



Training Material

Deliverable D3.2

Editor

Aggeliki Tsohou (UPRC)

Contributors

Konstantinos Lambrinoudakis (UPRC)

Georgia Panagopoulou (HDPA)

Konstantinos Limniotis (HDPA)

George Rousopoulos (HDPA)

Maria Alikakou (HDPA)

Efrosini Siougle (HDPA)

Leonidas Roussos (HDPA)

Reviewers

George Lioudakis (ABOVO)

Vasilis Zorkadis (HDPA)

Date

28th October 2021

Classification

Public



The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) under grant agreement No. 101005833

Acronyms

| ACRONYM | EXPLANATION |
|---------|---|
| CNIL | Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority) |
| DPIA | Data Protection Impact Assessment |
| GDPR | General Data Protection Regulation |
| ICT | Information and Communication Technology |
| SME | Small and Medium-sized Enterprise |

Table of Contents

| | | |
|----------|--|-----------|
| 1 | INTRODUCTION | 4 |
| 1.1 | Purpose of the document | 4 |
| 1.2 | Relations to other activities in the project | 4 |
| 1.3 | Structure of the document | 4 |
| 2 | TRAINING STRATEGY AND METHODOLOGY | 6 |
| 2.1 | Training Requirements identified from Stakeholders | 6 |
| 2.2 | Design Training Material to meet the Requirements | 6 |
| 2.3 | Delivery Means | 7 |
| 2.4 | Training Plan | 7 |
| 3 | TRAINING CONTENTS | 10 |
| 3.1 | Broad scope seminars content description and presentations titles | 10 |
| 3.1.1 | Introduction to Data Protection Terminology | 10 |
| 3.1.2 | ICT organizational GDPR roles – DPIA | 10 |
| 3.1.3 | Data Protection by Design and by Default in GDPR | 11 |
| 3.1.4 | Handling Data Breaches under the GDPR | 11 |
| 3.1.5 | Data Protection Policies and Notices | 11 |
| 3.1.6 | Online Marketing and Advertising, Cookies and trackers | 11 |
| 3.2 | Targeted content seminars content description and presentations titles | 12 |
| 3.2.1 | Security risk assessment vs. data protection risk assessment | 12 |
| 3.2.2 | Privacy by Design Requirements Elicitation | 12 |
| 3.2.3 | Encryption, Anonymization and Pseudonymization | 13 |
| 3.2.4 | Personal Data Breaches Management | 13 |
| 3.2.5 | Implementation of GDPR Data Protection/Privacy by Design | 13 |
| 4 | APPENDICES | 14 |

1 Introduction

The byDesign project aims to provide assistance to SMEs and other relevant stakeholders. To this end, one of the main pillars of the project (WP3) is the development of a specialized training programme about Data Protection by Design, targeting developers and other stakeholders of the ICT products and services creation chain.

1.1 Purpose of the document

The present deliverable aims to describe the design and preparation of the training activities to be performed within Task 3.3. More precisely, this deliverable encompasses all supportive material intended to be used during the trainings, as well as a description of the training methodology that is to be adopted, on the basis of this material.

1.2 Relations to other activities in the project

This deliverable, based on the Task 3.2 of the project, has been built according to the findings obtained from Task 3.1, in which all the necessary information from the stakeholders, regarding their requirements and needs on a data protection by design oriented educational programme, have been collected (see D3.1 of the project). More precisely, information regarding awareness and training needs that has been collected and analyzed, has been transformed into requirements for the training program (see D3.1), which, in turn, are being appropriately embedded into the development of the training program, as described in the present deliverable. Therefore, this deliverable gets direct input from Task 3.1.

Moreover, since this deliverable presents the educational material that will be used for the training program, as well as the structure of the program itself, it is directly related with the subsequent Task 3.3 (“Training activities”), providing the necessary input to this.

1.3 Structure of the document

This document consists of three sections, including the current introductory section, as well as of an Appendix. More precisely, the structure of the document is as follows:

- Section 2 describes the strategy and methodology that is to be adopted for the training programs, based on the requirements that have been elucidated in D3.1. The training plan is being explicitly given in this section.

D3.2 — Training material

- Section 3 presents the structure of the educational material, in terms of a table of contents and titles of the presentations. The material itself that will be used in the training programs is being explicitly given in the Appendix.

2 Training Strategy and Methodology

2.1 Training Requirements identified from Stakeholders

Within Task 3.1 “Awareness raising for producers of products, services and applications for SMEs” awareness and training needs have been collected, which were further analyzed and transformed into requirements for the training program. These requirements are reported in detail in Deliverable 3.1 “Training set-up and methodology” and are summarized in Table 1.

Table 1: Requirements identified from the stakeholders

| Type of Requirement | Number of Requirement | Description |
|---|-----------------------|---|
| Requirements Regarding Training in Conceptual Foundation and Practical Examples | Requirement 1 | Training on data protection/privacy and security risks through DPIA and security risk assessment practical cases/examples. |
| | Requirement 2 | Training on organizational GDPR roles through practical cases and examples. |
| | Requirement 3 | Training on data retention periods with industry-specific cases. |
| Requirements Regarding Training in Privacy by Design Methods and Techniques | Requirement 4 | Training on Data Protection/Privacy by Design requirements in existing ICT services, products, applications. |
| | Requirements 5 | Training on data protection/privacy-friendly default configurations for mobile applications. |
| | Requirement 6 | Training material on the adjustment of older systems/applications to become privacy friendly. |
| Requirements Regarding Training in Privacy Mechanisms | Requirement 7 | Training on the implementation of software tools to preserve personal data protection and to satisfy legitimacy principles. |
| Requirements Regarding Training in Handling of Data Breaches | Requirement 8 | Training on mechanisms on data breaches avoidance, monitoring and data breaches handling. |
| Requirements Regarding Training in General GDPR Knowledge | Requirement 9 | Guidelines on privacy by design self-assessment |

2.2 Design Training Material to meet the Requirements

The aim of the project team was to take into account the nine requirements enlisted in Table 1 and satisfy them through appropriate design of the training material.

