

Joint Controllership within a group of entities¹

Dr. Lukas Lezzi / Jutta-Sonja Oberlin

1. Introduction

It is crucial for compliance of intra-group² data processing activities under the GDPR (General Data Protection Regulation)³ to answer the question as to whether such cooperation in data processing constitutes order processing or processing by jointly responsible parties (Joint Controller).

2. Distinction Controller / Processor

2.1 Controller

A controller meets the following three criteria (i) natural or legal person, public authority, body or any other party that (ii) alone, or jointly with others, (iii) determines the purposes and means of processing personal data (Art. 4 No. 7 GDPR)⁴. In particular, the third criterion is of great relevance. In other words the "master of the data" has to be determined, meaning the person, who intentionally influences the goal and the means of the data processing⁵.

1 This article is a strongly reduced version of an article published by the authors in ZD 2018, 398 et seq.

2 The term "group" is used for a group of entities. According to Article 4 (19), a group of entities is a group consisting of a dominant entity and its dependent entities.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

4 Art. 29 Data Protection Working Party, Opinion 1/2010 on the terms "controller" and "processor", WP 169, 10 et seq.

5 Instead of many Martini, in: Paal / Pauly (ed.), Datenschutz-Grundverordnung, 2017, Art. 26 N 19.

2.2 Processor

The processor, however, is any natural or legal person who processes personal data on behalf of a controller or processor (Art. 4 No. 8 GDPR). The processor only carries out data processing operations in accordance with the strict instructions of the controller and is strongly bound by its instructions. The processor cannot decide independently as to the purpose and/or means of processing⁶. However, it should be noted that Art. 29 Data Protection Working Party has stated that the decision on the technical and organizational resources can be delegated to the processor, as long as the controller remains in control of essential parts of the processing (in particular, regarding access rights or storage periods)⁷.

3. Joint Controller

3.1 Term

Joint Controllorship is present, if two or more responsible persons together determine the purposes and the means of data processing (Art. 26 GDPR). The term "together" must be interpreted as "together with" or "not alone"⁸. It is sufficient to make a minimal contribution to the determination of the purpose and the means⁹. It is, therefore, not required that the jointly responsible parties have the same degree of co-determination over the entire data processing. However, mere cooperation, without any co-determination of purposes and means, cannot, in principle, justify shared responsibility¹⁰.

Each individual case should be examined whether a joint controllership is given or not taking all circumstances into consideration. In particular,

6 Gola, in: Gola (ed.), *Datenschutz-Grundverordnung VO (EU) 2016/679*, 2017, Art. 4 N 58.

7 Art. 29 Data Protection Working Party, Opinion 1/2010 on the terms "controller" and "processor", WP 169, 17; see. also in detail Monreal, *PinG* 06.17, 216 et seq., 219.

8 Art. 29 Data Protection Working Party, Opinion 1/2010 on the terms "controller" and "processor", WP 169, 22.

9 Horn, in: Knyrim, *Datenschutz-Grundverordnung*, 2016, 153 et seq., 157.

10 Art. 29 Data Protection Working Party, Opinion 1/2010 on the terms "controller" and "processor", WP 169, 24.

the overall picture (macro level) of data processing must be considered, even if at the micro level the parties pursue their own purposes¹¹.

On 5 June 2018 the European Court of Justice (ECJ) acknowledged the Joint Controllership of an operator of a Facebook fan page and Facebook¹². This decision shows that shared responsibility requires only a minor impact on data processing by one of the parties. It is noteworthy that the ECJ further states that it is not crucial for every responsible party to have access to personal data.¹³

3.2 Intra-Group relationship

The GDPR does not grant intra-group exemption. Consequently, every intra-group data transfer must be analyzed separately for compliance¹⁴.

In groups, one of the group entities provides often central services to all other group entities (e.g. the centralized data processing of customer or employee data). If such a service is included in the decision on the means and purposes of data processing activities or if it is granted the pursuit of its own interests, Joint Controllership must be assumed. In contrast, a controller processor relationship has to be assumed, if an group entity determines only the technical means of data processing, but has no actual impact on the goal or the essential means of processing.

