



Personal data breach notifications in the GDPR

Massimo Attoresi

**ENISA / Garante workshop on security of
personal data processing**

**Rome
8 February 2018**

Introduction

- In the GDPR, mandatory personal data breach notifications to DPAs and individuals affected will apply to organisations.
- Currently not regulated at EU level for “personal data” in general, as of 25 May legal obligation.
- Guidance by DPAs at EU level being prepared



Guidance from WP29

- Past: opinion 03/2014 on "Personal Data Breach Notification" in ePrivacy Directive + other
- New guidelines under GDPR adopted and submitted to comments for 6 weeks (256 comments).
- Final version adopted yesterday, will be published.
- National DPAs will provide more guidance and reporting forms



Legal basis

- Definition of personal data breach (PDB) in - Art. 4(12) + Art. 33 and 34 of the GDPR
 - ✓ Art. 33– Notification of a PDB to the supervisory authority
 - ✓ Art. 34 - Communication of a PDB to the data subject
 - ✓ Recital 85 lists possible harm to data subjects + 86 highlights priorities, 87 requires adequate measures to detect PDBs, 88 warns about disclosure circumstances
 - ✓ Recitals 73 (possible restriction in the communication to data subjects based on EU and national law under certain conditions)
- References in Art. 40 (codes of conduct), 58 (2)(e) (DPA power to order notification to data subjects)
- Verify whether other national or EU laws (eIDAS, NIS, ePrivacy etc.) apply. Build comprehensive approach.



What is a personal data breach ?



- An information **security breach**, leading to the compromise of
 - CONFIDENTIALITY and/or
 - AVAILABILITY and/or
 - INTEGRITYof **personal data** under the responsibility of the organisation as a controller
- If the GDPR is breached in a different way (e.g. no adequate legal basis, no notice to data subjects etc.) this is **NOT** a PDB !