The final training material addresses the following themes:

- Introduction to Data Protection Terminology
- Marketing and Advertising, Cookies and trackers
- Handling Data Breaches under the GDPR

D3.2 — Training material

- Personal data retention implementation
- Data subjects' rights implementation
- Encryption role and techniques
- Anonymization role and techniques
- Security risk assessment vs. data protection risk assessment
- Privacy by Design Requirements Elicitation
- Pseudonymization role and techniques

Table 2 presents how the designed training material meets the nine requirements:

| Training Themes | Met Requirement |
|--|---------------------------|
| <ul style="list-style-type: none">• Security risk assessment vs. data protection risk assessment• ICT organizational GDPR roles – DPIA – examples• Marketing and Advertising, Cookies and trackers | Requirement 1 – 2 - 3 |
| <ul style="list-style-type: none">• Data Protection by Design and by Default• Privacy by Design Requirements Elicitation | Requirement 4 – 5 – 6 - 9 |
| <ul style="list-style-type: none">• Encryption role and techniques• Anonymization role and techniques• Pseudonymization role and techniques | Requirement 7 |
| <ul style="list-style-type: none">• Handling Data Breaches under the GDPR and Online Privacy Notices and ePrivacy• Handling Data Breaches under the GDPR | Requirement 8 |

2.3 Delivery Means

The initial goal is that the training activities will include training events, organized physically in different cities in Greece, especially the main ICT industrial hubs (Athens, Thessaloniki, Patra, Herakleio). However, due to the ongoing Covid19 pandemic, several restrictions on traveling and gatherings and conventions are still enforced. Currently, the course of the pandemic cannot be predicted. Therefore, the realization of training seminars in physical locations is still under consideration, while alternative training delivery means are examined for the implementation of “virtual” training seminars. The current implementation schedule is that the project team will initiate the training activities using video conference technologies and will implement physical training events at due course, if possible.

By utilizing the experience that the project team gained from the organization of the “virtual” online workshops, the options for the video conference technologies to support the online training include the use of the solution GoToMeeting from the University of Piraeus and Cisco WebEx with an account of the same University. The online workshops within Task 3.1 were successfully held through Cisco WebEx, and thus this application is currently the most prominent solution.

2.4 Training Plan

Based on the collection of data that took place within Task 3.1, the stakeholders that were interested in this work can be divided according to their role in the ICT field into the following categories:

D3.2 — Training material

- Business role (e.g., department or unit managers, sales and marketing managers, customer relations managers, etc.)
- Requirements' analysis, solution design (e.g., system analysts, system engineers, etc.)
- Software development, programming (e.g., software application developer, chief operating officer, technical support engineer)
- Bachelor, Master and Ph.D. Students, with software programming experience

The schedule for the training activities includes (Task 3.3):

- Seven broad-scope seminars, each lasting one full day for attracting a large audience each (at least 50 persons)
- Thirteen workshops with more targeted content for more technically experienced audience, each hosting approximately 20 persons (software engineers and architects, technical managers, developers, etc.).
- Two seminars for the undergraduate and post-graduate students, targeting young and future ICT professionals. At least 100 students will participate in each seminar.

The project team has considered the above information and designed a training plan mapping the training contents (presented in section 2.2) with the identified stakeholders' categories and the training activities.

Table 2: Mapping of Training activities, stakeholders and contents

| Training Activity | Stakeholders' Role | Training Contents |
|-----------------------------|--|---|
| Seven broad-scope seminars | Business role, Requirements' analysis, Solution design | <ul style="list-style-type: none"> • Introduction to Data Protection Terminology • ICT organizational GDPR roles – DPIA – examples • Data Protection by Design and by Default • Handling Data Breaches under the GDPR and Online Privacy Notices and ePrivacy • Marketing and Advertising, Cookies and trackers |
| Thirteen technical seminars | Software development, programming, Requirements' analysis, Solution design | <ul style="list-style-type: none"> • Security risk assessment vs. data protection risk assessment • Privacy by Design Requirements Elicitation and Data Subjects' Rights • Handling Data Breaches under the GDPR • Personal data retention implementation • Data subjects' rights implementation • Encryption role and techniques • Anonymization role and techniques • Pseudoanonymization role and techniques |
| Two seminars for students | Bachelor, Master and Ph.D. Students | <ul style="list-style-type: none"> • Security risk assessment vs. data protection risk assessment • Privacy by Design Requirements Elicitation • Encryption role and techniques • Anonymization role and techniques • Pseudonymization role and techniques |

D3.2 — Training material

Each broad-scope seminar will include 50 participants, and thus we will target the participation of 350 stakeholders, holding roles in business, requirements' analysis and solution design.

