EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

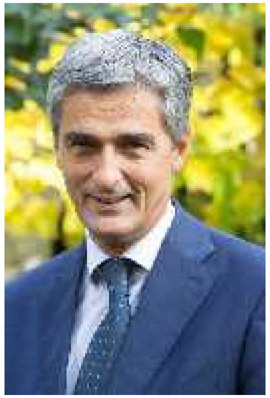
Risk-based approach for EU institutions

Massimo Attoresi

ENISA / Garante workshop on security of personal data processing

Rome
8 February 2018

The EDPS



Giovanni Buttarelli
EDPS

Wojciech Wiewiórowski
Assistant EDPS

The **European Data Protection Supervisor**:

an independent EU institution responsible for ensuring the protection of personal data by the EU institutions and bodies

The EDPS

1. **Supervise** data processing done by EU institutions and bodies;
2. **Advise** the EU legislator and appear before the EU courts;
3. **Monitor** new technologies with an impact on privacy;
4. **Cooperate** with other data protection authorities.

Powers to: obtain all necessary information & access to premises, ban processing, order controllers to comply with DS requests, refer to the Court

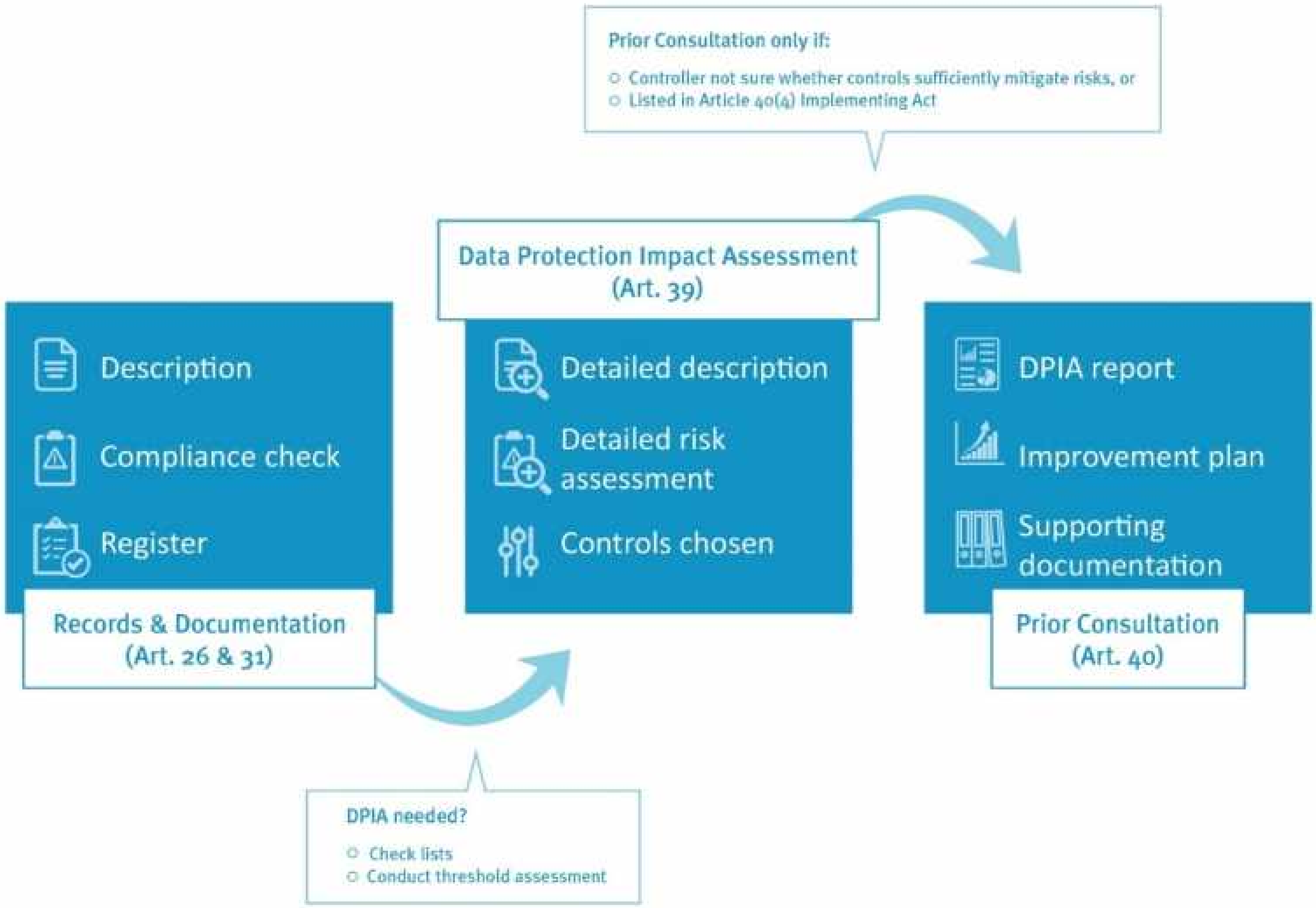
“Accountability” as the GDPR rationale

- Art. 24 GDPR – Controller to implement measures to protect individuals and their data taking into account the **nature, scope, context and purposes** of processing as well as the **risks** of varying likelihood and severity **for the rights and freedoms of natural persons**

+ controller to be able to demonstrate compliance

always a risk based approach on top of compliance !

Documentation overview



Prior Consultation only if:

- Controller not sure whether controls sufficiently mitigate risks, or
- Listed in Article 40(4) Implementing Act

Records & Documentation (Art. 26 & 31)

- Description
- Compliance check
- Register

Data Protection Impact Assessment (Art. 39)

- Detailed description
- Detailed risk assessment
- Controls chosen

Prior Consultation (Art. 40)

- DPIA report
- Improvement plan
- Supporting documentation

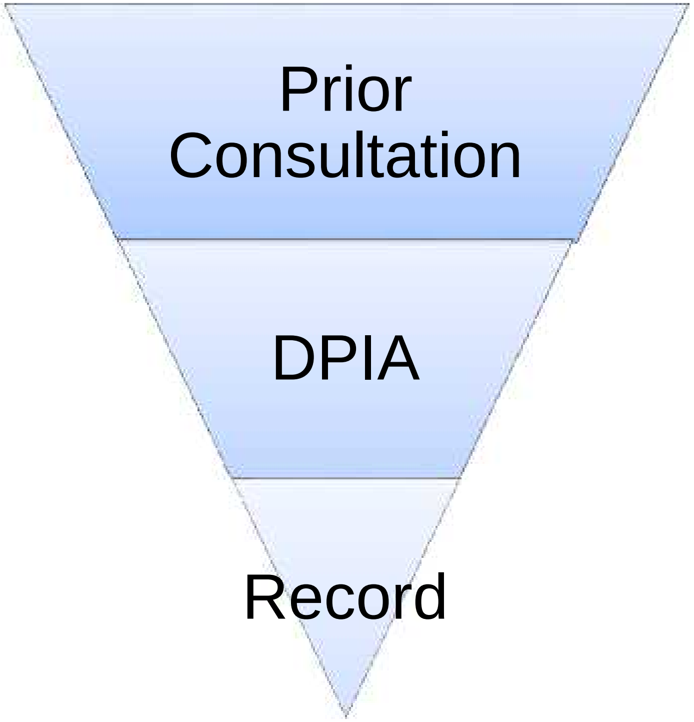
DPIA needed?

- Check lists
- Conduct threshold assessment

be careful: the articles here are NOT those of the GDPR but of the proposal for EU institutions

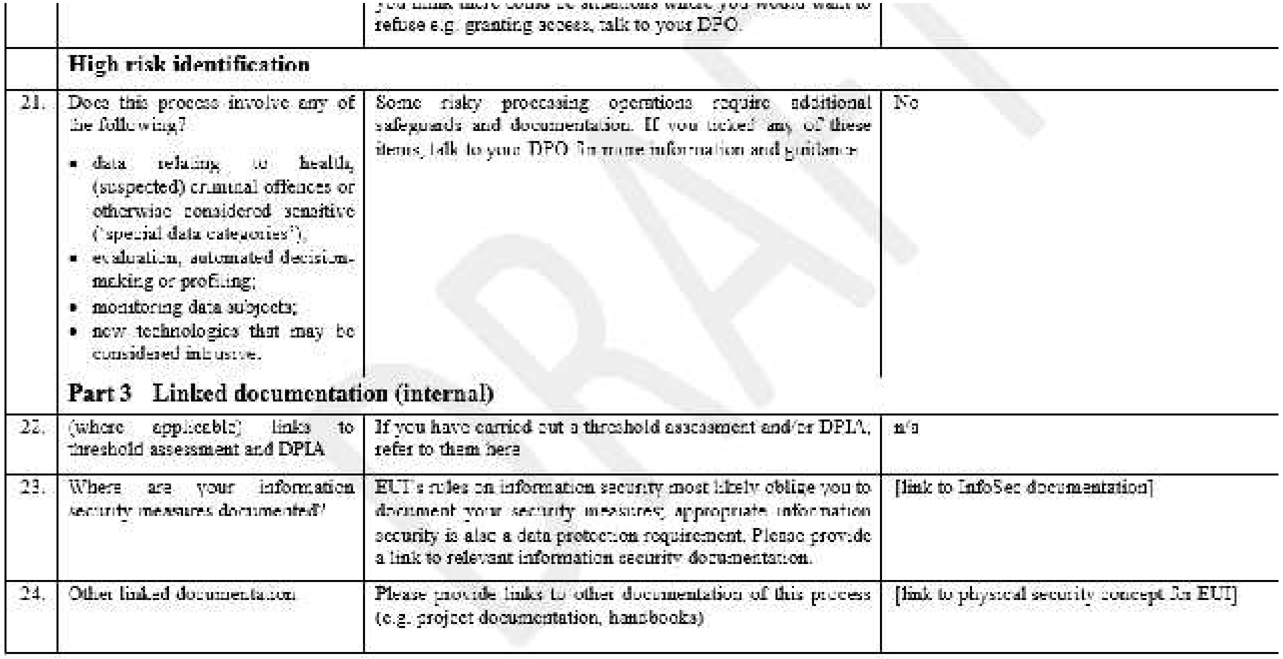
Extent of documentation

- Documentation requirements scale to the risks – small on small things, big on big things;
- Most processing operations will only require a record.
- Record obligations also for most processors



Draft documentation guidance by the EDPS to EUIs

- Template with
  - Mandatory information needed and its explanation
  - Compliance check with explanations
  - High risks factors demanding specific attention (then : ask DPO)
  - Links documentation, including security related one



		you think there could be situations where you would want to refuse e.g. granting access, talk to your DPO.	
	High risk identification		
21.	Does this process involve any of the following? ▪ data relating to health, (suspected) criminal offences or otherwise considered sensitive ('special data categories'), ▪ evaluation, automated decision-making or profiling; ▪ monitoring data subjects; ▪ new technologies that may be considered intrusive.	Some risky processing operations require additional safeguards and documentation. If you ticked any of these items, talk to your DPO for more information and guidance.	No
	Part 3 Linked documentation (internal)		
22.	(where applicable) links to threshold assessment and DPIA	If you have carried out a threshold assessment and/or DPIA, refer to them here	n/a
23.	Where are your information security measures documented?	EUI's rules on information security most likely oblige you to document your security measures; appropriate information security is also a data protection requirement. Please provide a link to relevant information security documentation.	[link to InfoSec documentation]
24.	Other linked documentation	Please provide links to other documentation of this process (e.g. project documentation, handbooks)	[link to physical security concept for EUI]

When to do a DPIA?

- Article 35 GDPR
  - DPIA if “high risks” for individuals are likely to be there
  - Examples for what “in particular” is “high risk”, but no exhaustive catalogue
  - DPA has to issue a list of kinds of processing operations requiring DPIA (35(4)). That list will be non-exhaustive!
  - EDPS may issue a list of kinds of processing operations “*prima facie*” not requiring DPIA (35(5))
- Lists & Threshold Assessment
  - If it’s on *the* 35(4) list, do a DPIA;
  - If not, but still appears risky, perform a threshold assessment.
- Operationalising “high risk”: WP29 approach is list of derived indicators from text and recitals of GDPR; EDPS guidance based on that

Threshold Assessments

- WP29 approach: derived list of indicators
  - Evaluation/scoring
  - Automated decision-making with legal or similar significant effect
  - Systematic monitoring
  - Special categories of data
  - Large-scale processing
  - Matching/combining datasets against reasonable expectations
  - Vulnerable data subjects
  - New technology / innovative solutions
  - Processing preventing DS from exercising a right / using a service
- Rule of thumb: two boxes ticked means doing a DPIA.
- If need for DPIA is confirmed, threshold assessment and record already provide a starting point.

How to do a DPIA?

- No methodology imposed, any methodology that complies with requirements can be used
- EDPS provides *a* template with a baseline methodology
- Description, risks and controls
  - *What do we want to do?*
  - *How could it affect people?*
  - *How do we minimise this impact while still fulfilling the task at hand?*
- Risks to whom?
  - ***in the first place, to people affected***
  - *... indirectly, compliance risks for your organisation*

Data protection principles

- Lawfulness, fairness and transparency
- Purpose limitations
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality **= security**

DPIA baseline methodology

- Risks for individuals’ fundamental rights as a mind-set
- Data flow description: starting point
- Bi-dimensional analysis
  - data flow diagram activities
  - data protection principles, as proxies
  - possible negative impact on individuals’ rights
- Guiding questions for each and every data protection principle
- Template for DPIA report

Risk mgm within DPIA report

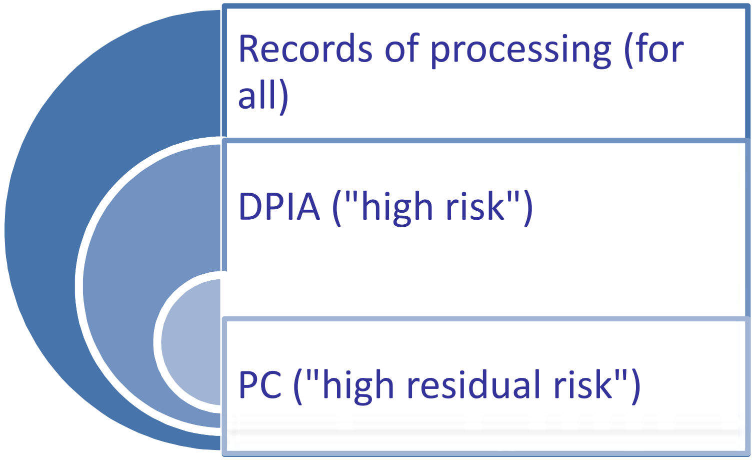
Nr	Item in data flow diagram	Description of risk	Associated data protection principle(s)	Severity (gross)	Likelihood (gross)	Controls	Severity (residual)	Likelihood (residual)
1	Electronic repository of personal files	Unauthorised secondary use	Purpose limitation, Security	3	3	Staff receive DP training. Access control list limits access to those with need to know. Accesses are logged and logs analysed; see points A, B, C of EUI Security Policy XYZ.	3	1
2	Electronic repository of personal files	Corruption of data	Data quality, security	4	1	Changes are logged and backups kept	1	1
…								
n								

IT security dimension in DPIAs

- Security of personal data is one data protection principle
- Need for an IT security risk management process
- Difference with “usual” organisational ISRM?
  - focus on possible adverse effects on fundamental rights and freedoms of people whose data are processed
- Issue: should we repeat IT risk assessment twice ????
  - Possibly NOT, but then need for integration of perspectives:
  - ➢ protect organisation’s assets
  - ➢ protect individuals whose date are processed

When to go for prior consultation?

- ...when not sure if risks are properly mitigated or **risks cannot be properly mitigated**
- Documentation to send to the EDPS: record & DPIA report, treatment plan, ISRM docs
- EDPS will provide recommendations.
- For EUI there may be implementing acts in the future requiring prior consultation for specific things
- Member states may decide for prior consultation when processing in “public interest”



Records of processing (for all)

DPIA ("high risk")

PC ("high residual risk")

Thank you for your attention!

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

@EU_EDPS