Information sessions

The General Data Protection Regulation

Notification of a personal data breach

19th October 2017

Esch-sur-Alzette (Belval)

Vincent Legeleux

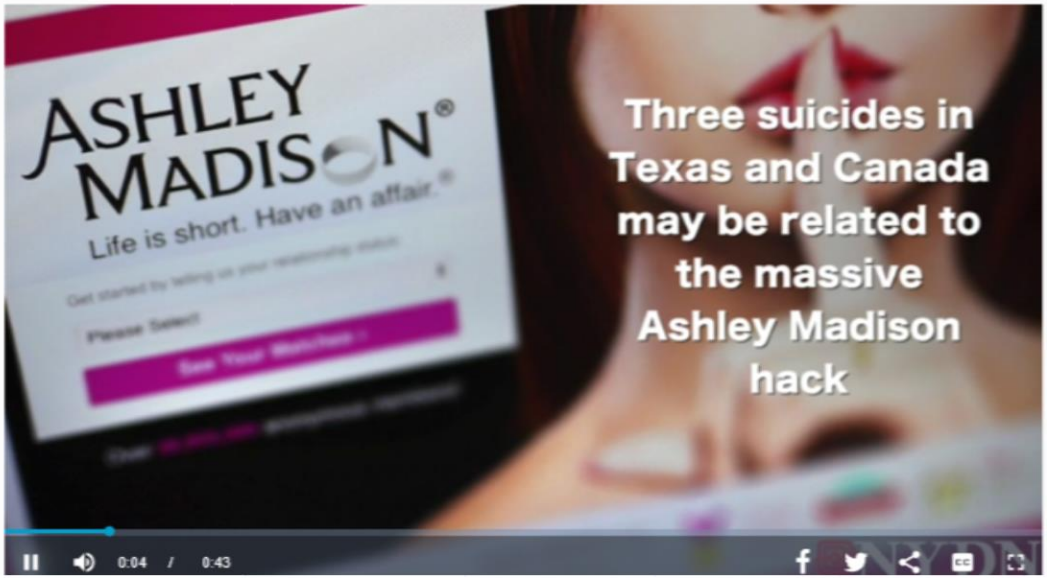
IT department

In the News

www.businessinsider.fr
www.theguardian.com
www.securestate.com

Impact on individuals

Ashley Madison leak may be linked to 3 suicides, $500,000 reward being offered to identify the hackers

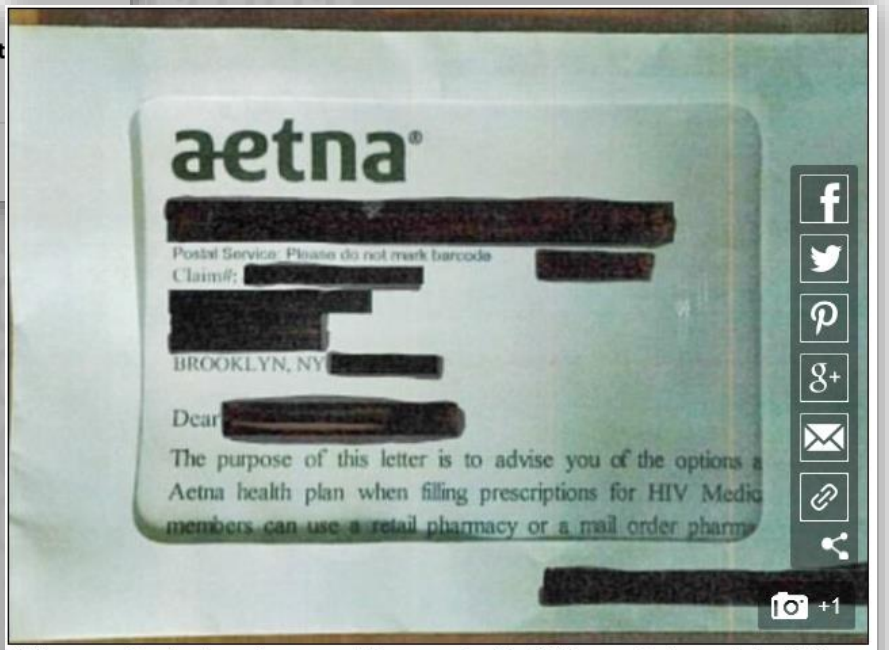


Not only an IT issue

Aetna revealed 12,000 patients' HIV statuses by sending letters with giant envelope 'window' that exposed confidential information

- The health insurer sent letters to patients taking medications for HIV or taking pre-exposure medication to prevent getting the virus
- A photo of the envelope reveals how it exposed confidential information
- Lawyers say some patients' relatives and neighbors learned of their HIV status as a result
- Patients were in Arizona, California, Georgia, Illinois, New Jersey, New York, Ohio, Pennsylvania and Washington, D.C
- Aetna said 'this type of mistake is unacceptable' and promised it won't again

By MIA DE GRAAF FOR DAILYMAIL.COM
PUBLISHED: 18:50 BST, 24 August 2017 | **UPDATED:** 00:49 BST, 25 August 2017



Without opening the letter, it was possible to see details of HIV prescriptions and details for purchasing more. This is a redacted photo of one patient's letter from Aetna

Definition

Art 4 (12) : « ‘personal data breach’ means 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»

General Data Protection Regulation

Part I:

Concepts & Notions

Part II:

Obligations under GDPR

General Data Protection Regulation

http://www.dreamstime.com

Key Elements

INCIDENT

Data Breach (IT or other)

Attack or Accident

(Potential) Impact

Risk

Actors involved: data subject, organisation, public, ..

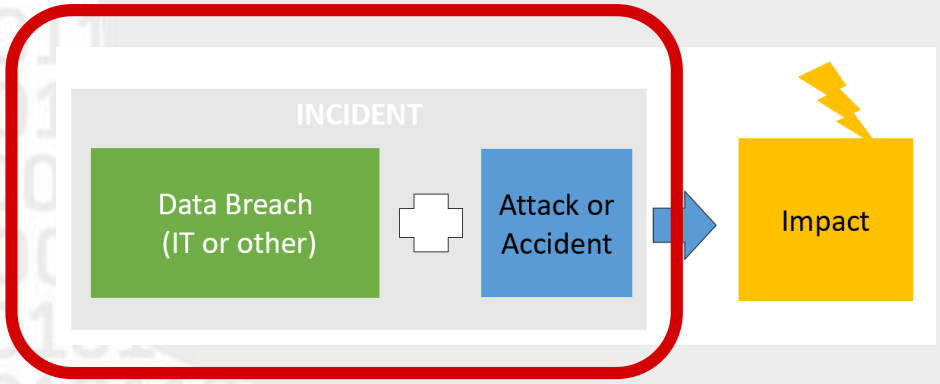
...

Different impacts (financial, reputation, rights and freedoms, ...).

...

Incident

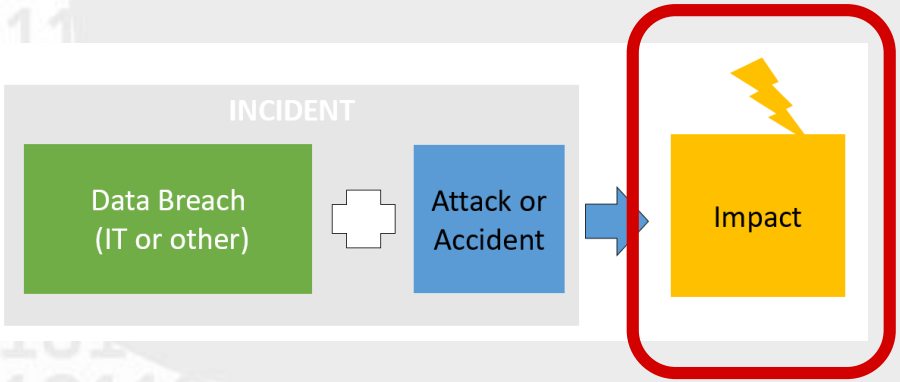
CIA criterias about a data breach



Criterias	Examples
Confidentiality	- Stolen user credentials from a dating website - Stolen credit card credentials - Laptop lost by a client advisor
Integrity	User mistake on an Hospital IT system triggers false statements on the patients files
Availability	Ransomware attack in a bank, no backup, harddrive is encrypted and unreadable.