4. Agreement between the joint controller

According to Art. 26 para. 1 GDPR, if there is joint responsibility, an agreement has to be concluded between the jointly responsible persons, which regulates the distribution of obligations of the GDPR between the involved parties. Art. 26 para. 1 and 2 GDPR stipulate the content.

11 Art. 29 Data Protection Working Party, Opinion 1/2010 on the terms "controller" and "processor", WP 169, 25.

12 Judgment C-210/16 of 5 June 2018.

13 Judgment C-210/16 of 5 June 2018, N 38.

14 The mention of the legitimate transfer of customer or employee data within a group in recital 48 does not help further qualify this transfer.

4.1 Formal requirements

There is no legal obligation for a written agreement. However, due to the rule of drafting in a transparent manner and the obligation to make the essential content of such an agreement available to the data subjects, but also for reasons of proof, a written agreement will usually be necessary.

4.2 Content

4.2.1 Allocation of functions within the data processing

According to Art. 26 para. 2 GDPR, the agreement must duly reflect the actual functions and relationships of the joint controllership with regard to the data subjects. Accordingly, the agreement has to regulate the distribution of tasks and decision-making powers for determining the purpose and means of data processing. Moreover, the distribution of tasks regarding the fulfillment of the data subject rights has also to be stipulated¹⁵. The term "duly reflect" is not defined, but has to be interpreted in the sense that the division of tasks in the agreement has to be easily understandable to the data subject¹⁶.

4.2.2 Regulation of data subjects' rights

According to Art. 26 para. 1 GDPR, the agreement must specify which of the jointly responsible parties fulfills which data subject rights. Specifically, it must be agreed on how the distribution of tasks for the following rights should be exercised: information obligations (Art. 13, 14 GDPR), right to information and the right to access (Art. 15 GDPR), right to rectification (article 16 GDPR), right to be forgotten (Art. 17 of the GDPR), right to restriction (Art. 18 of the GDPR), data portability (article 20 of the GDPR), right to object (Art. 21 GDPR), rights in connection with automated decisions as well as the fulfillment of the duty to inform on data breaches (Art. 34 GDPR).

The agreement may further specify, on an optional basis, a point of contact for data subjects. However, this communication has no legally binding

¹⁵ Piltz (see above fn. 6), Art. 26 N 19.

¹⁶ Piltz (see above fn. 6), Art. 26 N 18.

effect on the persons concerned and is to be understood as more than a service offer, since the persons concerned may assert their rights against all those jointly responsible¹⁷.

4.2.3 Regulation of other duties

The remaining duties among the jointly responsible persons can be freely allocated, but only to the extent that no EU or Member State legislation already regulates the distribution.

However, it is questionable which duties can be transferred to another controller. In particular, organizational and technical obligations are considered: Records of processing activities (Art. 30 GDPR), security of processing (Art. 32 GDPR), carrying out data protection impact assessments (Art. 35) and privacy by design (Art. 25) and the appointment of a data protection officer (Art. 39 GDPR).

Compliance with the GDPR principles (Art. 5 GDPR) and the need for a legal basis (Arts. 6, 7, 9 and 10 GDPR) cannot be delegated¹⁸.

The agreement should – as far as permissible – divide all obligations under the GDPR between the responsible parties, because otherwise the redistributed obligations must continue to be observed by all parties involved¹⁹.

4.3 *Transparent communication of the substance of the agreement*

Art. 26 para. 2 sentence 2 GDPR stipulates that the substance of the agreement must be made available to the persons concerned. According to the agreed doctrine, the term "essential" includes the division of responsibilities with regard to the fulfillment of the data subject's rights and obligations by law, as well as the name of the contact point for the persons concerned²⁰.

17 Martini (see above fn. 5), Art. 26 N 28 et seq.

18 Veil, in: Gierschmann/Schlender/Stentzel/Veil (ed.), *Kommentar zur DatenschutzGrundverordnung*, 2018, Art. 26 N 40, Art. 26 N 55.

19 Horn (see above fn. 9), S. 159.

20 See, e.g. Martini (see above fn. 5), Art. 26 N 32; Hartung, in: Kühling / Buchner, *General Data Protection Regulation*, 2017, Art. 26 N 26; Horn (see above fn. 9), 161.

Important is that all rights of the data subject set in the agreement need to be communicated. This means that the internal agreements between the joint controller about liability consequences or cost structures need not be disclosed. In addition, the division of tasks in the area of organizational duties cannot be qualified as "material" because the data subjects cannot derive any rights from these obligations of the GDPR²¹.

In regard to the form of said communication, the GDPR merely states that the essentials of the agreement are to be made available to the data subjects. However, this does not require active communication. The retrievability on a website is sufficient for this²².

To be compliant with the principle of transparency, the essential content of the agreement should be integrated into the privacy policy, which will inform the data subjects about all data processing activities in place. In regard to the relationships between the entities of a group this represents a suitable approach in the field of customer data. In the area of the processing of employee data, it would also be possible to offer said information on an in-house information platform.

5. Practical example for an intra-group joint controllership

As a central service provider, a group entity processes the personal data of the employees of the other group entities over the entire life cycle of the employment relationship (such as application, employment, payroll accounting, performance appraisals, termination, social security benefits, etc.). The means of such processing are largely determined by the service entity. In addition, this service entity analyses the personal data of the employees with a view to standardizing the amount of wage and bonus payments within the group.

This shows that the central service entity has a large influence on the circumstances of the data processing of the employee data of the other group entities and in fact also coordinates and agrees with the other group entities on many of the processing purposes, such as the type and manner of performance reviews. In this case, the service entity also pursues its own interests and does not merely act as an "extended arm" of the other enti-

21 Different opinion Veil (see above fn. 18), Art. 26 N 64.

22 Martini (see above fn. 5), Art. 26 N 34 et seq.; see. see also recital 58, which explicitly provides for the possibility of being made available on a public information website.

ties. According to the above, the entities involved in this constellation would have to be qualified as jointly responsible persons. Accordingly, an agreement pursuant to Art. 26 GDPR must be concluded between the service entity and the other entities in the group. In this context, it would appear appropriate to locate the contact point for employees within the service entity and provide the necessary information on an internal information platform.

6. Conclusion

Due to the more extensive duties of the controller in the GDPR, it is advisable to assume joint controllership in case of doubt and to draft the necessary contracts. Of course, this can only apply where no national law determines the relationship between the joint controller.

However, if group aims to avoid an intra-group data processing by a service group entity being qualified as a joint controllership, it should ensure that the service entity only can determine the technical means of data processing. Most importantly, the service has to be restricted from deciding the essential technical means or even the purpose of the processing.

An agreement in regard to joint controllership should have the following content:

- Definition of purpose and duration of the data processing activities
- Describe the type of personal data and category of data subjects
- Describe the data flows and relationships between the joint controller
- Describe the legal basis of processing under article 6 and 9 GDPR and their allocation to those responsible
- Determining which duties must continue to be performed by all joint controller (principles of data processing and legal grounds)
- Definition of the contact point for the persons concerned
- Division of the organizational fulfillment of the affected rights
- Sharing of external communication with data subjects (in particular information about the agreement and data processing) and with the supervisory authorities (on privacy impact assessment and privacy breaches)
- Agreement on the appointment of the representative such as mentioned in article 27 para. 3 GDPR
- Agreements on the technical design for the fulfillment of data subject rights

Dr. Lukas Lezzi / Jutta-Sonja Oberlin

- Agreements on the technical measures for data security and for the Measures for Privacy by Design and by Default
- Agreements on the data breach reporting processes
- Agreements on keeping the record of processing activities
- Description of the procedure and safeguards in place for data transfers to a third country without adequate protection
- Mutual information obligations in case of relevant organizational changes of the joint control
- Intra-liability agreements, if one or more co-responsible parties have settled all the damage

Furthermore, the essential content (e.g. the part from which the data subjects can derive rights) of this agreement is to be made available to the persons concerned. This duty is most reasonably taken over by the entity which collects data in the first place or which is the point of contact for data subjects.