ONTIER

PRIVACY AND DATA PROTECTION INTERNATIONAL TEAM

06th April 2017
#9

Index

RECORDS OF PROCESSING ACTIVITIES

The General Data Protection Regulation formally introduces an obligation on both Data Controllers and Data Processors to maintain a record of their processing activities.

Current situation

Under Article 18 Directive 95/46/EC, Data Controllers have an obligation to notify the relevant Supervisory Authority of their processing operations before carrying out any wholly or partly automatic processing operation unless there is an exemption from notification (for example, when the processing operations are unlikely to affect adversely the rights and freedoms of data subjects). In the cases where an exemption from notification exists, the obligation to keep a register of processing operations carried out, containing information regarding the processing is on the Data Controller.

As part of the notification, Data Controllers must provide the following information to the Supervisory Authority:

a) the name and address of the Data Controller and of its representative, if any;

b) the purpose of the processing;

c) a description of the category or categories of data subjects and of the data or categories of data relating to them;

d) the recipients or categories of recipients to whom the data might be disclosed;

e) proposed transfers of data to third countries; and

f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken to ensure security of processing.

There is currently no obligation on Data Processors to register its processing operations with the relevant Supervisory Authority.

What's new?

The duty to maintain a record of processing activities is not necessarily a novelty for Date Controllers but for Data Processors, this obligation is entirely new.

The current obligation on Data Controllers to notify, or request authorisation from, the Supervisory Authority on its processing activities will no longer apply. Instead, under Article 30 of the GDPR, Data Controllers and Data Processors are obliged to maintain an internal record of their processing activities it carries out and under its responsibility. The Records should also assure and be able to demonstrate, at any time, that the processing activities of an organisation are compliant with the GDPR.

There are exceptions to this obligation. For an enterprise or an organisation employing less than 250 people, it is not mandatory to keep internal records of the processing activities. This obligation will apply for smaller enterprises and organisations however, if such processing activities:

• are likely to result in a risk to the rights and freedoms of data subjects;
• are not occasional; or
• the processing includes “special categories of data” (e.g. processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs) or personal data relating to criminal convictions and offences.

The records to be kept by Data Controllers concerning processing activities under its responsibility must contain the following information:

a) their own identification and contact details, as well as the contacts of the joint controller (where applicable), and the data protection officer;the purposes of the processing;

b) the purposes of the processing;

c) the description of the categories of data subjects and categories of personal data;

d) the categories of recipients to whom the data have been or will be disclosed, including recipients in third countries or international organisations;

e) 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 some specific case of transfers, it must provide evidence of the existence of suitable safeguards for that transfer);

f) where possible, the envisaged time limits for erasure of the different categories of data; and

g) where possible, a general description of the technical and organisational security measures.

Under Article 30(2) of the GDPR, Data Processorsalso have an obligation to maintain records of all categories of the processing activities carried out on behalf of a Data Controller. However, the information required to be recorded is not as extensive as those for Data Controllers. As such, the records of Data Processors must contain:

• their own identification and contact details and of each Data Controller on behalf of which the it acts, and, where applicable, the respective representatives, and the data protection officer;
• the categories of processing carried out on behalf of each 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 some specific case of transfers, it must provide evidence of the existence of suitable safeguards for that transfer; and
• where possible, a general description of the technical and organisational security measures.

