Request for clarification of non-obligations for joint controllers

1: Introduction

We welcome the clarifications provided in the EDPB's recent *'Guidelines 07/2020 on the concepts of controller and processor in the GDPR'*, with their importance for the continued development of Europe's data-aware market and the conservation of its citizens' rights. The guidelines state that an important objective is that the "concept of '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."[1] In the case of joint controllers, one would expect this broad interpretation of control to come with associated limits to the controllers' obligations. The guidelines do suggest such limits by stating that the "level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case"[2]. This commentary requests clarifications on the implications of these differing levels of responsibility.

A recurring example in this commentary is that of two companies X and Y, who wish to temporarily share personal data they control with a third-party Z for some joint purpose. The example used, though many others are relevant, is of a blood pressure monitoring company (X) and a hospital (Y). Both X and Y wish to assess how blood pressure changes are predictive of a disease. To protect the data subjects' privacy, X and Y both refuse to share their data directly with the other for analysis. By sharing instead with a third party, Company Z, and requiring that the data is subsequently deleted, privacy is preserved while the benefits of building such a predictive model are still realised. New technical advances, such as federated learning, could enable similar results without the intermediary company, Z; but, except for Section 5, the commentary will focus on the example as given for simplicity.

We assume that each company has separately decided to collect the data relevant to their part, they separately determine the length of time such data is stored, and separately obtain their customers' consent or other suitable legal basis for the data collection. Until they share their respective data with company Z for joint purposes, they are separate controllers. When they share the data for their joint purpose, the guidance would suggest that they may become joint controllers for the period that the collaboration lasts. The status of company Z will depend on its exact role, and Section 5 will request some clarifications on this in different situations. It is assumed here that the output of the collaboration holds no personal data, since it is simply a model of the relationship between X and Y's respective data sets.

Having a suitable legal framework facilitating the sharing of such data in a privacy sensitive way is vitally important for ensuring competition in the European market. Without such a framework, there is a risk that companies will never share the benefits of their data. This has two important implications. First, customers are likely to lose out on the potential benefits of data. Secondly, because the accuracy of machine learning models increases with data set size and number of relevant features, many industries are likely to end up with a few incumbants with natural monopolies. This could have large impacts on citizens' freedoms

[1] Paragraph 14

[2] Paragraph 56

and our hope is that suitable mechanisms can be found for inhibiting this tendency towards monopoly. Privacy-sensitive and reciprocal data sharing provides one such mechanism for industries to protect against monopoly. The aim of this commentary is to build up enough clarifications that such an enterprise can be built on a suitable legal basis.

The commentary contains four further substantive sections, each with an associated request for clarification:

- Section 2: Non-obligations for joint-controllers
- Section 3: Liability for non-obligations of joint-controllers
- Section 4: Obligations after the expiry of temporary joint-controller relationships
- Section 5: The status of Company Z

2: Non-obligations for joint-controllers

The executive summary to the guidelines suggests that a relationship of joint-control creates a joint responsibility towards data subjects. It says: “Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers”[3]. One might imagine that this leaves joint controllers jointly and severally liable for all responsibilities that are due to controllers under GDPR. However, this would contradict article 56 of the guidelines, which state that “the level of responsibility of each of them [joint-controllers] must be assessed with regard to all the relevant circumstances of the particular case.” It seems, rather, that the obligations under GDPR can be separated in such a way that a particular
joint-controller is only responsible for a subset of the GDPR’s obligations as long as all of the GDPR’s obligations are met by at least one of the joint controllers. We seek further clarification in the final Guidance that this interpretation is correct.

In the example described above, company X and company Y may be seen as becoming joint controllers when they jointly build models of the relationship between blood pressure changes and disease. In order to improve the data subjects’ privacy, the companies have enforced technical barriers so that each only has access to their subset of the subject data. These technical barriers also result in technical barriers to any individual company fulfilling all of the joint controllers’ obligations under GDPR. Company X, for example, only has the technical capability to implement the data subjects’ rights relating to the blood pressure data. Any rights relating to the disease data would have to be implemented by Company Y. Case law states that “the ‘effective control’ and the conception that the data subject has of the controller must be taken into account”[4]. In this case, the data subject’s relationship is restricted to one of the companies, and the effective control by Company X of Company Y’s data is very limited. One would expect that all obligations related to this data (the disease data) fall to Company Y. It would be helpful if the EDPB could confirm in its Guidance that, in such a situation, Company X is not responsible for the obligations relating to that portion of the data where Company Y is fulfilling the GDPR’s obligations, and similarly for Company Y with regard to Company X.

---

[3] Executive summary. Page 4, “Relationship among joint controllers”

[4] Judgment in Jehovah’s witnesses, C-25/17, ECLI:EU:C:2018:551, Paragraph 21

It would also be helpful to clarify in this situation what additional obligations, if any, Company X might be obliged to undertake should it become a joint controller for the temporary period given. The rights to be informed, of access, to rectification, to erasure, to restrict processing, to data portability, to object, and rights in relation to automated decision making and profiling are all obligations that are responsibilities of Company Y. Are there any obligations that fall to Company X in relation to this data (the disease data in this example)?

