Guide for multi-controller situations under the GDPR
Serkan Kurt LLM CIPP/E CIPM

Everyone has heard about data processing agreements, at least everyone in Europe who is somewhat familiar with the field of data protection. A data processing agreement is a fundamental document for mitigating risks when you are dealing with data processors. But what do you do when you are dealing with another data controller?

The purpose of this article is to guide the reader in situations where multiple controllers are involved in one or more related processing activities under the GDPR. This includes situations where one controller transfers personal data to another controller who then independently processes the personal data (controller-recipient relationship). It also includes so called 'joint control', this term is explained in paragraph 2.

Multi-controller situations introduce certain risks that have not been sufficiently discussed in the data protection community. This article will explain how to mitigate those risks and will discuss in particular the multi-controller agreement. A type of agreement that is, contrary to the processing agreement, unknown to many.

The following guide is intended for those with basic knowledge of European data protection laws and regulations.

1. The big picture

To understand how to deal with multi-controller situations it is important to keep in mind one fundamental purpose of European data protection laws and regulations. That purpose is to effectively protect the fundamental rights and freedoms of natural persons with regard to the processing of their personal data.¹ This purpose cannot be achieved if you cannot hold organizations and natural persons responsible for their actions. For example, if two organizations together decide to start a joint project where they process personal data, then it should not be possible for one of those organizations to hide from its responsibility behind the other. Otherwise an organization responsible for processing personal data might not feel sufficiently compelled to take into account the protection of the fundamental rights and freedoms of natural persons. It would also limit the possibilities of citizens to exercise their rights. When in doubt whether an organization or natural person is a (joint) controller and/or processor it can be helpful to have a look at the big picture. Looking at the big picture means finding out who would need to be held responsible to effectively protect the people who the GDPR aims to protect.

¹ Recitals 1-3 of the GDPR.
2. Core concepts

Before discussing multi-controller situations any further it is wise to define the concepts of a controller and a processor. Article 4 of the GDPR provides us with these definitions:

“… (7) ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; …

(8) ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; …”

Article 4 of the GDPR mentions the possibility for an entity to be a controller ‘jointly with others’. Joint control is when two or more parties jointly determine the purposes and means for a processing activity (article 26 GDPR). Joint control is a multi-controller situation.

Parties can exchange personal data without being joint controllers. For example if your organisation sells personal data to another organisation that uses it for their marketing. In this case both organisations are controllers. But the purposes and means are determined separately. Therefore they are independent controllers. For the purposes of this article this is also classified as a multi-controller situation.

In theory one can imagine all sorts of multi-controller situations. For example, one organisation can be an independent controller for one processing activity, a joint controller for another and a processor for yet another. These relationships can be classified as hybrid. It can be quite hard to determine which concept best matches an entity in relation to a certain processing activity. It is advisable to perform a study and to debate your findings with some colleagues in the field of data protection. Lastly, the opinion of the Article 29 Working Party on the concepts of controller and processor is very useful in this matter.

3. Liabilities and fines

If you are dealing with a multi-controller situation it means you need to pay extra attention to the risk of liability and fines, especially when you are a joint controller. In the GDPR it is explicitly mentioned that every joint controller is liable for the entire damage caused by a processing activity (articles 82(2) and 82(4) GDPR). The only exception to this is when the controller proves he is in no way responsible for the event causing the damage (article 82(3)

---

3 An example of a hybrid relationship can be found here: Article 29 Working Party 16th of february 2010, Opinion 1/2010 on the concepts of “controller” and “processor”, p. 25.
4 Article 29 Working Party 16th of february 2010, Opinion 1/2010 on the concepts of “controller” and “processor”.
GDPR).\(^6\) A joint controller might be able to claim back some of the damages he has paid for from another joint controller depending on their respective responsibilities in causing the event (article 82(5) GDPR). You should also be aware that a supervisory authority might fine more than one joint controller.\(^7\)

Because of the risk of liabilities and fines it can be desirable to have a level of control over another controller. The means of control range from a contractual obligation to use encryption to the contractual right to instruct employees of another controller. Furthermore, it is advisable to come to a very clear (written) agreement with your counterpart(s) about indemnification for liabilities and fines before engaging in processing activities.

4. Other risks

Dealing with a multi-controller situation doesn’t only entail the risk of liability for damages and the risk of being fined. It is possible to think of more risks that are related to data protection. For example the risk of reputational damage. Another example is the risk that a supervisory authority orders your organisation to suspend its processing activity (article 58(2)(f) GDPR) which can affect your organisation’s operations.

5. Determining the distribution of responsibilities

Joint controllers are required to transparently determine a distribution for their respective responsibilities for compliance with the GDPR. Despite the distribution agreed upon between joint controllers, the data subjects can exercise their rights under the GDPR against every controller (article 26(3) GDPR). In other words, distributing responsibilities does not release you from the responsibilities you have towards data subjects. It can be deduced from this that it’s not unlikely that a joint controller can be held liable or that he is fined for matters that he (jointly) determined to be outside of his individual responsibility.\(^8\)

Transparency determining and distributing responsibilities in this context means that data subjects should be informed of the essence of the arrangement between the joint controllers (article 26(2) GDPR). It’s best practice to explain the arrangement in your privacy notice.

