Impact on data subjects rights and freedoms: Personal Data breach and Data Protection Impact Assessment

Uni.lu / Restena

28th January 2019

Alain Herrmann

Oups ! I lost your data…


© MARK ANDERSON
WWW.ANDERTOONS.COM
ANDERSON
"Here's what you're going to do. You're going to give those 3 million people their credit card numbers back and you're going to say you're sorry."

Since May 25th, 2018

(until December 31st, 2018)

172 data breach notifications

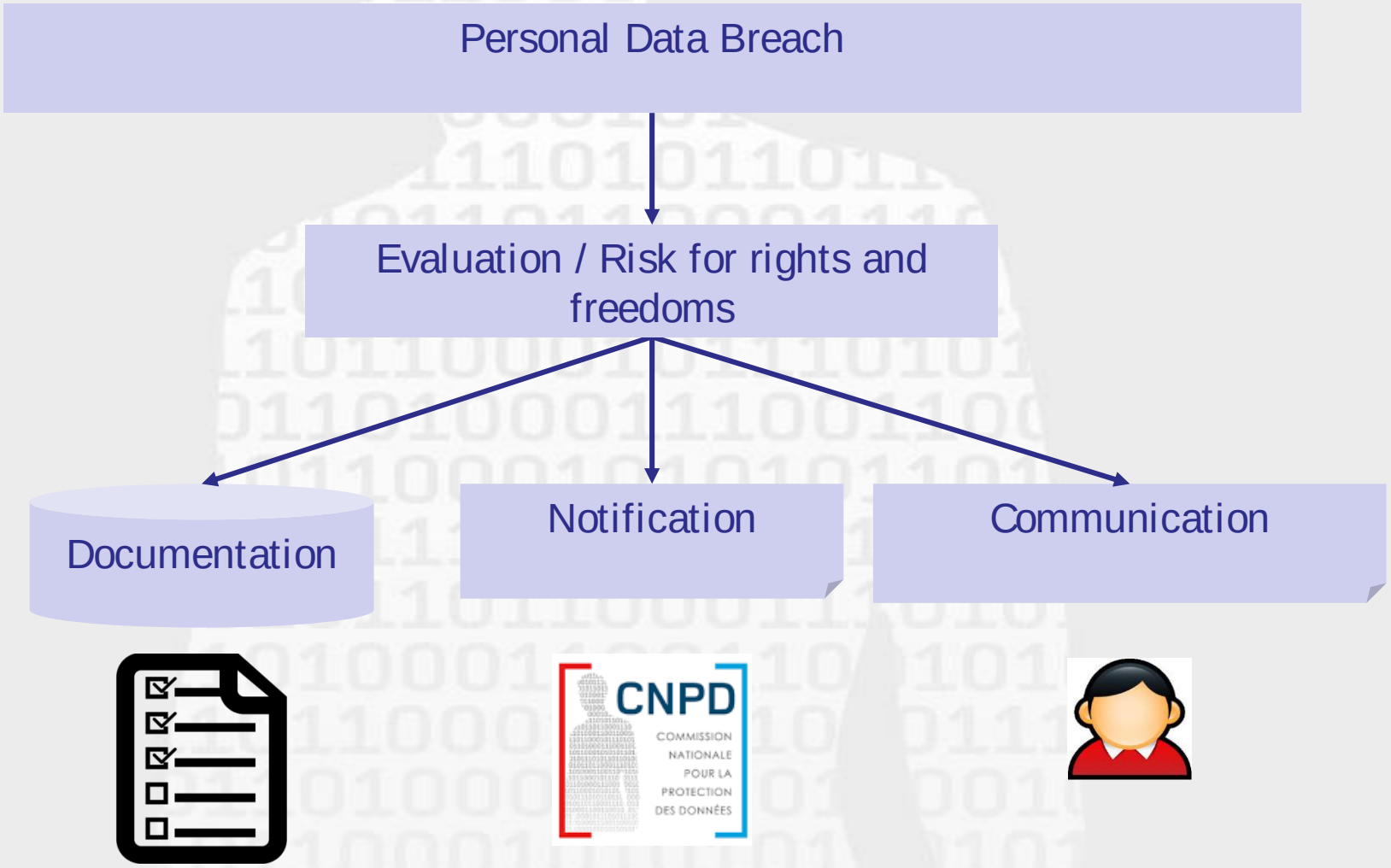
57% human errors

Only 29 % detected the day it occurred


I HAVE A NEW HOBBY. IT'S CALLED PHISHING.
www.dilbert.com scottadams@aol.com
I SEND FAKE BANKING E-MAILS TO GULLIBLE EXECUTIVES. THEN I FIND OUT THEIR FINANCIAL INFOR-MATION AND USE IT TO STEAL THE MONEY THEY DON'T DESERVE.
8-12-05 ©2005 Scott Adams, Inc./Dist. by UFS, Inc
Dear Customer,
This is your bank. We forgot your social security number and password. Why don't you send them to us so we can protect your money.
Sincerely,
I. B. Banker
LOOKS LEGIT.


AIRPORT SECURITY
INTERNATIONA
AIRPORT

Principaux éléments à considérer



Risk for the rights and freedoms for individuals (it's you)?

This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached.

- nature of the personal data involved in a breach (ex: special categories of data)
- the potential damage to individuals that could result can be especially severe, in particular where the breach could result in:
  - identity theft or fraud,
  - physical harm,
  - psychological distress,
  - humiliation or damage to reputation,
  - financial loss

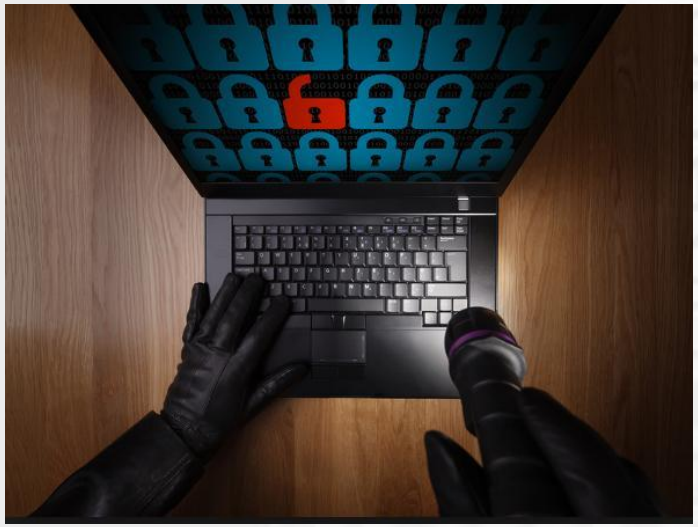
If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.

Important to take care about the context of the breach:

- Is the breach linked to an human error?
  - ✓ reduces the risk for individuals

- Is the breach linked to a targeted attack?
  - ✓ enhances the risk for individuals

  (ex: phishing attack that was successful, website used for payments hacked)



DPIA: Assess impacts of the processing to rights and freedoms of individuals

Rights and freedoms of individuals?

How do we identify and assess risks?

- Consider the potential impact on individuals and any harm or damage your processing may cause – whether physical, emotional or material. In particular, look at whether the processing could contribute to:

  - inability to exercise rights (including but not limited to privacy rights);
  - inability to access services or opportunities;
  - loss of control over the use of personal data;
  - discrimination;
  - identity theft or fraud;
  - financial loss;
  - reputational damage;
  - physical harm;
  - loss of confidentiality;
  - re-identification of pseudonymised data; or
  - any other significant economic or social disadvantage

- ✓ It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA.

- ✓ The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach.

✓When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.

What are these 'rights and freedoms' which have such a pivotal role in how an individual's data are to be cared for?

- ✓ Right to have your details used in line with data protection regulations
- ✓ Right to information about your personal details
- ✓ Right to access your personal details
- ✓ Right to know if your personal details are being held
- ✓ Right to change or remove your details
- ✓ Right to prevent use of your personal details
- ✓ Right to remove your details from a direct marketing list
- ✓ Right to object
- ✓ Right to freedom from automated decision making
- ✓ Right to refuse direct marketing calls or mail

What are my (data protection) freedoms then?

- The right to respect for private and family life (The European Convention on Human Rights (ECHR))

- In the EU, the Charter of Fundamental Rights, freedoms receive more amplified consideration. Title II contains 14 articles, one of which (article 8) directly covers personal data…

    1. *Everyone has the right to the protection of personal data concerning him or her.*
    2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
    3. *Compliance with these rules shall be subject to control by an independent authority*

How do we assess necessity and proportionality?

- ✓ Do your plans help to achieve your purpose?
- ✓ Is there any other reasonable way to achieve the same result?

In particular, you should include relevant details of:

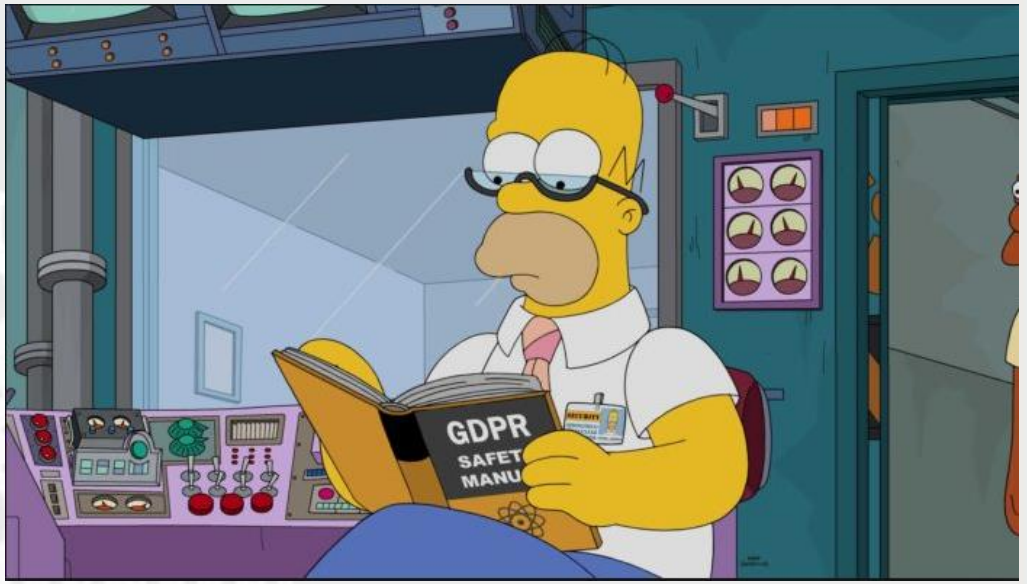
- your lawful basis for the processing;
- how you will prevent function creep;
- how you intend to ensure data quality;
- how you intend to ensure data minimisation;
- how you intend to provide privacy information to individuals;
- how you implement and support individuals' rights;
- measures to ensure your processors comply; and
- safeguards for international transfers.

How do we identify mitigating measures?

Against each risk identified, record its source. You should then consider options for reducing that risk.

For example:

- deciding not to collect certain types of data;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- using a different technology;
- putting clear data-sharing agreements into place;
- making changes to privacy notices;
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights.



This is not an exhaustive list, and you may be able to devise other ways to help reduce or avoid the risks.

You should ask your DPO for advice.

Commission nationale pour la protection des données

1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette (Belval)
261060-1
www.cnpd.lu
info@cnpd.lu