The data processor in the General Data Protection Regulation (GDPR)

The aim of this document, prepared by the Catalan Data Protection Authority in conjunction with the Spanish Data Protection Agency and the Basque Data Protection Agency, is to identify key points to be taken into account when establishing the relationship between the data controller and the data processor, and to identify the issues that directly affect how that relationship is managed.

It will also offer guidance and recommendations for drawing up the document by which the relationship should be regulated.

1.- What are data processors and what is their main role?

The data processor is the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The types of processor and manners of regulating the relationship may be as varied as the types of services that access to personal data may bring about. These can include services whose main aim is the processing of personal data (a company or public entity that offers an information storage service in its servers, for instance) and others that process personal data solely as a consequence of the activity they provide on behalf of the data controller (for example, the manager of a municipal public service).

Though the definition may seem clear, numerous situations arise in practice in which it may prove difficult to draw the line between a processor and a data controller. To help make this distinction we must bear in mind that it is the controller that decides the purpose of the processing and use of the information, while data processors have to carry out the instructions of whoever entrusts them to perform a certain service in relation to the processing of personal data to which they have access as a consequence of the provision of that service.

When the Revised Text of the Public Sector Contracting Act, approved by Royal Decree 3/2011 of 14 November, is applied it must be taken into account that additional provision 26a of this law stipulates that if any public sector contracting involves access by the contractor to data of a personal nature whose processing is the responsibility of the contracting entity, the contractor is considered the data processor. In these cases the system established by the GDPR is also applied.

2.- What processing can a processor carry out on the data with which it has been entrusted?

The processor may carry out all processing operations (whether or not by automated means) that the controller formally mandates it to do. The definition of processing enables us to be more specific, in accordance with the life cycle of information: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

In any case, these processing operations must be clearly defined in the agreement finally adopted.

3.- What level of decisions can be taken by a processor?

The data processor can take any organisational or operational decision necessary to provide the service for which it has been contracted. In no case may the purposes or uses of the data be altered, nor may the data be used for the processor's own purposes.

The decisions taken by a processor must respect the instructions given by the data controller.

4.- Can the data controller choose any data processor?

The controller must choose a processor that provides sufficient guarantees to implement and maintain appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. Consequently, the controller has a duty of diligence when choosing the data processor.

Recital 81 of the GDPR stipulates that the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of the Regulation, including for the security of processing.

The GDPR provides that adherence of the processor to an approved code of conduct or an approved data protection certification mechanism may be used as an element to demonstrate that it offers sufficient guarantees.

5.- How should the relationship between the controller and the processor be regulated?

The relationship between the controller and the processor should be governed by a contract or other legal act which binds them. This must be in writing, including in electronic form.

The possibility of regulating this relationship through a unilateral legal act from the controller is one of the innovations provided for in the GDPR. The legal act must establish and define the position of the processor and must legally bind that processor. This would be the case, for example, of an administrative resolution with recorded notification to the data processor.

In any case, whether in a contract or another legal act, the content must meet the requirements established in the GDPR, to which reference will be made in later sections.

The content of the legal act or contract may be based on standard contractual clauses established by the European Commission or by the supervisory authority, even when they form part of a certificate granted to the controller or the processor.

The standard contractual clauses included in Annex 1 of this document are not considered standard clauses for the purposes of Article 28.8 of the GDPR, but are simply guidelines for those concerned to adapt to the needs of their own organisation.

6.- Who is responsible for the processing carried out by the processor?

The controller never loses this responsibility under any circumstance. Consequently, it continues to be responsible for ensuring the personal data are correctly processed and for safeguarding the rights of the data subjects. The data controller has an obligation to exercise special diligence in the selection and supervision of the processor.

7.- Does the GDPR only apply to processors established in the territory of the European Union?

No, the Regulation applies to data processing in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing itself takes place within the Union.

However, the GDPR also applies to the processing of personal data of data subjects who reside in the Union by a controller or a processor not established in the Union where the processing activities are related to:

a) the offer of goods or services to such data subjects in the Union irrespective of whether connected to a payment;

b) the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.

8.- Are there special rules for contracting a processor not established in the European Union or that carries out the processing outside the territory of the Union?

The disclosure of personal data in the framework of a data processor contract to a country that does not form part of the Union is governed by the rules established in the Regulation for international transfers.

The transfer of data to a third country may not under any circumstance result in a reduction in the level of protection of natural persons established in the Regulation. This principle also applies in onward transfers of personal data from that third country to another or to an international organisation.

If data is to be transferred to countries that do not guarantee an adequate level of protection, the controller must demonstrate that the processor is able to provide appropriate safeguards and ensure that enforceable data subject rights and effective legal remedies for data subjects are available.

9.- If the functions of the data protection officer are outsourced to a third party, is the latter considered the processor?

Yes, the GDPR provides that the data protection officer must be able to access the data being processed. Consequently a data processing contract must be executed.

10.- Must data subjects be informed of the contracting of a processor?

The GDPR does not establish the obligation to inform that a data processor has been contracted. Nonetheless, in certain circumstances (depending on the nature of the processing or of the data being processed, or other concurrent circumstances) it may be advisable to provide this information for the sake of greater transparency in the processing of the personal data.

11.- What is the minimum content of a contract or other legal act governing the processing?

It must at least establish the subject-matter, duration, nature and purposes of the processing, the type of personal data and the categories of data subjects, as well as the obligations and rights of the controller.

In particular, the contract or other legal act must contain:

A. The instructions of the data controller

Instructions with respect to the processing must be clearly documented. The processing activities to be carried out by the processor should be clearly and precisely identified, in accordance with the type of service provided and the manner of providing it. It is particularly important to expressly establish the disclosures to third parties that the controller authorises the processor to make or which derive from the service provided.

The controller's instructions must also be followed in the case of transfers of personal data to a third country or an international organisation, produced as a result of the service provision. If the processor is required to carry out the transfer to a third country by 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.

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

B. Duty of confidentiality

The manner must be established for the processor to ensure that persons authorised to process the personal data have expressly committed themselves to confidentiality or, where applicable, are subject to an appropriate statutory obligation of confidentiality.

Compliance with this obligation must be documented and all information necessary to demonstrate such compliance made available to the controller.

C. Security measures

The contract or other legal act must establish the processor's obligation to adopt all security measures required pursuant to Article 32 of the GDPR.

The controller is responsible for evaluating the risks inherent in the processing to determine the appropriate measures to be taken in order to ensure the security of the information being processed and the rights of the data subjects. It also corresponds to the controller to assess the risks that are presented by the personal data processing, taking into account the means employed (technologies, resources, etc.) and other circumstances that may affect security, for example where the processor is undertaking other processing operations.

Based on the foregoing, the specific security measures may be established in an extensive list or by referral to a national or international standard or framework.

Thus, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including among others and where applicable:

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 organisational measures for ensuring the security of the processing.

Adherence to an approved code of conduct or possession of an approved certification mechanism may be used as an element by which to demonstrate compliance with the requirements set out above.

The controller and processor should take steps to ensure that any natural person acting under the authority of the controller or the processor and who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

D. Subcontracting

The contract or other legal act must establish the system of subcontracting. The GDPR stipulates that when the service required results in a third party processing the personal data, the initial processor may not engage another processor to carry out that service without prior written authorisation of the controller.

Such authorisation may be specific (identification of the particular entity) or general (only authorising the subcontracting, without specifying the entity).

In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

It may be useful for the contract or other legal act to establish the manner (which in any event must be in writing) and time limit for the controller to raise an objection.

In any case, the other processor must be subject to the same conditions (instructions, obligations, security measures, etc.) and in the same way (written contract or other binding legal act) as the initial processor as regards the appropriate 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 remains fully liable to the controller for the performance of that other processor's obligations.

Where the legislation on public sector contracts is applied, the specific provisions of that law should also be taken into consideration.

E. The rights of data subjects

The contract or other legal act should stipulate how the processor should assist the controller in fulfilling that controller's obligation to respond to requests from data subjects for exercising their rights laid down in Chapter III of the GDPR:

- Access to personal data
- Rectification
- Erasure (right to be forgotten)
- Restriction of processing
- Data portability
- Objection
- Not to be the subject of automated individual decision-making (including profiling)

The contract or other legal act must clearly establish whether the processor should deal with and respond to requests for exercising these rights, or stipulate expressly that the processor's sole obligation is to inform the controller that a right has been exercised.

If the former is the case, the contract or legal act must establish the manner and time limits for dealing with or, where applicable, responding to the requests for exercising rights. In the case of the second option, the manner and time limit must be established in which the request and, where applicable, the information corresponding to the exercising of the right, must be communicated to the controller.

Data subjects' right to information is a right not subject to request and, consequently, not subject to the provisions of Article 28.3.e of the GDPR. Nonetheless, in cases where the processor has to collect the data, it is advisable that the contract or legal act establish the manner and the time in which the right to information should be given.

F. Cooperation to ensure fulfilment of the controller's obligations

The contract or other legal act should establish the way in which the processor should assist the controller in ensuring compliance with the obligations deriving from application of the corresponding security measures, the notification of personal data breaches to supervisory authorities, the communication of such personal data breaches to data subjects, the carrying-out of data protection impact assessments and, where applicable, from prior consultation of the supervisory authority.

The fulfilment of this obligation is subject to the nature of the processing and the information available to the processor.

The controller may delegate compliance with these obligations to the processor.

G. Final destination of the data after completion of the processing

The contract or other legal act must stipulate whether, after completion of the provision of services relating to processing, the processor should destroy the personal data and any copy of same or return them either to the controller or to another processor designated by the controller.

The contract or other legal act should clearly establish which of the two options the controller has chosen, as well as the manner and the time limit for carrying it out.

In any case, the data should be returned to the controller when their storage is required by Union or Member State law.

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

H. Cooperation with the controller to demonstrate compliance

The contract or other legal act should establish the obligation of the processor to 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, including inspections, conducted by the controller or another auditor mandated by the controller.