3: Liability for non-obligations of joint controllers

The guidelines note that “both controllers and processors can be fined in case of non-compliance with the obligations of the GDPR that are relevant to them”[5]. In the example given above, it would be useful to confirm that the obligations relating to data collected by Company Y are not relevant to Company X, and vice versa. In particular, Company X could not be fined for situations where Company Y does not fulfil its obligations under GDPR relating to data about diseases, even though Company X and Company Y may be joint controllers of the data.

4: Obligations after the expiry of temporary joint-controller relationships

In the envisioned example, if Company X and Company Y become joint controllers for the period of time that they engage in their shared activity, it would seem that their obligations as joint-controllers under GDPR expire once the joint effort is completed, and at that point the two companies are simply individual controllers of the data that they each have. Can the EDPB provide greater clarity as to what obligations, if any, remain after the expiry of the joint controllership?

5: The status of Company Z

Company Z sits between the other two companies in the example, enabling them to cooperatively produce shared benefits. Its status under GDPR will depend on its exact role in the collaboration. This section aims to confirm the status in three potential situations.

In its most active role, Company Z may have initiated the project between Companies X and Y and formulated the structure for data sharing. An example would be if Company Z was itself developing research on the relationship between blood pressure and disease and decided to ask Companies X and Y to support the research. Company Z would appear to be “determining the means and processing of the data” and so would appear to be a joint controller. More specifically, it would appear that Company X and Company Z are joint controllers of the data managed by company X, and separately Company Y and Company Z are joint controllers of the data managed by company Y, with Company X and Company Y not joint controllers of each other’s data. These statuses are however only temporary and so

[5] Paragraph 9

it would be helpful to understand if there are any obligations remaining on Company Z after it has deleted all private data.

A less active role for Company Z would occur if it was simply asked by one of the others to do this research. In this case Company X and Y may have “determined the means and purposes of the processing” and so Company Z is potentially properly considered a processor. This would seemingly continue to be the case, even if Company Z was given some professional lee-way in exploring different models of the relationships between the datasets. Again, it would be helpful to understand if there are any obligations remaining on Company Z after it has deleted all private data.

Company Z could also play a role which is even less active if new technologies, such as federated learning, are used. Federated learning is a collection of new technologies that provide methods to build shared machine learning models of data, while enforcing privacy and separation of control of the data. In this case, Company Z could simply be acting as a messaging system between the other two companies, with all data transferred between Company X and Y in an encrypted way. In this situation it appears that Company Z is not even a processor, since it is only acting to transport encrypted data between the other two.

Conclusion:

Through this commentary, we hope to clarify some non-obligations in the case of joint-controller relationships, as well as limitations to an individual joint controller’s liability. We believe that these clarifications will have important implications for building a strong legal framework on which the benefits of large data could be achieved in a privacy sensitive way. This in turn would improve the competitiveness of the European market, reduce the risk of data monopolies and increase the freedoms of Europe’s citizens.

About the author:

Blaise Thomson is the CEO of Bitfount, a UK-based SME helping industries benefit from shared data in a privacy-preserving way, Director at Alfa IQ, a Joint Venture with FTSE-listed Alfa Financial Systems, and Honorary Fellow at Judge Business School, Cambridge University. Prior to Bitfount, Blaise led the Apple engineering office in Cambridge, UK, was the Co-Founder of Vocal IQ, and was a Research Fellow in Artificial Intelligence at Cambridge University. Blaise is a French, British and South African citizen.

Extract of key paragraphs from the guidelines:

9. The accountability principle is directly addressed to the controller. However, some of the more specific rules are addressed to both controllers and processors, such as the rules on supervisory authorities' powers in Article 58. Both controllers and processors can be fined in case of non-compliance with the obligations of the GDPR that are relevant to them and both are directly accountable towards supervisory authorities by virtue of the obligations to maintain and provide appropriate documentation upon request, co-operate in case of an investigation and abide by administrative orders. At the same time, it should be recalled that processors must always comply with, and act only on, instructions from the controller.

14. As the underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data, the concept of '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.

45. As further elaborated in Part II, section 2, the qualification of joint controllers will mainly have consequences in terms of allocation of obligations for compliance with data protection rules and in particular with respect to the rights of individuals.

56. 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, the CJEU has clarified that those operators may be involved at different stages of that processing 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**.**

61. Joint controllership also requires that two or more entities have exerted influence over the means of the processing. This does not mean that, for joint controllership to exist, each entity involved needs in all cases to determine all of the means. Indeed, as clarified by the CJEU, different entities may be involved at different stages of that processing and to different degrees. Different joint controllers may therefore define the means of the processing to a different extent, depending on who is effectively in a position to do so.