For the technical seminars the allocation of events and stakeholders is presented below:

- The training material will be divided into five seminars:
 - **Seminar 1:** Security risk assessment vs. data protection risk assessment
 - **Seminar 2:** Privacy by Design Requirements Elicitation and Data Subjects' Rights, Personal data retention implementation, Data subjects' rights implementation
 - **Seminar 3:** Handling Data Breaches under the GDPR
 - **Seminar 4:** Encryption, Anonymization, Pseudonymization
 - **Seminar 5:** Use cases and practical guidelines
- All stakeholders will attend the five seminars
- Seminars 1-4 will be conducted three times (12 seminar sessions)
- Seminar 5 will be conducted once for all participants (1 seminar session)

Therefore, the training plan for the technical seminars includes the following activities:

Table 3: Training Plan for the Technical Seminars

| Seminars | Conducted * times | Number of Participants per seminar series | Total number of participants |
|-----------------|--------------------------|--|-------------------------------------|
| Seminars 1-4 | 3 | 20 | 60 |
| Seminar 5 | 1 | 60 | 60 |

3 Training Contents

The description of the content and the titles of the presentations material to be used for the training activities are subsequently listed. The content of the presentations is included in the Appendix.

3.1 Broad scope seminars content description and presentations titles

3.1.1 Introduction to Data Protection Terminology

- a. Examples of Key GDPR Definitions:
 - i. Personal data, Data subject, Special categories of personal data, Processing, The roles of Data Controller/Joint Controllers/Processor, Recipients and third parties definitions, the role of Supervisory Authority.
- b. Data Protection Principles
 - i. definitions,
 - ii. Use cases
- c. Legal bases
 - i. Definitions,
 - ii. Use cases
- d. Data subjects' rights definitions
 - i. General obligations and modalities, Right of access, Right to rectification, Right to erasure, Right to restriction, Right to data portability, Right to object and automated individual decision-making
 - ii. Use cases

The relevant material is available in Appendix 1.

3.1.2 ICT organizational GDPR roles – DPIA

- a. DPO – role and responsibilities
- b. Chief Information Security (CISO) responsibilities
- c. DPO and CISO relationship and possible conflict of interest
- d. Privacy team
- e. Relationship between personal data protection and security
- f. The notion of risk in data protection
- g. Personal Data Protection Risks Vs Security Risks
- h. DPIA as a GDPR accountability tool and ICT role
- i. Role of the DPO with respect to DPIA and records of processing activities

The relevant material is available in Appendix 2.

3.1.3 Data Protection by Design and by Default in GDPR

- a. Relevant Challenges, Main elements, Importance
- b. Roles and stakeholders
- c. Software development with Data Protection by Design and by Default
- d. DPbD (early) approaches
- e. By default vs. by design

The relevant material is available in Appendix 3.

3.1.4 Handling Data Breaches under the GDPR

- a. Definition of GDPR Data Breach
- b. Incident handling process
- c. Quantifying the risk for data subjects
- d. Notification to the supervisory authority
- e. Communication to the data subject

The relevant material is available in Appendix 4.

3.1.5 Data Protection Policies and Notices

- a. Transparency requirements in GDPR
- b. Privacy notices under GDPR – Examples

The relevant material is available in Appendix 5.

3.1.6 Online Marketing and Advertising, Cookies and trackers

- a. e-Privacy Directive - e-Privacy Regulation - scope changes
- b. Direct marketing via phone
- c. Marketing via electronic messages
- d. Opt-in/Opt-out effectiveness
- e. e-Marketing examples
- f. Targeted/Behavioral ads, Real time bidding
- g. Tracking technologies – relevant legislation
- h. Cases of cookies
- i. HDPa–requirements – examples

The relevant material is available in Appendix 6.

3.2 Targeted content seminars content description and presentations titles

3.2.1 Security risk assessment vs. data protection risk assessment

- 1. Information Security Risk Assessment**
 - a. The concept of risk
 - b. ISO 27005:2018
 - c. Information security risk assessment processes
- 2. Personal Data Impact Assessment**
 - a. Data Protection Impact Assessment in the GDPR
 - b. CNIL DPIA Methodology, Guides and Tool
 - c. DPIA processes
- 3. Information Security Risk Assessment vs. Personal Data Impact Assessment**
 - a. Variations regarding Data in Consideration
 - b. Variations regarding Impact in Consideration
- 4. Data Protection Impact Assessment Tools and Practical Issues**
 - a. Data protection impact assessment standards, methods and tools
 - b. Practical challenges
 - c. Examples

The relevant material is available in Appendix 7.

3.2.2 Privacy by Design Requirements Elicitation

- 1. Introduction**
 - a. The Concept of Privacy Requirements
- 2. Privacy Requirements Elicitation Methodologies**
 - a. LINDUUN
 - b. SQUARE for Privacy
 - c. PriS
 - d. RBAC
 - e. STRAP
 - f. The i* method
 - g. Privacy Requirements Elicitation Technique (PRET)
 - h. Preparing Industry to Privacy by Design by supporting its Application in Research (PRIPARE)
 - i. Modelling and Analysis of Privacy-aware Systems (MAPaS Framework)
 - j. Goal-Based Requirements Analysis Method (GBRAM)
- 3. Personal Data Retention**
- 4. Data Subjects' Rights Management**

The relevant material is available in Appendix 8.