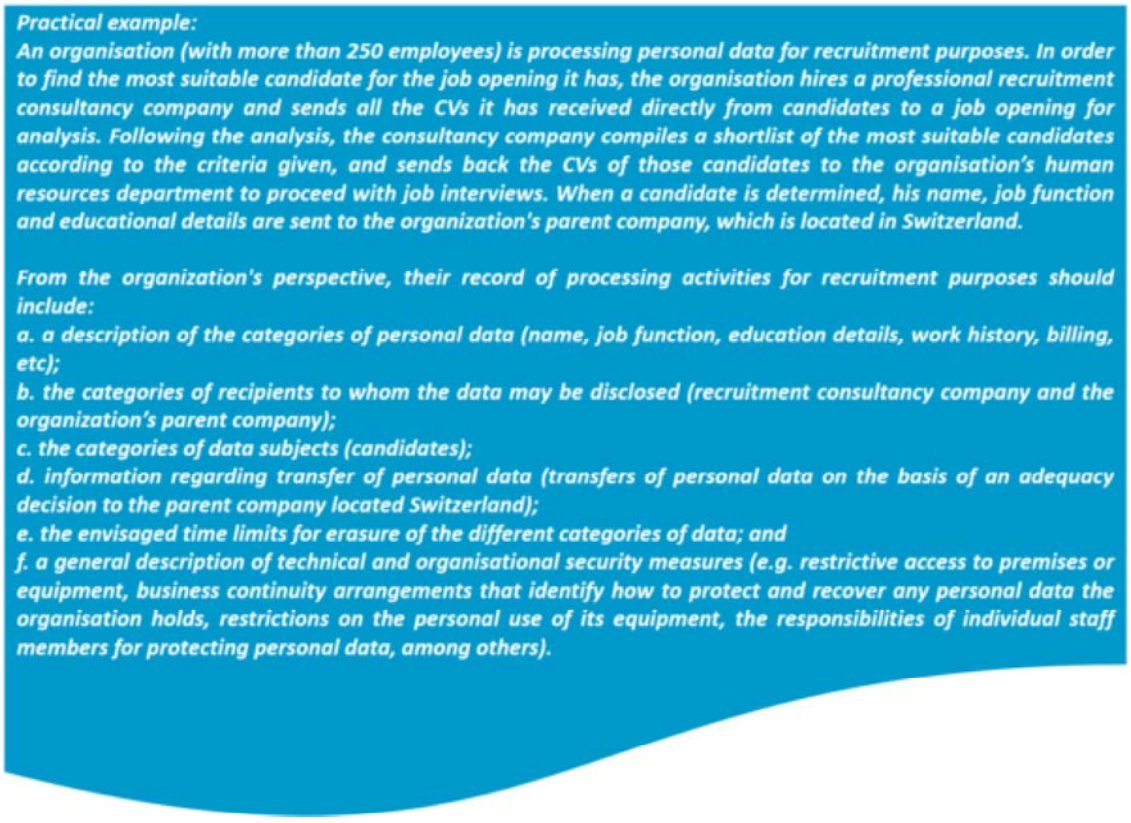
It is important to bear in mind that the Supervisory Authority may monitor the processing activities carried out by a Data Controller or a Data Processor. Therefore, at any time and

upon the Supervisory Authority's request, Data Controllers and Data Processors must make their records available to it.

The records must be in writing, including in electronic form. The obligation to keep records of processing activities also applies to a Data Controller's representative and Data Processor's representative where applicable.

What to do to adapt?

If an organisation currently does not maintain records concerning the processing activities it carries out, they should immediately start to do so. The first step should be to proceed with an inventory of the personal data processed under its responsibility. After the data mapping is completed, it should begin to formally register and record its processing activities. The records must be in writing, including in electronic form and shall contain all the information referred above (depending on whether it is a Data Controller or Data Processor).



Practical example:

An organisation (with more than 250 employees) is **processing personal data for recruitment purposes**. In order to find the most suitable candidate for the job opening it has, the organisation hires a professional recruitment consultancy company and sends all the CVs it has received directly from candidates to a job opening for analysis. Following the

analysis, the consultancy company compiles a shortlist of the most suitable candidates according to the criteria given, and sends back the CVs of those candidates to the organisation's human resources department to proceed with job interviews. When a candidate is determined, his name, job function and educational details are sent to the organisation's parent company, which is located in Switzerland.

From the organisation's perspective, their record of processing activities for recruitment purposes should include:

a) a description of the categories of personal data (name, job function, education details, work history, billing, etc);

b) the categories of recipients to whom the data may be disclosed (recruitment consultancy company and the organization's parent company);

c) the categories of data subjects (candidates);

d) information regarding transfer of personal data (transfers of personal data on the basis of an adequacy decision to the parent company located Switzerland);

e) the envisaged time limits for erasure of the different categories of data; and

f) a general description of technical and organisational security measures (e.g. restrictive access to premises or equipment, business continuity arrangements that identify how to protect and recover any personal data the organisation holds, restrictions on the personal use of its equipment, the responsibilities of individual staff members for protecting personal data, among others).

TEAM

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

Ana Rocha (Portugal)
Ana Festas Henriques (Portugal)

Derek Stinson (UK)
Paula Enríquez (UK)

Read more:

about us

Share on:

Linkedin Twitter

Subscribe:

our Newsletters

Contact us:

Website | LinkedIn

Rua Vitor Cordon Nº 10A - 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