Data Protection and Cybersecurity Breaches: the impact of the GDPR

Olivier MATTER
Team Leader for International Cooperation
Geneva Cybersecurity Law & Policy Conference
Geneva
21 June 2018

A long and winding road…
General Data Protection Regulation

...adopted in April 2016

Legal basis

• Definition in GDPR - Art. 4(12) + Art. 33 and 34
  ✓ Art 33 – Notification of a personal data breach to the supervisory authority
  ✓ Art 34 - Communication of a personal data breach to the data subject
  ✓ Recitals 85,86,87 and 88 (possible restriction in the communication to data subjects based on EU law and institutions decisions under certain conditions)
• References in Art. 70 (EDPB) (g), (h)

Related Work of Article 29 Working Party

• Guidelines on Personal Data Breach notification under GDPR, adopted on 3 October 2017 and last revised and adopted on 6 February 2018
• Endorsed by the EDPB
What is a personal data breach?

- Art 4 (12) “a breach of security leading to the accidental unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

OR

- An information security breach, leading to the compromise of
  - CONFIDENTIALITY and/or
  - AVAILABILITY and/or
  - INTEGRITY
  of personal data under the responsibility of the controller

Step by step duty perspective for controllers

- High risk
- Risk
- Always

Communication to data subjects

Notification to the Competent National Authority

Accountability & Security
Incident management procedure

Plan & Preparation

Review and improvement

Initial assessment

Detailed assessment & evidence collection

Containment & recovery

Always focus and priority on the protection of data subjects!

Notification to the Competent Supervisory Authority -1

• In what circumstances?
  ➢ Personal data breach likely to result in a risk to the data subject.

• What?
  ➢ Nature of breach
  ➢ Categories of data and data subjects and approx. n°
  ➢ DPO or other contact point
  ➢ Likely consequences & measures to mitigate

• When?
  ➢ Without undue delay, not later than 72 h after the controller becomes aware
Notification to the Supervisory Authority -2

• HOW TO DEFINE THE MOMENT The CONTROLLER BECOMES AWARE?
  • Reasonable degree of certainty
  • Internal Process established to detect and address a personal data breach!
• Role of processor
  ➢ Notify the Controller **WITHOUT UNDUE DELAY!**
  ➢ Assist Controller with all necessary means

Information to data subjects

• In what circumstances?
  ➢ Personal data breach **likely to result in a HIGH risk** to the data subject.
• When?
  ➢ Without **undue delay – as soon as possible**
• What?
  ➢ Nature of breach
  ➢ DPO or other contact point
  ➢ Likely consequences
  ➢ Measures planned/taken to mitigate adverse effects
Assessment of risks to data subjects

• Recitals 75 and 76 of GDPR

• Assessing Risk: based on potential severity and likelihood to the rights and freedoms of data subjects – Objective assessment

• Difference with risk of DPIA (hypothetical event - actual event)

• What type of breach? Specific context

Assessment of risks to data subjects - 2

• What data?
  ➢ Personal data? Nature
  ➢ Special categories of personal data? Sensitivity
  ➢ How many data subjects? How much data? Volume

• Taking into account especially:
  ➢ Special categories of individuals (children or other vulnerable individuals)
  ➢ Characteristics of the data controller? (hospital, etc)

  CONTROLLER SHOULD CONSIDER A PRIOR ASSESSMENT OF A COMBINATION OF ALL ABOVE IN ADVANCE- POSSIBLE USE OF MATRIX
13

Is the breach likely to result in a high risk to individuals’ rights and freedoms?

Yes

No

Is the breach likely to result in a risk to individuals’ rights?

Yes

No

Controller detects/is made aware of a security incident and establishes if a personal data breach has occurred.

The controller becomes “aware” of a personal data breach and assesses risk to individuals.

Notify competent supervisory authority.

Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the breach.

Sanctions and remedies

AEPD (ES):
(2010 Annual Report)

CNIL (FR):
(2011 Annual Report)
Sanctions and remedies

The new rules
• Each DPA can impose administrative sanctions:
  up to 20 000 000 € / 4% annual turnover

And the other sanctions?

Thank you for your attention!

www.edps.europa.eu
edps@edps.europa.eu

@EU_EDPS