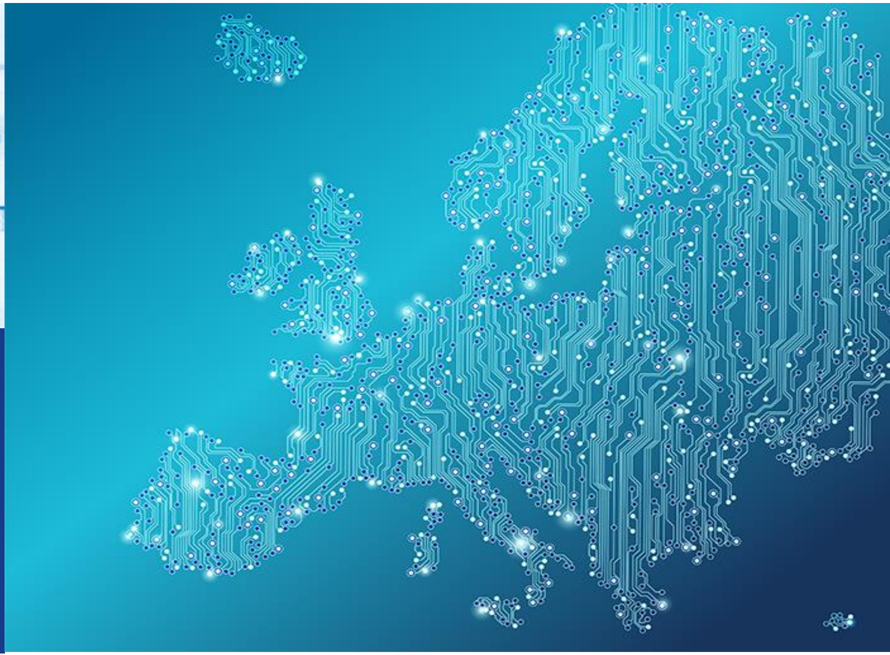


Supporting security of personal data processing

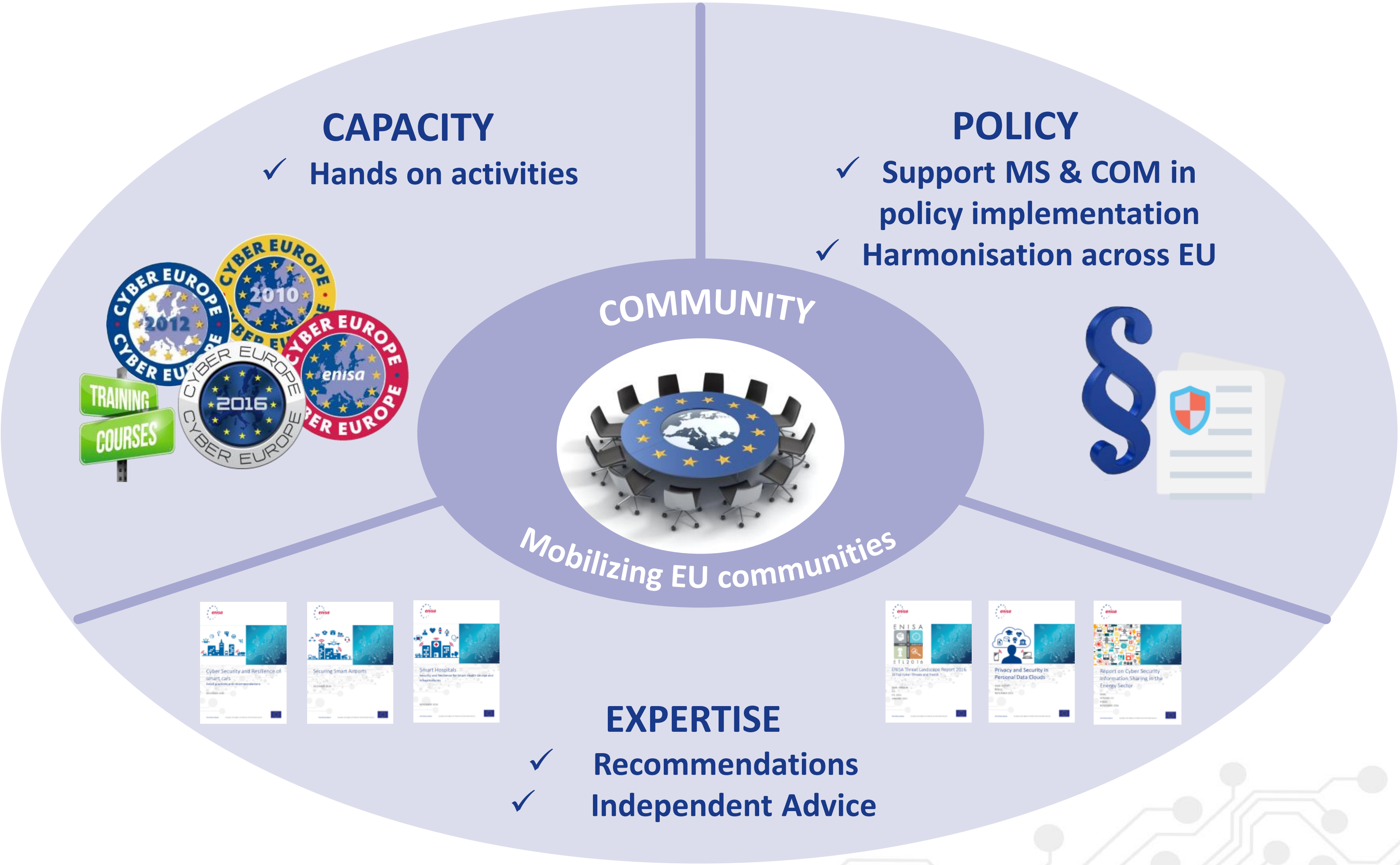
Dr. Prokopios Drogkaris | NIS Expert

ENISA – Garante Workshop | Rome | 08.02.2018

European Union Agency for Network and Information Security

Securing Europe's Information society

Positioning ENISA activities


CYBER EUROPE 2010
CYBER EUROPE 2012
CYBER EUROPE 2016
CYBER EUROPE enisa
TRAINING
COURSES
Cyber Security and Resilience of smart cars
Good practices and recommendations
Securing Smart Airports
Smart Hospitals
ENISA ETL2016
ENISA Threat Landscape Report 2016
Privacy and Security in Personal Data Clouds
Report on Cyber Security Information Sharing in the Energy Sector

CAPACITY

- ✓ Hands on activities

POLICY

- ✓ Support MS & COM in policy implementation
- ✓ Harmonisation across EU

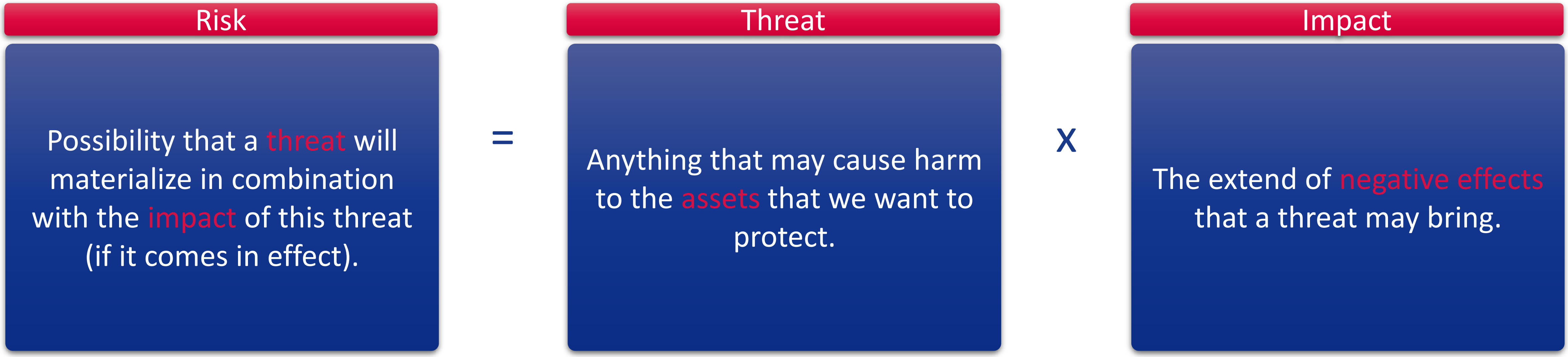
COMMUNITY

Mobilizing EU communities

EXPERTISE

- ✓ Recommendations
- ✓ Independent Advice

The notion of risk in information security



Risk

Possibility that a threat will materialize in combination with the impact of this threat (if it comes in effect).

=

Threat

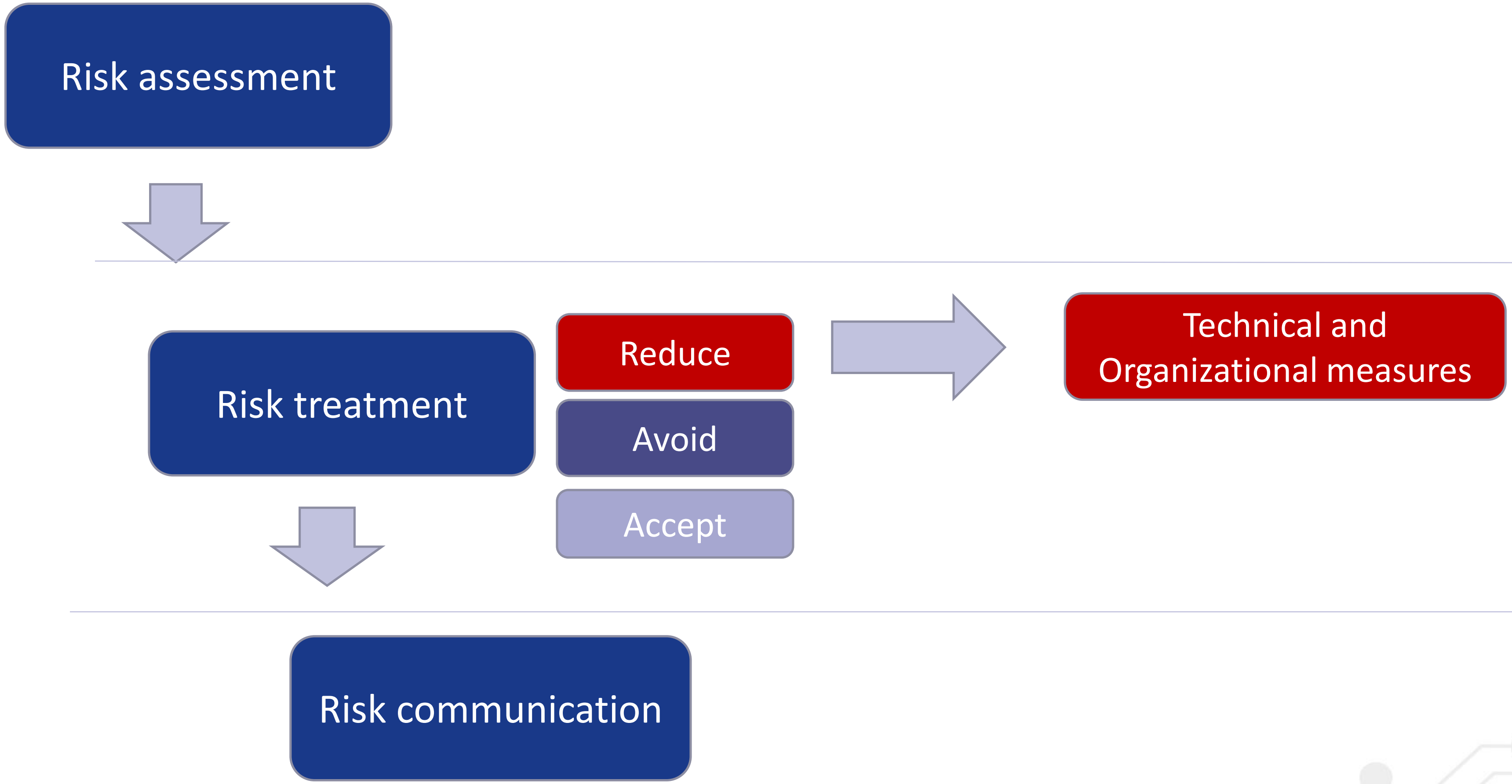
Anything that may cause harm to the assets that we want to protect.

X

Impact

The extend of negative effects that a threat may bring.

Information security risk management



Risk assessment

Risk treatment

Reduce

Avoid

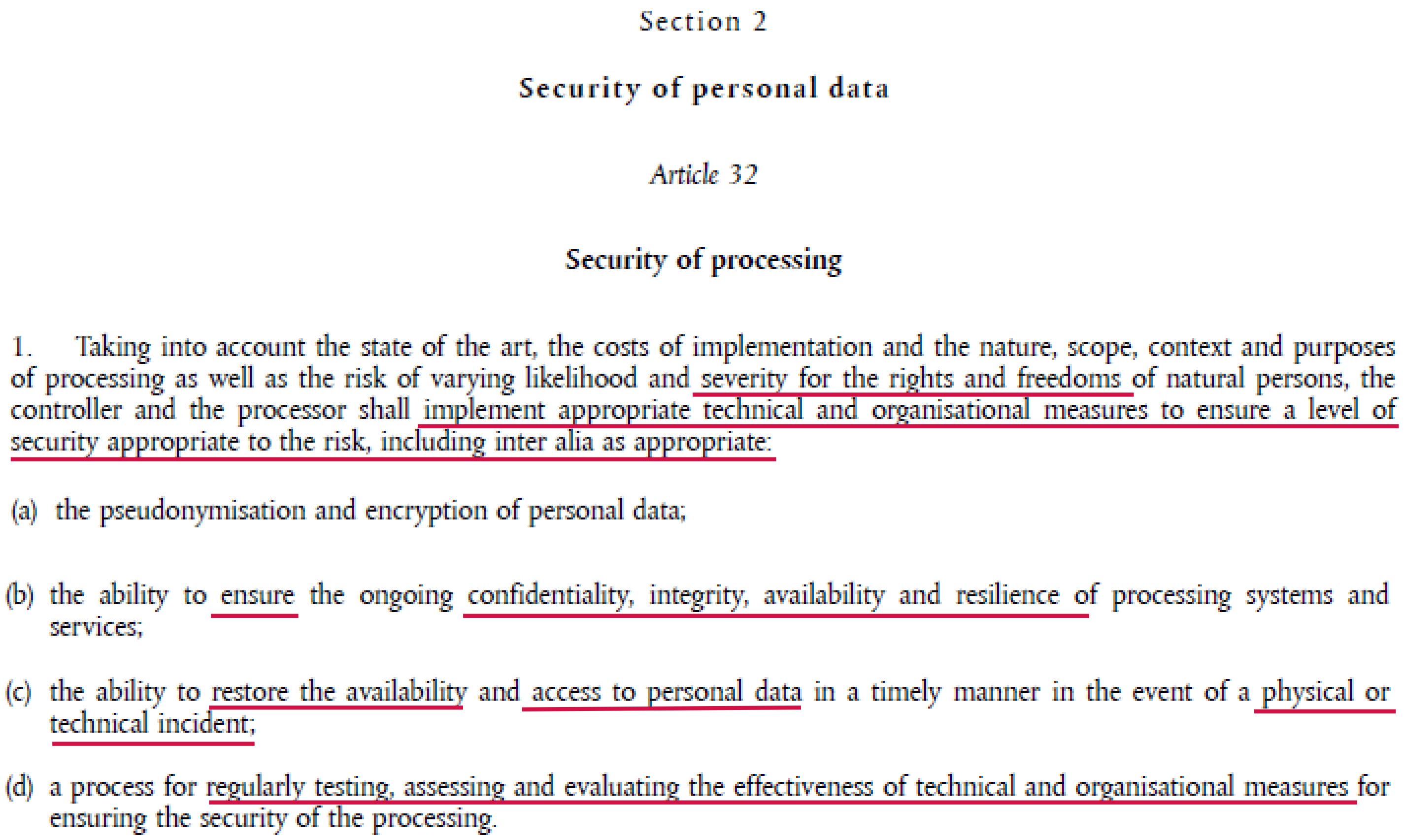
Accept

Technical and Organizational measures

Risk communication

More information security?

more effort from data controllers and data processors regarding information security



Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The notion of risk to privacy and personal data

Risk

With regard to **rights and freedoms of data subjects**

- Differs from financial or business risk!
- Independent of scale (even one person is enough!)

=

Threat

Any internal or external factor that could lead to a **personal data breach**

Any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

X

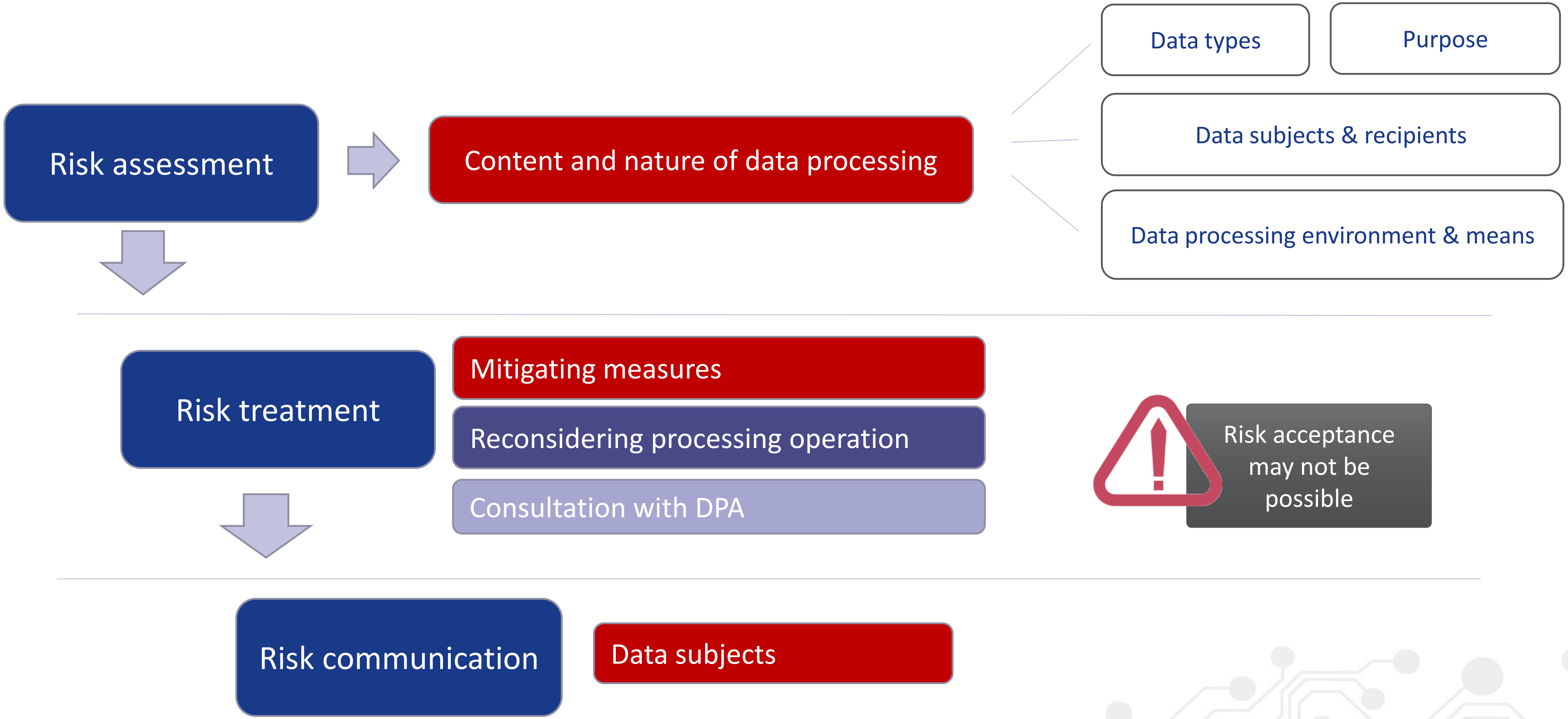
Impact

Negative effects to **data subjects**

⚠ **Secondary effects** should also be considered!

- Identity theft
- Financial loss
- Physical or psychological harm
- Insult, humiliation
- Annoyance
- Discrimination
- Damage to reputation
- Threat to life

A data protection risk management framework



Risk assessment

Content and nature of data processing

Data types

Purpose

Data subjects & recipients

Data processing environment & means

Risk treatment

Mitigating measures

Reconsidering processing operation

Consultation with DPA

Risk acceptance may not be possible

Risk communication

Data subjects

Security risk assessment for the processing of personal data

enisa

Step 1

Definition of the processing operation and its context

- Types of personal data
- Categories of data subjects
- Means of processing
- Recipients

Step 2

Understanding and evaluation of impact

- Confidentiality
- Integrity
- Availability

Step 3

Definition of possible threats and evaluation of their likelihood

- Network and technical resources
- Processes/procedures related to the data processing operation
- Different parties and people involved in the data processing operation
- Business sector and scale of processing

Step 4

Evaluation of risk

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨	🟥
	Medium	🟩	🟨	🟥
	High	🟨	🟥	🟥

Adoption of measures appropriate to the risk

Security policy

SM.A.1	The organization should develop and document a security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties.	🟩
SM.A.2	The security policy should be reviewed and revised, if necessary, on an annual basis.	
SM.A.3	The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organisation measures adopted for the security of personal data, the data processors or other third parties involved in the processing of personal data.	🟨
SM.A.4	An inventory of specific policies/procedures related to the security of personal data should be created and maintained, based on the general security policy.	
SM.A.5	The security policy should be reviewed and revised, if necessary, on a semester basis.	🟥
	Related to ISO 27001:2013 - A.5 Security policy control	

Database security

SM.M.1	Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly.	🟩
SM.M.2	Database and applications servers should only process the personal data that are actually neededs to process in order to achieve its processing purposes.	
SM.M.3	Encryption solutions should be considered on specific files or records through software or hardware implementation.	🟨
SM.M.4	Encrypting storage drives should be considered	
SM.M.5	Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information	
SM.M.6	Techniques supporting privacy at the database level, such as authorized queries, privacy preserving data base querying, searchable encryption, etc., should be considered.	🟥
	Related to ISO 27001:2013 - A. 12 Operations security	

From theory to practise – Payroll use case

A retail SME that processes personal data of its employees for salaries, benefits and social security […] The processing operation is facilitated by the HR IT system, which is deployed within the premises of the SME, and the HR officer operates it.

PROCESSING OPERATION DESCRIPTION	EMPLOYEES PAYROLL MANAGEMENT	
Personal Data Processed	Contact information (last and first name, address, telephone number,) social security number, taxation Identifier, date of employment, salary information	
Processing Purpose	Payroll management (payment of salaries, benefits and social security contributions)	
Data Subject	Employees	
Processing Means	Human Resources IT System	
Recipients of the Data	External	Financial Institutions
	External	Social Insurance Schemes
Data Processor Used	In-house (no data processor)	

Payroll use case – Assessing the risk

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Medium	**Low**	**Low**
	Overall Impact Evaluation	**MEDIUM**

THREAT ASSESSMENT	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	**Low**	**1**
Processes/Procedures related to the processing of personal data	**Low**	**1**
Parties/People involved in the processing of personal data	**Medium**	**2**
Business sector and scale of processing	**Low**	**1**
Overall Threat Occurrence Probability	**LOW (5)**	

IMPACT LEVEL

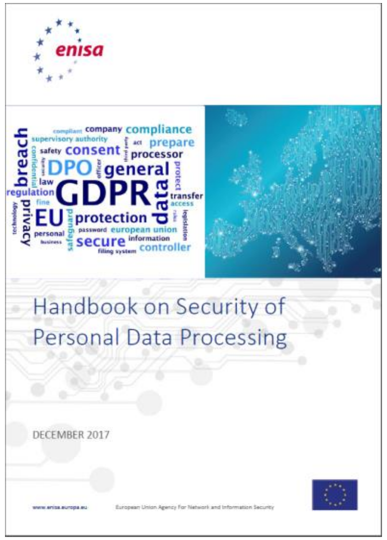
THREAT OCCURRENCE PROBABILITY

	Low	Medium	High / Very High
Low	🟩	🟨 **X**	🟥
Medium	🟩	🟨	🟥
High	🟨	🟥	🟥

Overall Findings

Guidelines for SMEs on the security of personal data processing

DECEMBER 2016

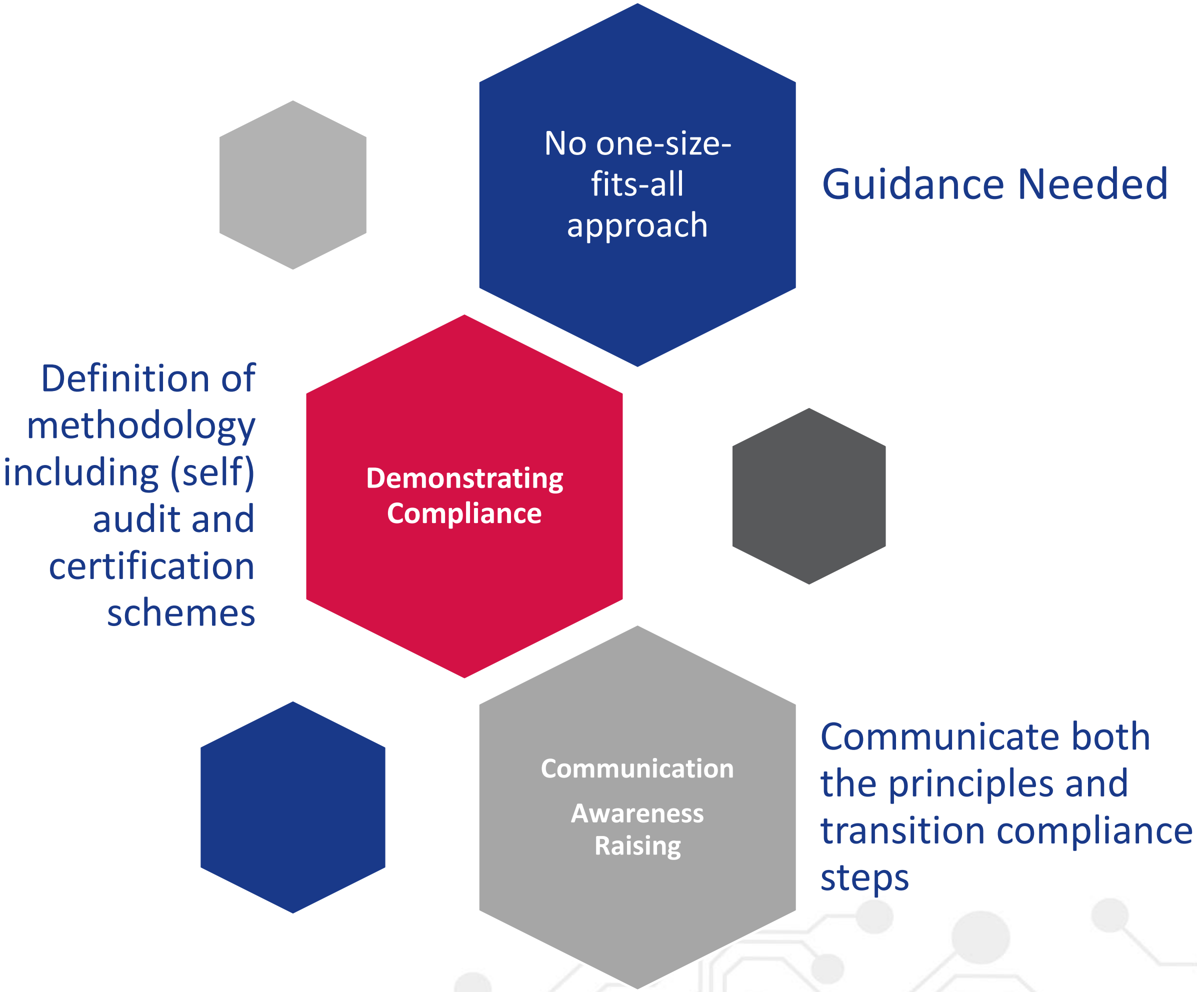


Handbook on Security of Personal Data Processing

DECEMBER 2017

www.enisa.europa.eu

European Union Agency For Network and Information Security



No one-size-fits-all approach

Guidance Needed

Demonstrating Compliance

Definition of methodology including (self) audit and certification schemes

Communication

Awareness Raising

Communicate both the principles and transition compliance steps

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu