Security incidents affecting personal data: an ‘exploratory travel’ from technology to law

(*under Chatham House Rule)

DPO meeting – 8 May 2015

Mario Guglielmetti
Legal officer
Unit Supervision and Enforcement

EUROPEAN DATA PROTECTION SUPERVISOR

***

“When law and technology come together, magical things happen”

“Security risks management: **starting points!**”

1. The technological (digital) environment: **high degree of interconnectivity and interdependency!**

Public-private networks;

Networks-devices (smartphones, *etc.*);

Controllers-processors* (cloud, *etc.*)

2. Variety of possible threats, vulnerability, events (*the great plurality of ‘incident source(s)-incidents points of entry!*):

Intentional/accidental;

Internal/external;

Human/technical;

Basic/sophisticated ..

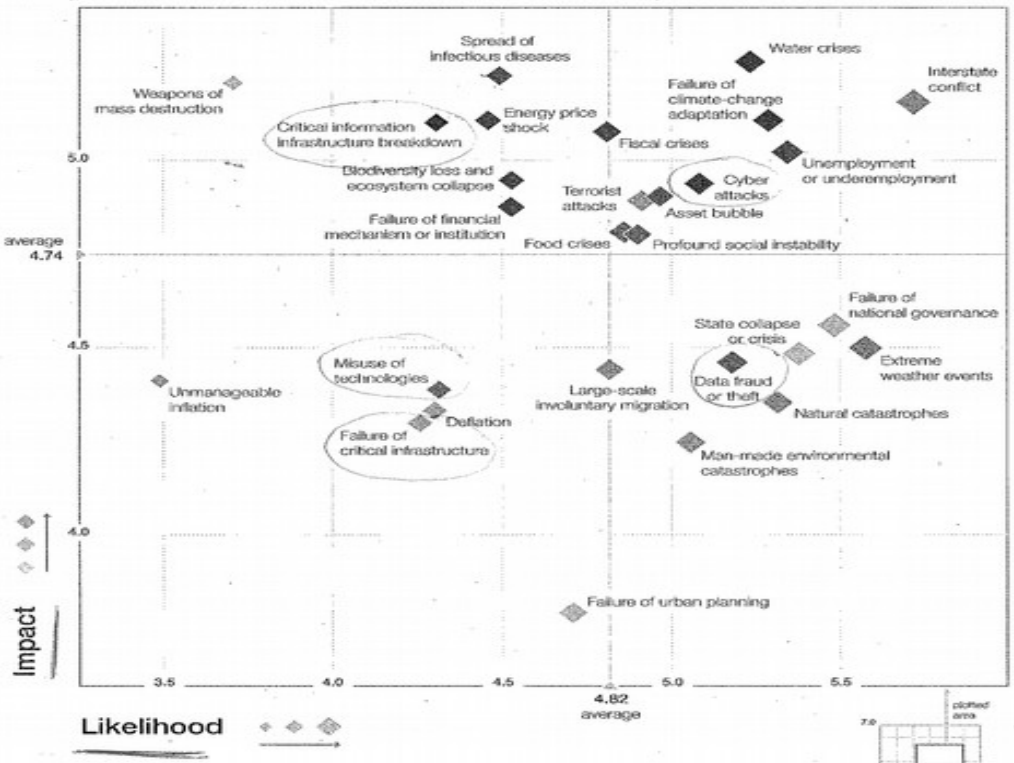
3. Variety of possible damages!:

Impact on: (i) confidentiality; (ii) integrity; (iii) availability.

Effect of: loss of reputation, trust, privacy, disruption of operation, loss of financial assets, lawsuits ..

now, Your experience?

Figure 1: The Global Risks Landscape 2015 — WORLD ECONOMIC FORUM —



Top 10 risks in terms of **Likelihood**

- Interstate conflict
- Extreme weather events
- Failure of national governance
- State collapse or crisis
- Unemployment or underemployment
- Natural catastrophes
- Failure of climate-change adaptation
- Water crises
- Data fraud or theft
- Cyber attacks

Top 10 risks in terms of **Impact**

- Water crises
- Spread of infectious diseases
- Weapons of mass destruction
- Interstate conflict
- Failure of climate-change adaptation
- Energy price shock
- Critical information infrastructure breakdown
- Fiscal crises
- Unemployment or underemployment
- Biodiversity loss and ecosystem collapse

Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Source: Global Risks Perception Survey 2014.
Note: Survey respondents were asked to assess the likelihood and impact of the individual risks on a scale of 1 to 7, 1 representing a risk that is not likely to happen or have impact, and 7 a risk very likely to occur and with massive and devastating impacts. See Appendix B for more details. To ensure legibility, the names of the global risks are abbreviated. Also see Appendix A for the full name and description.

