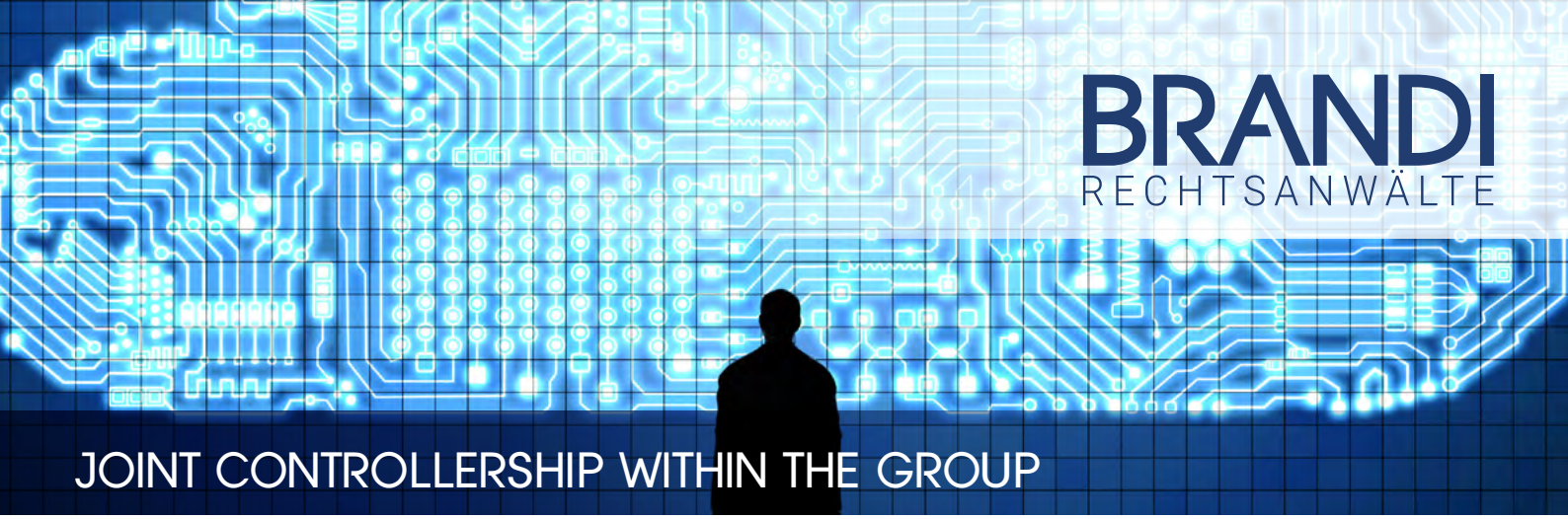

BRANDI
RECHTSANWÄLTE

# JOINT CONTROLLERSHIP WITHIN THE GROUP

Information on data protection I August 2024

## Introduction

For many companies that are part of a group structure, there is a need to transfer personal data within the group or to process it jointly in some other way, for example if one company carries out personnel administration or accounting for all other companies in the group or provides IT support. Of relevance here is not only the classic case of data transfer in the sense of direct transmission, but also the retrieval of information or access by a group company to data assigned to another group company as the controller, for example in the case of shared databases and systems as well as group-wide directories.

If personal data is to be exchanged within a group of companies, a legal basis is required for this. Companies belonging to a group are covered by the data protection term „group of undertakings" within the meaning of Art. 4 No. 19 GDPR. In principle, companies in such a group of companies are each independent entities, so that the data transfers are to be qualified as transfers to another company and thus as data processing requiring justification. Since a special legal basis (so-called „group privilege") or other privileged regulation for data transfers within the group cannot be found in either the GDPR or the BDSG, the general permissions must be applied in this respect.

## When do I need an intra-group agreement on joint controllership?

In principle, various options are conceivable for justifying data transfers and safeguarding them under data protection law, without there being a ranking order in the examination of possible authorizations. For example, a legitimate interest of the respective group company within the meaning of Art. 6 (1) (1) (f) GDPR, which is also expressly mentioned in recital 48 with regard to internal administrative purposes, including the processing of personal data of customers and employees, or a data transfer for fulfillment of the contract (Art. 6 (1) (1) (b) GDPR) - especially with regard to the transfer of employee data in the case of a „group-dimensional employment relationship". In addition, cooperation within the group may correspond to intra-group data processing within the meaning of Art. 28 GDPR or joint controllership between participating companies within the meaning of Art. 26 GDPR.

According to Art. 26 (1) (1) GDPR, the latter exists if two or more controllers jointly determine the purposes and means of data processing. Therefore, if the parties agree to jointly determine the manner in which the data is processed, a case of joint controllership can generally be assumed in this respect. This is often supported by the fact that two companies work together as partners and, in contrast to the situation of data processing, there is no hierarchical divide between the parties. As a rule, the conclusion of a joint controllership agreement is particularly suitable when different companies access the same systems or data sets for different purposes. Ultimately, however, it depends on the specific design of the processes and the will of the parties involved.

As the concept of joint controllership often best reflects the actual processing situation within a group and maps the internal processes particularly well, securing data transfers by concluding a corresponding agreement is generally preferable to the concept of data processing. Ultimately, however, the selection of the right data protection instrument, in particular the dividing line between data processing and joint controllership, depends on the specific design of the processes and the will of the parties involved.

Compared to data processing, joint controllership has a disadvantage in that recourse to Art. 26 GDPR cannot constitute an independent authorization for cross-company data processing, but must be formally based on the legal basis of the legitimate interest. In view of the defined responsibilities within the group, however, it is assumed that the interests of the data subjects worthy of protection regularly take a back seat, but this must be assessed and documented. Joint controllership also means that the parties involved are jointly and severally liable externally for any data protection violations in accordance with Art. 26 (3) GDPR.

However, it also has the advantage that the parties can divide their legal obligations, such as informing those affected, among themselves. The concept of joint controllership also has the advantage that any number of companies can participate in an agreement and it is generally possible for another company to join at a later date. Joint controllership also leads to greater flexibility with regard to the access and utilization options of the individual companies. It should also be noted that the companies involved cannot exempt themselves from joint liability anyway by not regulating a situation that corresponds to joint controllership under the actual circumstances. If, despite the existence of the requirements of Art. 26 (1) (1) GDPR, the agreement required under Art. 26 (1) (2) GDPR is missing, this can be seen as an independent breach of data protection.

The following questions, among others, can be used to better differentiate between joint controllership and data processing:

- Who decides which data is collected?
- Who decides how long data is processed?
- Who decides who can access the data?
- Who decides for what purpose the data is processed?
- Who decides whether data may be deleted?

## Practical approach

If there is a joint controllership according to the actual circumstances or if the cooperation of several companies is to be actively structured as a joint controllership, Art. 26 (1) (2) GDPR requires an agreement to transparently define which party fulfills which obligation under the GDPR. This applies in particular to the exercise of data subjects' rights and information obligations. The agreement must also reflect the respective actual functions and relationships of the joint controllers in accordance with Art. 26 (2) GDPR. Depending on how the rights and obligations are to be divided between the parties involved and how questions of responsibility and liability are to be settled internally, various structuring options are conceivable.

In order to meet the requirements and avoid overloading the agreement, it is advisable to create a separate matrix in addition to the actual agreement, in which the individual processing procedures are then worked out and the respective responsibilities of the individual parties are determined. If the matrix is attached to the main agreement as an annex, this also offers the advantage that it is relatively easy to add further processes to the matrix at a later date if the collaboration is extended. Depending on how extensive the cooperation between the companies involved is, the matrix to be created can be quite complex. Finally, in order to summarize the essential contents once again and to comply with the provision of Art. 26 (2) (2) GDPR, according to which the data subject must be informed of the essentials of the agreement, it is necessary to prepare an overview document.

If two or more companies work together as joint controllers, data subjects must also be informed of this fact and the relevant information documents and consent requests must be adapted accordingly. The other data protection regulations must also be observed. Data transfers to third countries, for example, must always be secured.

## Conclusion

If data is to be exchanged within the group, systems and databases shared and data records processed jointly, a legal basis is required for this in the absence of a „group privilege". It is often advisable to actively organize the collaboration as a joint controllership and to conclude a joint controllership agreement, as the concept has various advantages. If, according to the actual circumstances, there is already a case of joint controllership within the group, a corresponding agreement must also be concluded between the parties involved. The agreement on joint controllership can then be adapted to the respective responsibility relationships and tailored to the actual circumstances. We will be happy to assist you with the specific design.

Christina Prowald

**Contact:**

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

**Christina Prowald**
Research Associate

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net