ONTIER

26th April 2017
#10

Index

DATA BREACH

The GDPR introduces a duty on Data Controllers and Data Processors to keep record and report certain types of data breach to the relevant supervisory authority and, in some cases, the data subjects.

Current situation

Although there are some specific sector rules that determine an obligation on organisations to notify a data breach (e.g.: Directive 2002/58/EC on the electronic communications sector), there is no general personal data breach notification regime under Directive 95/46/EC.

What's new?

Data Controllers and Data Processors will now be subject to a general personal data breach notification regime.

Under Article 33 of the GDPR, the Data Controller is obliged to notify the supervisory authority after it becomes aware that a "personal data breach" has occurred without undue delay and where feasible, no later than 72 hours after becoming aware of it. If the notification is made after this period, the Date Controller will need to state the reason(s) for the delay.

A personal data breach is defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."*

The notification to be made under Article 33 must contain the following minimum information:

a) a 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;

b) the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) a description of the likely consequences of the personal data breach; and

d) a description of the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If it is not possible to provide all the required information at the same time, it can be provided in phases without undue further delay.
The Data Controller is exempted from this notification obligation if, upon verifying the personal data breach, it is unlikely to result in a risk to the rights and freedoms of the data subjects.
Under Article 34 of the GDPR, if the personal data breach also represents a high risk to the rights and freedoms of data subjects, the Data Controller is required to notify the data subject about the breach without undue delay. When determining if a communication is needed, the Data Controllers should take into consideration the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. The communication shall be in accessible language, describing the nature of the personal data breach and at least provide the following information:

a) the name and contact details of the data protection officer or other contact point where more information can be obtained;

b) a description of the likely consequences of the personal data breach;

c) a description of the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

However, this communication is not required when one of the following conditions are met:

a) the Data Controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b) the Data Controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

c) it would involve disproportionate effort. Instead, a public communication or similar measure whereby the data subjects are informed in an equally effective manner should be made.

The supervisory authority may require such communication to be sent if after an evaluation, it considers the personal data breach is likely to result in a high risk. The supervisory authority may also conclude that one of the conditions referred above has been met exempting the Data Controller from the obligation of notifying data subjects.
In additional to the notification obligation, the Data Controller is obliged to maintain an internal data breach register documenting all violations of personal data, including facts relating to them, their effects and the remedy adopted. Such documentation shall be made available to the supervisory authority to verify the compliance with the personal data breach notification obligation.
Finally, Data Processors are also required to notify the Data Controller after it becomes aware of a personal data breach without undue delay.

What to do to adapt?

Every organisation that is a Data Controller should ensure internal rules and procedures are implemented to prevent, detect, report and investigate any personal data breach that may occur.

The rules and procedures to be implemented should be able to:

- evaluate without undue delay if a personal data breach has occurred and whether or not personal data had been protected by appropriate technical protection measures;
- effectively limit the likelihood of identity fraud or other forms of misuse:
- recognize a personal data breach representing a high risk for to the rights and freedoms of data subjects;
- ensure internal breach reporting procedures are in place to facilitate decision-making quickly about whether it is necessary to notify the supervisory authority and/or the public;

and
- ensure immediate and effective communication of a personal data breach can be made to the data subject (if required) to allow him or her to take the necessary precautions.

Under Recital 88 of the GDPR, it is recommended that ”*such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.”*
It is also mandatory to keep a record of any personal data breach, even if a particular breach does not require notification to the supervisory authority.
A Data Processor should bear in mind that it must also implement rules and procedures to detect, investigate and notify the Data Controller after it becomes aware of a personal data breach that occurs in relation to its processing activities without undue delay.

Practical example:
A lawyer keeps personal data of clients on his professional cell phone.
While updating the software, unencrypted documents are temporarily uploaded to an internet directory as a backup. During that time, the same documents were visible to an internet search engine and they could be easily accessed. Some of those files contained confidential and highly sensitive information relating to the judicial proceedings of some clients.
Upon becoming aware of the breach, the lawyer and/or his law firm must immediately adopt the following procedures:
1) document the personal data breach, comprising the facts relating to the personal data breach, its effects and the remedial action taken;
2) notify the supervisory authority within 72 hours after becoming aware of the personal data breach (unless there is a reasonable cause not to do so within that time period);
3) as there is a high risk to the rights and freedoms of some clients, communicate the personal data breach to the relevant clients without undue delay.

Practical example:

A lawyer keeps personal data of clients on his professional cell phone.
While updating the software, unencrypted documents are temporarily uploaded to an internet directory as a backup. During that time, the same documents were visible to an internet search engine and they could be easily accessed. Some of those files contained confidential and highly sensitive information relating to the judicial proceedings of some clients.
Upon becoming aware of the breach, the lawyer and/or his law firm must immediately adopt the following procedures:

1) document the personal data breach, comprising the facts relating to the personal data breach, its effects and the remedial action taken;

2) notify the supervisory authority within 72 hours after becoming aware of the personal data breach (unless there is a reasonable cause not to do so within that time period);

as there is a high risk to the rights and freedoms of some clients, communicate the personal data breach to the relevant clients without undue delay.

TEAM

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

Ana Rocha (Portugal)
Joana Cunha de Miranda (Portugal)

Derek Stinson (UK)
Paula Enríquez (UK)

ONTIER SPAIN **ONTIER UK** **ONTIER PORTUGAL**

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

This article is provided for information purposes only and does not constitute legal advice. Professional legal advice should be obtained before taking or refraining from any 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.