General Data Protection Regulation

GUIDE FOR PROCESSORS

SEPTEMBER 2017 EDITION

Applicable from 25 May 2018 across the whole of the European Union, the General Data Protection Regulation (GDPR) strengthens European residents' rights bearing on their data and increases accountability on the part of all stakeholders processing such data (controllers and processors), whether or not they are established in the European Union.

The Regulation lays down specific obligations that must be followed by processors, who are likely to be held liable in the event of a breach.

This guide sets out to assist processors in implementing these new obligations.

All of the good practices reported by professionals may be added to it in time.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Contents

Are you a processor in the meaning of the General Data Protection Regulation?

You are a processor if you process personal data on behalf of, on instructions from and under the authority of a controller.

For the record, **the controller** is the person or body which "*determines the purposes and means of the processing*" (Article 4 of the GDPR – Definitions).

A **very wide variety of service providers have the capacity of processor** in the legal sense of the term. Processors' activities can concern a very specific task (sub-contracting of mail delivery) or be more general and wide-ranging (management of the whole of a service on behalf of another organisation, such as managing the pay of employees or agents for example).

The following are particularly concerned by the GDPR:

- IT service providers (hosting, maintenance, etc.), software integrators, cybersecurity companies or IT consulting companies (formerly known as IT engineering service companies/SSII in French) that have access to data,
- marketing or communication agencies which process personal data on behalf of clients, and
- more generally, any organisation providing a service which entails personal data processing on behalf of another organisation.
- A public authority or association may also be considered as such.

Insofar as they do not have access to or process personal data, software publishers and manufacturers of equipment (such as clocking terminals, biometric equipment or medical equipment) **are not concerned**.

NB:

- An organisation which is a processor is generally the controller for processing which it carries out on its own behalf, rather than for its clients (managing its own staff for example).
- When an organisation determines the purposes and means of processing, it may not be considered a processor: it shall be considered the controller of said processing (Article 28.10 of the GDPR).

Example of qualification of processor and controller

Company A provides a marketing letter delivery service using the client data files of companies B and C.

Company A is a processor for companies B and C insofar as it processes the necessary client data for sending the letters on behalf of and on instructions from companies B and C.

Companies B and C are their clients' management controllers, including as regards the delivery of marketing letters.

Company A is also the controller regarding the management of staff it employs, and the management of its clients which include companies B and C.

Tool: to determine whether you are a processor or the controller, see the Opinion 1/2010 of the Article 29 Data Protection Working Party (WP29) of 16 February 2010, which sets out the bundle of indicators to be used when **analysing on a case-by-case basis**:

- level of instructions given by the client to the service provider: what margin of manoeuvre does the service provider have in delivering its service?
- extent of monitoring over the execution of the service: to what extent does the client "supervise" the service?
- added-value provided by the service provider: does the service provider boast in-depth expertise in the field?
- degree of transparency over use of a service provider: is the service provider's identity known to the data subjects using the client's services?

Official text

Article 4 of the GDPR for the definitions of controller and processor

Article 28.10 of the GDPR on the notion of controller

Are you subject to the General Data Protection Regulation?

You come within the scope of the GDPR as a processor:

- **if you are established in the EU** or;
- **when you are not established in the EU**, if:

  your "*processing activities are related to*

  - *the offering of goods or services to data subjects in the EU;*
  - *or the monitoring of their behaviour as far as their behaviour takes place within the EU*" (Article 3 of the GDPR).

Official text

Article 3 of the GDPR on the Territorial Scope

What is the primary change introduced by the General Data Protection Regulation for processors?

Today:

The obligations of the French Data Protection Act (*Loi Informatique et Libertés*) **are only enforceable as regards the controller**. Indeed, where a processor is used:

- the **contract** between said processor and the controller must indicate the **processor's obligations in terms of protecting data security and confidentiality** and stipulate that the former may only act on instructions from the latter;
- said processor must provide **sufficient guarantees** to ensure the implementation of the security and confidentiality measures set out in Article 34 of the French Data Protection Act;
- this requirement does not release the controller from its obligation to ensure compliance with such measures.

From 25 May 2018:

The GDPR establishes the **accountability principle as regards all stakeholders involved in personal data processing, from the moment such data concern European residents**, whether or not said stakeholders are established within the EU1.

It stipulates **specific obligations that must be followed by processors,** which shall particularly assist controllers in their ongoing efforts to bring their processing operations into compliance.

Official text

Articles 28, 30.2 and 37 of the GDPR on the processor's obligations

1 Recital 13 of the GDPR gives a reminder that adoption of "*a Regulation is necessary to provide legal certainty and transparency for economic operators (...), to provide natural persons in all Member States with* ***the same level of legally enforceable rights and obligations and responsibilities for controllers and processors***".

What are your obligations from 25 May 2018?

When you operate as a processor in the implementation of a personal data processing operation, you must provide your client with "***sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject***" (Article 28 of the GDPR).

In particular, you must assist and advise your client in its compliance with some of the obligations set forth in the GDPR (impact assessments, breach notification, security, destruction of data, contribution to audits).

In practice, this means:

1. A transparency and traceability obligation

You must:

- Draw up with your client a **contract** or other legal document specifying the obligations of each party and setting out the provisions of Article 28 of the GDPR.
- List in writing your client's instructions bearing on the processing of its data to demonstrate that you are acting "*on documented instructions from the controller*".
- Ask your client for written authorisation if, as a processor, you then engage another processor.
- Provide your client with **all necessary information for demonstrating compliance with your obligations** and for enabling the performance of audits (on the basis, for example, of the CNIL standard for the issuing of privacy seals in terms of audit procedures).
- Maintain a **record** of who your clients are and describe the processing you carry out on their behalf.

2. Consideration of the principles of data protection by design and by default

- You are obliged to provide your clients with the **necessary guarantees** that the processing you carry out on their behalf meets the requirements of the GDPR and protects the data subjects' rights. This particularly means that:
    - **by design**, the tools, products, applications or services with which you provide your clients properly take on board the data protection principles, and
    - **by default**, your tools, products, applications or services guarantee that only the data required for the purposes of the processing are processed, as regards the amount of data collected, the extent of their processing, the period of their storage and number of persons having access thereto.
- **To give an example**, these principles may entail:
    - allowing your client to apply default settings at the very least to data collection and not making it a technical requirement to enter data into an optional field
    - only collecting data that are strictly necessary for the purposes of the processing (data minimisation)

- automatically and selectively clearing data from an active database at the end of a certain period, or
- managing IT access rights and clearances on a "data-by-data" basis or at the request of the data subjects (for the social networks for example).

3. An obligation to guarantee the security of data processed

- Those of your employees who process your clients' data must be subject to a confidentiality obligation.
- You must notify your client of any breach of its data.
- You must make every effort to guarantee a level of security appropriate to the risks.
- At the end of your service and in line with your client's instructions, you must:
  - delete all data or return them to your client
  - destroy the existing copies unless there is a legal obligation to retain them.

4. An assistance, alert and advice obligation

- If you are of the opinion that an instruction from your client infringes the rules governing data protection, **you must inform the latter thereof immediately**.
- When a data subject exercises his/her rights (access, rectification, erasure, portability, to object, not to be subject to an automated individual decision, including profiling) you must, **insofar as this is possible**, **assist your client** in responding to said request.
- Given the information at your disposal, **you must assist your client** in guaranteeing compliance with the obligations bearing on the security of processing, notification of a data breach and impact assessment with regard to data protection.

Where should you start?

1. Check whether you have to designate a data protection officer

The Data Protection Officer (DPO) is tasked with overseeing compliance with the GDPR within the organisation which designated him/her.

As a processor, you will be required to designate a DPO in 2018 if:

- You are a public body or authority, or
- Your core activities involve you conducting, on your clients' behalf, regular and systematic monitoring of data subjects on a large scale, or
- Your core activities involve you processing on a large scale, on your clients' behalf, so-called "sensitive" data or data relating to criminal convictions and offences.

Over and above these compulsory cases, designation of a DPO is recommended as this way you will have an expert tasked with the practical implementation and management of compliance with the GDPR.

Examples

The guidelines on data protection officers of the WP29 adopted on 5 April 2017 provide two examples of when **it is compulsory for a processor to designate a DPO**:
Example no.1: a small family business active in the distribution of household appliances in a single town uses the services of a processor whose core activity is to provide website analytics services and assistance with targeted advertising and marketing. The activities of the family business and its customers do not generate processing of data on a 'large scale', considering the small number of customers and the relatively limited activities. However, the activities of the processor, having many customers like this small enterprise, taken together, are carrying out large-scale processing. The processor must therefore designate a DPO under Article 37(1)(b) of the GDPR. At the same time, the family business itself is not under an obligation to designate a DPO.
Example no.2: a medium-size tile manufacturing company subcontracts its occupational health services to an external processor, which has a large number of similar clients. The processor shall designate a DPO under Article 37(1)(c), provided that the processing is on a large scale. However, the manufacturer is not necessarily under an obligation to designate a DPO.

The DPO designated by a processor also oversees activities carried out by the processor organisation when acting as a data controller in its own right (e.g. HR, IT, logistics).

For more information:

See the page on this subject on the CNIL website

Official text

Article 37 of the GDPR on the obligation for a processor to designate a DPO

2. Analyse and revise your contracts

This contract must define:

- the subject-matter and duration of the service you are carrying out on your client's behalf
- the nature and purposes of the processing

- the type of personal data that you are processing on your client's behalf
- the categories of data subjects
- the obligations and rights of your client as the controller
- your obligations as the processor as set out in Article 28 of the GDPR

Clause examples

This guide gives an example of sub-contracting clauses pending the adoption of standard contractual clauses in the meaning of Article 28.8 of the GDPR. These examples of clauses can be inserted into your contracts. They must be tailored and specified according to the sub-contracting service concerned. Please note that they do not constitute a subcontract in themselves.

Official text

Recital 81 and Article 28 of the GDPR on the processor's obligations

3. Draw up a record of processing activities

As the processor, you must maintain a **record of the categories of processing activities** that you carry out on your clients' behalf.

This record must be maintained in writing and contain:

- the name and contact details of each client on behalf of which you process data
- the name and contact details of each sub-processor, where applicable
- the name and contact details of the DPO, where applicable
- the categories of processing carried out on behalf of each client
- the transfers of data outside the EU that you carry out on your clients' behalf, where applicable
- where possible, a general description of the technical and organisational security measures that you set up.

NB

Please also note that you are considered to be the controller for operations you carry out on your own data (for example for managing your staff or your clients) and, as such, **two records must be maintained**: one for the processing operations with regard to which you are the controller and another for the processing operations that you carry out as the processor, on your clients' behalf.

Sample record

A sample record is shown in Step 2: map your personal data processing, in the online guide General Data Protection Regulation: Getting ready in 6 steps

Official text

Article 30-2 of the GDPR on the maintenance of a record by a processor

Article 30-1 of the GDPR on the maintenance of a record by a controller

If I use another processor, what are my obligations?

As a processor, you may only recruit another processor after obtaining **written authorisation from your client**. This authorisation may, at the parties' choosing, be:

- **specific**, which means granted for a specific processor, or
- **general**; you will need to inform your client of any intended change concerning the addition or replacement of processors, thereby giving your client the opportunity to object to such changes.

The processor you recruit is subject to **the same obligations as those stipulated in your contract with your controller client**. It must, in particular, provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing meets the requirements of the GDPR.

Be aware!

If the processor you recruit does not comply with its obligations, you are **fully liable** as regards the controller for this processor's compliance with its obligations.

Official text

Articles 28.2 and 28.4 of the GDPR on a processor engaging another processor

Do the current contracts with my clients need to be amended?

Yes, all of the ongoing subcontracts will have to include the compulsory clauses as set out in the GDPR, on 25 May 2018.

All processors are therefore advised to:

- anticipate this change in applicable legal framework **by already incorporating, via an amendment, the clauses in ongoing contracts with their clients, whilst providing that these shall not come into force until 25 May 2018**
- conduct, from this date, **checks and/or audits** to ensure that you are complying with your obligations as a processor and to make the necessary adjustments.

Clause examples

This guide gives an example of sub-contracting clauses pending the adoption of standard contractual clauses in the meaning of Article 28.8 of the GDPR. These examples of clauses can be inserted into your contracts. They must be tailored and specified according to the sub-contracting service concerned. Please note that they do not constitute a subcontract in themselves.

What is my role in the event of a data breach?

A **data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

You must notify your client of any personal data breach without undue delay after having become aware of it.

On the basis of this notification, your client, as the **controller**, shall have to notify said data breach **to the competent supervisory authority** in accordance with Article 33 of the GDPR and communicate such a breach to the data subject in accordance with Article 34 of the GDPR.

Subject to your client's agreement and provided that this is clearly stipulated in the contract between you and your client, the latter may instruct you to carry out, **on its behalf**, this notification to the authority and, where applicable, to the data subjects (see clause examples at the end of this guide).

Official text:

Articles 4.12, 33 and 34 of the GDPR

What is my role with regard to the impact assessment?

Your client, as the **controller**, shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data in accordance with Article 35 of the GDPR. It is not, therefore, your responsibility to carry out such an assessment.

That said, you must **assist your client in carrying it out and provide any necessary information**. Said assistance must be stipulated in the contract between you and your client.

Official text:

Article 28.3 f) of the GDPR and WP29 guidelines on data protection impact assessment (p.13)

Am I able to benefit from the one-stop-shop mechanism?

If you are established in several EU Member States, you may benefit from the one-stop-shop mechanism.

This enables bodies carrying out cross-border processing (establishments in several Member States or processing operations affecting data subjects in several Member States) to refer to a single national supervisory authority which will make decisions that are applicable to all of the Member States concerned by such processing. This authority is called the "*lead supervisory authority*".

Your lead supervisory authority will be the authority of **your main establishment**, i.e. the place of your central administration in the EU. If you do not have a central administration in the EU, this will be the establishment in the EU where the main processing activities take place.

Official text

Articles 4.16, 56 and Recital 36 of the GDPR and WP29 Guidelines for identifying a controller or processor's lead supervisory authority (p. 9)

What are my obligations if I am not established in the EU?

If you do not have an establishment in the EU, you are subject to all of the provisions in the GDPR when:

- you process, on your client's behalf, data pertaining to data subjects within the EU
- you provide, on your client's behalf, goods or services or track the behaviour of such data subjects.

In such cases you must **designate a representative** in the EU to be the **interlocutor of the data subjects and supervisory authorities** for any question bearing on such processing.

Official text:

Articles 3 and 27 of the GDPR

What are the risks if I do not comply with my obligations?

Any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive **full compensation from the controller or processor for the damage suffered**.

You may thus be held **liable for the damage suffered** and be subject to **major administrative penalties** of up to €10m or €20m depending on the category of offence or, in the event of an undertaking, up to 2% or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Said fines can apply, for example, in the following cases:

- if you act outside of your client's lawful instructions or contrary to said instructions;
- if you do not help your client to comply with its obligations (particularly notification of a data breach or performance of an impact assessment);
- if you do not provide your client with information demonstrating compliance with the obligations or enabling audits to be conducted;
- if you do not inform your client that an instruction would infringes the GDPR;
- if you engage another processor without your client's prior authorisation;
- if you engage another processor which does not provide sufficient guarantees;
- if you do not designate a DPO when this is a requirement, or
- if you do not maintain a record of the categories of processing activities you carry out on your clients' behalf.

Official text:

Articles 82 and 83 of the GDPR

Example of sub-contracting contractual clauses

The example of sub-contracting clauses below is provided pending the adoption of standard contractual clauses in the meaning of Article 28.8 of the GDPR. These examples of clauses can be inserted into your contracts. They must be tailored and specified according to the sub-contracting service concerned. Please note that they do not constitute a subcontract in themselves.

[...], located in [...] and represented by [...]

(hereinafter, "***the controller***")

of the one part,

AND

[...], located in [...] and represented by [...]
(hereinafter, "***the processor***")

of the other part,

I. Purpose

The purpose of these clauses is to define the conditions in which the processor undertakes to carry out, on the controller's behalf, the personal data processing operations defined below.

As part of their contractual relations, the parties shall undertake to comply with the applicable regulations on personal data processing and, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 which is applicable from 25 May 2018 (hereinafter "***the General Data Protection Regulation***").

II. Description of the processing being subcontracted out

The processor is authorised to process, on behalf of the controller, the necessary personal data for providing the following service(s) [...].

The nature of operations carried out on the data is [...] .

The purpose(s) of the processing is(are) [...].

The personal data processed are [...] .

The categories of data subjects are [...].

To perform the service covered herein, the controller shall provide the processor with the following necessary information [...].

III. Duration of the contract

This contract enters into force on [...] for a duration of [...] .

IV. Processor's obligations with respect to the controller

The processor shall undertake to:

1. process the data **solely for the purpose(s)** subject to the sub-contracting
2. process the data **in accordance with the documented instructions** from the controller appended hereto. Where the processor considers that an instruction infringes the General

Data Protection Regulation or of any other legal provision of the Union or of Member States bearing on data protection, it shall **immediately inform** the controller thereof. Moreover, where the processor is obliged to transfer personal data to a third country or an international organisation, under Union law or Member State law to which the processor is subject, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest

3. guarantee the **confidentiality** of personal data processed hereunder
4. ensure that the **persons authorised to process the personal data** hereunder:
   - have committed themselves to **confidentiality** or are under an appropriate statutory obligation of confidentiality
   - receive the appropriate personal data protection training
5. take into consideration, in terms of its tools, products, applications or services, the principles of **data protection by design and by default**

6. Sub-contracting

Choose one of the following two options

Option A *(general authorisation)*

The processor may engage another processor (hereinafter "***the sub-processor***") to conduct specific processing activities. In this case, the processor shall inform the controller, in writing beforehand, of any intended changes concerning the addition or replacement of other processors. This information must clearly indicate which processing activities are being subcontracted out, the name and contact details of the sub-processor and the dates of the subcontract. The controller has a minimum timeframe of [...] from the date on which it receives said information to object thereto. Such sub-contracting is only possible where the controller has not objected thereto within the agreed timeframe.

Option B *(specific authorisation)*

The processor is authorised to engage the entity [...] (hereinafter the "***sub-processor***") to carry out the following processing activities: [...]

Where the processor recruits other sub-processors, it must obtain the prior, specific, written authorisation of the controller.

Irrespective of the option *(general or specific authorisation)*

The sub-processor is obliged to comply with the obligations hereunder on behalf of and on instructions from the controller. It is the initial processor's responsibility to ensure that the sub-processor provides the same sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing meets the requirements of the General Data Protection Regulation. Where the sub-processor fails to fulfil its data protection obligations, the initial processor remains fully liable with regard to the controller for the sub-processor's performance of its obligations.

7. Data subjects' right to information

Choose one of the following two options

Option A

It is the controller's responsibility to inform the data subjects concerned by the processing operations at the time data are being collected.

Option B

At the time data are being collected, the processor must provide the data subjects concerned by the processing operations with information about the data processing it carries out. The wording and format of the information must be agreed with the controller prior to collecting the data.

8. Exercise of data subjects' rights

The processor shall assist the controller, insofar as this is possible, for the fulfilment of its obligation to respond to requests for exercising the data subject's rights: right of access, to rectification, erasure and to object, right to restriction of processing, right to data portability, right not to be subject to an automated individual decision (including profiling).

Choose one of the following two options

Option A

Where the data subjects submit requests to the processor to exercise their rights, the processor must forward these requests as soon as they are received by email to [...] (*indicate a contact within the controller's establishment*).

Option B

The processor must respond, in the name and on behalf of the controller within the periods referred to by the General Data Protection Regulation, to data subjects' requests to exercise their rights, with regard to data covered by the sub-contracting provided for hereunder.

9. Notification of personal data breaches

The processor shall notify the controller of any personal data breach not later than [...] hours after having become aware of it and via the following means [...]. Said notification shall be sent along with any necessary documentation to enable the controller, where necessary, to notify this breach to the competent supervisory authority.

Possible option

Once the controller has agreed, the processor shall notify the competent supervisory authority (the CNIL), in the name and on behalf of the controller, of the personal data breaches without undue delay and, where feasible, not later than 72 hours after having become aware of them, unless the breach in question is unlikely to result in a risk to the rights and freedoms of natural persons.

The notification shall at least:

- describe 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;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- 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.

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.

Once the controller has agreed, the processor shall communicate, in the name and on behalf of the controller, the personal data breach to the data subject without undue delay where said breach is likely to result in a high risk to the rights and freedoms of natural persons.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and at least

- describe 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;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- 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.

10. Assistance lent by the processor to the controller regarding compliance with its obligations

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

The processor assists the controller with regard to prior consultation of the supervisory authority.

11. Security measures

The processor undertakes to implement the following security measures:

[Describe the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia

- 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;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing]

The processor undertakes to implement the security measures set out in the [code of conduct, certification].

[Insofar as Article 32 of the GDPR provides that the controller and processor are responsible for implementing the security measures, it is recommended to precisely determine the responsibilities of each of the parties in terms of the measures to be implemented]

12. Fate of data

At the end of the service bearing on the processing of such data, the processor undertakes to:

At the parties' choosing:

- destroy all personal data, or
- return all personal data to the controller, or
- return the personal data to the processor designated by the controller

Together with said return, all existing copies in the processor's information systems must be destroyed. Once destroyed, the processor must demonstrate, in writing, that this destruction has taken place.

13. The Data Protection Officer

The processor communicates to the controller **the name and contact details of its data protection officer**, if it has designated one in accordance with Article 37 of the GDPR.

14. Record of categories of processing activities

The processor states that it **maintains a written record** of all categories of processing activities carried out on behalf of the controller, containing:

- the name and contact details of the controller on behalf of which the processor is acting, any other processors and, where applicable, the data protection officer;
- the categories of processing carried out on behalf of the controller;
- 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) of the GDPR, the documentation of suitable safeguards;

- where possible, a general description of the technical and organisational security measures, including inter alia:
  - 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;
  - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

15. Documentation

The processor provides the controller with the **necessary documentation for demonstrating compliance with all of its obligations** and for allowing the controller or any other auditor it has authorised to conduct audits, including inspections, and for contributing to such audits.

V. Controller's obligations with respect to the processor

The controller undertakes to:

1. provide the processor with the data mentioned in II hereof
2. document, in writing, any instruction bearing on the processing of data by the processor
3. ensure, before and throughout the processing, compliance with the obligations set out in the General Data Protection Regulation on the processor's part
4. supervise the processing, including by conducting audits and inspections with the processor.