3.2.3 Encryption, Anonymization and Pseudonymization

- 1. Symmetric encryption**
- 2. Asymmetric encryption**
- 3. Hash functions – MAC – Digital signatures**
- 4. PGP - IP SEC – VPN**
- 5. Anonymization**
- 6. Pseudonymization**

The relevant material is available in Appendix 9.

3.2.4 Personal Data Breaches Management

- 1. Attacks frequently causing data breaches and organizational and technical measures for preventing / mitigating the impacts**
 - a. Ransomware attacks
 - b. Data exfiltration attacks
 - c. Internal human risk source
 - d. Lost or stolen devices and paper documents
 - e. Mispostal
 - f. Social engineering

The relevant material is available in Appendix 10.

3.2.5 Implementation of GDPR Data Protection/Privacy by Design

- 1. Implementing the DP principles using DPbyDesign/Default - examples**
 - a. Transparency
 - b. Lawfulness
 - c. Fairness
 - d. Purpose Limitation
 - e. Data minimisation
 - f. Accuracy
 - g. Storage Limitation
 - h. Integrity and confidentiality
 - i. Accountability

The relevant material is available in Appendix 11.

4 Appendices

Appendix 1

Introduction to Data Protection Terminology



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

“Introduction to Data Protection Terminology”

*Facilitating GDPR compliance for SMEs and promoting Data Protection by
Design in ICT products and services*

(www.bydesign-project.eu)





Introduction to Data Protection terminology



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

A. Key GDPR Definitions: *Personal data*

Data subject

Special categories

Processing

Data Controller / Joint controllers

Processor

Recipients - Third Parties

Supervisory Authority

B. Data Protection Principles

C. Legal bases

D. Data subjects rights



A. *What is data protection?*

Data protection is the fair and proper use of information about people.

It's part of the fundamental *right to privacy* – but on a more practical level.

It's really about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society. It's also about removing unnecessary barriers to trade and co-operation. It exists in part because of international treaties for common standards that enable the free flow of data across borders.

Data protection is essential to innovation. Good practice in data protection is vital to ensure public trust in, engagement with and support for innovative uses of data in both the public and private sectors.

The greek data protection regime is set out in the Act 4624/2019 and GDPR.



GDPR article 4: **DEFINITIONS**

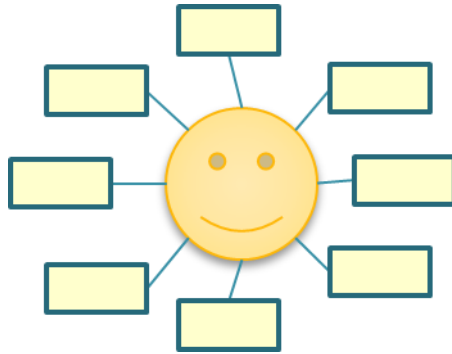


Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

- 1) ‘**personal data**’
- 2) ‘**processing**’
- 3) ‘restriction of processing’
- 4) ‘profiling’
- 5) ‘pseudonymisation’
- 6) ‘**filing system**’
- 7) ‘**controller**’
- 8) ‘**processor**’
- 9) ‘**recipient**’
- 10) ‘**third party**’
- 11) ‘**consent**’
- 12) ‘data breach’
- 13) ‘**genetic data**’
- 14) ‘**biometric data**’
- 15) ‘data concerning health’
- 16) ‘main establishment’
- 17) ‘representative’
- 18) ‘enterprise’
- 19) ‘group of undertakings’
- 20) ‘binding corporate rules’
- 21) ‘**supervisory authority**’
- 22) ‘supervisory authority concerned’
- 23) ‘cross-border processing’
- 24) ‘relevant and reasoned objection’
- 25) ‘information society service’
- 26) ‘international organisation’



PERSONAL DATA



Ex. personal data: name and surname, a home address, an email address such as name.surname@company.com, an identification card number, location data (for example the location data function on a mobile phone), an Internet Protocol (IP) address, a cookie ID, the advertising identifier of your phone, data held by a hospital or doctor, which could be a symbol that uniquely identifies a person

Ex. non personal data: a company registration number, an email address such as info@company.com, anonymised data

*any information relating to an identified or identifiable natural person (**'data subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*

(example: document including initials uploaded on '<https://diavgeia.gov.gr>')



Few more words...



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

Personal data means information about a particular *living individual*. This might be anyone, including a customer, client, employee, partner, member, supporter, business contact, public official or member of the public. It doesn't need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data.

Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data that has been *de-identified*, *encrypted* or *pseudonymised* but can be used to reidentify a person remains personal data and falls within the scope of the GDPR. Personal data that has been rendered *anonymous* in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

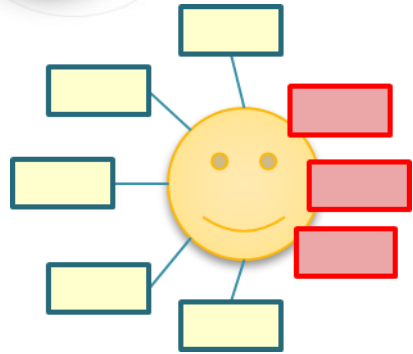
The GDPR protects personal data regardless of the technology used for processing that data – it's technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order).

It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper;

In all cases, personal data is subject to the protection requirements set out in the GDPR.



Special categories of data



data revealing: *racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*

- «**genetic data**»: data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question,
- «**biometric data**»: data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person
 - ex. facial images or dactyloscopic data
- «**health data**»: data related to the physical or mental health of a natural person
- Separate «special» category: **criminal convictions and offenses**



What does 'processing' mean?

