Free translation into English

Spanish DPA - February 2017

Example of contractual clauses when the data processor processes the data in its premises and exclusively with its systems

(These clauses are for guidance only and shall be adapted to the specific circumstances of the processing activity undertaken)

1. Subject-matter of the processing agreement

By virtue of these clauses, the following entity ...., is entitled to act as a data processor, in order to process on behalf of ...., the data controller, the personal data which are necessary to render the services of ....**..**

The processing activities shall consist of: *(detailed description of the service)*

The specific processing activities to be carried out are:

- ☐ Collection
- ☐ Recording
- ☐ Structuring
- ☐ Modification
- ☐ Conservation
- ☐ Extraction
- ☐ Consultation
- ☐ Disclosure by transmission
- ☐ Diffusion
- ☐ Interconnection
- ☐ Matching process
- ☐ Restriction
- ☐ Erasure
- ☐ Destruction
- ☐ Conservation
- ☐ Disclosure
- ☐ Other:..

2. Identification of the concerned information

In order to carry out the activities derived from the compliance with the subject-matter of this processing agreement, the *entity/body*...................................., data controller, shall make available to the entity ...., data processor, the information described below:

• …………………………………………

• …………………………………………

3. Term

This agreement has a term of ....[1]

Upon termination of this agreement, the data processor shall *delete/return to the data controller/return to another data processor designated by the data controller (choose the applicable option)* the personal data and delete any copy in its possession.

---

[1] In some events, in particular, certain events subject to administrative law (public contracts, management agreements of public services, etc.), the term of the processing agreement may be restricted by the term set forth in the legislation that apply to the rendering of services.

Example of contractual clauses when the data processor processes the data in its premises and exclusively with its systems

(These clauses are for guidance only and shall be adapted to the specific circumstances of the processing activity undertaken)

4. Obligations of the data processor

The data processor and its entire staff shall:

a. Use the personal data that are processed, or which are collected for their incorporation, only for the purpose which is the subject-matter of this processing agreement. In no event, it will be entitled to use the data for its own purposes.

b. Process the data in accordance with the instructions of the data controller.

   If the data processor considers that any instruction violates the GDPR or any other EU/Member State's data protection provision, the data processor shall immediately inform the data controller thereof.

c. Keep an inventory in writing[2] of all of the categories of processing activities carried out on behalf of the data controller, which shall contain:

   1. The name and contact details of the data processor(s) and of each data controller on behalf of which the data processor acts and, as the case may be, of the representative of the data controller or data processor and of the Data Protection Officer.

   2. The categories of processing activities carried out on behalf of each data controller.

   3. As the case may be, the transfers of personal data to a third country or international organization, including the identification of said third country or international organization and, in case of transfers under Article 49(1), 2nd para. of the GDPR, the documentation of appropriate guarantees.

   4. A general description of the technical and organizational security measures regarding:

      a) The pseudonymisation and encryption of personal data.

      b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

      c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

      d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

d. Not disclose the data to third parties, unless expressly authorized by the data controller, in the events legally admissible.

   The data processor may disclose the data to other data processors of the same data controller, in accordance with the instructions of the data controller. In this case, the data

---

[2] The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organization employing fewer than 250 persons, unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) of the GDPR or personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR.

Free translation into English

Spanish DPA - February 2017

Example of contractual clauses when the data processor processes the data in its premises and exclusively with its systems

(These clauses are for guidance only and shall be adapted to the specific circumstances of the processing activity undertaken)

controller shall previously identify in writing the recipient entity, the data to be disclosed and the security measures to be applied to the disclosure.

If the data processor shall transfer personal data to a third country or international organization, by virtue of EU/Member State law applicable to the data processor, it shall previously inform the data controller of this legal requirement, unless such law prohibits it by important reasons of public interest.

e.   Subcontracting

(Choose one of the options)

Option A   *Not subcontract any of the activities that are the subject-matter of this agreement and which entail the processing of personal data, except the ancillary services that are necessary for the normal performance of the data processor's services.*

If it was necessary to subcontract any processing activity, this fact shall be previously disclosed in writing to the data controller, no later than ....[3], indicating the processing activities intended to be subcontracted and identifying in a clear and unambiguous manner the subcontracting entity and its contact details. The subcontracting may be carried out if the data controller does not object in the agreed term.

The subcontractor, which shall also be considered a data processor, shall likewise be obliged to comply with the obligations which are set forth in this agreement for the data processor and with the data controller's instructions. The original data processor shall regulate the new relationship in order that the new data processor shall be imposed the same terms and conditions (instructions, obligations, security measures …) and formalities, regarding the appropriate processing of personal data and the guarantee of the data subjects' rights. In case of breach by the sub-processor, the initial data processor shall be fully liable to the data controller for the compliance of that other processor's obligations.

Option B   *The data processor is authorized to subcontract in the company .... the following processing activities: ....*

In order to subcontract in other companies, the data processor shall notify in writing the data controller, identifying in a clear and unambiguous manner the subcontracting company and its contact details. The subcontracting may be carried out if the data controller does not object in the term of………………[4].

The subcontractor, which shall also be considered a data processor, shall likewise be obliged to comply with the obligations which are set forth in this agreement for the data processor and with the data controller's instructions. The original data processor shall regulate the new relationship in order that the new data processor shall be imposed the same terms and conditions (instructions, obligations, security measures …) and formalities, regarding the appropriate processing of personal data and the guarantee of the data subjects' rights. In case

---

[3] A minimum notice period is advisable.
[4] A minimum notice period is advisable.

Spanish DPA - February 2017

Example of contractual clauses when the data processor processes the data in its premises and exclusively with its systems

(These clauses are for guidance only and shall be adapted to the specific circumstances of the processing activity undertaken)

of breach by the sub-processor, the initial data processor shall be fully liable to the data controller for the compliance of that other processor's obligations.

f.   Keep secret the personal data it accessed by virtue of this processing agreement, even after its termination.

g.   Ensure that the persons authorized to process the personal data have expressly committed themselves to confidentiality[5] in writing and to observe the applicable security measures, of which they should have been informed appropriately.

h.   Keep available to the data controller the documentation which evidences the compliance with the obligation set forth in the former paragraph.

i.   Guarantee the necessary data protection training of the persons authorized to process personal data.

j.   Assist the data controller regarding the answer to the exercise of the rights of:

   1.   Access, rectification, erasure and objection

   2.   Restriction of the processing

   3.   Data portability

   4.   Not to be subject to automated individual decisions (including the elaboration of profiles)

   (Choose one of the options)

Option A   *The data processor shall answer, on behalf of the data controller, and within the legal term, the requests of exercise of the rights of access, rectification, erasure and objection, restriction of the processing, data portability and not to be subject to automated individual decisions regarding the data that are the subject-matter of the processing agreement.[6]*

Option B   *When the data subjects exercise their rights of access, rectification, erasure and objection, restriction of the processing, data portability and not to be subject to automated individual decisions before the data processor, it shall notify the data controller by email to the address ………… (address indicated by the data controller). The notification shall be made immediately and, in no event, no later than the working day following the reception of the request[7], jointly, as the case may be, with another information that could be relevant to answer the request.*

---

[5] If there is a statutory confidentiality duty, the nature and scope thereof must be expressly stated.
[6] Even though the delegation in the data processor is a data controller's decision, it is particularly recommended when data are exclusively processed in the data processor's systems.
[7] Recommended term and support in order that the data controller may timely answer the request.

Spanish DPA - February 2017

Example of contractual clauses when the data processor processes the data in its premises and exclusively with its systems

(These clauses are for guidance only and shall be adapted to the specific circumstances of the processing activity undertaken)

k. Right of information

(Choose one of the options)

Option A   *The data processor, upon collection of the data, shall provide the information on the data processing activities that will be carried out. The drafting and format to provide this Information shall be agreed with the data controller prior the data collection.*

Option B   *The data controller shall provide the information upon collection of the data.*

i. Notification of the data security breaches

The processor shall notify the data controller, without undue delay, and in no event within the maximum term of ....[8], and through ......, the security breaches concerning the personal data under its custody and to which it becomes aware, jointly with all the information relevant to document and notify the incident.

This notification shall not be necessary when it is unlikely that this breach constitutes a risk for the rights and freedoms of the individuals. At least the following information shall be provided if available:

a) Description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.

b) The name and contact details of the Data Protection Officer or other contact point where more information can be obtained.

c) Description of the likely consequences of the personal data breach.

d) Description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

(Choose one or the two options)[9]

Option A   *The data processor shall notify the data security breaches to the Data Protection Authority.*

The notification shall contain at least the following Information:

a)   Description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.

---

[8] The term shall be less than 72 hours in any event.

[9] Although it is the data controller which must notify the security breaches to the data protection authority or the data subjects, when the data are exclusively process in the data processor's systems, it may be advisable to allocate these functions to the data processor.

Spanish DPA - February 2017

Example of contractual clauses when the data processor processes the data in its premises and exclusively with its systems

(These clauses are for guidance only and shall be adapted to the specific circumstances of the processing activity undertaken)

b) *The name and contact details of the Data Protection Officer or other contact point where more information can be obtained.*

c) *Description of the likely consequences of the personal data breach.*

d) *Description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

Option B *The data processor shall notify the data security breaches to the data subjects, without undue delay, when it is likely to result in a high risk to the rights and freedoms of individuals.*

The notification shall be made in a clear and plain language and shall, at least:

a) *Explain the nature of the personal data breach.*

b) *Indicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained.*

c) *Describe the likely consequences of the personal data breach.*

d) *Describe 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.*

m. Assist the data controller regarding the data protection impact assessment, where required.

n. Assist the data controller regarding the preparation of the prior consultation to the Data Protection Authority, where required.

o. Make available to the data controller all information necessary to demonstrate compliance with its obligations as well as to conduct audits or inspections, conducted by the data controller or another auditor mandated by the controller.

p. Implement the following security measures:

(Choose one or the two options)

Option A *The following security measures, in accordance with the risk assessment carried out by[10]......, on (date) ......:*

• *.........................*

• *.........................*

• *.........................*

Option B *The security measures set forth in[11] ....*

In any event, it shall implement mechanisms in order to:

---

[10] Indicate whether the risk assessment shall be made by the data controller or the data processor.

[11] Indicate the code of conduct, the seal, the certification or another standard where the applicable measures are defined.

Example of contractual clauses when the data processor processes the data in its premises and exclusively with its systems

(These clauses are for guidance only and shall be adapted to the specific circumstances of the processing activity undertaken)

> a) Guarantee the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
>
> b) Restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
>
> c) Regularly test, assess and evaluate the effectiveness of technical and organizational measures for ensuring the security of the processing.
>
> d) Pseudonymised and encrypt the personal data, as the case may be.

q. Appoint a Data Protection Officer[12] and disclose his/her identity and contact details to the data controller.

r. Destination of the data

(Choose one of the three options)

Option A   *Return to the data controller the personal data and, if applicable, the media containing them, upon termination of the activities.*

The return shall encompass the full deletion of the data existent in the IT equipment used by the data processor.

However, the data processor may keep a copy, with the data duly blocked, in so far a liability arising from the performance of this agreement may be claimed.

Option B   *Return the personal data to the data processor designated in writing by the data controller and, if applicable, the media containing them, upon termination of the activities.*

The return shall encompass the full deletion of the data existent in the IT equipment used by the data processor.

However, the data processor may keep a copy, with the data duly blocked, in so far a liability arising from the performance of this agreement may be claimed.

Option C   *Delete the data, upon termination of the activities. Once deleted, the data processor shall certify the deletion in writing and provide the data controller with the certificate.*

However, the data processor may keep a copy, with the data duly blocked, in so far a liability arising from the performance of this agreement may be claimed.

5. **Obligations of the data controller**

The data controller shall:

a) Provide the data processor with the data to which clause 2 of this agreement refers.

---

[12] The Data Protection officer shall be appointed when:
a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;
c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

Spanish DPA - February 2017

Example of contractual clauses when the data processor processes the data in its premises and exclusively with its systems

(These clauses are for guidance only and shall be adapted to the specific circumstances of the processing activity undertaken)

b)   Carry out a personal data impact assessment of the processing activities to be carried out by the data processor.

c)   Carry out the applicable prior consultations.

d)   Ensure, previously and during all the processing activities, the data processor's compliance with the GDPR.

e)   Monitor the processing, including to conduct inspections and audits.