It can also be beneficial to determine a distribution of responsibilities in other multi-controller situations. In complex relationships the data subject can be confused about the role that each party plays. Determining the distribution of responsibilities will allow you to properly inform the data subject about who he can turn to for complaints and requests.

---

\(^6\) It should be noted that the phrase ‘not in any way responsible for the event giving rise to the damage’ in article 82(3) GDPR is still open to interpretation. Under Directive 95/46/EC the phrasing was slightly different, namely: ‘not responsible for the event giving rise to the damage’.

\(^7\) The GDPR does not provide specific rules about punitive sanctions for joint controllers. Article 83(2) GDPR determines that the amount of administrative fines shall depend on the circumstances.

\(^8\) This conclusion is also implied by articles 82(2) and 82(3) of the GDPR.
6. Remarks about independent controllers

Even when you are an independent controller of processing activities you can desire some level of control over the processing activities of another party. For example, this can be in your interest for the purposes of reputation management and compliance. To illustrate this I will use the example of one independent controller (X) selling personal data to another independent controller (Y). Y is a ‘recipient’ of the personal data as defined in article 4(9) GDPR and will use the personal data for the purposes of marketing.

Let’s say the customers of X agree to the transfer to Y under the assumption that X would look out for their interests. If the personal data leaks from Y because of poor security then that can hurt the reputation of X. Therefore X should ask for some contractual guarantees that Y will have proper security to mitigate the risk. This can be supplemented by audits.

X should also come to an agreement with Y about the purpose for which the personal data will be used by Y. The reason for this is as follows. Transferring personal data to the recipient is a processing activity. Consequently you are only allowed to do it if you comply with the principle of purpose limitation. A prerequisite for purpose limitation is the determination of a (clearly defined) purpose (article 5(1)(b) GDPR). If X hands over personal data to Y without knowing for what purpose it will be used, then X can not comply with the purpose limitation principle. Additionally, to determine whether a processing activity is compatible with a purpose one must take into account the existence of appropriate safeguards (article 6(4)(e) GDPR). Contractual arrangements about the purposes for which personal data will be used can be seen as such safeguards.9

It is possible to think of more examples. The GDPR has many articles where the interests of the controller have to be weighed against the interests of the data subject. Contractual safeguards can play a significant role in balancing those interests.

7. Checklist

The following checklist can be used when you suspect that you are dealing with a multi-controller situation:

- How should the relationship between the parties be defined? Which parties are a controller, a processor and/or recipient? Are the parties joint controllers? Is there a hybrid relationship?
- What responsibilities do the parties have (by law)?
- Who will be liable for damages of data subjects? Is there a risk that your organisation will be fined?

---

9 According to the Article 29 Working Party contractual arrangements are relevant in determining whether a processing activity is compatible with a purpose: Article 29 Working Party 2nd of April 2013, Opinion 03/2013 on purpose limitation, p. 63-64.
- This question is very relevant for determining what matters have to be dealt with between the parties. Joint control obviously entails a greater risk of being fined for mistakes made by others.

- Is it mandatory or wise to determine a distribution of responsibilities?
- The GDPR requires joint controllers to determine their respective responsibilities (article 26(1) GDPR).
  - The data subjects have to be informed of the essence of the distribution of responsibilities (article 26(2) GDPR). It's best practice to make this part of your privacy notice.
  - Independent controllers that exchange personal data can also (re)distribute certain responsibilities, for example the responsibility to properly inform data subjects.
  - Suggestion: It can be wise to contractually link the liabilities that the parties have towards each other to the distribution of responsibilities.

- Should the parties indemnify each other for claims by data subjects and for fines from the supervisory authority? Should there be indemnifications for other damages (for example reputational damage)?

- Is it necessary to make additional arrangements between the parties? Not only for the purpose of compliance, but also to mitigate reputational and organisational risks. The following is a non-exhaustive list of subjects that might require some thought and/or additional arrangements:
  - Audits
  - Cooperation with authorities
  - Cooperation between parties and the exchange of information
  - Data breach
  - Data processing outside of the European Economic Area
  - Data retention
  - Documentation and records of processing activities
  - Employee and contractor confidentiality
  - Information to be provided to the data subjects
  - Data protection by design and by default
  - Purposes of the processing of data
  - Rights of the data subjects (access, rectification, erasure, restriction)
  - Security
  - The use of processors and (sub)processors
  - Transfer of data to third parties
  - Termination of data processing

8. Summary

This article can be summed up as follows. Dealing with a multi-controller situation starts with assessing the situation and figuring what your organisation’s relationship is to another controller. When you have defined the relationship you can determine what risks accompany this type of relationship. In the case of a multi-controller situation you have a higher risk of paying for someone else’s mistakes. Some important examples of risk are liability for
damages, the possibility of fines and reputational damage. The most important tool for mitigating the risks involved with multi-controller situations is the multi-controller agreement.

9. Final remarks

After reading this article you might still have many more questions. Unfortunately dealing with multi-controller situations can be very complex. Providing cut-and-dried answers for every question is simply not possible. Feel free to ask questions to the author of this article through LinkedIn or the following website:

www.skna.nl

Article version

1.0 (13 November 2017)