Almost anything you do with data counts as processing!

GDPR: “Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means”

- *collection,*
- *recording,*
- *organisation,*
- *structuring,*
- *storage,*
- *adaptation or alteration,*
- *retrieval,*
- *consultation,*
- *use,*
- *disclosure by transmission,*
- *dissemination or otherwise making available,*
- *alignment or combination,*
- *restriction,*
- *erasure or destruction*





Examples of processing :

- staff management and payroll administration
- access to/consultation of a contacts database containing personal data
- sending promotional emails
- shredding documents containing personal data
- posting/putting a photo of a person on a website
- storing IP addresses or MAC addresses
- video recording (CCTV)



DATA SUBJECT



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

‘personal data’ means any information relating to *an identified or identifiable natural person ...*’

This is the technical term for the individual whom particular personal data is about.

What are **identifiers** and **related** factors?

An individual is ‘identified’ or ‘identifiable’ if you can distinguish them from other individuals.

A **name** is perhaps the most common means of identifying someone.

However whether any potential identifier actually identifies an individual depends on the context.

A combination of identifiers may be needed to identify an individual.

*****GDPR provides a non-exhaustive list of identifiers, including: name; identification number; location data; and an online identifier. ‘Online identifiers’ includes IP addresses and cookie identifiers which may be personal data. Other factors can identify an individual.**





“...relates to...”

What is the meaning of ‘relates to’?

Information must ‘relate to’ **the identifiable individual** to be personal data.

Not simply identifying a natural person – it must concern him/her in some way.

***To decide whether or not data relates to an individual, you may need to consider:

- the *content* of the data – is it directly about the individual or their activities?;
- the *purpose* you will process the data for; and
- the *results* of or *effects* on the individual from processing the data.

Data can reference an identifiable individual and not be personal data about that individual, as the information does not relate to them.

There are circumstances where it is difficult to determine whether data is personal data.

Good practice: you should treat the information with care, ensure that you have a clear reason for processing the data and, in particular, ensure you hold and dispose of it securely.

Inaccurate information may still be personal data if it relates to an identifiable individual.



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

Data Controller



‘Any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the *purposes* and *means* of the processing of personal data’

ATTENTION! where the purposes and means of such processing are determined by Union or Member State law, the **controller** or the **specific criteria for its nomination** may be provided for by Union or Member State law



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

What is namely a 'data controller'?



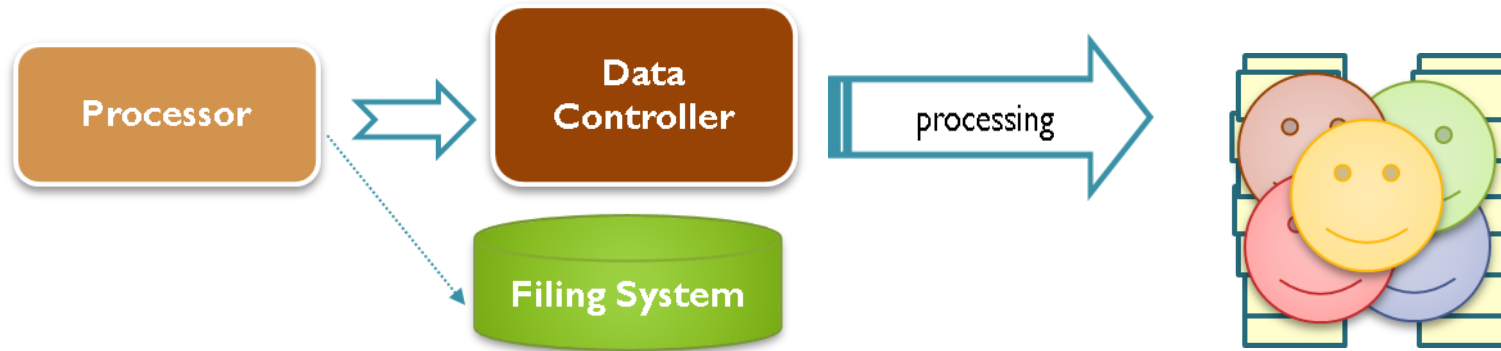
A controller is the person that **decides how and why to collect and use the data**. This will usually be an organisation, but can be an individual (*eg. a sole trader, a doctor, a lawyer etc*).

If you are an employee acting on behalf of your employer, the employer would be the controller.

The controller must make sure that the processing of that data complies with data protection law.



Processor



“a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”...and in accordance with their instructions

*****NOT an employee!!!**

***Processors have some direct legal obligations, but these are more limited than the controller's obligations

- ✓ Typical case of processor is the «subcontractors», as long as they process personal data.
- ✓ In public sector, processors may be other public authorities, ex.: Taxisnet, G-Cloud, IDIKA.



Example of **CONTROLLER - PROCESSOR**

Q. Organisation A provides payroll processing services to corporate customers. Organisation A provides those services to its customers in accordance with each customer's instructions. Organisation A also uses those data to perform benchmarking analysis, so that it can sell further services allowing customers to compare their payroll data to industry averages.

Does Organisation A fall within the definition of a "controller" or a "processor"?

A. Depending on the facts, the same entity can be a controller in respect of some processing activities and a processor in respect of other processing activities. In this example, Organisation A is a processor in respect of the payroll processing services it provides directly to its customers, and a controller in respect of the benchmarking services, as it is processing personal data to create benchmarks for its own purposes.





JOINT CONTROLLERS



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



“two or more controllers jointly determine the purposes and means of processing”

Joint controllership exists with regard to a specific processing activity when different parties determine jointly the purpose and means of this processing activity. They must in a transparent manner *determine* their respective responsibilities for compliance with the obligations under GDPR, in particular as regards the exercising of the rights of the data subject by means of an *arrangement* between them *unless*, the respective responsibilities of the controllers are determined by Union or Member State *law* to which the controllers are subject.

Therefore, assessing the existence of joint controllers requires examining whether the determination of purposes and means that characterize a controller are decided by more than one party.

“Jointly” must be interpreted as meaning “together with” or “not alone”, in different forms and combinations.

Not all processing involving several entities give rise to joint controllership. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing



Examples of JOINT CONTROLLERS



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

1. A **travel agency** sends personal data of its customers to the **airline** and a **chain of hotels**, with a view to making reservations for a travel package.

The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. Each of the actors processes the data for carrying out their own activities and using their own means. In this case, the **travel agency**, the **airline** and the **hotel** are three different data controllers processing the data for their own and separate purposes and there is no joint controllership.

2. The **travel agency**, the **hotel chain** and the **airline** then decide to participate jointly in setting up an internet-based common platform for the common purpose of providing package travel deals. They agree on the essential means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out joint marketing actions. In this case, the travel agency, the airline and the hotel chain, jointly determine why and how personal data of their respective customers are processed and will therefore be joint controllers with regard to the processing operations relating to the common internet-based booking platform and the joint marketing actions. However, each of them would still retain sole control with regard to other processing activities outside the internet-based common platform.



3. **Several research institutes** decide to participate in a specific joint research project and to use to that end the **existing platform** of one of the institutes involved in the project.

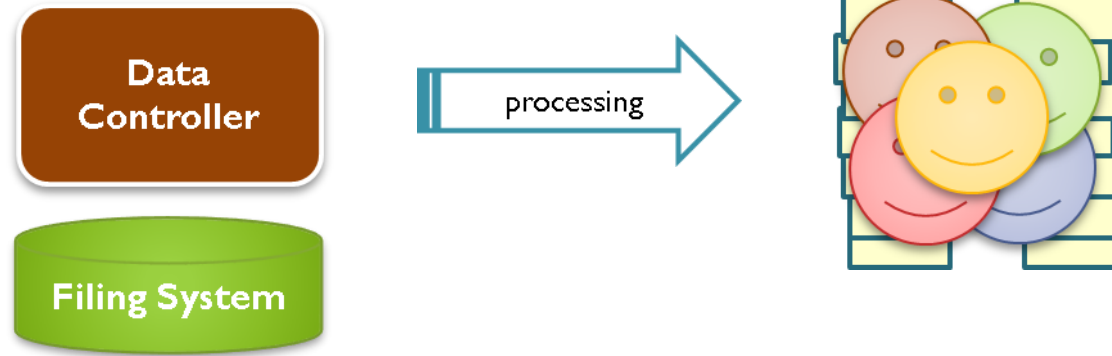
Each institute feeds personal data it already holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.



Filing System



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



«**filing System**»:

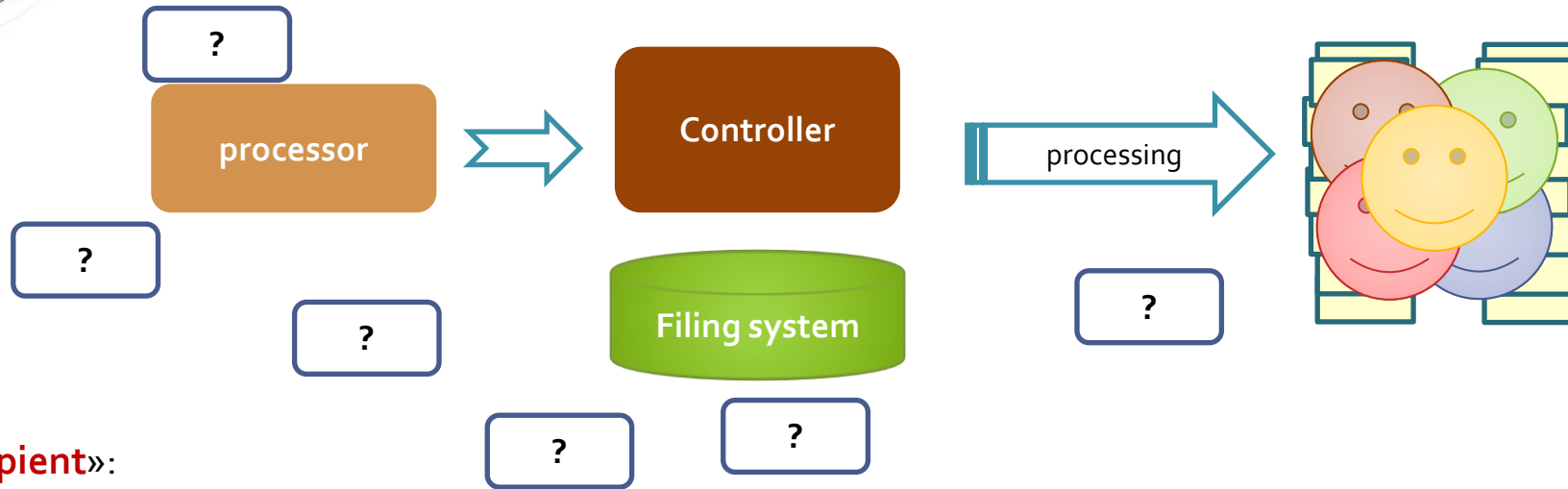
- any structured set of personal data
- accessible according to specific criteria,
- whether centralised, decentralised or dispersed on a functional or geographical basis



Other parties - Definitions



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



«Recipient»:

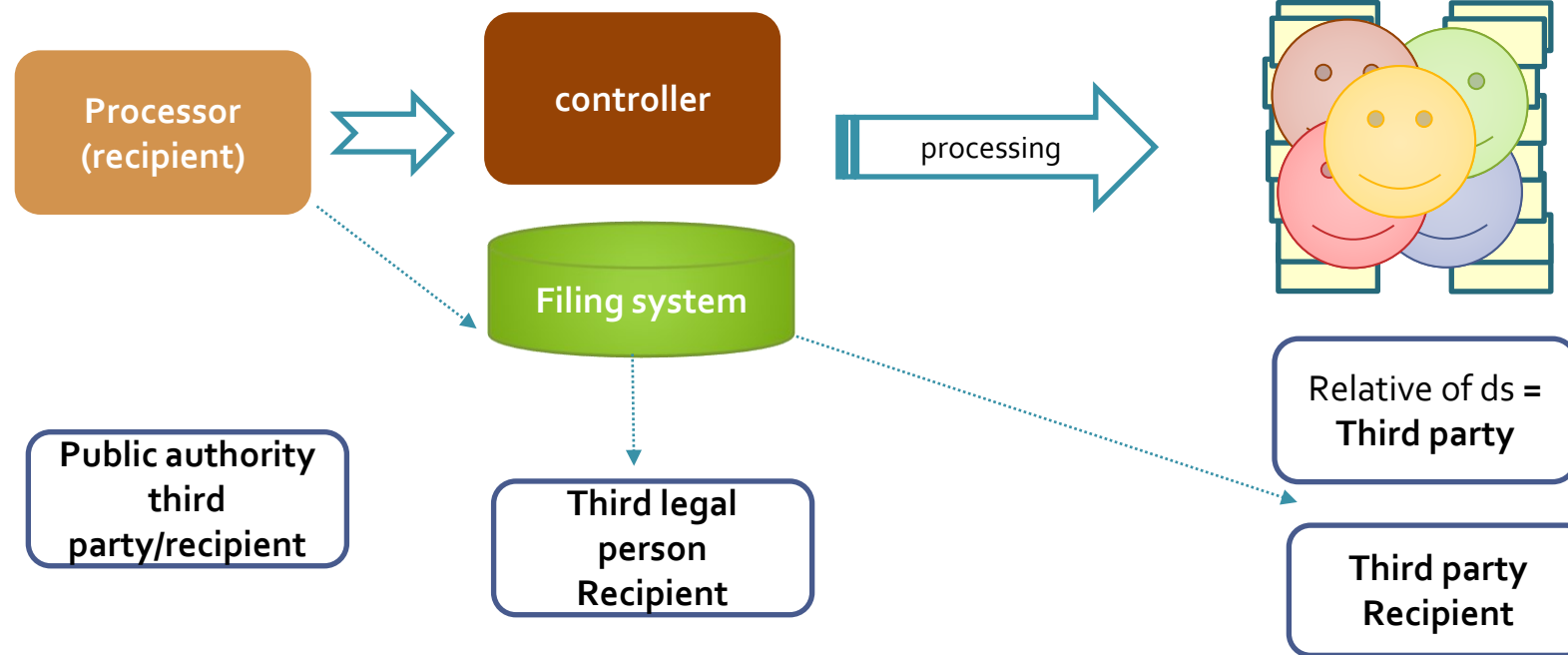
- a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
- *However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients;*

«Third Party»: any natural or legal person, public authority, agency or body, except for:

- data subject,
- processor and
- Persons who, under the direct authority of the controller or processor, are authorised to process personal data



Recipients and third parties



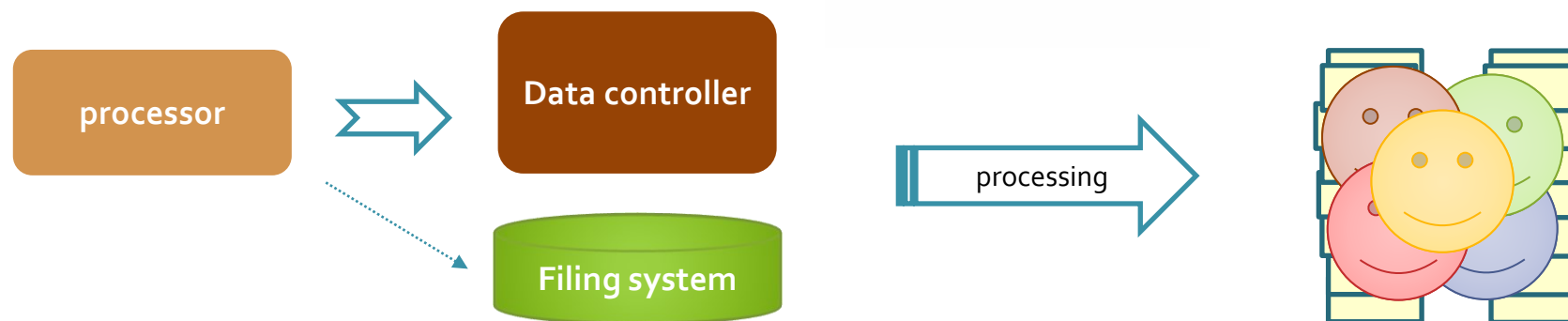
- ✓ Processors are «recipients», not «third parties».
- ✓ The exemption of public audit authorities applies to individual cases, in order to facilitate their work
 - ✓ These authorities though are data controllers for the data they process for their purposes



