25 Necessity of a contract on data processing

When does the GDPR require the conclusion of a contract on data processing?

Article 28 para. 3 s. 1 GDPR demands a data processing agreement whenever the processing of personal data is carried out by a processor on behalf of a controller. The aspects that are to be dealt with in a corresponding contract are also listed in Article 28 para. 3 GDPR.

It should be considered, however, that not every cooperation of two parties is to be regarded as data processing. In particular data processing must be distinguished from a joint controllership. For the latter also a contract is necessary, which is regulated in Article 26 GDPR.

In order to answer this question as well as the following questions, it is therefore necessary to clarify which bodies are controllers, processors or joint controllers. One body may be classified differently with regard to different data processing processes within the same research project. It would be conceivable, for example, that a TTP would carry out pseudonymisation as a data processor, but that consent management would be carried out under joint control.

The assignment results directly from the **actual circumstances** and the requirements of the GDPR. Article 4 No. 7 GDPR defines the "controller" as

> *"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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;" [Highlighting not in original text]*

By way of comparison, the data processor is defined as follows pursuant to Art. 4 No. 8 GDPR:

> *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;"*

The decisive legal criterion for the distinction between controller and processor is the determination of the *purposes* and *means* of processing. Whoever determines purposes and means becomes a controller. If two or more jointly determine the purposes and means, they are considered joint controllers. If, on the other hand, one body carries out processing operations subject to instructions only, this body would have to be regarded as a processor. In individual cases it may be difficult to distinguish between a controller and a data processor. This applies in particular if one party does not determine both (purposes and means) or all parties determine both in unequal parts. Particularly difficult but frequent are cases in which either one determines the purposes and the other the means or both bodies can have a say in both points, but there is an imbalance.

The German legal literature lacks empirical values from the old legal situation, as the German legislator had not implemented the joint responsibility contrary to the wording of the Data Protection Directive (Directive 95/46/EC) and in the past only had to distinguished between controller and processor.

From this perspective, it can be said that the joint controllers are a new legal category. This has given rise to a variety of legal views.[78] For example, a minority opinion assumes that each of the joint controllers must always define both the purposes and the means and that this must be done equally balanced; at the same time, this opinion assumes that the "means" of processing are the data processed.[79]

In its decision of 5 June 2018 on joint responsibility for Facebook fanpages, the European Court of Justice contradicted a requirement of equally balanced determinations of both means and purposes.[80] Although this judgement still was based on the old legal situation under the Data Protection Directive, no

78 *Schreiber*, Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden, ZD 2019, 55.
79 *Schütze/Spyra*, Art. 26 DS-GVO: Gemeinsam Verantwortliche, Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V., Version 1.0 Stand: 17. 06. 2018, S. 5f.
80 *EuGH*. Urt. v. 05. Juni 2018, AZ: C-210/16. Rn. 38.

indications for a deviating assessment result in respect to the GDPR. With the prevailing opinion in legal literature it is to be held in addition that the **means** of the processing are not the processed data, that rather are the object of the processing, but the question of how a processing is accomplished.[81] This includes, in particular, data processing systems and processes. For example the means of processing include consent management systems, quality assurance measures record linkage techniques and duplicate resolutions, as well as joint definition of processes and workflows, communication principles including autonomous implementations, tests and the rollout of extensions for tools and workflows.

In January 2018 the Datenschutzkonferenz (DSK) published a short paper in which the German data protection authorities give important remarks for the future interpretation of the GDPR concerning data processing.[82] In March 2018 DSK published another short paper on joint controllers.[83] The two short papers must be read together as they complement each other. Although the short papers of the DSK are subject to reservation, they currently provide relevant guidance. The DSK sees the **decisive aspects in the definition of the purposes**, while the decision on the technical and organisational aspects of the processing may partly be delegated to the processor. This means, that to a certain extent, a processors scope for making decisions with regard to the means of the processing within a framework set by the controller does not per se exclude the classification as data processing.[84]

The data protection authorities have stated that the criteria for distinguishing between controller and processor, as applied under the old law, are no longer viable. Nevertheless they formulate comparable parameters, according to which it is a central criterion that the processor acts only and strictly instruction-bound.

> *"According to Art. 29 GDPR the service provider which is active due to an order is instruction-bound. He therefore does not carry out the processing for the controller as a third party in the sense of Art. 4 No. 10 GDPR. Rather, there is an "internal relationship" between the controller placing the order and his processor. Processing by the processor is therefore generally regarded as belonging to the controller."*[85]

This results in one of the main differences between data processing and joint controllership: the data processor is, so to speak, part of the controller. As a rule, the processor is allowed to do everything that the controller is allowed to do. Data transfers between controller and processor are allowed because they

81 Petri, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 4 Nr. 7 Rn. 20, Fn. 34.
82 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018.
83 DSK, Kurzpapier Nr. 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO, Stand 19.03.2019.
84 DSK, Kurzpapier Nr. 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO, Stand 19.03.2019, p. 2.
85 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018, p. 1.

are treated like internal transfers. The controller is not a third party within the meaning of Article 4 No. 10 GDPR.

In contrast, there is no similar privilege between joint controllers. The entire cooperation, including the data transfers between the parties, would therefore have to be covered by a consent or legal basis. In the case of a declaration of consent, this would also have to refer to all controllers.[86]

It must therefore be examined on a case-by-case basis who determines the purposes and means. In difficult cases, the focus must be on who determines the purposes and whether one party may only process data strictly instruction-bound.

Since the TTP of UMG is legally a part of UMG, it should be noted that there can be no data processing relationships or joint controllerships between the TTP and the UMG as they are one entity. If, on the other hand, the TTP of the UMG acts for other bodies such as the DZHK, an assessment will be necessary. Since a TTP can take on different tasks and each task must be evaluated to determine whether it is being handled by joint controllers or a data processor, this can result in different classifications in different projects but also within a single project. If a TTP should become active in different roles within a single project, all roles could also be covered by a single contract. The GDPR does require contractual regulations, but not separate contract documents.

> *In which cases is it possible to act as joint controllers instead of working on the bases of a contract on data processing? (This would be much more suitable for scientific cooperation than data processing according to Article 28 GDPR.)*

As stated before, the cooperating parties cannot freely agree on their roles by defining them in a contract. The actual modalities of cooperation are decisive.

The DSK has listed examples in which joint controllership is to be assumed in Annex C of the abovementioned short paper on data processing.[87] Special reference is made to clinical trials for medicinal products. A joint controllership according to the DSK would exist if several participants (e.g. sponsors, study sites and physicians) each make decisions on processing in certain areas. The tasks of a TTP are not explicitly mentioned in the short paper. Typically, a TTP will make decisions on its own to a lesser extent than the DSK had assumed.

If a TTP only carries out pseudonymisations of IDAT which are provided for this purpose in an individual case and only specifies the measures necessary for this (with a certain decision-making power), this will presumably be understood as data processing according to Article 28 GDPR.

86 DSK, Kurzpapier Nr. 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO, Stand 19.03.2019, p. 1.
87 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018, p. 4, 5.

Should, on the other hand, the TTP collect personal data in addition to a specific research project of another controller also, e.g. as a register or repository, so that these data can be used later also by other controllers, this may qualify as a joint controllership for the platform thus created.

According to which argumentation criteria can joint controller processing be used and what are its consequences (in comparison to data processing)?

Joint controller processing has some minor advantages for the bodies involved, as some of the duties according to GDPR can be delegated between the joint controllers and both controllers are not instruction-bound.

However, there are also disadvantages that may not be counterbalanced by the advantages:

Firstly, as explained above, the privilege concerning transmission and further processing between joint controllers without a separate legal basis is no longer granted, which would, however, apply to data processing under Article 28 GDPR.

Secondly, all joint controllers are jointly liable for infringements of the GDPR and the damages that may arise as a result. This applies in the relation to the data subject independently of the contract clauses, which the parties can agree on in a contract according to Article 26 GDPR. In the internal relationship between the contracting parties (joint controllers) certainly clauses can be drafted in order to compensate such duties. Nevertheless the liability risk increases. There will especially include the risk that another joint controller may be insolvent and damages will have to be borne by the rest of the joint controllers alone.

Additionally, joint controlling must be reflected in the declarations of consent as the consent would have to cover the processing of all joint controllers.[88] Both the data processing and the joint control must be considered with the information duties under Article 13, 14 GDPR.

The DSK assumes that a joint control can increase the risk for the rights and freedoms of the data subjects and therefore a data protection impact assessment is more likely to be necessary.[89]

Contracts must be closed both in the case of data processing according to Article 28 GDPR as well as in the case the joint controllership according to Article 26 GDPR. The absence of such a contract is considered an infringement of the GDPR and can lead to administrative fines. In joint controllership, the law requires that the essence of the agreement shall be made available to the data subject in an applicable way (Article 26 para. 2 S. 2 GDPR).

88 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018, p. 1.
89 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018, p. 4.

Are existing contracts to be adapted and amended after the GDPR came into effect, e.g. because they regulate the transfer of functions ("Funktionsübertragung") and the waiver of data processing (under former data protection law)?

It cannot be said in general terms that all data protection related contracts, which came into force before the GDPR, can be continued without examination and without change. The DSK stated that however contracts concerning data processing can stay in force without amendment if they already fulfil the requirements of the GDPR.[90] It should therefore be assessed whether the requirements contained in Article 28 GDPR are met by the specifics of a project.

The German characteristic "transfer of functions" ("Funktionsübertragung") has only very limited significance under the GDPR. Since the old German data protection law only distinguished between a controller and a data processor and did not cover the concept of joint controllers, it could be determined in the case of the transfer of functions to other bodies that such a body would qualify not as a data processor but a separate controller. Under the GDPR, however, it cannot be determined without further ado on the basis of the idea of a transfer of functions whether there is a separate controller or a joint controller.

A separate controllership is a reasonable option if the controller transfers data to another controller without determining the purpose or means, to a situation in which the separate controller is in a position to process the data within determined limits at his own discretion. Any cooperation that is determined by means and purpose at the discretion of the initial controller are determined to be processing on behalf of the controller or joint controllership.

Neither the old nor the new law allowed cooperating bodies to agree with each other on whether there was a data processing. Therefore, no effective waiver could exist in a contract. Contracts that included a transfer of functions or an agreement that included a waiver for data processing should be checked very thoroughly.

Summarizing the above it can be concluded that data processing on behalf of the controller as well as joint controllership require a contractual basis. Both relationships can be part of a corporation contracted which would not be unusual. It should be assessed on a case-by-case basis which procedure would be best and in which cases neither would apply if the data processing is just a scientific task that would not be part of either category. Any project can encompass tasks that either processing, controllership or scientific work which are neither processing nor controllership. The corporation contract can assign these tasks to any of these categories.

90 DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO, Stand 16.01.2018, p. 2.