## 

**ANNEX 1**

**Example of contractual clauses in cases where the processor processes the data on its own premises and exclusively with its own systems**

*(The clauses are purely for guidance and should be adapted to the specific circumstances of the processing being carried out)*

**1. Subject matter of the processing contract**

These clauses authorise ................, the data processor, to process on behalf of the data controller ................, the personal data necessary to perform the service of .....................

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

The specific processing operations to be carried out are:

 Collection  Recording

 Structuring  Alteration

 Storage  Retrieval

 Consultation  Disclosure by transmission

 Dissemination  Combination

 Alignment  Restriction

 Erasure  Destruction

 Communication  Others:..................

**2. Identification of the information concerned**

To perform the services arising from compliance with the purpose of this contract, the entity/body....................................., which is the data controller, makes available to the entity ......................................, the data processor, the information described below:

**• .............**

**• .............**

**• .............**

**3. Duration**

This contract shall remain valid until.............................1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

In some instances, in particular certain cases subject to administrative law (collective agreements, public service management contracts, etc.), the duration of the contract may be limited to the duration the enforceable legislation establishes for the provision of services.

Once this contract has terminated, the processor shall *delete / return to the controller / return to another processor designated by the controller (indicate the option selected)* the personal data and delete any existing copy in its power.

**4. Obligations of the data processor**

The processor and all its staff shall:

1. Use the personal data which are the subject of the processing, or which are collected for inclusion, solely for the purpose which is the subject of this contract. On no account may the said data be used for the processor’s own purposes.
2. Process the data in accordance with instructions received from the controller.

The processor shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

1. Maintain a written record2 of all categories of processing activities carried out on behalf of the controller. That record shall contain all of the following information:
2. The name and contact details of the processor or processors and of each controller on behalf of which the processor is acting and, where applicable, of the controller's or the processor's representative, and the data protection officer.
3. The categories of processing carried out on behalf of each controller.
4. Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards.
5. A general description of the technical and organisational security measures relating to:

* the pseudonymisation and encryption of personal data;
* the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
* the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
* the process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2 The obligations referred to in paragraphs 1 and 2 of the GDPR shall not apply to an enterprise or an organisation 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 Regulation.

1. Not disclose the data to third persons except with the specific authorisation of the controller in legally admissible situations.

The processor may disclose the data to other processors of the same controller, in accordance with the instructions of that controller. In this case, the controller must previously identify in writing the entity to which the data must be disclosed, the data to be disclosed and the security measures that must be applied to proceed with the disclosure.

If the processor has to transfer personal data to a third country or an international organisation by virtue of a Union or Member State law to which the processor is subject, the processor must inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

1. Subcontracting

*(Choose one of the options)*

***OPTION A***

*Not subcontract any of the services that form part of the subject matter of this contract and which involve the processing of personal data, except for auxiliary services necessary for the normal functioning of the processor’s services.*

*If any processing needs to be subcontracted, the controller must be previously informed in writing of this circumstance, giving prior notification of ........................... 3. Such notification must indicate the processing operations to be subcontracted and must clearly and unambiguously identify the subcontracted company, including its contact details. The subcontracting may be carried out provided the controller does not raise any objection within the established time limit*

*The subcontractor, which is also considered a processor, is equally obliged to fulfil the obligations that this document establishes for the initial processor and to follow the instructions laid down by the controller. The initial processor should regulate the new relationship, in such a manner that the new processor is subject to the same conditions (instructions, obligations, security measures, etc.) and to the same formal requirements as the initial processor as regards the correct processing of the personal data and safeguarding of data subjects’ rights. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.*

***OPTION B***

*The processor is hereby authorised to subcontract to the company ....... the service provisions involved in the following processing operations:*

*....................*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3 It is advisable to establish a minimum period for the notification.

*To subcontract to other companies, the processor must notify the controller in writing and must clearly and unambiguously identify the subcontracted company, including its contact details. The subcontracting may be carried out provided the controller does not raise any objection within the time limit of ...............4.*

*The subcontractor, which is also considered a processor, is equally obliged to fulfil the obligations that this document establishes for the initial processor and to follow the instructions laid down by the controller. The initial processor should regulate the new relationship, in such a manner that the other processor is subject to the same conditions (instructions, obligations, security measures, etc.) and to the same formal requirements as the initial processor as regards the correct processing of the personal data and safeguarding of data subjects’ rights. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.*

1. Maintain the duty of confidentiality with respect to the personal data to which it has had access by virtue of this contract, including once performance of the contract has concluded.
2. Ensure that persons authorised to process the personal data have committed themselves expressly and in writing to confidentiality5 and to comply with the corresponding security measures, of which they must be duly informed.
3. Make available to the controller all information necessary to demonstrate compliance with the obligation established in the previous section.
4. Ensure personnel authorised to process personal data receive the appropriate data protection training.
5. Assist the controller in responding to requests for exercising the following rights:
6. Access, rectification, erasure and objection
7. Restriction of processing
8. Data portability
9. Not to be the subject of automated individual decision-making (including profiling)

*(Choose one of the options)*

***OPTION A***

*The processor must respond, on behalf of the controller and within the established time limit, to requests to exercise the rights of access, rectification, erasure and objection, restriction of processing, data portability and not to be the subject of automated individual decision-making, in relation to the data which are the subject matter of the processing contract.*6

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4 It is advisable to establish a minimum period for the notification.

5 If there is a statutory obligation of confidentiality, the nature and extent of that obligation must be expressly recorded in writing.

6 Though it is up to the controller whether to delegate response to the processor, such delegation is particularly advisable in situations where the data are processed exclusively on the processor’s systems.

***OPTION B***

*When data subjects apply to the processor to exercise the rights of access, rectification, erasure and objection, restriction of processing, data portability or not to be the subject of automated individual decision-making, that processor must send notification of same by email to the address .............. (address indicated by the controller). The notification must be immediate and in no case later than the day following the working day on which the request was received7, and must be accompanied, where applicable, by any other information that may be relevant to respond to the request.*

1. Right of information

*(Choose one of the options)*

***OPTION A***

*At the time of collecting the data, the processor must provide information relating to the data processing that will be carried out. The drafting and format in which this information is provided must be agreed with the controller prior to initiating the data collection.*

***OPTION B***

*It is the controller’s responsibility to facilitate the right of information at the time of collecting the data.*

1. Notification of personal data breaches

The processor must notify the controller without undue delay and in any case within a maximum period of ……..8 , and via ........., of any breach of security concerning the data in its charge that it becomes aware of, and must provide all relevant information to enable the incident to be recorded and communicated.

Notification is not necessary when the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7 Period and means recommended in order to enable the controller to respond to the request within the established time limit.

8 The time period must be no more than 72 hours under any circumstance.

The notification should provide, at least, the following information, if available:

1. 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.
2. Name and contact details of the data protection officer or other contact point where more information can be obtained.
3. Description of the likely consequences of the personal data breach.
4. Description of the measures taken or proposed to be taken by the controller 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, it must be provided in phases without undue further delay.

*(Choose one of the options)9*

**OPTION A**

The processor must notify any personal data breach to the competent data protection authority.

The notification should provide, at least, the following information:

1. *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.*
2. *Name and contact details of the data protection officer or other contact point where more information can be obtained.*
3. *Description of the likely consequences of the personal data breach.*
4. *Description of the measures taken or proposed to be taken by the controller 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, it must be provided in phases without undue further delay.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9 Though notification of data breaches to the supervisory authority or the data subjects corresponds to the controller, in cases where the data are being processed exclusively with the processor’s systems it may be advisable to attribute these functions to that processor.

**OPTION B**

The processor must notify any personal data breach to the data subjects without undue delay when it is likely to result in a risk to the rights and freedoms of natural persons.

The notification must be made in clear, plain language, and should at least:

1. *describe the nature of the personal data breach;*

1. *communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*
2. *describe the likely consequences of the personal data breach;*
3. *describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*
4. Provide support, where appropriate, when the controller carries out data protection impact assessments.
5. Provide support, where appropriate, when the controller carries out prior consultations of the supervisory authority.
6. Make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Regulation and allow for and contribute to audits or inspections conducted by the controller or another auditor mandated by the controller.
7. Introduce the following security measures:

*(Choose one or both of the options)*

**OPTION A**

The following security measures, in accordance with the risk assessment carried out by10…….... , on …… :

* *………………….*
* *………………….*
* *………………….*

**OPTION B**

The security measures established in11.................... .....................................................

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10 Indicate whether the risk assessment was carried out by the controller or the processor.

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

In any case, mechanisms must be introduced to:

1. ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
2. restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
3. regularly test, assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of the processing;
4. pseudonymise and encrypt the personal data, where necessary.
5. Designate a data protection officer12 and inform the controller of his or her name and contact details.
6. Final destination of the data after completion of the processing.

*(Choose one of the three options)*

**OPTION A**

Return all the personal data and, where applicable, any medium on which copies may exist, to the controller after the end of the provision of services relating to processing.

Such return must include the complete deletion of all existing data on the computer systems employed by the processor.

Notwithstanding the above, the processor may retain a copy with the data duly blocked while liability arising from performance of the service may exist.

**OPTION B**

Return all the personal data and, where applicable, any medium on which copies may exist, to the processor explicitly designated by a written mandate of the controller, after the end of the provision of services relating to processing.

Such return must include the complete deletion of all existing data on the computer systems employed by the processor.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

12 The data protection officer must be designated where:

1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. 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;
3. the core activities of the controller or the processor consist of the processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

Notwithstanding the above, the processor may retain a copy with the data duly blocked while liability arising from performance of the service may exist.

**OPTION C**

Destroy the data after the end of the provision of services relating to processing. Once destroyed, the processor must certify the destruction in writing and deliver the certificate to the controller.

Notwithstanding the above, the processor may retain a copy with the data duly blocked while liability arising from performance of the service may exist.

**5. Obligations of the data controller**

The data controller shall:

1. deliver to the processor the data referred to in Clause 2 of this document;
2. carry out a data protection impact assessment of the processing operations the processor must carry out;
3. carry out the corresponding prior consultations;
4. ensure, prior to and throughout the processing, that the processor complies with the GDPR;
5. supervise the processing, including the performance of inspections and audits.