The concept of controller and processor in practice

Daniela Fábián Masoch

March 15, 2019

Table of contents

1 Introduction

If several persons are involved in the processing of personal data, the question inevitably arises as to their data-protection-related role. With the introduction of the GDPR and the provisions regarding the relationship of controllers and processors in article 28 and joint controllers in article 26, the difficulties in determining the correct roles of the parties remain. Organizations are increasingly faced with the challenge of determining their role(s), in particular in complex situations and business models where multiple parties in different jurisdictions are involved in the processing activity, each with varying degrees of autonomy, control and responsibility.

The distinction between the different roles is crucial to allocate responsibilities, and in particular to determine which party must primarily comply with the data protection principles, data subjects' privacy rights and notification obligations. The distinction is further essential to determine the applicable law in a cross-border context, the contractual arrangements, and the allocation of liability for damages resulting from unlawful processing.

Following the GDPR, each person that processes personal data is, from a data protection perspective, either a controller or a processor. If several controllers are involved in the processing of personal data, they are, depending on the concrete situation, either joint controllers or independent controllers. The GDPR defines in article 4 the terms "controller," "processor," and "processing," and in article 26 the concept of "joint controller:"

The **"controller"** is 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.

"Joint controllers" are controllers that jointly determine what data shall be processed for what purpose and by which means.

The **"processor"** is the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The term **"processing"** covers any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The term **independent controllers** is not defined in the GDPR. The term, as used in this article, means controllers that, differently than joint controllers, do not determine the purposes and means jointly for the processing of personal data, but each for itself for own and different purposes from each other.

In this article, we will explore the essential factors for determining the roles of the parties, and in particular the relationship between customers and service providers, and their consequences.[1]

[1] Detailed analyses on the concept and several examples can be found in (a) the WP169, (b) the ICO guidance, (c) the Leitfaden Bitkom and (d) the DSK Kurzpapier Nr. 13.

2 The essential factors for determining the role(s) of the parties

2.1 The essential factors

The principal factors for determining if a party is a controller, joint controller or a processor are on the one hand the degree of autonomy of each person in determining for what purposes, how and in what manner personal data is processed, and on the other hand the degree of control over the content of personal data. Such determination is always a factual one and must be taken on a case-by-case basis considering each specific processing operation.

In a first step, however, it must be assessed whether the organization that is holding personal data "processes" such data, and if so, in which ways. While the definition of "processing" is pervasive and covers anything that is done with personal data, there are situations where an organization holding personal data does not qualify as neither a controller nor a processor because it does not process the data in the sense of the law. The ICO provides an example[2], where a courier service is contracted by a local hospital to deliver envelopes containing patient's medical records to other health service institutions. While the courier is in physical possession of the personal data, it does not process the data contained in the letters, since it may not open the mail to access any personal data or other content. Processing personal data implies a degree of access to or the ability to control the use of the data itself. The physical possession of the letters containing personal data is not sufficient. The organization that chooses to use the delivery services to transfer personal data is the controller in this scenario and is responsible for complying with the requirements under the GDPR, and, in particular, to organize such services in such a way that the personal data are adequately protected and, if necessary, an obligation of confidentiality is in place. The critical factor in this case is that the service provider has no plan, intention and interest to process the personal data.

The mail delivery service will, however, be a controller in its own right in respect to any personal data such as, for example, individual senders' and recipients' names and addresses it holds to arrange delivery or tracking.

2.2 Controller

An organization is a controller if, through its managers and staff, it decides why and how personal data shall be processed and therefore controls the overall purposes and means of data processing. As a general rule, the legal entity is considered the controller rather than the individual that acts on behalf of the legal entity.[3] The capacity for determining the purposes and means of processing may derive from legal circumstances, such as a legal obligation, or from factual circumstances.

The controller processes (or engages another person to process on its behalf) personal data for its own purposes and typically determines:

- to initiate a processing activity;
- what personal data to collect, from whom, from what sources and for what purposes;
- how the data shall be processed;
- whether to share personal data with third parties and if so with whom;
- whether to engage one or several processors for processing the data on its behalf;
- whether to modify, anonymize or delete the data; and
- for how long the data is stored.

[2] ICO guidance where additional explanation can be found in notes 33-39

[3] WP 169, section III.1.c

The controller usually interacts directly with data subjects who expect the organization to be the controller, although direct interaction is not a prerequisite and may not always be the case, such as, for example, in a clinical trial context where the pharmaceutical company, and sponsor of the trial, does generally not even know the identity of the study participants. The controller must retain control over the data but must not necessarily have access to or process the personal data.[4]

An organization that processes personal data based on a legal obligation, for example, a tax authority or a social insurance office, or a specialist that processes personal data in accordance with its own professional obligations, such as a legal attorney or an accountant, is generally considered a controller and retains overall responsibility for the specific processing activity. However, in cases where an accountant provides other than accountant services, such as payroll services, it becomes a processor.

2.3 Joint controller

Where two or more controllers jointly determine the purposes and means of data processing according to the criteria mentioned above, they are joint controllers. The wish of the parties involved to be jointly responsible is not sufficient to assume joint controllership. The factual circumstances and the behavior in determining the purposes and means are essential. The European Court of Justice provided some clarifications in its decision of June 2018 (Wirtschaftsakademie) where it ruled that the operator of a Facebook fan page is a joint controller with Facebook for the processing of personal data.[5] In a further decision of July 2018 (Jehovan), the European Court of Justice further clarified that it is sufficient that a person or entity that exerts influence over the processing of personal data, for its own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller.[6] In spite of these decisions, the uncertainty as to which level of co-determination is sufficient to assume joint controllership is still unclear and must be examined on a case-by-case basis.

2.4 Processor

A service provider is a processor under the conditions, that the service provider (a) processes personal data (b) on behalf of the controller and (c) under the controller's instructions. These factors are essential for the service provider to be a processor. Otherwise, and in particular, where the service provider has a certain degree of autonomy in making decisions or in controlling the content of the data, it may be a controller, eventually a joint controller. This does not mean, however, that the processor may not take any decisions. In practice, the controller may delegate some decisions relating to the technical and organizational questions to the processor, such as which hardware or software to use while still determining substantial questions such as the type of personal data to be processed, the retention period or the access rights.[7] The question arises as to the degree to which the processor may decide on the means of processing on behalf of the controller without himself becoming a controller. The GDPR states in article 28 para. 10 that a processor becomes a controller as soon as it determines the purposes and means of processing. In practice, this means, that as soon as the processor goes beyond the instructions of the controller, it becomes a controller. This is the case where a service provider uses the data for its own purposes, for example, for conducting analytics and improving its own services. When determining if a service provider is a processor or a controller, respectively a joint controller for a specific processing activity, the following should be taken into consideration:

[4] Decision C-210/16 Wirtschaftsakademie, note 38

[5] Decision C-210/16 Wirtschaftsakademie, note 44

[6] Decision C-25/17 Jehovan, consideration of the questions referred, the third and fourth questions

[7] WP 169, section III.2

- the margin of maneuver that is left to the processor. The more detailed instructions the controller gives, the smaller is the margin of maneuver for the service provider;
- the level of control the controller wants to exercise;
- the expectations of the data subjects of who the controller is. This will depend on the information received from the controller.[8]

Typically, a processor

- processes the data based on a mandate by the customer;
- has no control over the data and does not decide what data to collect and how to use it;
- has no own business interest in processing the data;
- is contractually or legally prohibited to use the data for own purposes;
- provides technical and operational support to the customer;
- has no contractual relationship with the data subjects concerning the processing activity;
- is not expected by the data subjects to be the controller.

Depending on the specific circumstances, the level of instructions and the control by the customer, the service provider may be a processor, joint or independent controller.[9]

3 The consequences for each role

3.1 The organization is a controller

If an organization qualifies as a controller, it is responsible for complying with the data protection principles, and in particular must have a legal basis for processing the personal data and must comply with the GDPR requirements, such as providing notice to data subjects and granting data subject access rights. The organization has the freedom to engage one or several processors to process personal data on its behalf, subject to specific instructions regarding the purposes and ways of processing while remaining in control of and responsible for the data. In this case, the organization must ensure to have a Data Processing Agreement in place with such processors in line with article 28 GDPR.

A controller may also share personal data with another controller, without being a joint controller. For example, if an address broker sells personal data to an organization that processes that data for customer relation and marketing purposes, both organizations are controllers. Because they determine their purposes and means of processing separately from each other they are considered **independent controllers.** The GDPR does not mandate any particular contract or arrangement in this case, unless personal data is shared cross-border from the EEA to a country that does not provide an adequate level of data protection, in which case appropriate safeguards must be put in place, such as EU Standard Contractual Clauses. Nevertheless, because each party is responsible and liable for complying with the GDPR, and, in particular, with the principle of purpose limitation, it is recommended to establish a Data Sharing Agreement outlining the main obligations of the parties.

3.2 The organization is a joint controller

If the organization is a joint controller, it must, together with the other joint controllers, enter into an arrangement (such as a Joint Controller Agreement) setting out their respective responsibilities in complying with the GDPR. While the controllers must jointly determine the purposes and means of processing, such

[8] WP 169, section III.2

[9] Examples can be found in the WP 169, the ICO guidance and the DSK Kurzpapier article Nr. 13

determination and the related responsibilities must not be equally shared among the parties but must be clearly outlined in the arrangement, in particular as regards:

- responding to data subject access rights;
- carrying out any data protection impact assessments;
- notifying data breaches; and
- informing individuals about the processing of their data according to article 13 and 14 GDPR.

Further, the essence of the arrangement must be made available to data subjects who can reach out to each joint controller to exercise their privacy rights.

3.3 The organization is a processor

If the service provider is a processor, it must only process personal data on behalf of the controller and only on its instructions. The obligations of the parties must be specified in a Data Processing Agreement based on article 28 GDPR. The processor must, also, comply with all statutory obligations such as maintaining a record of processing activities or appointing a data protection officer, if the requirements under the GDPR are met.

Keep in mind the following:

- An organization may be a controller for certain processing activities and a processor for other processing activities.
- Not all service providers are also processors (if so, they must, however, sign a data processing agreement).
- While it is essential that the controller determines the purposes of the processing, in practice, the decision on the technical and organizational means for processing, such as storage, retrieval or erasure, is often delegated to the service provider. Special attention is required in assessing case by case whether the service provider still qualifies as a processor or as a joint controller.

4 The contractual arrangements

4.1 Data Processing Agreement

The data processing agreement between the controller and the processor must include the following minimum requirements according to article 28 GDPR:

- the subject matter and the duration of processing;
- the nature and purposes of processing;
- the categories of personal data and data subjects;
- the obligations and rights of the controller (legal ground for processing and audit rights);
- the obligations of the processor, including (a) to process personal data only on documented instructions from the controller, (b) to ensure that only persons that have committed themselves to confidentiality are authorized to process the data; (c) to take all technical and organizational measures (article 32 GDPR) appropriate to the risk; (d) to only engage sub-processors with the prior specific or general written authorization of the controller, to inform the controller about new sub-processors and to contractually impose on such sub-processors the same obligations as imposed on the processor, whereby the processor remains liable to the controller for any failure of the sub-processors; (e) to assist the controller for inquiries and data subjects' access requests; data breach notification and carrying out of data protection impact assessments; (f) at the end of the provision of services, and at the choice of the controller, to delete or return the personal data to the controller; (g) to make available to the controller all information necessary to demonstrate compliance with the

obligations laid down in article 28 GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller; (h) to inform the controller immediately if, in the processor's opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions;

- a procedure on how to prove compliance with the obligations laid down in article 28 GDPR.

Further, clarification in respect to the roles of the parties, cross-border data transfers, notification obligations, allocation of costs for assistance and audits or a provision regarding the liability are recommended, although those provisions are not mandatory under article 28 GDPR.

4.2 Joint Controller Arrangement

According to article 26 GDPR, the joint controllers must, using an arrangement between them, determine their respective responsibilities for compliance with the obligations under the GDPR. The law does not specify in detail what elements must be covered and therefore the parties have, in contrary to the data processing agreement under article 28 GDPR, a certain level of flexibility. The arrangement, be it an agreement or a policy, should outline the purposes and means of the processing and cover the following questions:

- Who provides notice to the data subjects following article 13 and 14 GDPR?
- With whom should the data subjects exercise their privacy rights (contact person)?
- Who will handle data subjects' access requests and other rights?
- Who will handle complaints and requests from supervisory authorities?
- Who will make available the essence of the joint controller arrangement to data subjects?
- Who will appoint a DPO, if required?
- Who will determine, document and monitor the technical and organizational security measures?
- Who will carry out a data protection impact assessment, if needed?
- Who will engage processors, if any?
- Who will keep the record of processing activities?
- Who will determine if a data breach must be notified to supervisory authorities and data subjects and handle such notifications?