« ***Security*** breach, ***personal data*** breach, **or ..*both*?** »

What about the following?

-Generic **phishing attack** is received by users (but the attack is promptly detected and no passwords, user names, .. are given)

-An **equipment failure** has caused the temporary interruption of a main Information System

-A user reports the **theft of Agency's portable computer** containing sensitive information

-A staff member **accessed personal data** he/she is not authorised to access

EUROPEAN DATA PROTECTION SUPERVISOR

« The Challenge »

We need:

• A **systemic** and **holistic** approach and **proximity** (control works better when close to the possible incidents point of entry);

• Support by the **highest level** of leadership;

• *A **formal framework** (« write down what you do, do what you write down »)*

• *subject to **audit and review cycles***

• *still, flexible enough to allow **forward looking responses to emerging risks.***

« The **RACI** Matrix »

- **Responsible**: the concept of « ownership » of the incident;

Responsibility may or may not be legal; R. even for risk reduced to an acceptable level (residual risk).

- **Accountable (Internally)**: to whom R is accountable;
- **Consulted**: he/she has information and/or capability which are necessary for the handling of the incident;
- **Informed**: must be notified of results (of the incident handling), but doesn't need to be consulted.

Who is responsible?/ Who is accountable? To whom?/ Who must be consulted? For what?/ Who must be informed?

EUROPEAN DATA PROTECTION SUPERVISOR

« The Incident Management. **Steps**: »

1. **Incident detection and reporting**;

2. Incident handling:

Assessment (different gravity assessment models in use, e.g.: SE = DPC x EI + CB*)

Containement

3. Incident record

How RACI fits into this? *And in case of processor's DB?*

ENISA: Severity = data protection context x ease of identification + circumstances of the breach

EUROPEAN DATA PROTECTION SUPERVISOR

« Communication: »

- (*internally and/or externally*) Info to DS (after conclusion of the investigation) « *except in cases in which such provision of info could cause serious harm to the organization* » (examples?) (info to DS as containement?);

- (*internally*) Info to LISO: all IT security incidents;

- (*internally*) Info to DPO: all security incidents related to PD. Role of the DPO? (internal supervisor, contact point ..)

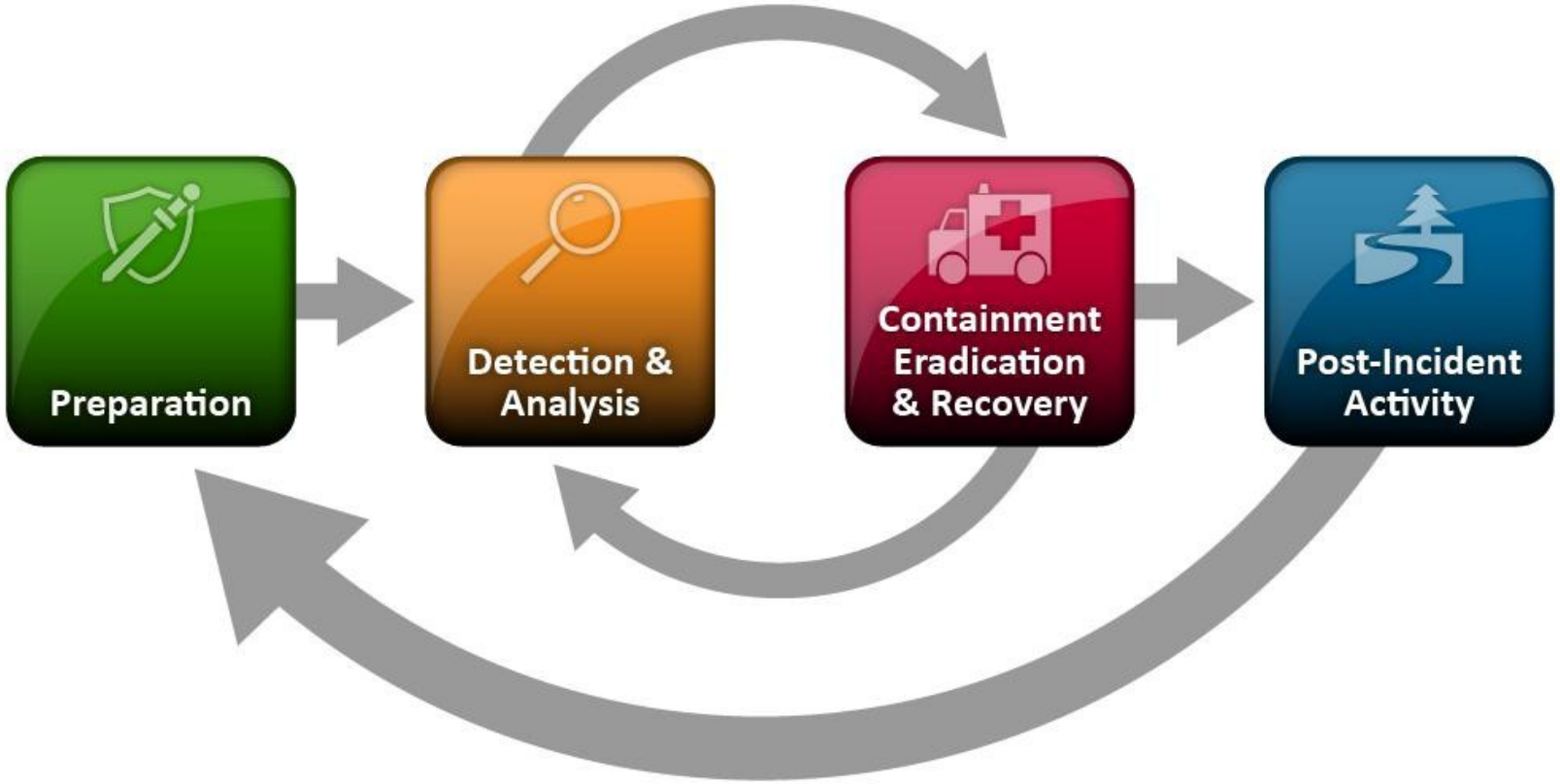
***

Reporting mechanism for IT security incidents affecting personal data:

- *« Information systems security events must be reported through designated channels as quickly as possible.*
- *In case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to PD processed by Commission information systems, the system owner needs to inform the DPO » (COM Guidance on data breach)*

EUROPEAN DATA PROTECTION SUPERVISOR

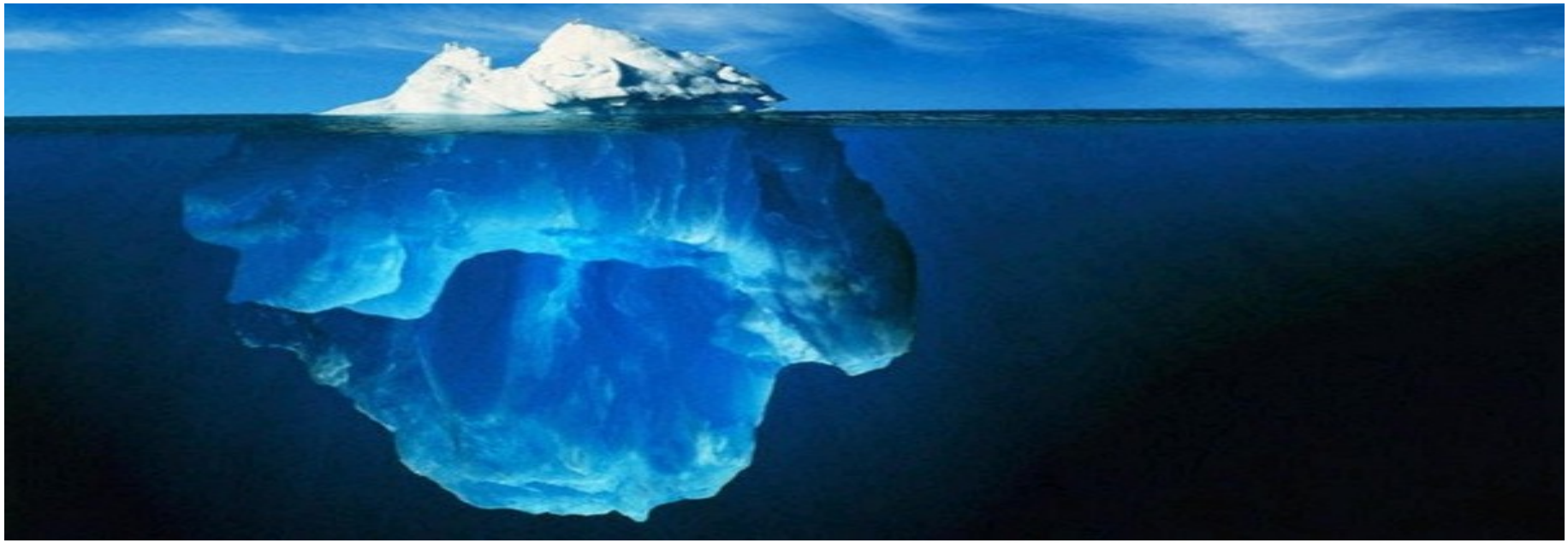
« NIST incident response life-cycle »



EUROPEAN DATA PROTECTION SUPERVISOR

“finally .. **Back to the future** (law)!”

*One (general) remark: the GDPR may seem to ‘look at PDB’ from the perspective of a formal requirement (the ‘top of the iceberg’). For (some) **holistic** view see interfaces of PDB with DPIA; Security measures; Privacy by design/by default – Art. 30; 33; 23.*



Why notifying?

- As a security safeguard
- As openness about privacy practices
- To restore control over personal information
- To ensure public trust

“Question time (please vote) ! ”

*Art. 31 (GDPR) – The controller (the **externally accountable** person) shall notify the PDB to the supervisory authority.*

*1. On **what**: “**All**” DB OR “DB likely to result in **(high) risks** for the individual such as...”*

(note, second option implies a DB severity assessment focussed on the DS harm; should a different threshold be set out for DBN to supervisors?)

*2. On **when**: **24** hours ‘after having became aware’ (*upon notification from incident owner) or provide justification OR **72** hours OR **two-steps**, that is first preliminary and second phase notification?*

*

3. On **the content**:

- Is it always ‘possible’ and ‘appropriate’ to describe **categories and number of DS** and **categories and number of data records** concerned?

- Other elements of content are more ‘stable’: **nature of PDB**; **contact details** of DPO (or others *which?); **measures recommended** to mitigate adverse effects; **consequences** (*OR ‘likely’ consequences?); **measures taken** or proposed to be taken by controller address the PDB.

4. On **the Incident record**:

- Documentation to enable to verify complaince with DBN article OR … *and with* article on security of processing? (Art. 30)

**

*Art. 32 (GDPR) – The controller (the **externally accountable** person) shall notify the PDB to the DS.*

Questions (please vote):

- *On **what**: DB likely to **adversely affect** the protection of PD or the legitimate interests of the DS OR "DB likely to result in (**high) risks** for the individual such us..."? (note: Art. 31 always implies a DB severity assessment focussed on the DS harm);*

- *On **when**: without undue delay (stable, no vote)*

**

*3. On **the content** of the DBN:*

- Nature of the DB, *plus:*
- DPO contact details (stable, no vote);
- Consequences OR 'likely' consequences 'as identified by controller' (the legally R.);
- Measures taken or proposed by the controller to address the DB;
- Measures the DS should take to mitigate the adverse effects.

EUROPEAN DATA PROTECTION SUPERVISOR

**

*4. On when **NOT** to notify the DB:*

-The controller has implemented appropriate techological and organizational measures (e.g. encryption); *or (additional cases):*

-The controller has taken subsequent measures that ensure that the 'risk thresold' for the DS is no longer reached;

-Disproportionate effort (and public communication instead?);

-The DBN would adversely affect a substantial public interest (would it cover the « serious harm to the organization » referred before? Is 'postponing' an option?)

EUROPEAN DATA PROTECTION SUPERVISOR

Thank you for your participation!

For more information:

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS