PROTECTING INDIVIDUALS IN THE DIGITAL WORLD

agencia española protección datos

In face of a personal data breach, when and how shall data subjects be communicated? (art. 34 GDPR)

What objective?

Protect individuals from the consequences of a personal data breach.

When?

Where there is a high risk to the rights and freedoms of individuals.

To whom?

To those individuals who are at high risk due to the breach.

Deadline?

Without undue delay.
Before the consequences can affect people and in time for them to protect themselves.

How?

With a communication addressed to each of those affected.
For example, by email, SMS, instant messaging or post.

If it is a disproportionate effort or if it is not known precisely who may have been affected, a public announcement can be made, provided it is equally effective.

Minimum content of the communication

Nature

What has happened.
Describe whether it is a cyberincident, cyberattack, data sent by mistake, loss of documentation/device, etc.

What data has been affected.
Specify if it concerns basic data, contact details, email, username and password, copies of ID or passport, contracts, invoices, profiles, locations, etc..

In what way.
Specify whether it is due to illegitimate access, data extracted, disclosed to third parties or public, altered, deleted, unusable or unavailable, etc.

Consequences

What impact it may have on individuals.
Impairment of their fundamental rights, impossibility of exercising other rights, identity theft, impossibility of providing a service correctly, fraud, discrimination, physical or psychological harm, among others.

Aggravating circumstances.
The recipient of your data is the person you have reported, the compromised password is used in other services, the data has been openly published on the internet, etc.

Measures

Taken and proposed by the controller in order to:

- **Solve** the breach.
- **Minimise the consequences** on individuals.

Contact and identification

- **Commercial or public** identification of the controller.
- **DPD** contact details or **other means** of contact for further information.

To be taken into account

Do not use expressions that distort the message.
such as "Your data is not at risk", "you are not at risk", "your data has not been affected", "you can rest assured, we have already reported it to the AEPD" ...

Do not omit relevant details, so that people can assess the risk appropriately and according to their particular circumstances.

It does not involve a single action or act. It can be implemented in different actions depending on the information the manager has about the magnitude of the breach and the people affected.

It is not a communication to those concerned:

- Communicating a breach to a client entity or company.
- Other notices or instructions to individuals that do not include the minimum content of art. 34.
- Unjustified public communication, without minimum content or which is not equally effective (corporate website or portals not visited by those affected or similar).

Guideliness on Personal Data Breach Notification