Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

byDesign

Information Security Risk Assessment and Personal Data Protection Risk Assessment

Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services *(www.bydesign-project.eu)*

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ

ΚΕΝΤΡΟ ΕΡΕΥΝΩΝ
ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ

ICT abovo
Information & Communication Technologies

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Agenda of the Seminar

- Introduction
- Information Security Risk Assessment
- Personal Data Impact Assessment
- Information Security Risk Assessment vs. Personal Data Impact Assessment
- Data Protection Impact Assessment Tools and Practical Issues

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Introduction

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Relevant Challenges

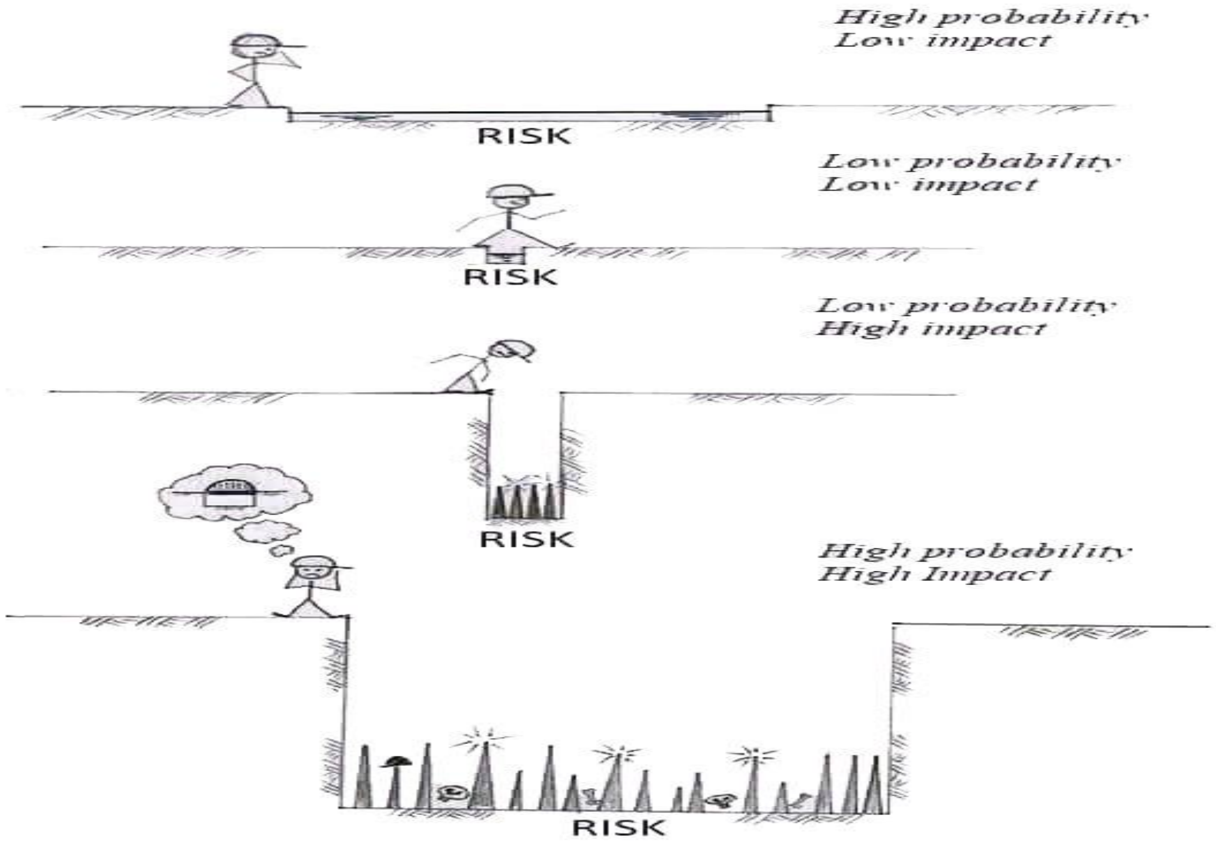
- “How much” should we protect information systems and personal data?
- How can we select safeguards to protect personal data that are appropriate to the nature, scope, context and purposes of data processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons?
- How to communicate technical challenges and solutions to the management so that they can approve investments in controls?

The Concept of Risk

- A risk is a hypothetical scenario that describes a feared event and all the threats that would allow this to occur.
- Risk is a function of:
  - The supporting assets
  - The nature and number of vulnerabilities that pertain the supporting assets
  - The nature of a threat and the occurrence probability
  - The nature and extend of the consequences (impact) that the individuals (data subjects) and the organizations will experience in case of data breach

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

The Concept of Risk



Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Information Security Risk Assessment

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Information Security Risk Assessment Methods Commonly…

- Are based on a general, high-level models of the information system
- Assess the value of information system assets
- Identify and analyse vulnerabilities
- Identify and analyse threats
- Measure the potential impact from a security incident
- Calculate risk factors
- Propose appropriate countermeasures

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

ISO 27005:2018 Guidelines for information security risk management

- is applicable to all types of organizations (e.g., commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization’s information security
- Supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach
- Contains the description of the information security risk management process and its activities

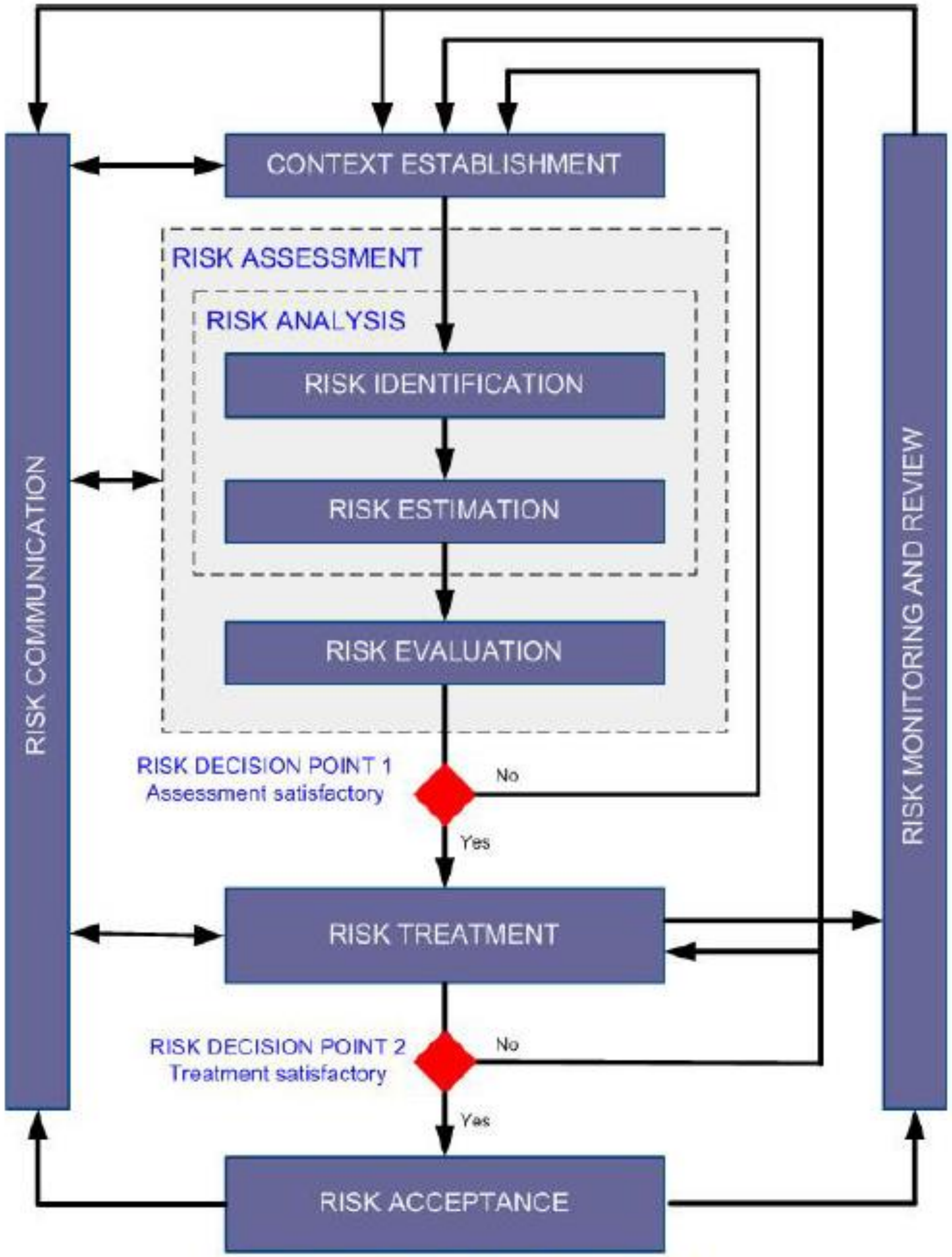
Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

ISO 27005:2018 Guidelines for information security risk management

Information security risk assessment is commonly part of a risk management process that consists of:

- the context establishment,
- the risk assessment,
- the risk treatment,
- the risk acceptance,
- the risk communication and consultation, and
- the risk monitoring and review.

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Context Establishment

- Context establishment is a step that precedes information security risk assessment
- Context establishment includes the specification of:
    - basic criteria:
        - risk evaluation criteria
        - impact criteria
        - risk acceptance criteria
    - scope and boundaries, which identifies all relevant assets to be considered in the risk assessment
    - the organization of responsibilities

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Information security risk assessment: Risk identification

- Aims to determine what could happen to cause a potential loss, and to gain insight into how, where and why the loss might happen
- Risk identification considers risks deriving from sources that are either under the control of the organization, or not.
- Risk identification includes the:
    - Identification of assets,
    - Identification of threats,
    - Identification of existing controls,
    - Identification of vulnerabilities, and
    - Identification of consequences.

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Risk identification – Identification of Assets

- An asset is anything that has value to the organization and which therefore requires protection
- The security experts should consider that an information system consists of more than hardware and software
- The level of detail when identifying assets may vary and should ensure sufficient information for the risk assessment
- Risk identification results in a list of assets to be risk-managed, and a list of business processes related to assets and their relevance to each process

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Risk identification – Identification of Assets

Primary assets:

- Business processes & activities
- Information

Supporting assets of all types:

- Hardware
- Software
- Network
- Personnel
- Site
- Organization’s structure

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Risk identification – Identification of Assets

Primary Assets

Example of Business processes and activities:

- Processes whose loss or degradation make it impossible to carry out the mission of the organization
- Processes that contain secret processes or processes involving proprietary technology
- Processes that, if modified, can greatly affect the accomplishment of the organization's mission
- Processes that are necessary for the organization to comply with contractual, legal or regulatory requirements

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Risk identification – Identification of Assets

Primary Assets

Example of information:

- Information vital for the exercise of the organization's mission or business
- Personal information, based on regulation
- Strategic information required for achieving objectives determined by the strategic orientations
- High-cost information whose gathering, storage, processing and transmission require a long time and/or involve a high acquisition cost

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Risk identification – Identification of Assets

Supportive Assets

Example of hardware:

- Data processing equipment
- Transportable equipment, such as laptops
- Fixed equipment, such as servers
- Processing peripherals, such as printers
- Data medium, such as storage
- Electronic medium, such as memory keys
- Other media, such as paper

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Risk identification – Identification of Assets

Supportive Assets

Example of software:

- Operating system
- Service, maintenance or administration software
- Package software or standard software, such as database management software, web server software
- Business applications, such as commercial or custom-developed software to support business functions and services

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Risk identification – Identification of Assets

Supportive Assets

Example of network assets:

- Medium and support, such as telecommunications media or equipment and protocols
- Passive or active relay, such as routers and switches
- Communication interface, such as adaptors

Example of personnel:

- Operation/ Maintenance staff
- Developers
- Users
- Decision Makers

Risk identification – Identification of Assets

Supportive Assets

Example of site assets:

- Premises and external environment
- Utilities
- Zones

Example of organization assets:

- Authorities
- Structure
- Subcontractors / Suppliers / Manufacturers

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Risk identification – Asset valuation

- Asset valuation aims to provide the value per identified asset with respect to disclosure, modification, nonavailability and destruction
- Definition of a scale for valuation (qualitative or quantitative) and the criteria for assigning a particular degree on that scale to each asset
- Possible criteria to determine an asset’s value refer to original cost, replacement or re-creation cost or other abstract values
    - Example criteria: violation of legislation, loss of goodwill, disruption to business activities, financial loss, endangerment of personal safety
- Some assets can be assessed based on known monetary value, and other not
    - Example scale: negligible, very low, low, medium, high, very high, and critical

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Risk identification – Impact assessment

- Impact is considered different to the asset value
- An information security incident can impact more than one asset or only a part of an asset
- Normally the impact will be assessed closely to the asset valuation (first risk assessment) and then lower to it due to the installation of controls reducing impact
- Example of impacts:
  - Financial replacement value of lost (part of) asset
  - Cost of acquisition, configuration and installation of the new asset
  - Opportunity cost

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Risk identification – Identification of threats

- A threat refers to a source that has the potential to harm assets such as information, processes and systems
- Threats may be of natural or human origin and could be accidental or deliberate
- Threat identification aims to result in a list of threats, threat types and sources

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Risk identification – Identification of threats

Example of threats and respective types of threats

Type	Threats
Physical damage	Fire
	Water damage
	Pollution
	Major accident
	Destruction of equipment or media
	Dust, corrosion, freezing
Natural events	Climatic phenomenon
	Seismic phenomenon
	Volcanic phenomenon
	Meteorological phenomenon
	Flood
Loss of essential services	Failure of air-conditioning or water supply system
	Loss of power supply
	Failure of telecommunication equipment
Technical failures	Equipment failure
	Equipment malfunction
	Saturation of the information system
	Software malfunction
	Breach of information system maintainability

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Risk identification – Identification of threats

Example of human threats sources

Type	Threats
Hacker, cracker	Challenge Ego Rebellion Status Money
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration
Terrorist	Blackmail Destruction Exploitation Revenge Political Gain Media Coverage
Industrial espionage	Competitive advantage Economic espionage
Insiders	Curiosity Ego Intelligence Monetary gain Revenge

Risk identification – Identification of existing controls

- This step ensures the avoidance of unnecessary work or cost, such as the duplication of controls
- During this step security experts should verify that the existing controls function properly and are effective
  - Estimation of the effect of the control regarding how it reduces the threat likelihood and ease of exploiting the vulnerability, or impact of the incident
  - Management reviews and audit reports should also be examined

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Risk identification – Identification of vulnerabilities

- Vulnerabilities are properties or issues that can be exploited by threats to cause harm to assets or to the organization
- Vulnerabilities arising from different sources need to be considered, for example, those intrinsic or extrinsic to the asset
- An incorrectly implemented or malfunctioning control or control being used incorrectly could itself be a vulnerability
- The presence of a vulnerability does not cause harm in itself, as there needs to be a threat present to exploit it

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Risk identification – Identification of vulnerabilities

Types	Examples of vulnerabilities	Examples of threats
Hardware	Insufficient maintenance/faulty installation of storage media	Breach of information system maintainability
	Lack of periodic replacement schemes	Destruction of equipment or media
	Susceptibility to humidity, dust, soiling	Dust, corrosion, freezing
	Lack of efficient configuration change control	Error in use
	Susceptibility to voltage variations	Loss of power supply
Software	No or insufficient software testing	Abuse of rights
	No 'logout' when leaving the workstation	Abuse of rights
	Wrong allocation of access rights	Abuse of rights
	Complicated user interface	Error in use
	Lack of documentation	Error in use
	Uncontrolled downloading and use of software	Tampering with software
Network	Unprotected communication lines	Eavesdropping
	Lack of proof of sending or receiving a message	Denial of actions
	Transfer of passwords in clear	Remote spying
Personnel	Lack of security awareness	Error in use
	Unsupervised work by outside or cleaning staff	Theft of media or documents
Site	Lack of formal procedure for user registration and de-registration	Abuse of rights
	Lack of procedures for classified information handling	Error in use
	Lack of information security responsibilities in job descriptions	Error in use

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Risk identification – Identification of vulnerabilities

- Technical vulnerabilities can be identified using automated testing methods, such as:
  - Automated vulnerability scanning tool
  - Security testing and evaluation
  - Penetration testing
  - Code review

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Risk identification – Identification of consequences

- This steps regards the consequences that losses of confidentiality, integrity and availability may have on the assets, in terms of (but not limited to):
    - Investigation and repair time
    - (Work)time lost
    - Opportunity lost
    - Health and Safety
    - Financial cost of specific skills to repair the damage
    - Image reputation and goodwill

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Information security risk assessment: Risk Analysis

- A risk analysis methodology may be qualitative or quantitative, or hybrid
  - Qualitative methodologies use a qualitative scale (e.g., low, medium and high) for assessing attributes to describe the magnitude of potential consequences and the likelihood that those consequences will occur
  - Quantitative methodologies use a scale with numerical values for both consequences and likelihood, using data from a variety of sources (e.g., historical incident data)

Risk Analysis – Assessment of consequences

- Consequences or business impact can be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or past data
- Consequences can be expressed in terms of monetary, technical or human impact criteria, or other criteria relevant to the organization.
- In some cases, more than one numerical value is required to specify consequences for different times, places, groups or situations

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

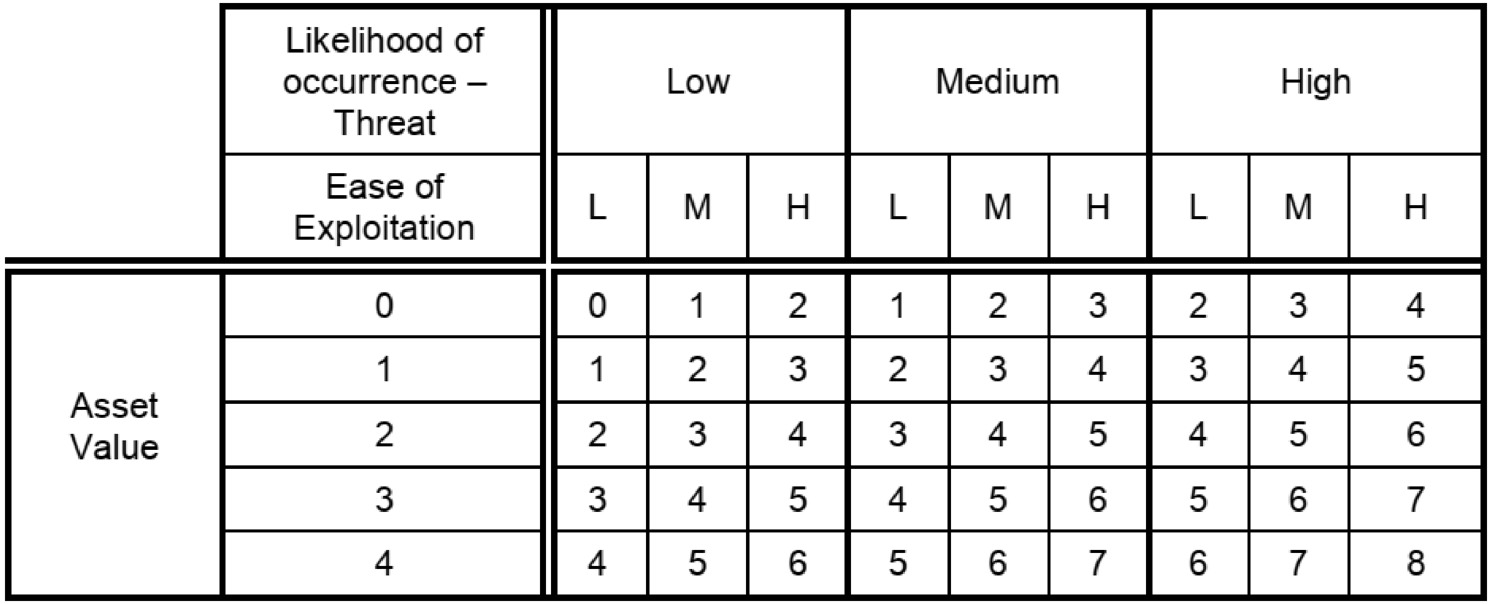
Risk Analysis – Assessment of incident likelihood

- After identifying the incident scenarios, the likelihood of each scenario and impact occurring is assessed, using qualitative or quantitative analysis techniques, considering:
  - experience and applicable statistics for threat likelihood
  - for deliberate threat sources: the motivation and capabilities, which will change over time, and resources available to possible attackers, as well as the perception of attractiveness and vulnerability of assets for a possible attacker
  - for accidental threat sources: geographical factors, e.g., the possibility of extreme weather conditions, and factors that could influence human errors and equipment malfunction
  - vulnerabilities, both individually and in aggregation
  - existing controls and how effectively they reduce vulnerabilities

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Risk Analysis – Determination of Level of Risk

- The risk is estimated as a combination of the assigned values of the likelihood of an incident scenario and its consequences
- Indicative example of risk matrix is presentec in the Figure



	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

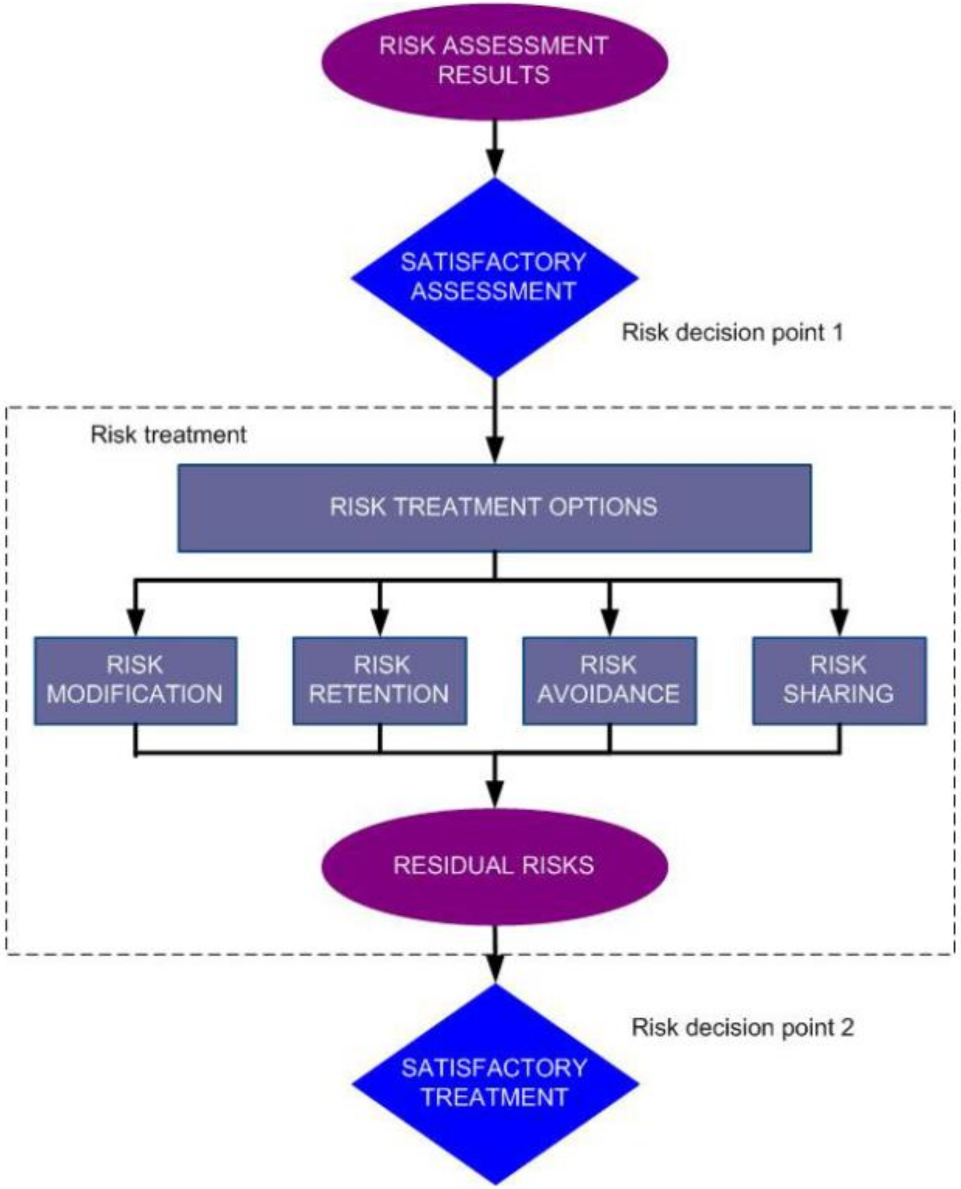
Information security risk assessment: Risk evaluation

- The level of risks is compared against risk evaluation criteria and risk acceptance criteria (defined when establishing the context)
- Decisions are based on the acceptable level of risk:
  - Whether an activity should be undertaken
  - Priorities for risk treatment considering estimated levels of risks
- During the risk evaluation stage, contractual, legal and regulatory requirements are factors that should be considered in addition to the estimated risks

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Information security risk treatment

- There are four options available for risk treatment:
  - risk modification
  - risk retention
  - risk avoidance, and
  - risk sharing



Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Data Protection Impact Assessment

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

What is Data Protection Impact Assessment and when is it necessary?

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Data Protection Impact Assessment in the General Data Protection Regulation

- According to the GDPR data protection impact assessment (DPIA) is obligatory when a personal data processing involves high risk to the rights and freedoms of natural persons
  - The evaluation of level of risk considers the nature, scope, context and purposes of the processing
  - The decision and conduction of DPIA before initiating the processing of personal data

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Data Protection Impact Assessment in the General Data Protection Regulation

- A DPIA is particularly obligatory in the cases that the personal data processing involves:
  - systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
  - processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences
  - systematic monitoring of a publicly accessible area on a large scale

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

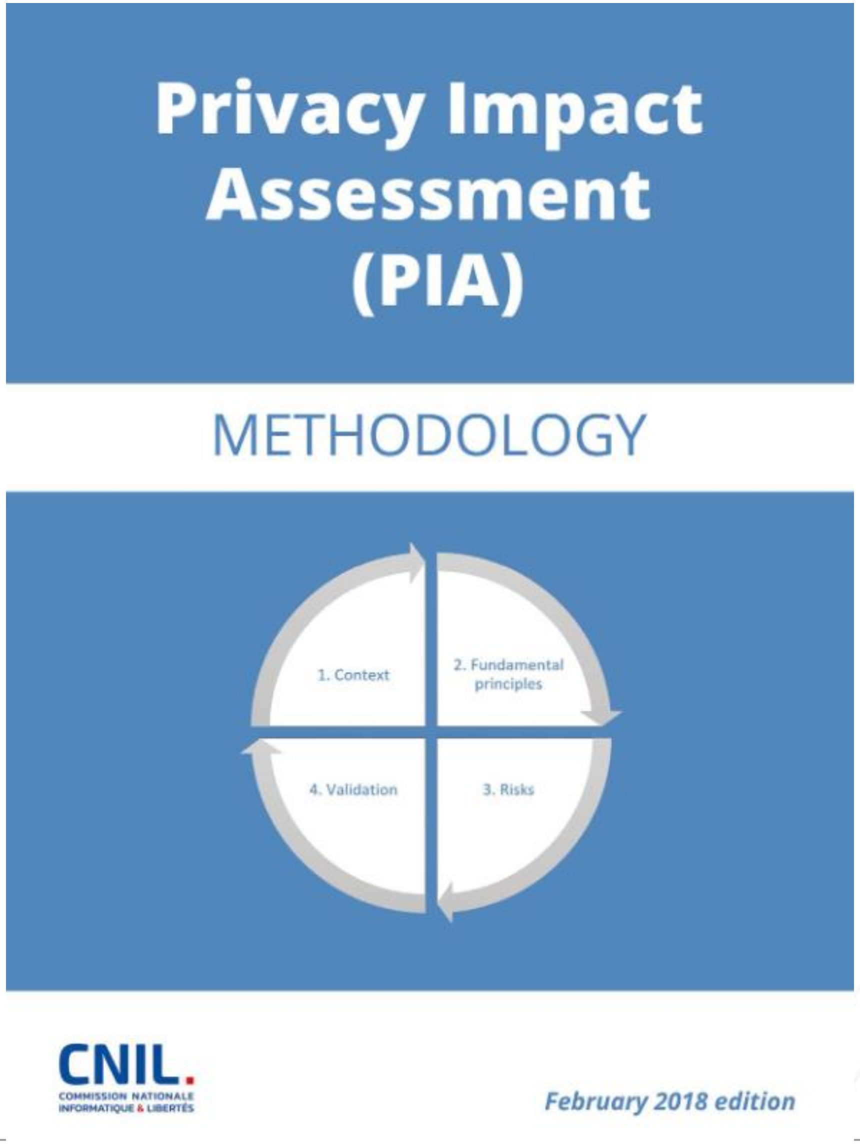
Data Protection Impact Assessment in the General Data Protection Regulation

- The DPIA shall contain at least:
  - a systematic description of the **envisaged processing** operations and the purposes of the processing
  - an assessment of the **necessity** and **proportionality** of the processing operations in relation to the purposes
  - an **assessment of the risks** to the rights and freedoms of data subjects
  - the **measures** envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR considering the rights and legitimate interests of data subjects and other persons concerned

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

CNIL DPIA Methodology, Guides and Tool

- CNIL (Commission Nationale de l'Informatique et des Libertés) is the National Personal Data Protection Authority in France
- CNIL has published a set of good practices to address the privacy risks and assist DPIA implementation:
    - A methodology
    - Templates
    - A knowledge base
    - An example application
- CNIL has also released a software tool to assist the implementation of the methodology



Privacy Impact Assessment (PIA)

METHODOLOGY

1. Context

2. Fundamental principles

3. Risks

4. Validation

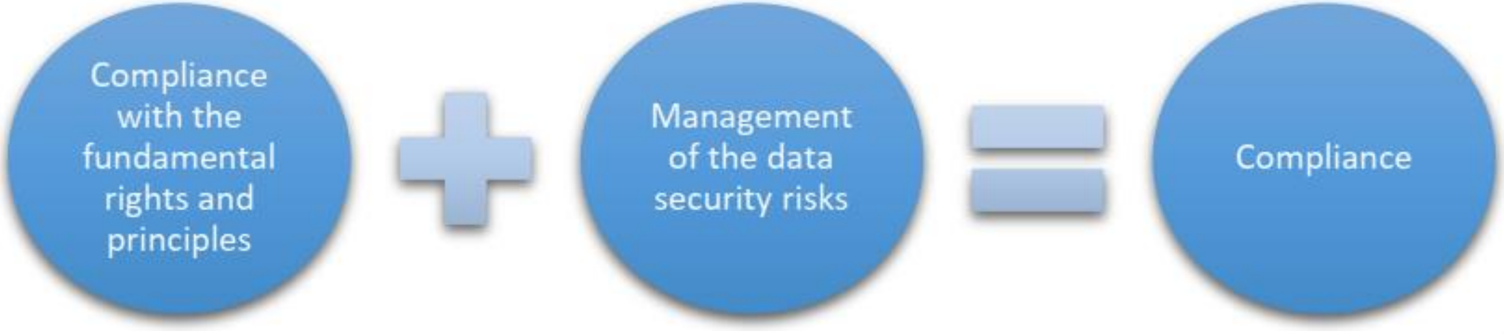
CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

February 2018 edition

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Two Pillars of the CNIL DPIA Methodology

- The compliance approach of the DPIA is based on two pillars:
  - The fundamental rights and principles, which are “non-negotiable”, established by law and which must be respected, regardless of the nature, severity and likelihood of risks
  - The management of data subjects’ privacy risks, which determines the appropriate technical and organisational controls to protect personal data


Compliance with the fundamental rights and principles
+
Management of the data security risks
=
Compliance

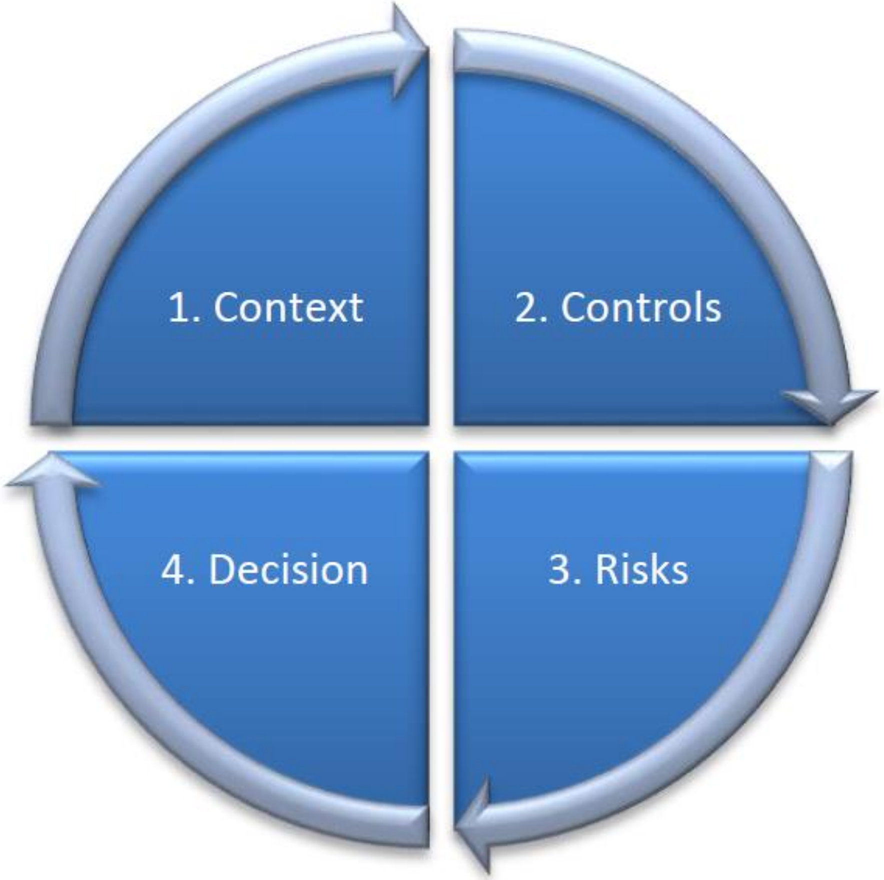
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

The Steps of the CNIL DPIA Methodology

- The main steps of PIA-CNIL methodology are:
  - Define and describe the context of the processing of personal data under consideration and its stakes
  - Identify existing or planned controls (procedural / technical / organisational) guaranteeing compliance with legal requirements, and to treat privacy risks in a proportionate manner
  - Assess privacy risks associated with data security and ensure they are properly treated
  - Make the decision to validate the manner in which it is planned to comply with privacy principles and treat the risks or review the preceding steps

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

The Steps of the CNIL DPIA Methodology



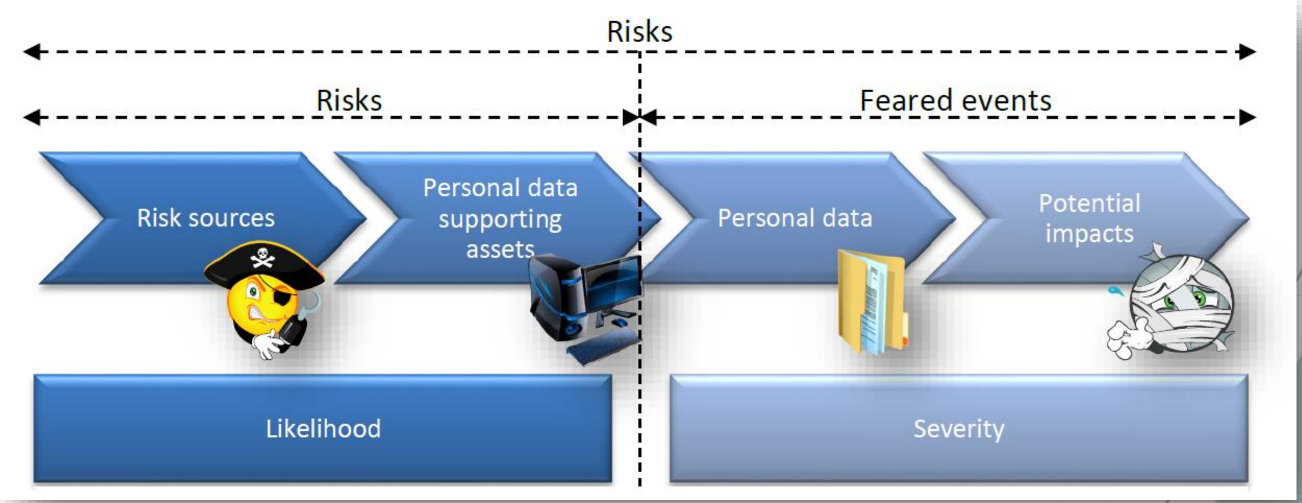
- DPIA is a continuous improvement process
- It may require several iterations to achieve an acceptable privacy protection system
- It requires a monitoring of changes over time (in context, controls, risks, etc.), for example, every year, and updates whenever a significant change occurs

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

The Concept of Risk in DPIA

A **Risk** is a hypothetical scenario that describes:

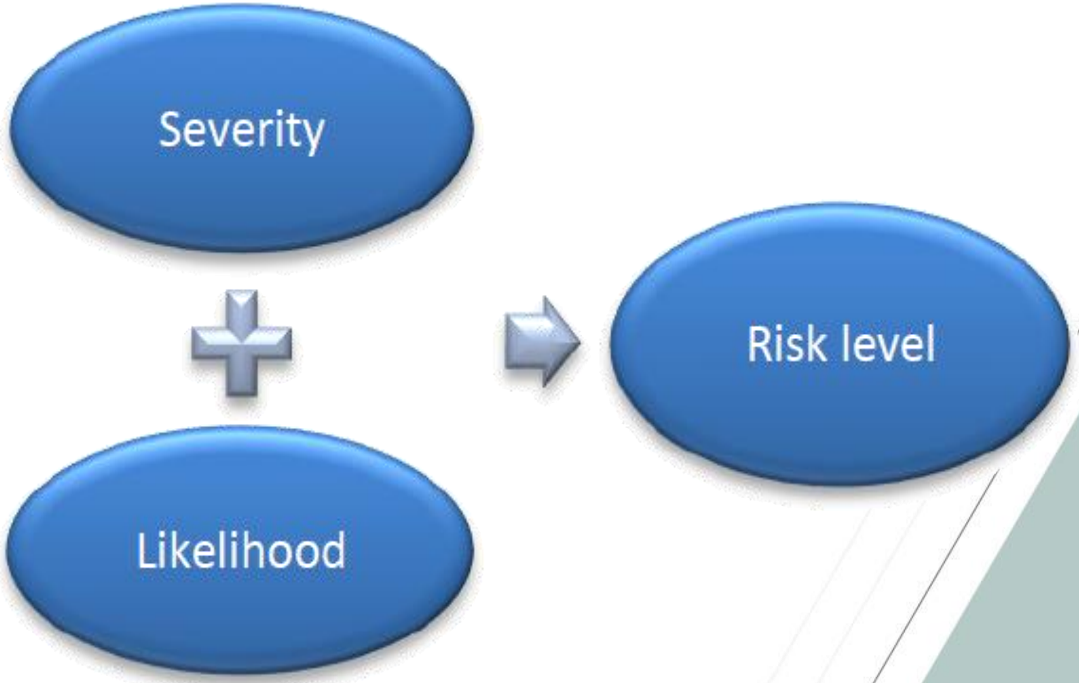
- how **Risk Sources** (e.g., an employee bribed by a competitor)
- could exploit the vulnerabilities in **personal data supporting assets** (e.g., the file management system that allows the manipulation of data)
- in a context of **threats** (e.g., misuse by sending emails)
- and allow **feared events** to occur (e.g., illegitimate access to personal data)
- on personal data (e.g., customer file)
- thus, generating **potential impacts** on the privacy of data subjects (e.g., unwanted solicitations, feelings of invasion of privacy, etc.)



Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

The Concept of Risk in DPIA

- The risk level is estimated in terms of severity and likelihood:
  - **severity** represents the magnitude of a risk. It primarily depends on the prejudicial nature of the potential impacts, and
  - **likelihood** expresses the possibility of a risk occurring. It primarily depends on the level of vulnerabilities of the supporting assets when under threat and the level of capabilities of the risk sources to exploit them



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Step 1: Context of personal data processing

- Aims at the definition of the outline of the processing of personal data
- Contains:
  - The description of the purpose of processing(s) of personal data
  - The identification of Data Controller and any Data Processor(s)
  - The identification of the categories of personal data and their recipients
  - The identification of the retention period of personal data
  - The description of the processes and personal data supporting assets for the entire personal data life cycle (from collection to erasure)

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Step 2: Controls - Study of the fundamental principles

Assessment of the controls guaranteeing the proportionality and necessity of the processing

- **Purpose** : Specified, explicit and legitimate purpose
- **Basis**: lawfulness of processing, prohibition of misuse
- **Data Minimisation**: limiting the amount of personal data to what is strictly necessary
- **Quality of data**: preserving the quality of personal data, accurate and kept up-to-date
- **Retention periods**: period needed to achieve the purposes, in the absence of another legal obligation imposing a longer retention period

Assessment of controls protecting data subjects' rights

- **Information**: respect for data subjects’ right to information
- **Consent**: obtaining the consent of the data subjects or existence of another legal basis justifying the processing of personal data
- **Right to object**: respect for the data subjects’ right of opposition
- **Right of access and data portability**: respect for the data subjects’ right to access their data and move them
- **Right to rectification and erasure**: respect for the data subjects’ right to correct their data and erase them
- **Transfers**: compliance with obligations relating to transfer of data outside the European Union
- **Processors:** identified and governed by a contract

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Step 3: Study of the risks related to the security of data - Assessment of existing or planned controls

- Existing controls are identified:
    - **Controls bearing specifically on the data being processed:** encryption, anonymization, partitioning, access control, traceability, etc.
    - **General security controls regarding the system in which the processing is carried out**: operating security, backups, hardware security, etc.
    - **Organizational controls (governance):** policy, project management, personnel management, management of incidents and breaches, relations with third parties, etc.

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Step 3: Study of the risks related to the security of data - Risk assessment: potential privacy breaches

- Definition of three feared events:
    - **Illegitimate access to personal data** (data are known to unauthorised persons; breach of personal data confidentiality)
    - **Unwanted change of personal data** (data are altered or changed; breach of personal data integrity), and
    - **Disappearance of personal data** (data are not or no longer available; breach of personal data availability)

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Step 3: Study of the risks related to the security of data - Risk assessment: potential privacy breaches

- For each feared event:
  - Determination of the potential **impacts** on the data subjects’ privacy if it occurred
  - Estimation of its **severity**, particularly depending on the prejudicial nature of the potential impacts and, where applicable, controls likely to modify them
  - Identification of the **threats** to personal data supporting assets that could lead to this feared event and the risk sources that could cause it
  - Estimation of its **likelihood**, particularly depending on the level of vulnerabilities of personal data supporting assets, the level of capabilities of the risk sources to exploit them and the controls likely to modify them

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Step 3: Study of the risks related to the security of data - Risk assessment: potential privacy breaches

- Identification of threats to personal data supporting assets that could lead to each feared event
- For each identified threat:
    - Selection of the **risk sources** that could cause it
    - Estimation of its **likelihood**, particularly depending on the level of **vulnerabilities** of personal data supporting assets, the level of **capabilities** of the risk sources to exploit them and the **controls** likely to modify them

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Step 3: Study of the risks related to the security of data - Risk assessment: potential privacy breaches

- Identification of impacts to the data subjects caused by each feared event.
- For each feared event:
  - Determination of the potential **impacts** on the data subjects' privacy if it occurred
  - Estimation of its **severity**, depending especially on the prejudicial effect of the potential impacts

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Step 3: Study of the risks related to the security of data - Risk assessment: potential privacy breaches

- For each feared event:
  - Determination if the risks identified (A risk is based upon a feared event and all threats that would make it possible) can be considered acceptable in view of the existing or planned controls
  - If not, proposal of additional controls and re-assessment of the level of each of the risks in view of the latter, so as to determine the residual risks

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Step 4: Validation of the DPIA

- Preparation of the material required for validation
- Consolidation of the findings
  - visual presentation of the controls selected to ensure compliance with the fundamental principles
  - visual presentation of the controls selected to contribute to data security, depending on their compliance with best security practices
  - visual map of the risks depending on their severity and likelihood
  - Definition of action plan based on the additional controls identified during the previous steps

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Step 4: Validation of the DPIA

- Formal validation of the DPIA
- Decision on whether the selected controls, residual risks and action plan are acceptable, with justifications, in light of the previously identified stakes and views of the stakeholders.
- In this way, the PIA may be:
  - validated
  - conditional on improvement (explain in what way)
  - refused (along with the processing under consideration)
- Where necessary, repetition of the previous steps so that the DPIA can be validated

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Information Security Risk Assessment vs. Personal Data Impact Assessment

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Variations regarding Data in Consideration

- In the same information system, the information security risk assessment and the Data protection impact assessment would have a different focus on the categories of data in consideration:
  - Information security risk assessment aims to protect all types of data that the information system processes
  - Data protection impact assessment aims to protect the personal data that they information system processes

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Variations regarding Impact in Consideration

- Impact is one of the components for the calculation of risk factors
- The nature and type of impact is different for information security risk assessment and data protection impact assessment:
  - Information security risk assessment mainly focuses on categories of impact that result from a breach and affect the organization, such as:
    - Loss of reputation
    - Commercial and financial interests
    - Disruption of business processes
  - Data protection impact assessment mainly focuses on categories of impact that result from a breach and affect the individuals (data subjects), such as:
    - Inconvenience
    - Receipt of unsolicited mail and targeted advertisement
    - Loss of opportunities
    - Psychological ailments

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Variations regarding Impact in Consideration

- The analysis of threats, impacts and risks in information security risk assessment is more focused on business interests
- The analysis of threats, impacts and risks in data protection impact assessment is more focused on individual freedom, rights and interests
    - The impact categories in information security risk assessment methods are commonly more complex, scalable and various
- The analysis in data protection impact assessment focuses on the principle of proportionality; data types and means of processing should be tight to the purpose of processing

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Data Protection Impact Assessment Tools and Practical Issues

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Data protection impact assessment standards, methods and tools

Standards and Methods

- ISO 29134:2017, Information technology — Security techniques — Guidelines for privacy impact assessment
- CNIL Data Protection Impact Assessment Guides
- Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)
- Information Commissioner’s Office (ICO) Guide for Data protection impact assessments
- Etc.

Tools

- CNIL PIA software tool
- Templates, e.g., ICO DPIA template *https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx*
- OneTrust automated PIA & DPIA
- TrustArc Privacy Management Platform
- Etc.

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Practical Challenges

- Data protection impact assessment focuses on categories of impact that affect the freedoms and rights of individuals (i.e., data subjects)
- The assessment of impacts for a feared event (a.k.a., risk) involves:
  - The identification of types of impact that may occur due to the materialization of the risk (e.g., psychological ailments)
  - The assessment of magnitude level within the type of impact (e.g., minor depression, serious depression, development of a phobia, etc.)
- Data protection impact assessment methods work on the development of taxonomies and scales for data protection impacts, but it seems imperative to involve data subjects as representatives to help assessing the impact of feared events

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Feared Event: Illegitimate access to data

Industry Medical Services

Risk category: Illegitimate access to data

Threat	Severity	Likelihood
➢ Masquerading of Identity	Maximum Level: 4	Negligible Level: 1
➢ Unauthorised Use of an Application	Maximum Level: 3,5≈4	Negligible Level: 1
➢ Threats during data transmission	Significant Level: 3	Negligible Level: 1
➢ Misuse of physical resources	Significant Level: 3	Negligible Level: 1

Industry Education

Risk category: Illegitimate access to data

Threat	Severity	Likelihood
➢ Masquerading of Identity	Significant Level: 3	Limited Level: 2
➢ Unauthorised Use of an Application	Significant Level: 3	Limited Level: 2
➢ Threats during data transmission	Limited Level: 2	Negligible Level: 1
➢ Misuse of physical resources	Significant Level: 3	Negligible Level: 1

Industry Public Administration

Risk category: Illegitimate access to data

Threat	Severity	Likelihood
➢ Masquerading of Identity	Significant Level: 3	Limited Level: 2
➢ Unauthorised Use of an Application	Significant Level: 3	Negligible Level: 1
➢ Threats during data transmission	Significant Level: 3	Limited Level: 2
➢ Misuse of physical resources	Significant Level: 3	Negligible Level: 1

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Feared Event: Unwanted modification of data

Industry Medical Services

Risk category: Unwanted modification of data

Threat	Severity	Likelihood
➢ Masquerading of Identity	Maximum Level: 4	Negligible Level: 1
➢ Hardware Malfunction	Significant Level: 2,5≈3	Negligible Level: 1
➢ Software Malfunction	Limited Level: 2	Negligible Level: 1

Industry Education

Risk category: Unwanted modification of data

Threat	Severity	Likelihood
➢ Masquerading of Identity	Significant Level: 3	Limited Level: 2
➢ Hardware Malfunction	Significant Level: 3	Limited Level: 2
➢ Software Malfunction	Limited Level: 2	Negligible Level: 1

Industry Public Administration

Risk category: Unwanted modification of data

Threat	Severity	Likelihood
➢ Masquerading of Identity	Significant Level: 3	Limited Level: 2
➢ Hardware Malfunction	Limited Level: 2	Negligible Level: 1
➢ Software Malfunction	Limited Level: 2	Negligible Level: 1

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Feared Event: Data disappearance

Industry Medical Services

Risk category: Data disappearance

Threat	Severity	Likelihood
➢ **Masquerading of Identity**	Maximum Level: 4	Negligible Level: 1
➢ **Technical failure**	Significant Level: 3	Limited Level: 2
➢ **Application Software Failure**	Limited Level: 2	Negligible Level: 1
➢ **Communications breaches**	Maximum Level: 4	Limited Level: 2
➢ **Malfunction to physical resources**	Significant Level: 3	Negligible Level: 1

Industry Education

Risk category: Data disappearance

Threat	Severity	Likelihood
➢ **Masquerading of Identity**	Significant Level: 3	Limited Level: 2
➢ **Technical failure**	Significant Level: 3	Limited Level: 2
➢ **Application Software Failure**	Limited Level: 2	Limited Level: 2
➢ **Communications breaches**	Significant Level: 3	Limited Level: 2
➢ **Malfunction to physical resources**	Significant Level: 3	Negligible Level: 1

Industry Public Administration

Risk category: Data disappearance

	Severity	Likelihood
➢ **Masquerading of Identity**	Limited Level: 2	Limited Level: 2
➢ **Technical failure**	Limited Level: 2	Negligible Level: 1
➢ **Application Software Failure**	Limited Level: 2	Significant Level: 3
➢ **Communications breaches**	Limited Level: 2	Limited Level: 2
➢ **Malfunction to physical resources**	Limited Level: 2	Negligible Level: 1

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Thank you for your participation!