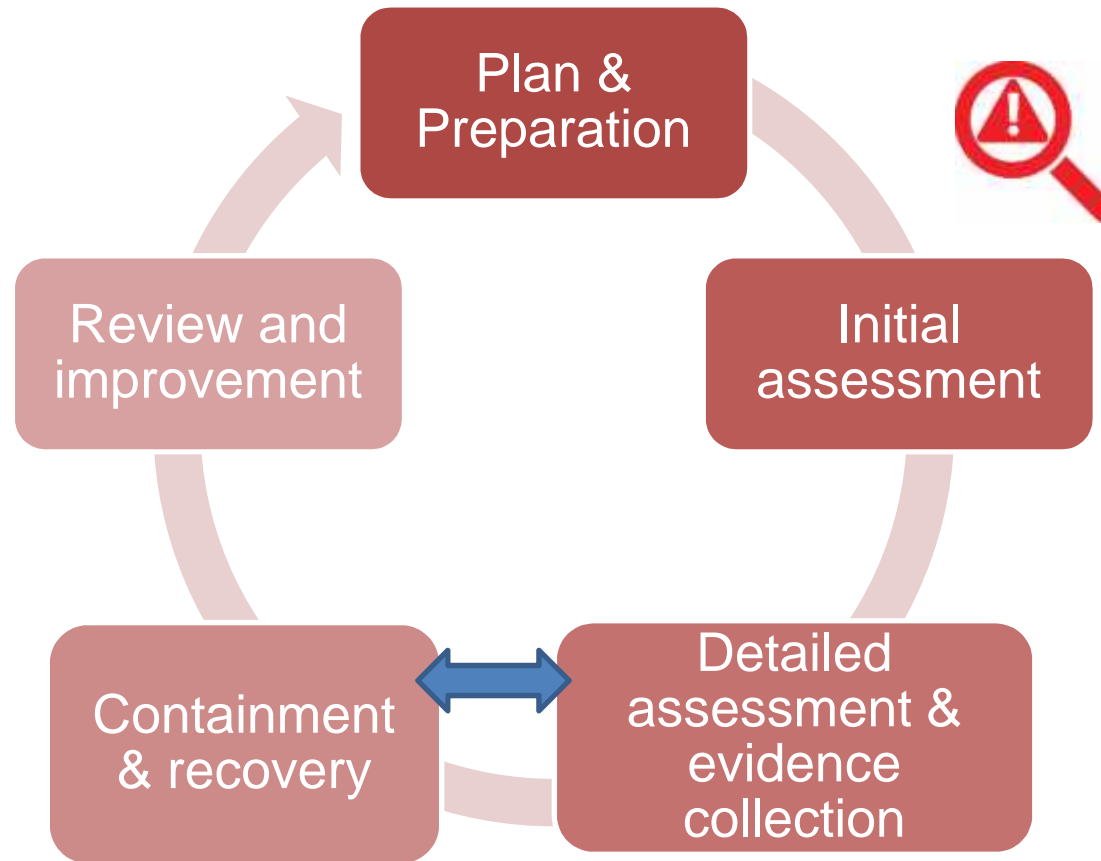


Security

- Overall information security management
- Security incident management procedure
 - Usually all types of information in scope
 - If personal data are affected, IT security is part of the technical and organisational measures of Art. 32 and of the obligation of data protection by design and by default.
 - Need to **integrate/plug-in specific data protection requirements into the incident management procedure**



Incident management procedure



Always focus and priority on the protection of data subjects !

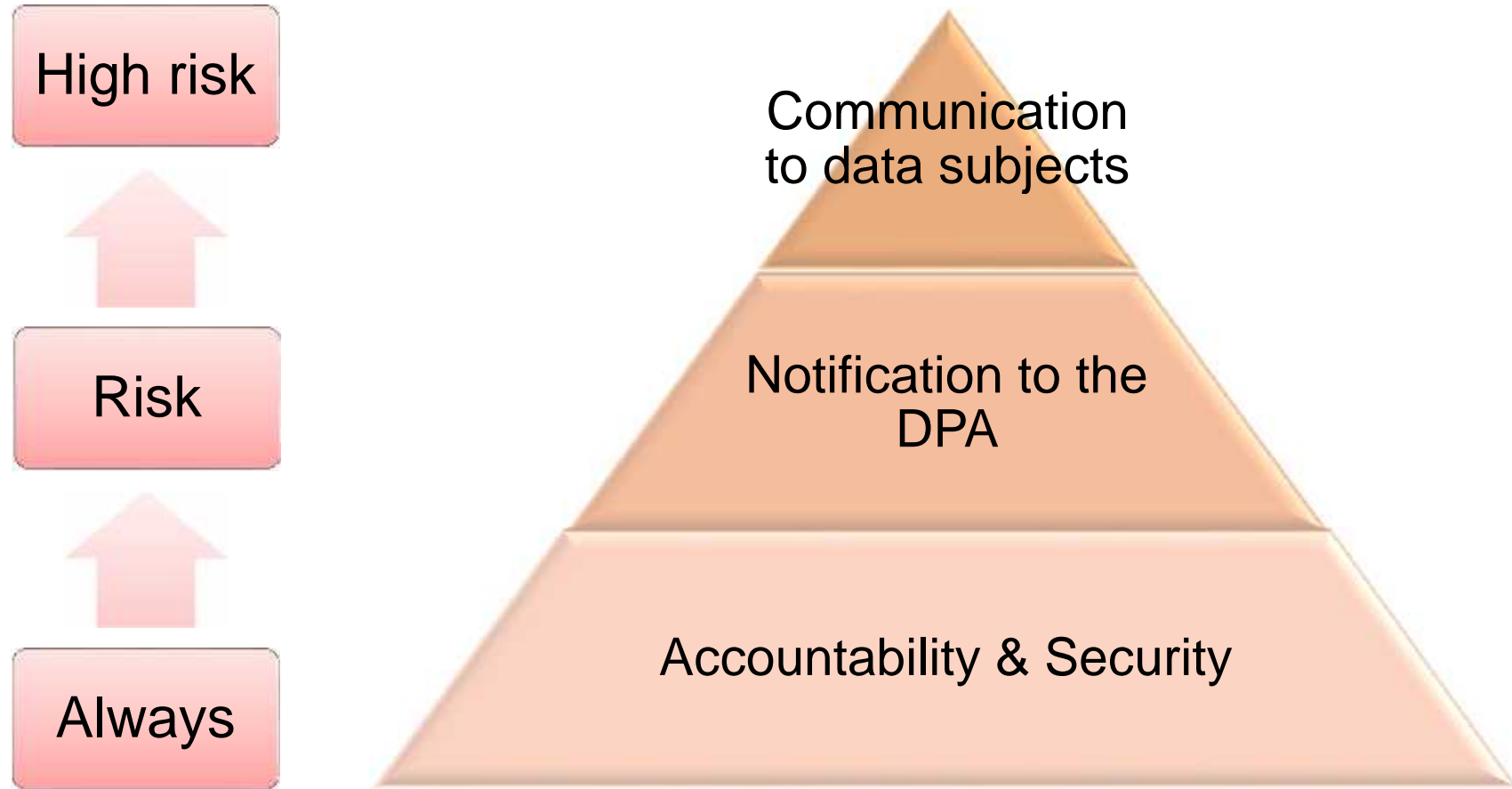
Accountability

- Organisation to inform their DPO
 - ... in any case liaise with your Security Officer on a permanent basis
- Organisation to document personal data breach: facts, effects, remedial and notification actions, including rationale for decisions and relevant evidence
 - for future references....
 - for DPA to verify compliance
- Processor (contractor) to assist the controller


IMPORTANT



Step by step duty perspective for organisation





Notification to the DPA - 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 approx. n° of records
 - Categories of data subjects and approx. n°
 - Likely consequences
 - Measures planned/taken
 - Contact details of the DPO or other contact point



Notification to the DPA - 2

- When ?
 - Without undue delay, not later than 72 h after the organisation becomes **aware** 
 - Phased notifications
 - Possibility of a **delayed notification** 
 - ✓ need for proper reasons
- Role of processor
 - To notify the controller without undue delay
 - Assist controller with all necessary means and providing the necessary info in due time
 - The organisation becomes aware when the processor (contractor) let them know

Information to data subjects - 1

- In what circumstances?
 - Personal data breach **likely to result in a HIGH risk** to the data subject.
- When ?
 - Without **undue delay**
 - Exemptions:
 - Appropriate measure prior to the breach (e.g. strong encryption and keys unavailable)
 - Steps to reduce or avoid high risk taken
 - Disproportionate effort
 - Possible restrictions (public interest, prejudice to other individuals etc.) as in national law
- How ?
 - Dedicated, direct, effective (multiple) channels maximising chances to target affected individuals
 - Clear and plain language
 - Possible alternative formats, many languages



Information to data subjects - 2

- What ?
 - Nature of breach
 - Contact details of the DPO or other contact point
 - Likely consequences
 - Measures planned/taken
- What else?
 - Advice to individuals as to what is in their capability to protect themselves from adverse effects (e.g. password reset, use of alternative communication channels etc.)




Assessment of risks to data subjects - 1

- Risk: based on potential severity and likelihood
- What type of breach?
- What data?
 - Personal data?
 - Special categories of personal data?
- How many data subjects?
- How much data?
- Relation to other personal data?
- Chance of identification



Assessment of risks to data subjects - 2

- Mitigating measures?
 - Was the data encrypted?
 - Anonymized or pseudonymised?
- Which freedoms and rights are affected? 
- Severity for the data subject?
- Taking into account especially:
 - Special characteristics: vulnerable individuals?
 - Characteristics of the data controller?

DPO involvement

- Provide advice on necessity of Personal Data Breach notification, where requested
- Recommend mitigation measures
- Contact person for data subjects
- Contact person for the DPA
- Liaise with Security Officers on Info Security Risk Management and data breach policy



Thank you for your attention!

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



[@EU_EDPS](https://twitter.com/EU_EDPS)