4.3 Data Sharing Agreement

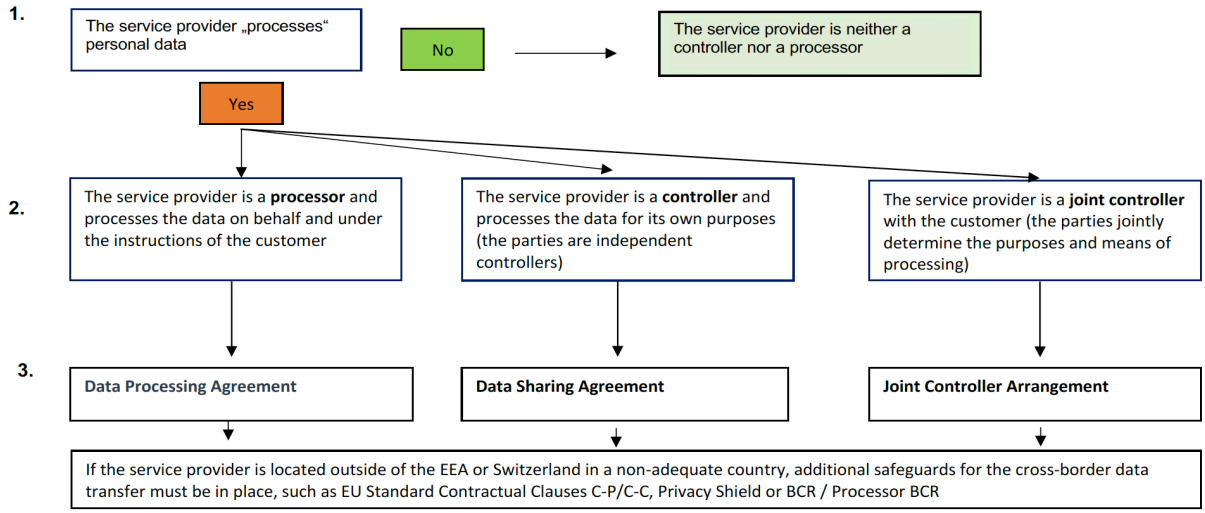
The GDPR is silent concerning data sharing agreements between independent controllers. An agreement is currently only mandated where controllers share personal data cross-border to a non-adequate country (EU Standard Contractual Clauses for Controllers[10]). However, even if there is no cross-border transfer of personal data, it is recommended taking into account the nature of the data sharing and the sensitivity of the personal data to be shared to outline, at a minimum, the principal obligations of the parties, and in particular to only process the data in accordance with the general privacy principles, the purposes of processing, whether the data can be disclosed to third parties, and if so, under what condition, the agreement to provide mutual assistance, if reasonably required, the implementation of security measures as well as indemnification and liability.

[10] EU Standard Contractual Clauses for Cfor conontrollers

5 The procedure for determining the roles and the appropriate contractual arrangement

Summarizing, the steps to be taken whenever multiple parties are involved in the processing of personal data, and in particular, where one or several service providers are engaged, are the following:

1. Assess what services the service provider shall provide and if such services require the processing of personal data.
2. Assess the role(s) of the service provider.
3. Establish the appropriate contractual arrangement(s) covering the responsibilities of the parties.



6 Conclusion

With the introduction of the GDPR and the provisions on the relationship between controllers and processors in article 28 and joint controllers in Article 26, the difficulties in determining the roles of the parties remain. The evaluation is particularly difficult in complex situations and business models in which several parties in different jurisdictions are involved in the processing activity, each with different degrees of autonomy, control and responsibility.

The main factors in determining whether a party is a controller, joint controller or processor are, on the one hand, the degree of autonomy of each party in determining for what purposes, how and in what manner personal data are processed and, on the other hand, the degree of control over the content of personal data. The determination of roles is always factual and must be made on a case-by-case basis, taking into account each processing operation.

7 References

- Article 29 Data Protection Working Party: Opinion 1/2010 on the concept of "controller" and "processor" (referenced as WP 169)
- Information Commissioner's Office (ICO): Data controllers and data processors: what the difference is and what the governance implications are (referenced as ICO guidance)
- Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom): Begleitende Hinweise zu der Anlage Auftragsverarbeitung (referenced as Leitfaden Bitkom)
- Judgement of the EU Court of Justice in *Wirtschaftsakademie,* C-210/16, EU:C:2018:388 (referenced as Decision C-210/16 Wirtschaftsakademie)
- Judgement of the EU Court of Justice in Jehovan todistajat C-25/17, EU:C:2018:551 (referenced as Decision C-25/17 Jehovan)
- Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK): Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DS-GVO, Stand 17.12.2018 (referenced as DSK Kurzpapier Nr. 13)
- Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (2004/915/EC) (referenced as EU Standard Contractual Clauses for Controllers)

Daniela Fábián Masoch
FABIAN PRIVACY LEGAL GmbH
Bäumleingasse 10
4102 Basel
Switzerland

Tel: +41 61 544 44 01
Email: daniela.fabian@privacylegal.ch

Daniela is the founder and e and executive director of FABIAN PRIVACY LEGAL, a law firm specialized in international European and Swiss data protection laws, governance, legal compliance, risk management and program implementation. Daniela is an attorney at law, admitted to the bar in Switzerland, and Certified Privacy Professional CIPP/E, CIPM, FIP with over 25 years of legal and practical experience in data protection, security and related matters. She advises multinational companies in a variety of sectors in the EU, Switzerland and the US in assessing, building and implementing privacy strategies, governance models and global privacy programs, with a pragmatic and commercial approach. Before commencing her own business in 2015, Daniela held various positions at Novartis, including the position of Global Head Data Privacy with the responsibility for setting the Group privacy strategic direction and for building, implementing and overseeing the global privacy function and group-wide privacy compliance program, including Binding Corporate Rules.