The impact

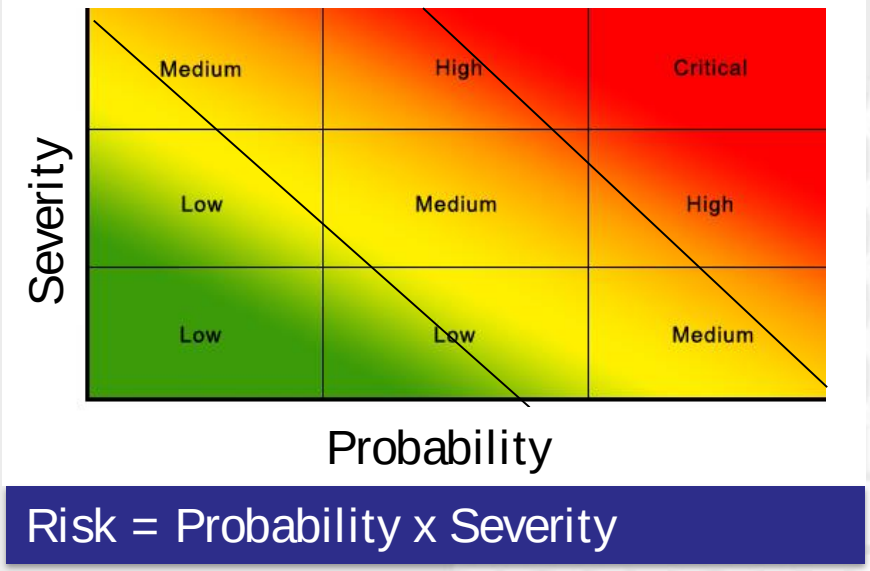
on the rights and freedoms of natural persons



Criterias	Example	Impact
C	- Stolen user credentials from a dating website - Stolen credit card - Laptop lost by a client advisor	- Divorce - Suicide - Financial losses - Reputation
I	- User mistake on an Hospital IT system triggers false statements on the patients files.	- Death - Wrong treatment
A	- Ransomware attack in a bank, no backup, hard drive is encrypted and unreadable.	- Financial Loss - Business losses

The risk

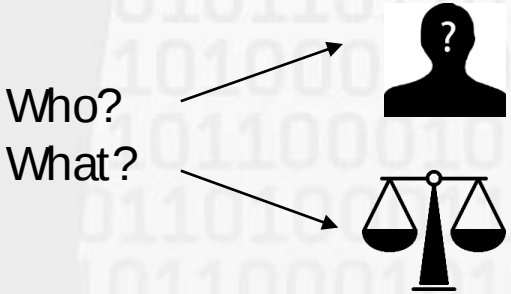
How to assess the impact.



Risk = Probability x Severity

Elements to take into account:

- Type, sensitivity and volume of data
- How easy can the individuals be identified?
- Severity of the consequences for the individuals
- Special characteristics of the individuals
- Number of individuals
- Special characteristics of the controller



Concerned individual(s)

Rights and freedoms of natural persons

Part I:

Concepts & Notions

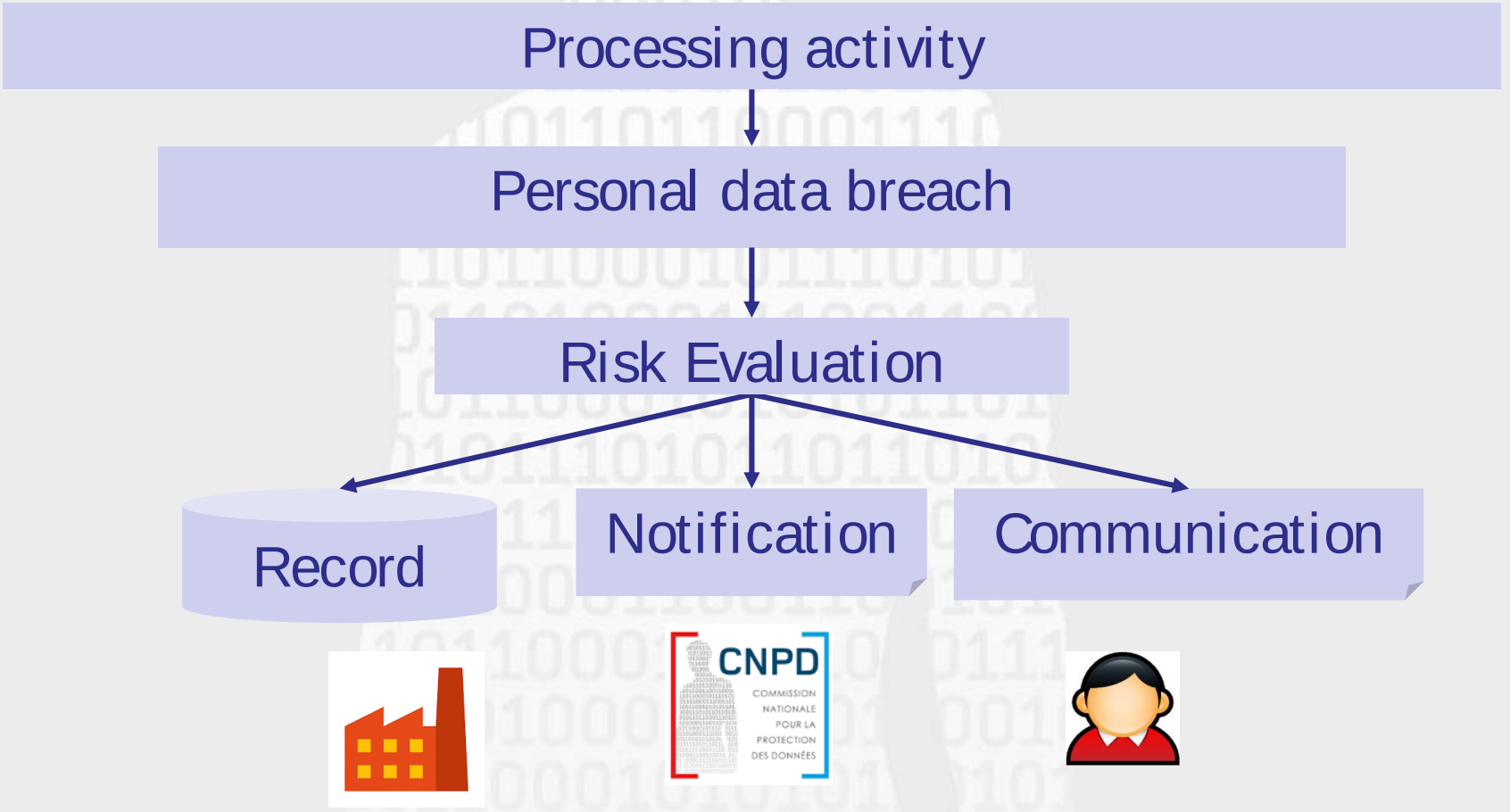
Part II:

Obligations under GDPR

General Data Protection Regulation

https://www.dreamstime.com

Key elements to take into consideration



Processing Personal Data

Principles relating to processing of personal data:

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). (Art. 5 (f))

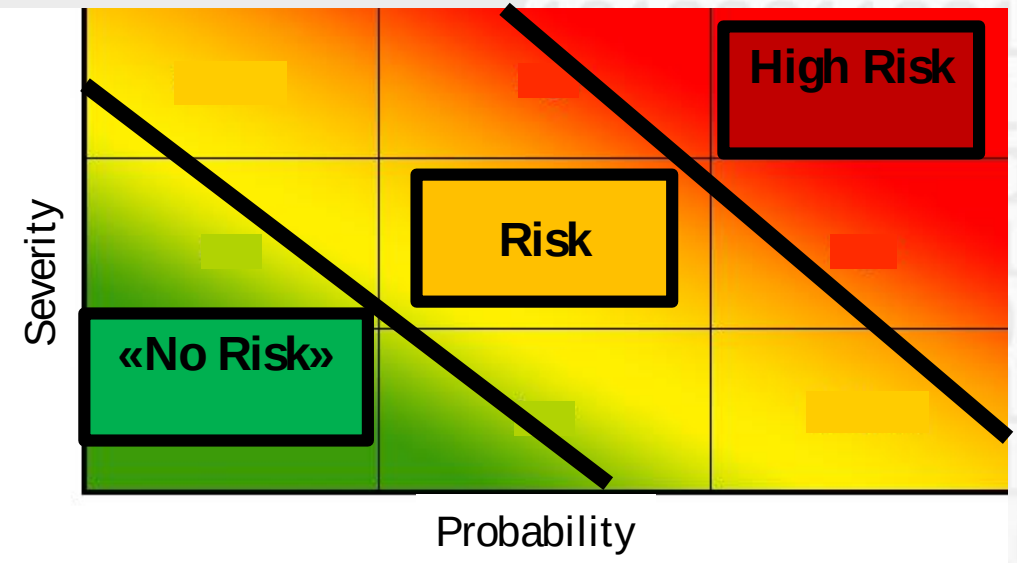
- **Security measures are mandatory** (avoid or mitigate an incident)
- Be able to detect and manage an incident (mitigate the impact)

General Data Protection Regulation

- **Even if all precautions were taken and security measures were applied an incident can happen.**
  - **An incident does not mean «sanction»** – the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them. (Art. 83 (d))
  - **Non-notification of an incident is an aggravating criteria** – the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement(Art. 83 (h)) is a condition for imposing administrative fines.

Risk Assessment

- When evaluating the risk, the probability and the Severity have to be taken into account.
- The GDPR recognizes 3 levels:
  - (1) «No» Risk
  - (2) Risk
  - (3) High Risk



Risk = Probability x Severity

The **risk to the rights and freedoms** of natural persons, of **varying likelihood and severity**, may result from personal data processing which could lead to physical, material or non-material damage… (Recital 75)

Risk should be evaluated on the basis of **an objective assessment**, by which it is established whether data processing operations involve a risk or a high risk. (Recital 76)

General Data Protection Regulation

Required actions

Le GDPR requires several actions **related to the risk** level.

Communication (Art. 34) → Communication

Notification (Art. 33 (1)) → Notification

Record (Art. 33 (5)) → Internal Doc.

« No » Risk

Risk

High Risk

Data breach records

The controller shall document **any personal data breaches**, comprising the facts relating to the **personal data breach**, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.(art. 33 (5))

- Should include «what happened?»
- It is **not needed to keep those records separated** they can be integrated in your incident management sytem.
- Those records should be kept accessible to the CNPD in the case of a control.
- Keep track of the «lessons learned»
- The need for keeping the records comes from the **accountability** stated in Art.5 (2)

- If the data breach does not present a risk for the individuals no other action is requested by the GDPR.

General Data Protection Regulation

Notification to the CNPD

In the case of a personal data breach, the controller shall without undue delay and, where feasible, **not later than 72 hours** after having become aware of it, **notify the personal data breach to the supervisory authority competent** in accordance with Article 55, **unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons**. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. (Art. 33)

- What should be included?
- Caution, **delays are short** (72hrs). Be prepared, have a procedure ready.
- If all the information is not available it is possible to complete the notification in a second step but with justification.

- **The CNPD will provide tools to notify** (secured email, web page etc…)

General Data Protection Regulation

Notification of a personal data breach to the supervisory authority

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Relationship between the processor and the controller

The **processor** shall notify the **controller** without undue delay after becoming aware of a personal data breach. Art. 33 (2)

General Data Protection Regulation

Without undue delay

72H

Processor

Controller of the data

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Communication to the data subject

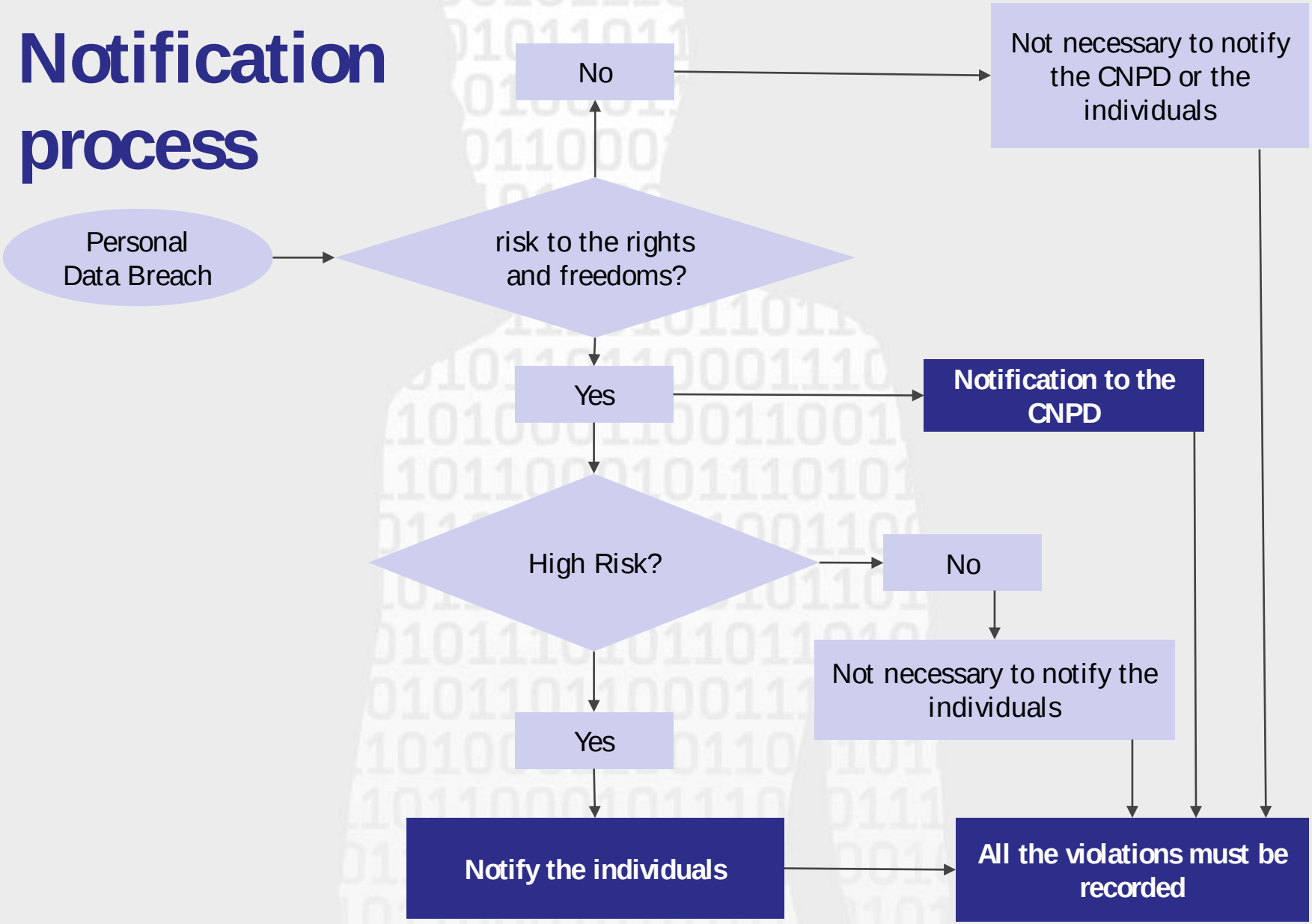
When the **personal data breach** is likely to result in a **high risk to the rights and freedoms** of natural persons, the **controller** shall **communicate** the personal data breach to the **data subject** without **undue delay**. (Art. 34 (1))
The **communication** to the data subject referred to in paragraph 1 of this Article **shall describe in clear and plain language** the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3). (Art. 34 (2))

- **Very important: the purpose is to give the data subject means to protect itself when possible** (e.g. changing passwords, warn other people….)
- **Exceptions do exist** (e.g. encrypted data, counter measures already taken, public statement when individual statement would require disproportionate effort. Our recommandation **stay transparent.**
- This communication should be done in addition to the internal records and the notification.

General Data Protection Regulation

Communication of a personal data breach to the data subject

Notification process



Thank you for your attention !