Guidelines that such elements are not mandatory.

Moreover, we find the general recommendation – tantamount to an impact assessment – to document 'the relevant factors and the internal analysis carried out in order to allocate the different obligations,' stating that such recommendation is intrinsic to the accountability principle,[17] to be clearly excessive.

---

[14] An example where the final Guidelines could further elaborate on these aspects is that of clinical trials, pp. 21-22 of the draft Guidelines. Clinical trials are complex when it comes to the roles of controller, joint controller and processor, and who qualifies as what will be heavily dependent on, among other things, the setup of the study and how early on the study is taking place. The final Guidelines, therefore, could benefit from more detail regarding the described scenarios.

[15] See para. 66, p. 20 of the draft Guidelines.

[16] See para. 55, pp. 18-19 ibid.

[17] Para. 165, p. 42 ibid.

DPA enforcement

Similar observations as to contractual arrangements between controllers and processors could be made with respect to arrangements between joint controllers.

We believe that in most circumstances where joint controllers identify each other through an explicit arrangement,[18] such arrangement will reflect the factual circumstances around the processing at hand and serve as an essential tool to ensure both compliance on the part of joint controllers and effective protection for data subjects. From this perspective, the final Guidelines could expand on what circumstances might lead DPAs to override the arrangements thus reached.

In addition, we are concerned that paras 188-189 of the draft Guidelines could lead to inconsistent interpretations and enforcement decisions by different data protection authorities (DPAs). This may include situations where the lead DPA for one of the joint controllers may unilaterally extend its enforcement to a joint controller for which it is not the lead DPA. We believe the final Guidelines should address this possibility and highlight the use of the GDPR's consistency mechanism.

Data subject requests

Para. 187 of the draft Guideline states that '[r]equiring data subjects to contact the designated contact point or the controller in charge would impose an excessive burden on the data subject that would be contrary to the objective of facilitating the exercise of their rights.'[19]

While we appreciate the EDPB's intention to facilitate the exercise of data subjects' rights, it is not clear to us why directing data subjects to the appropriate contact point or controller would inherently be disproportionate for the data subject. On the contrary, depending on the circumstances around the processing, having access to a single and clear point of contact might be the best way to ensure effective protection.

For instance, it appears perfectly logical for a joint controller to connect the data subject to the contact point or the controller in charge via email or other similar channels where the latter is in a better position and has the technical means to fulfil the data subject's request.

---

[18] We have referred above to the fact that we find such possibility to be rarely used in actual negotiations, see p. 5 of our response.

[19] P. 45 of the draft Guidelines.

Legal obligations and controllership

Para. 22 of the draft Guidelines states that entities mandated by law to retain or provide data should be considered as controllers for the purpose of fulfilling such legal obligation. It must be noted that such legal obligations can be incumbent upon processors, who may be compelled (e.g. in the area of criminal tax law) to disclose personal data they process on behalf of controllers or to retain all or part of the data to evidence compliance with its own legal duties, e.g. commercial law or sectorial legal duties.

Such finding has important compliance repercussions for the processor-now-turned-controller, who would be required to carry out all controller obligations with respect to the specific processing activities related to such legal obligation.

The final Guidelines could acknowledge this type of situations and provide guidance on what controller obligations can be triggered in relation to the processor's legal obligations.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell

Privacy and Security Policy Officer

martin.bell@digitaleurope.org / +32 492 58 12 80

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK