Explanatory text on the decision-making circuit

Author: Martin Leiter, AK AV
(Arbeitskreis Auftragsverarbeitung
[Commissioned Data Processing
Work Group]) Version 002 of
15/04/2020
Update 003 of 16/02/2021 (adjustment to the current decision-making circuit)

The decision-making circuit is intended to provide assistance in assessing whether an entity that is different from the data controller and the data subject (hereinafter referred to as a "service provider" because they normally act for the data controller on the basis of a service contract) is a "commissioned processor" of the data controller within the meaning of Art. 4 (8), thus requiring the conclusion of a Commissioned Data Processing Agreement.

The described steps of the decision-making circuit are explained in more detail below.

Step 1 – Reference to persons

Does the information that is the subject of the processing constitute personal data within the meaning of the GDPR?

It only constitutes commissioned data processing if this is the case. Non-personal data processing (e.g. of statistical statements or other information that does not relate to an individual, specific or identifiable person) is not processed under the GDPR regime, and cannot therefore constitute commissioned data processing.

In this context, “person” always means “natural person”. This means that the use of data on legal persons is usually also not relevant with respect to data protection.

Note: statements on legal persons often also reflect the relationships of natural persons, e.g. owners and contact persons. If so, it constitutes reference to persons[1].

Step 2 – Object of the contract

Does the agreement between the data controller and the service provider concern processing of personal data?

This only constitutes commissioned data processing if this is the case (and the processing is not merely a secondary activity[2]). This means that the processing of personal data must (also) be the subject of the order, i.e. the underlying civil law agreement.

Note: since "destruction" also constitutes processing, data destruction (e.g. the physical destruction of data carriers by a service provider) is generally also regarded as commissioned data processing.

---

[1] ECJ C-92/09 and C-93/09 dated 9/11/2010: here, the ECJ had affirmed the applicability of data protection law if EU aid to legal persons containing the names of natural persons amounted to 30-70% of the total income of the natural person behind the legal person.

[2] Cf. Kotschy in Datenschutz - eine Standortbestimmung (Part I) in RdW 8/2018: *“If purchased goods are to be delivered by the seller to the buyer according to the sales contract, the question arises when using a freight forwarder whether the latter is a "commissioned data processor" or a "third party” with regard to the transmitted delivery data. The same applies, for example, to the execution of payments by a company to a natural person (e.g. employees) by way of a credit institute. There is a lot to suggest that the freight forwarder or the credit institute should be seen as a "third party", since the processing of data is not the focus of the stipulated service, but the transport and delivery of the goods or the transfer of funds. (...) If the processing of personal data is not the focus of the order and/or does not constitute an extensive part of the service of the agent, it will be assumed that this constitutes cooperation of a "third party“, and not "commissioned data processing".*

Step 3 – Forwarding

Does the service provider merely forward the data without being commissioned to inspect the data? In this case, it must be checked whether the use of the service provider expands the “circle of those in the know”. If this is not the case, and if this circle is not expanded by simply forwarding data (not even to the service provider themselves), then this does not constitute commissioned data processing.

Note: if the "forwarding service provider" is also commissioned with maintenance work in the context of which they are permitted to process personal data, e.g. in the event of a malfunction, then they are in any case a commissioned data processor.

Step 4 – Norms, judicature

Are there any special regulations for the specific processing situation?

In some cases, separate norms or rules of conduct pursuant to Art. 40 GDPR regulate responsibilities for data protection, and thus also, in particular in certain contexts, the "data controller" pursuant to Art. 4 (7) GDPR, e.g. for the exercise of the trade of list broker and direct marketing companies according to Section 151 GewO (Gewerbeordnung [Austrian Trade Act]) 1994. These rules of conduct also determine the data protection roles between direct marketing companies and customers when using marketing addresses.

In other cases, there is a case law of the data protection authority on the question of commissioned data processing, for example on the work of lawyers[3], tax consultants[4], debt collection agencies[5] or credit agencies[6].

Step 5 – Purposes

Who determines the purposes of the processing?

All data processing is done for a purpose (“Why” is the data processed?), i.e. the processing is intended to achieve a goal. This purpose can be to control another activity, such as the dispatch of a mail item, the creation of a status or to support another objective, e.g. transferring salaries to employees.

Data processing often has several purposes, e.g. customer databases serve on the one hand to provide customers with goods or services and to be able to invoice them, but also to control marketing activities. Clearly, there must be a (possibly different) legal basis for each of these purposes.

If the service provider (possibly together with the data controller) can decide on one of these purposes or has already decided (e.g. may use the data they use for their own marketing purposes), then the service provider is NOT (at least in the context of this activity) a commissioned data processor.

Note: if the service provider is not a commissioned data processor within the meaning of Art. 28 GDPR, the conclusion of a corresponding agreement is not necessary, but a legal basis according to Art. 6 GDPR is required for this use. It may furthermore be necessary to conclude a non-disclosure agreement.

3 K121.810/0013-DSK/2012, DSB-D122.215/0004-DSB/2014, DSB-D122.299/0003-DSB/2015

4 DSB-D122.767/0001-DSB/2018

5 K121.155/0015-DSK/2006, K121.330/0004-DSK/2008

6 DSB-D122.304/0012-DSB/2015 (on the calculated score values)

Step 6 – Means

Who determines the main means of processing?

All data processing is defined by its "means", i.e. the "way in which a result or goal is achieved". The term “means” not only describes the technical methods for processing personal data, but also “how” the data are processed; this includes questions such as "which data are processed?", "which third parties have access to these data?", "when are data deleted?" etc. [7].

Whoever decides on the key means of processing is themselves the data controller, but can give their commissioned data processor leeway in choosing the means. This leeway can be very wide with regard to the use of technical means, e.g. in external marketing, where the commissioned data processor decides on the means used depending on the civil law agreement.

If the data controller does not decide alone about the technical means, they should be fully informed about it. If, on the other hand, a service provider has influence on the purpose, they themselves are the data controller (see above).

Step 7 – Right of use

Can the service provider use the data for their own purposes?

If the service provider has the right to use data, i.e. to use them for their own purposes and/or for purposes defined by them, either for themselves or a third party, they are not a commissioned data processor for this processing operation, but are themselves the data controller – see above under Step 5 – Purposes.

This does not apply to the use of anonymised data or statistical evaluations, for example in order to improve the service provider's products, because anonymised data (i.e. data that can in no way be assigned to a specific or identifiable person) are not subject to data protection law. Note: this does not mean that the service provider also has the authority under civil law to carry out such (anonymised) evaluations. Whether this is permitted or not should be determined from the service contract.

Step 8 – Data subject rights

Who is responsible for answering questions from data subjects?

A key element of the data controller's obligations is exercising the rights of data subjects. Thismeans that the data controller is responsible for informing data subjects, providing information from databases and, in particular, deciding on data erasure and blocking.

The data controller may contractually instruct the commissioned data processor to carry out certain standard steps, e.g. to provide information on behalf of the data subject[8]. If, on the other hand, the service provider can independently decide how to deal with a request from a data subject, i.e. determine, for example, which data to disclose and which data to erase or not according to the request, this suggests that the service provider does not constitute a commissioned data processor but an independent data controller, because they themselves have the authority to decide on the processing of data.

Step 9 – Impression

What impression does the service provider make externally?

Ultimately, the impression that the commissioned data processor makes on affected parties, in particular data subjects, is important: if the commissioned data processor acts externally as if they are authorised to dispose of or make decisions with regard to data, this can mean that they themselves are the data controller, or at least considered as such by the data protection authority, and can be held accountable[9].

The principle of good faith and the requirement of transparency mean that the data controller must be disclosed in a proper manner, in particular so that data subjects can assert their rights under data protection law.

---

[6] WP 167 of Art. 29 Data Protection Working Party of 16/2/2010

[7] If this is the case and the service provider may act on behalf of the data controller vis-à-vis data subjects, the risk of being sanctioned for non-compliant behaviour naturally remains with the data controller.

[8] At most in the form of “joint responsibility” pursuant to Art. 26 GDPR