

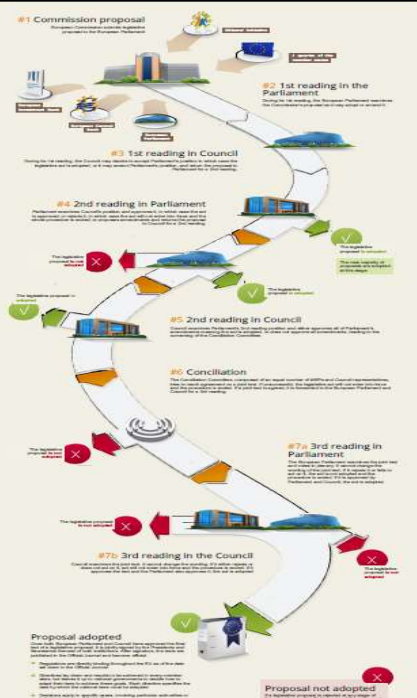


EDPS
EUROPEAN DATA PROTECTION SUPERVISOR

Data Protection and Cybersecurity Breaches: the impact of the GDPR

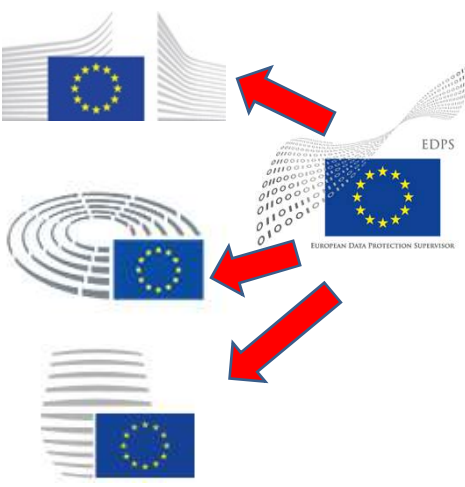
Olivier MATTER
Team Leader for International Cooperation

Geneva Cybersecurity Law & Policy Conference
Geneva
21 June 2018



#1 Commission proposal
#2 1st reading in the Parliament
#3 1st reading in Council
#4 2nd reading in Parliament
#5 2nd reading in Council
#6 Conciliation
#7a 3rd reading in Parliament
#7b 3rd reading in the Council
Proposal adopted
Proposal not adopted

A long and winding road...



EDPS
EUROPEAN DATA PROTECTION SUPERVISOR



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
 - INTEGRITYof personal data under the responsibility of the controller

5



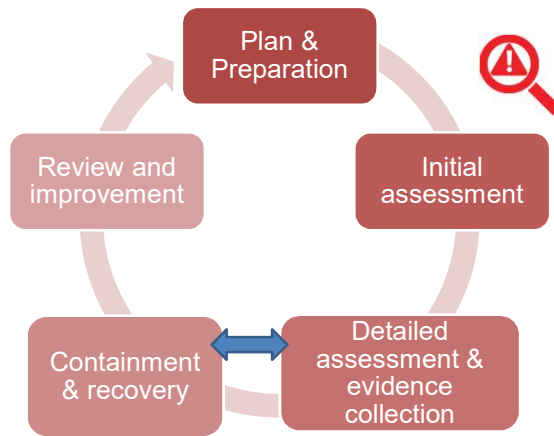
Step by step duty perspective for controllers



6



Incident management procedure



Always focus and priority on the protection of data subjects !

7



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**

8



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

9



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

10



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

11



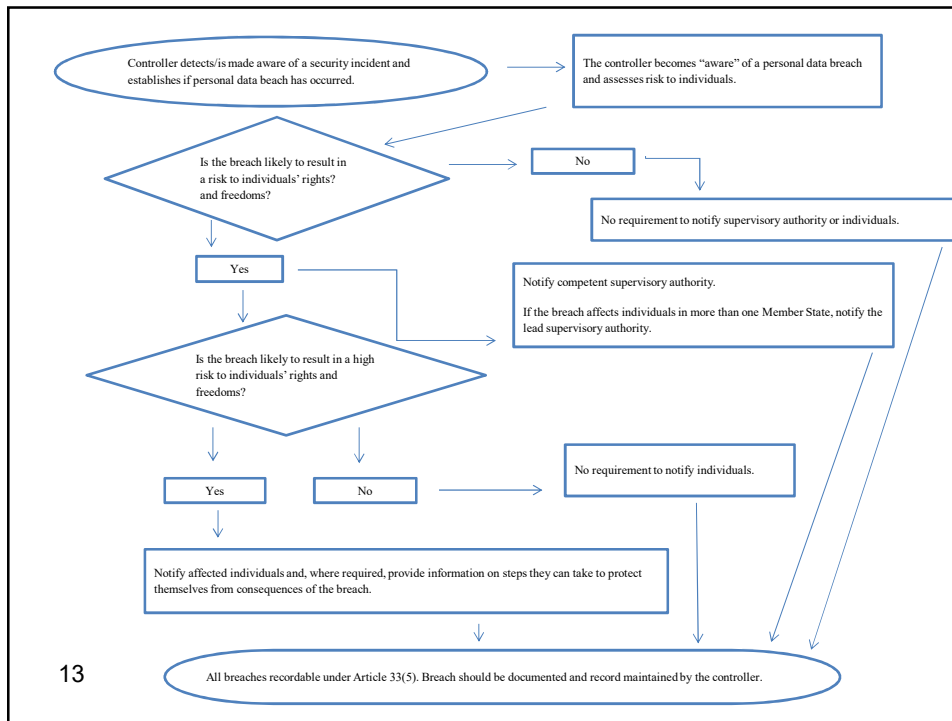
Assessment of risks to data subjects - 2

- 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**

12





Sanctions and remedies

What are DPAs doing?

AEPD (ES):
(2010 Annual Report)

CNIL (FR):
(2011 Annual Report)

	2008	2009	2010
TOTAL	22.013.632,57 €	24.872.979,72 €	17.497.410,02 €

Liste des sanctions prononcées en 2011

Date	Nom ou type d'organisme	Décision adoptée	Manquement principal	Thème
06/01/2011	Google	Sanction pécuniaire de 100 000 euros	Collecte excessive	Télécom
03/02/2011	Soutien scolaire*	Avertissement	Commentaires excessifs	Cours à domicile
03/03/2011	Soutien scolaire*	Avertissement	Commentaires excessifs	Cours à domicile
03/02/2011	Société commercialisant des coffrets cadeau*	Sanction pécuniaire de 50 000 euros	Non prise en compte du droit d'opposition	Commerce
17/03/2011	Société de crédits et de recouvrement de créances*	Avertissement	Commentaires excessifs	Banque
24/03/2011	Banque*	Avertissement	Collecte d'information	Banque
16/06/2011	PM Participation	Sanction pécuniaire de 10 000 euros	Collecte déloyale	Immobilier
30/06/2011	Organisme public**	Relais	sécurité et confidentialité	Secteur public
30/06/2011	Société anonyme d'habitations à loyer modéré*	Avertissement	Collecte déloyale et illicite	Secteur public - Immobilier
05/07/2011	Pages jaunes **	Avertissement public	Collecte et traitement déloyal	Télécom
05/07/2011	Fédération sportive*	Avertissement	Sécurité insuffisante	Sport
05/07/2011	Réseau d'agences immobilières **	Avertissement public	Commentaires excessifs	Immobilier
12/07/2011	Association LEXEEK **	Sanction pécuniaire de 10 000 euros et interdiction de traitement	Non prise en compte du droit d'opposition	Association
21/07/2011	Mouvement politique*	avertissement et procédure d'urgence	sécurité et confidentialité	Secteur public
15/09/2011	Entreprise de vente par correspondance	Avertissement	Non prise en compte du droit d'opposition	Immobilier
15/09/2011	Agence immobilière*	Avertissement	Absence de réponse aux demandes de la CNIL	Immobilier
13/10/2011	Hébergeur de données de santé*	Avertissement	Sécurité et collecte illicite	Santé
13/10/2011	Fournisseur d'accès télévision, téléphone et internet*	Avertissement	sécurité et confidentialité	Télécom
10/11/2011	Société d'aménagement urbain et rural*	Avertissement	Commentaires excessifs	Secteur public
01/12/2011	GROUPE DSE FRANCE	Sanction pécuniaire de 20 000 euros	Collecte déloyale	Immobilier

* Sanctions non rendues publiques par la formation restreinte. ** Recours auprès du Conseil d'Etat

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