Factsheet 12:
Data Processing Agreement: choice, form and substance of the contract

Any processing of personal data by a processor must be governed by a contract or other legal act drawn up in writing, including in electronic form, and binding. The controller and the processor may choose to negotiate their own contract, including all compulsory elements, or to rely, in whole or in part, on standard contractual clauses. The Article 28 GDPR lists the elements that have to be set out in the processing agreement. The processing agreement should not, however, merely restate the provisions of the GDPR; rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement.

1.1 Choice of processor

The controller is duty to use «only processors who provide sufficient guarantees to implement appropriate technical and organisational measures», so that the processing meets the requirements of the GDPR and ensures the protection of data subject rights.

The controller is therefore responsible for assessing the sufficiency of the guarantees provided by the processor and should be able to prove that it has taken all of the elements provided in the GDPR into serious consideration.

The controller's assessment of whether the guarantees are sufficient is a form of risk assessment, which will greatly depend on the type of processing entrusted to the processor, and needs to be made on a case-by-case basis, taking into account the nature, scope, context and purposes of the processing, as well as the risks for the rights and freedoms of natural persons.

The following elements should be taken into account by the controller in order to assess the sufficiency of the safeguards:

- The processor's expert knowledge (e.g. technical expertise on security measures and data breaches);
- The processor's reliability;
- The processor's resources.

The reputation of the processor on the market may also be a relevant factor to be taken into account by controllers. The controller should, with appropriate intervals, verify the guarantees of the processor, including through audits and inspections, where appropriate.

Update : 4th June 2024

Factsheet 12:
Data Processing Agreement: choice, form and substance of the contract

1.2 Form of the contract or other legal act

Any processing of personal data by a processor must be governed by a contract or other legal act, concluded between the controller and the processor, as required by Article 28(3) GDPR.

In order to avoid difficulties in demonstrating that the contract is actually in force, it is recommended that each party to the contract signs the contract.

Since the GDPR establishes a clear obligation to conclude a written agreement, where no other relevant legal act is in force, the absence of a contract constitutes a violation of the GDPR. Both the controller and the processor are responsible for ensuring that a contract or other legal act governs the processing.

In order to comply with the duty to enter into a contract, the controller and the processor may choose to negotiate their own contract, including all compulsory elements, or to rely, in whole or in part, on standard contractual clauses in relation to obligations under Article 28.

An agreement between the controller and the processor must comply with the requirements of Article 28 GDPR to ensure that the processor processes personal data in accordance with the provisions of the GDPR. Such an agreement should take into account the specific responsibilities of controllers and processors.

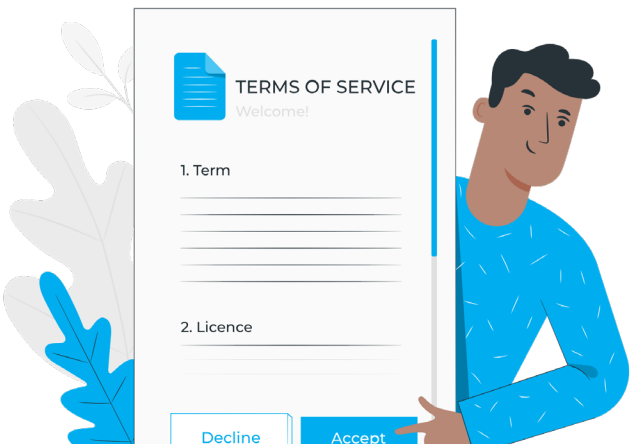
1.3 Content of the contract or other legal act

While the elements referred to in Article 28 of the Regulation constitute the core content of the agreement, the latter should be a way for the controller and the processor to further clarify how such core elements are going to be implemented with detailed instructions. Therefore, the processing agreement should not merely restate the provisions of the GDPR: it should include more specific and concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement.

At the same time, the contract should take into account «the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject». Generally speaking, the contract between the parties should be drafted in light of the specific data processing activity. For instance, there is no need to impose particularly stringent protections and procedures on a processor entrusted with a processing activity from which only minor risks arise. While each processor must comply with the requirements set out by the Regulation, the measures and procedures should be tailored to the specific situation.

Moving on to the required content of the contract or other legal act, European Data Protection Board interprets Article 28(3) in a way that it needs to set out:

- The **subject-matter** of the processing (for instance, video surveillance recordings of people entering and leaving a high-security facility). While the subject matter of the processing is a broad concept, it needs to be formulated with enough specifications so that it is clear what the main object of the processing is;



Update : 4th June 2024

Factsheet 12:
Data Processing Agreement: choice, form and substance of the contract

- The **duration** of the processing: the exact period of time, or the criteria used to determine it, should be specified; for instance, reference could be made to the duration of the processing agreement;

- The **nature** of the processing: the type of operations performed as part of the processing (for instance: "filming", "recording", "archiving of images", etc.) and **purpose** of the processing (for instance: detecting unlawful entry). This description should be as comprehensive as possible, depending on the specific processing activity, so as to allow external parties (e.g. supervisory authorities) to understand the content and the risks of the processing entrusted to the processor;

- The **type of personal data**: this should be specified in the most detailed manner as possible (for instance: video images of individuals as they enter and leave the facility). It would not be adequate merely to specify that it is "personal data pursuant to Article 4(1) GDPR" or "special categories of personal data pursuant to Article 9". In case of special categories of data, the contract or legal act should at least specify which types of data are concerned, for example, "information regarding health records", or "information as to whether the data subject is a member of a trade union';

- The **categories of data subjects**: this, too, should be indicated in a quite specific way (for instance: "visitors", "employees", delivery services etc.);

- The **obligations and rights of the controller**: the rights of the controller are further dealt with in the following sections (e.g. with respect to the right of the controller to perform inspections and audits). As regards the obligations of the controller, examples include the controller's obligation to provide the processor with the data mentioned in the contract, to provide and document any instruction bearing on the processing of data by the processor, to ensure, before and throughout the processing, compliance with the obligations set out in the GDPR on the processor's part, to supervise the processing, including by conducting audits and inspections with the processor.