ONTIER

PRIVACY AND DATA PROTECTION INTERNATIONAL TEAM

31th January 2017
#6

Index

OBLIGATIONS ON DATA CONTROLLERS AND DATA PROCESSORS

Any entity that process personal data has either the status of Data Controller (it decides on the purpose and the means of the processing) or Data Processor (it process personal data on behalf of the Data Controller). The GDPR introduces some new obligations for both and attributes, for the first time, direct responsibility to the Data Processor for the processing operations they perform in the context of service provisions developed for the Data Controller.

Current situation

The concepts of Data Controller and Data Processor are expressly defined in Directive 95/46/EC. A Data Controller is *"the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law"*; while a Data Processor is *"a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller"*. To sum up, the Data Controller is the company who decides on the purposes and means of the processing, and the Data Processor is a service provider who processes personal data on behalf of the Data Controller.

The Data Controller is obliged to: (i) rely on a legitimate legal ground in order to process personal data, mainly unambiguous consent of the data subject; (ii) provide certain information to the data subject, such as identity, purpose of the processing and the existence of their right of access, rectification, cancellation and objection; (iii) comply with the data quality principle (to conduct lawful processing and to collect only adequate, relevant and not excessive data for specified, explicit and legitimate purposes); (iv) implement appropriate technical and organizational measures to protect personal data (v) choose a Data Processor that guarantees adequate compliance with data protection rules and regulations (and to sign a contract or legal act that stipulates the obligations of the Data Processor); and (vi) register with the corresponding DPA before carrying out the processing.

On the other hand, the Data Processor should only: (i) follow at all times the instructions of the Data Controller and (ii) implement appropriate technical and organizational measures to protect personal data.

The Data Controller is the only entity that may be deemed liable before the corresponding DPA (administrative liability) and to the data subject when there is a breach data protection rules and regulations. Any failure by the Data Processor to comply with such rules and regulations could result in a fine for the Data Controller, but not for the Data Processor itself. In practice however, the contract regulating the relationship between both entities usually includes an indemnity clause by virtue of which the Data Processor agrees to hold the Data Controller harmless for any liability that may arise from the processing operations it has performed.

In the context of Directive 95/46/EC, there is only one case in which the Data Processor is directly responsible to the corresponding DPA and the data subject: when it carries out acts of processing outside the instructions or for purposes different than those delegated by the Data Controller. In this situation, the Data Processor will be considered as a Data Controller and, therefore, will directly be liable for its infringements.

What's new?

The GDPR maintains the Data Controller and Data Processor concepts introduced by Directive 95/46/EC. However, it introduces new obligations for both of them and, more importantly, it extends the old liability regime, making Data Processors directly

responsible for any infringements they commit.

Most of the new obligations affecting Data Controllers and Data Processors are subject to specific analysis in other chapters of this Guide. For that reason, this Chapter will only summarise them.

Under the GDPR, Data Controllers will be obliged to: (i) adapt their activity to the principles of privacy by design, privacy by default and accountability; (ii) enter into more comprehensive contracts with Data Processors; (iii) keep a record of the processing operations they perform (the duty to register with the corresponding DPA has been abolished); (iv) notify data breaches to the corresponding DPA and, where applicable, to the data subject; (v) appoint a representative in the event they are located outside the EU; (vi) designate a Data Protection Officer (DPO), in case large-scale processing operations are carried out; and (vii) carry out privacy impact assessments, in the event that certain type of processing is likely to result in high risk to the rights and freedoms of the data subjects.

