Data Processing Clauses

The examples of processing clauses below are proposed pending the adoption of standard contractual clauses within the meaning of Article 28.8 of general data protection regulation. These examples of clauses may be inserted in your contracts. They must be adapted and specified according to the processing activities concerned. Please note that they do not constitute, on a standalone basis, a data processing agreement.

…, located at … and represented by … (hereafter, “data controller”)

on the one hand,

AND

…, located at … and represented by … (hereafter, “data processor”)

on the other hand,

I. Objective

The purpose of these clauses is to define the conditions under which the data processor must carry out on behalf of the data controller the operations for the processing of personal data as set forth below.

Within the framework of their contractual relationship, the parties must comply with applicable data protection laws and, in particular, EU Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 which will apply as of May 25, 2018 (hereafter, “general data protection regulation”).

II. Description of the data processing activity

The data processor is authorized to process personal data on behalf of the data controller which are necessary to provide the following service(s) ….

The nature of data processing activities is ….

The purpose(s) of data processing is/are ….

The personal data processed are ….

The categories of data subjects concerned are ….

For the performance of the service covered by this agreement, the data controller will provide the data processor with the following necessary information ….
III. Duration of the agreement

The current agreement will enter into force on […] for a period of […].

IV. Obligations of the data processor to the data controller

The data processor must:

1. Process data only for the purpose(s) of the data processing [under this agreement];

2. Process data in accordance with the documented instructions of the data controller set out in the annex to the current agreement. If the data processor considers that an instruction infringes the general data protection regulation, or any provision of European Union law or of a Member State’s law related to data protection, it should immediately inform the data controller. In addition, if the data processor is required to transfer data to a third country or to an international organization, under European Union law or the Member State law to which it is subject, it must inform the data controller of this juridical obligation before processing the data, unless such law prohibits such information for important reasons of public interest;

3. Guarantee the confidentiality of personal data processed within the framework of this agreement;

4. Ensure that the persons authorized to process personal data under the current agreement:

   • respect the confidentiality of the data subjects or are subject to an appropriate legal obligation of confidentiality and

   • receive the necessary training in relation to personal data protection; and

5. Take into account, in relation to its tools, products, applications or services, the principles of data protection by design and data protection by default.

6. Data processing

Choose one of the two options

Option A (general authorization)

The data processor may use another data processor (hereafter, “sub-processor”) to carry out specific processing activities. In this case, it must inform the data controller prior to the processing and in writing of any change envisaged concerning the addition or replacement of other data processors. This information must clearly indicate the subcontracted processing activities, the identity and the contact details of the data processor, and the dates of the processing agreement. The data controller has a minimum period of […] from the date of receipt of this
information to present its objections. This sub-processing may only be carried out if the data controller has not raised any objections during the agreed period.

**Option B (specific authorization)**

The data processor is authorized to call upon the entity [...] (hereinafter, “sub-processor”) to conduct the following processing activities: [...].

The data processor must obtain the prior written consent of the data controller to hire other sub-processors.

**Either option (general or specific authorization)**

The sub-processor is required to comply with the obligations of this agreement on behalf of and according to the instructions of the data controller. The initial data processor must ensure that the sub-processor offers the same sufficient guarantees regarding the implementation of appropriate technical and organizational measures to ensure that the processing meets the requirements of the general data protection regulation. If the sub-processor does not meet its data protection obligations, the data processor remains fully liable to the data controller for the performance by the sub-processor of its obligations.

7. **Notice to data subjects**

*Choose one of the two options*

**Option A**

The data controller is responsible for providing notice to data subjects regarding processing activities at the time of data collection.

**Option B**

At the time of data collection, the data processor must provide data subjects with notice as to its data processing activities. The wording and format of such notice must be agreed upon with the data controller prior to data collection.

8. **Data subjects’ rights**

Where feasible, the data processor must assist the data controller in fulfilling its obligation to follow up on requests for the exercise of the data subjects’ rights: right of access, rectification, deletion and objection, right to restriction of processing, right to data portability, and right not to be subject to automated individual decision-making (including profiling).

*Choose one of the two options*

**Option A**

When the data subjects concerned submit requests for the exercise of their rights to the data processor, the data processor must address these requests upon receipt by email to [...] (indicate a contact person at the data controller).
Option B

The data processor must respond, on behalf and in the name of the data controller and within the timing set out in the general data protection regulation, to the requests of data subjects as to the exercise of their rights in relation to the data processed by the data processor under the current agreement.

9. Notification of personal data breaches

The data processor will notify the data controller of any personal data breach within a maximum period of [...] hours after becoming aware of it and by the following means [...]. This notification shall be accompanied by any relevant documentation to enable the data controller to notify the competent supervisory authority about this breach, if necessary.

Possible option

After obtaining the consent of the data controller, the data processor will notify the competent supervisory authority (CNIL) about the personal data breach, on behalf and in the name of the data controller, as soon as possible and if feasible, no later than 72 hours after becoming aware of it, unless the breach is not likely to entail a risk to the rights and freedoms of the data subjects.

The notification must include at least the following:

- A description of the nature of the personal data breach including, where possible, the categories and the approximate number of data subjects and the categories and approximate number of personal data records concerned;

- The name and contact details of the data protection officer or other contact point where more information can be obtained;

- A description of the likely consequences of the personal data breach; and

- A description of the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide the required information at the time of the notification, the information may be provided in phases without undue further delay.

After obtaining the consent of the data controller, the data processor will inform the data subject, on behalf and in the name of the data controller, of the personal data breach as soon as possible, where such breach is likely to entail a high risk to the rights and freedoms of the data subjects.

The data subject notification must describe in clear and simple terms the nature of the personal data breach and should include at least the following:
• A description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects and the categories and approximate number of personal data records concerned;

• The name and contact details of the data protection officer or other contact point where more information can be obtained;

• A description of the likely consequences of the personal data breach; and

• A description of the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10. The data processor will provide assistance to the data controller to comply with its obligations

The data processor must assist the data controller in carrying out data protection impact assessments.

The data processor must assist the data controller in carrying out a prior consultation with the supervisory authority.

11. Security measures

The data processor must implement the following security measures:

Describe the technical and organizational measures that ensure a level of security adapted to the risk, including:

• Pseudonymization and encryption of personal data;

• The means to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

• The means to restore the availability of and access to personal data within an appropriate time period in the event of a physical or technical incident; and

• A procedure to regularly test, analyze and evaluate the effectiveness of technical and organizational measures to ensure the safety of the processing.]

The data processor must implement the security measures provided for in [code of conduct, certification].

[Given that Article 32 of the general data protection regulation provides that the implementation of security measures is the responsibility of the data controller and the data processor, it is recommended to clearly allocate the responsibilities of each party with regard to the measures to be implemented.]

12. Outcome of the data processing
Upon completion of the services related to the data processing, the data processor must:

At the choice of the parties:

- Destroy all personal data;
- Return all personal data to the data controller; or
- Forward the personal data to the data processor appointed by the data controller.

The return or forwarding of data must be accompanied by the destruction of all existing copies of such data in the data processor’s information systems. Once the data are destroyed, the data processor must confirm the destruction in writing.

13. Data protection officer

The data processor will notify the data controller about the name and contact details of its data protection officer, if it has appointed one in accordance with Article 37 of the general data protection regulation.

14. Records of the categories of processing activities

The data processor must keep written records of all categories of processing activities carried out on behalf of the data controller comprising:

- The name and contact details of the data controller on whose behalf it is acting, any data processors and, where applicable, the data protection officer;
- The categories of processing activities performed on behalf of the data controller;
- Where appropriate, transfers of personal data to a third country or to an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in Article 49, paragraph 1, second subparagraph of the general data protection regulation, the documents evidencing the existence of appropriate safeguards;
- Where feasible, a general description of technical and organizational security measures, including, inter alia, if needed:
  - pseudonymization and encryption of personal data;
  - means to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - means to restore the availability of and access to personal data within an appropriate time period in the event of a physical or technical incident;
•a procedure to regularly test, analyze and evaluate the effectiveness of technical and organizational measures to ensure the safety of the processing.

15. **Documentation**

The data processor will make available to the data controller **the documentation necessary to demonstrate compliance with all of its obligations** and to enable audits, including inspections, carried out by the data controller or another auditor it has appointed, and contribute to these audits.

V. **Obligations of the data controller to the data processor**

The data controller must:

1. Provide the data processor with the data referred to in Section II of the current clauses;
2. Document in writing any instructions concerning the processing of data by the data processor;
3. Ensure, in advance and throughout the duration of the processing, that the data processor complies with the requirements of the general data protection regulation; and
4. Supervise the data processing, including conducting audits and inspections with the data processor.