BRANDI
RECHTSANWÄLTE

DATA TRANSFERS WITHIN ORGANIZATIONS

Information on data protection I June 2022

Introduction

The existence of a legal basis is generally required for data processing operations within a group of companies and, in particular, for the transfer of personal data to other companies within the group. In this respect, data processing within the group is also subject to the "prohibition with reservation of permission" set out in the General Data Protection Regulation (GDPR), according to which any processing of personal data requires the existence of an authorization under data protection law.

Groups or companies belonging to groups are subject to the term "group of undertakings" under data protection law, which the GDPR defines in Article 4 No. 19 as a controlling undertaking and its controlled undertakings. From the perspective of data protection law, companies in such a group of undertakings are also independent entities in principle. Accordingly, not only the classic transfer of data in the sense of a direct transfer, but also the mere retrieval or access by a group company to data assigned to another group company as the data controller – for example in the case of shared databases or group-wide directories – must be qualified as a transfer of data to another company and thus as data processing requiring justification.

The GDPR does not provide a special legal basis for data transfers within a group (so-called "group privilege"). Only recital 48 contains information on the transfer of data within a group of undertakings on the basis of weighing of interests. The German Federal Data Protection Act (BDSG) also lacks a corresponding privileging regulation, so that the exchange of data between companies belonging to the same group must be governed by the general permissive provisions, in particular those of Article 6 GDPR.

The additional requirements arising from the GDPR, for example for the processing of special categories of personal data from Article 9 GDPR or for the transfer of data to third countries from Article 44 ff. GDPR, must also be observed in principle for data processing within the group.

Justification of data transfers within a group

In principle, various options are conceivable for justifying and safeguarding data transfers within a group under data protection law, without there being any order of priority in the examination of possible authorizations. Some design variants are briefly outlined below.

Legitimate interests

The legal basis shall initially be the existence of a legitimate interest of the respective affiliated company within the meaning of Article 6 (1) (1) (f) GDPR. Recital 48 specifically states in the regard that controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. In this respect, the GDPR recognizes in principle that companies may have a specific interest in intra-group data transfers and data processing operations. As a result, however, recital 48 only states that the exchange of data within a group of undertakings must be possible in principle, but not that it is always permissible. The GDPR does not specify in which cases an internal administrative purpose and an overriding legitimate interest are to be affirmed and the processing operation can accordingly be based on Article 6 (1) (1) (f) GDPR, so that an examination of the individual case is again necessary.

The existence of a legitimate interest is conceivable, for example, if data is processed for the organization of appointments or for other communication purposes or is stored in a centrally managed database, for example, for purposes of address management or billing. In each case, however, the specific design of the system and the effects on the data subjects must be taken into account, and the conflicting interests must be weighed against each other. The effects for the data subject are likely to be more negligible the smaller the number of group companies included is, and the less recognizable it is to the data subject that a division into different group companies exists at all. It is advisable to document the weighing of interests and its result in order to be able to prove that the issue has been properly addressed in the event of a complaint.

Intra-group contract processing

If a group company receives data form another group company or has access to its data in order to process it on behalf of the other company, Article 28 GDPR in connection with Article 6 (1) (1) (f) GDPR may also be considered as a legal basis. The concept of contract processing within the meaning of Article 28 GDPR basically presupposes a relationship of superordination and subordination between the parties as well as the contractor being bound by instructions of the client.

The conclusion of an Data Processing Agreement within a group of undertakings is in principle also possible if, in relation to the situation of contract processing, contrary relationships of superordination and subordination under company law exist or the companies involved are on equal rank. However, when structuring the agreement in the above-mentioned cases, it must be ensured that the

company commissioned is in any case bound by the instructions of the client, irrespective of its other position under company law. If two companies belonging to the same group exchange data and both the one and the other company act on behalf of the other company, it is generally also possible to structure the Data Processing Agreement for this case in a reciprocal relationship.

Irrespective of such design variants, it must be taken into account in any case that only those data processing operations may be carried out by the contractor which are also covered by the specific order of the client. On the other hand, data processing that goes beyound the actual order cannot be justified in this way. As a matter of principle, it should be noted that only such data may be transmitted and processed as is also necessary for the fulfillment of the order. The concept of contract processing also reaches its limits where several group companies actually process or use personal data jointly. The same applies if data processing operations are difficult to map within the scope of a specific order and the data are also to be used more widely. In these cases, it is advisable to resort to a different design and legal basis.

It is conceivable that the concept of contract processing could be used, for example, if one company in the group takes on a specific, definable activity such as accounting for the other companies. Nevertheless, it must be checked in each individual case whether the concept of contract processing fits the actual processes within the group.

Joint controllership within the group

In addition, data transfers within the group can also be justified and secured by concluding a Joint Controller Agreement within the meaning of Article 26 GDPR. In contrast to the situation of contract processing, the concept of joint controllership provides that two or more parties process data jointly and also jointly determine the purposes and means of data processing. Nevertheless, the respective responsibilities of the parties are to be defined within the agreement.

While the concept of contract processing in principle presupposes the existence of a two-party relationship and thus requires the conclusion of seprate agreements in the case of the participation of several group companies, the concept of joint controllership allows the participation of any number of companies in one agreement. It is also possible in principle for another company to join at a later date. Joint controllership of the companies involved also allows greater flexibility with regard to the access and usage options of the individual companies.

It is usually a good idea to conclude a Joint Controller Agreement if different companies access the same systems or data sets for different purposes. Since the concept of joint controllership usually best reflects the actual processing situation and maps processes particularly well, it is often preferable to secure data processing by concluding a Joint Controller Agreement. Compared to contract processing, however, the joint controllership has the disadvantage that recourse to Article 26 GDPR cannot constitute an independent authorization for intra-group data processing. Formally, the legal basis is then the legitimate interest, whereby due to the defined responsibilities within the group, it is assumed that interests worthy of protection of the data subjects take a back seat, which, however, must be further evaluated and documented as part of weighing of interests. It is often argued that joint controllership also establishes common data protection standards within the group, so that it makes no difference to the data subject whether the personal data is processed by only one group company or whether several companies are involved.

Third country transfers

Due to the lack of group privilege, an intra-group data transfer must comply with the general requirements of the GDPR. This also applies with regard to the requirements for the transfer of data to group companies in third countries. If the group operates globally in this respect and, for example, uses group-wide data processing systems, the regulations of Article 44 ff. GDPR must be observed when transferring data. This requirement applies both if the headquarter of the group is located in a third country and if individual group companies are included in a third country, for example in relation to foreign sales companies.

To safeguard the international data transfer in addition to the mechanisms mentioned above, the safeguarding of an uniform data protection-compliant level by Binding Corporate Rules can also be considered, in addition to conclusion of Standard Contractual Clauses. Within the Binding Corporate Rules, principles and data protection guarantees are defined for the handling of personal data and group-wide data processing. The new Standard Contractual Clauses also contain data protection regulations adapted in four different modules to the possible processing situations between the parties involved. Unlike the Standard Contractual Clauses, the Binding Corporate Rules require recognition by the data protection supervisory authority, but then provide a legally secure framework for data transfers within the group.

Employee data protection

The respective employer of an employee is the controller with regard to its personnel data. This is not changed by the fact that the company is integrated into a group structure. Accordingly, taking into account the above considerations, the personnel data may not be transferred to and processed by other companies in the group without further ado. Rather, the existence of a legal basis for the data processing is also required in this respect in each case.

In addition to the justification options already described, the transfer of employee data can also be based on the legal bases of contract performance pursuant to Article 6 (1) (1) (b) GDPR and processing for purposes of the employment relationship pursuant to Section 26 BDSG, insofar as a group employment relationship exists. This is the case if the activity agreed in the employment contract has a clear connection to the group, if certain personnel decisions are the responsibility of the group parent company, or if employees are deployed at various companies within the group.

The legal basis of consent, on the other hand, is generally ruled out for reasons of practicability, also with regard to employee data, with particular regard to the aspects of voluntariness and revocability of consent, even if the use of Article 6 (1) (1) (a) GDPR in this respect would be conceivable in principle. For this purpose, it is advisable to point out the group structures at the beginning of the employment relationship and, if necessary, to obtain consent for group-wide data processing. Even then, of course, the exchange of data within the group must remain limited to the necessary constellations.

Conclusion

In the absence of a genuine “group privilege“, the general data protection requirements apply to data transfers within a group, which means that the existence of one of the legal bases in particular

remains necessary. The criteria for authorization depend, on the one hand, on the groups of persons affected by the processing and, on the other hand, on the specific processing operations within the group.

Depending on the desired design, the concepts of contract processing and joint controllership may be considered to safeguard the processing operations, in particular to avoid any imponderables and legal uncertainties with regard to the existence of an overriding legitimate interest. Insofar as employment relationships within the group of undertakings are structured on a “group-wide“ basis, the group-wide transfer and processing oft he corresponding employee data can also be based primarily on the fulfillment of the contract and processing for purposes of the employment relationship.

If the group operates internationally and personal data is also transferred to third countries, the general requirements of the GDPR with regard to transfers to third countries must be taken into account. Corresponding data transfers can be protected under data protection law, for example, by concluding Standard Contractual Clauses within the group or by agreeing Binding Corporate Rules.

Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 890
F +49 521 96535 - 113
M christina.prowald@brandi.net