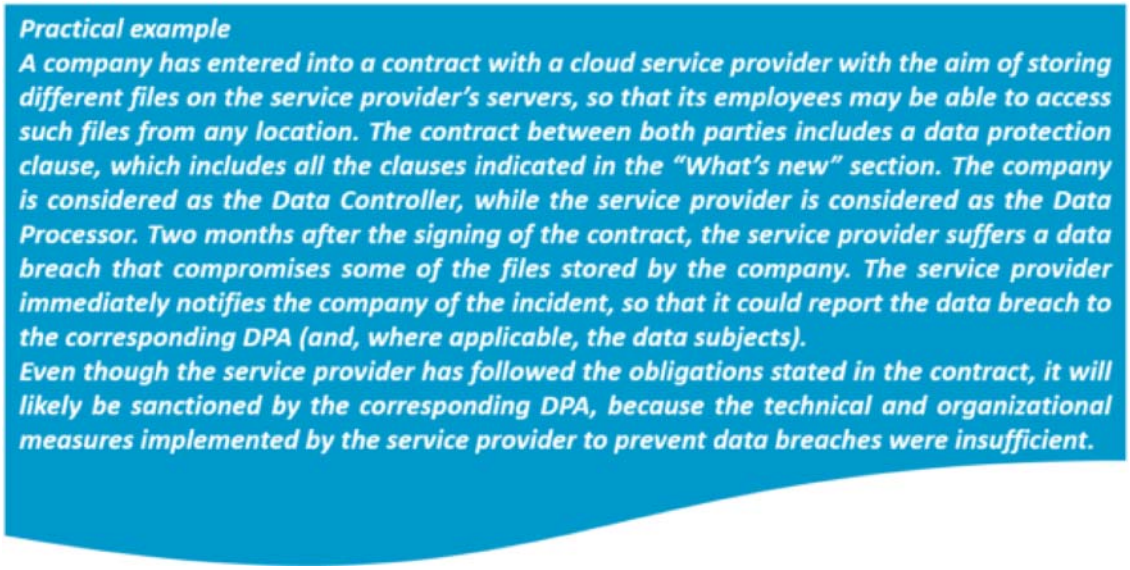
With respect to the contracting of Data Processors by Data Controllers, Article 28 of the GDPR expands the content that must be included in any data processing agreement. Thus, the Data Processor must now commit to: (i) only processing the personal data on documented instructions; (ii) ensuring that employees who have access to personal data have committed to confidentiality; (iii) establishing appropriate organizational and security measures to protect the data; (iv) obtaining a specific or general authorization to appoint new sub-processors; (v) deleting or return the personal data, at the choice of the Data Controller, after the end of the service provision; (vi) demonstrating compliance with the aforementioned obligations and allow to be audited; and (vii) notifying the Data Controller of any data breach it may suffer without undue delay. Furthermore, Data Processors will also be subject to other obligations stated in the GDPR, such as the designation of a DPO and compliance with international data transfer provisions.

Notwithstanding the responsibility of the Data Processors to the Data Controllers and the data subjects for any infringements they commit, the competent DPA may also directly sanction the Data Processors themselves. As a result, this will force Data Processors to be more diligent on the compliance with the regulations.

Finally, the GDPR expressly regulates the existence of joint controllers: where two or more controllers jointly determine the purpose and means of the processing, they should enter into an agreement between them in order to determine their respective responsibilities. A summary of the arrangement must also be made available to the data subjects.

What to do to adapt?

Data Controllers and Data Processors must comply with all the obligations mentioned in this Chapter. The contracts signed between the Data Controller and its Data Processors must be adapted to this new situation regulating the responsibility regime.



Practical example: A company has entered into a contract with a cloud service provider with the aim of storing different files on the service provider's servers, so that its employees may be able to access such files from any location. The contract between both parties includes a data protection clause, which includes all the clauses indicated in the "What's new" section. The company is considered as the Data Controller, while the service provider is considered as the Data Processor. Two months after the signing of the contract, the service provider suffers a data breach that compromises some of the files stored by the company. The service provider immediately notifies the company of the incident, so that it could report the data breach to the corresponding DPA (and, where applicable, the data subjects).

Even though the service provider has followed the obligations stated in the contract, it will likely be sanctioned by the corresponding DPA, because the technical and organizational measures implemented by the service provider to prevent data breaches were insufficient.

TEAM

Joaquin Muñoz Rodríguez (Spain)
Pablo Uslé Presmanes (Spain)

Ana Rocha (Portugal)
Ana Festas Henriques (Portugal)

Derek Stinson (UK)
Paula Enríquez (UK)

ONTIER SPAIN ONTIER UK ONTIER PORTUGAL

Read more:

about us

Share on:

Subscribe:

our Newsletters

Contact us:

Website | LinkedIn

Rua Vitor Cordon Nº 10A, 4º piso - 1249 - 202 Lisboa | Portugal
Tel. (+351) 213 223 590 / Fax (+351) 213 223 599

Rua Pedro Homem de Melo, n.º 55, 8º piso - 4150 - 599 Porto | Portugal
Tel. (+351) 223 190 888 / Fax (+351) 220 924 945

PORTUGAL / **SPAIN** / **U.K** / BOLIVIA / / BRAZIL / CHILE / CHINA / COLOMBIA

USA / ITALY / MEXICO / PERU / VENEZUELA

action as a result of the contents of this document. If you have any queries regarding this article, please contact CCA Ontier or ar@cca-ontier.com.