...last but not least



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



«Supervisory Authority»:

- Member states shall determine the full status of operation and independence
- HDPA is enshrined in Greek Constitution (art. 9A) and its status is governed by Act. 3051/2002



Few more words...



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

DPA's are independent public authorities that:

- **supervise** the application of the data protection law, through *investigative* and *corrective powers*,.
- **provide expert advice** on data protection issues and
- **handle complaints** lodged against violations of the GDPR and the relevant national laws.
- **there is, at least, one** in each EU Member State.

***The main contact point for issues on data protection is the DPA in the EU Member State where your company/organisation is based. However, if your company/organisation processes data in different EU Member States or is part of a group of companies established in different EU Member States, that main contact point may be a DPA in another EU Member State.



B. Data Protection Principles



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

Lawfulness, Fairness and Transparency

processed lawfully, fairly and in a transparent manner in relation to the data subject

Purpose limitation

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Data minimisation

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Accuracy

accurate and, where necessary, kept up to date

Storage limitation

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

Integrity and confidentiality

processed in a manner that ensures appropriate security of the personal data using appropriate technical or organisational measures

Accountability!

The controller shall be responsible for, and be able to demonstrate compliance with all the above





i. Lawfulness, fairness and transparency

‘personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject’

Fairly means transparent processing, especially when it comes to data subjects.

Data controller must inform data subjects, before the beginning of the processing, at least for the purpose of it, the name and the address of the controller.

Unless it is provided by law, processing shouldn't be hidden or covered.

Data subjects have the right to access their data, in any case.

Apart from the obvious, this principle aims in building trust between data controller and data subject!



ii. Purpose limitation

‘Data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes’

****further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*

The purpose of the processing must be clearly defined *before* the beginning of the processing

The lawfulness of processing is strongly connected with its purpose

Processing with no clear purpose is not lawful!

Further use of data for new purpose needs new legal base, if the new purpose is incompatible with the first one

****ex.: transfer to third parties is a new purpose and new legal base is needed!*

Further use for purposes compatible with the first one is lawful and no new legal base is needed.

GDPR doesn't define 'compatible' => ad hoc interpretation



iii. Data minimization



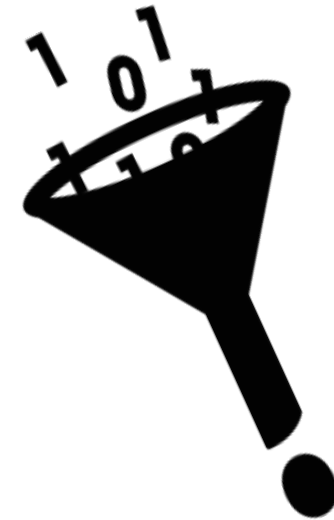
Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

‘adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’

The data categories selected for the processing must be relevant and necessary for the fulfillment of the purpose of this processing, Data controller must strictly limit the collection of data to those are directly linked to the specific purpose of the processing

Privacy - friendly solutions should be selected with the use of new technology, ex.:

- Non use of personal data, or pseudonymisation





iv. Accuracy



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

‘accurate and, where necessary, kept up to date’

every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

Data controller shouldn't use data without taking measures that guarantee that data are accurate and up to date

There are cases that data must be often updated to avoid damage to the data subjects
ex. Bank institutions that check on the solvency of their customers



v. Storage limitations



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

‘kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed’

***personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and security measures exist in order to safeguard the rights and freedoms of the data subject

Data subject must be informed, apart from the purpose, about the period for which the personal data will be stored

When this period ends, processing may continue only for scientific or historical research purposes or statistical purposes

***In the public sector, this period should be defined in law



vi. Integrity and Confidentiality



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

‘processed in a manner that ensures appropriate security of the personal data, including protection against *unauthorised* or *unlawful* processing and against *accidental loss, destruction* or *damage*,
using appropriate technical or organisational measures!

Data controller and processor have the obligation to take appropriate measures against any unauthorised processing.

The appropriate level of security is defined from:

- The **state of the art** for the security measures
- The implementation costs of the measures, and
- The level of ‘sensitivity’ of the data processed

Added safeguard for a safe processing is the general duty of all the persons related to the processing (controllers or processors) to ensure data privacy



vii. Accountability



The controller shall be responsible for, and be able to demonstrate compliance with the aforementioned principles

According to WP Art.29, in the core of accountability is the obligation of data controller to: implement measures that ensure the enforcement of measures taken for data protection and have appropriate documents to prove and demonstrate GDPR compliance towards to HPA and data subjects

Data controller must *at any time* be able to demonstrate to data subjects, public and supervisory authorities its compliance with the data protection rules.

****Privacy policy is one element that could show such compliance (first reference in e-privacy 2009)*



C. Legal Bases

When is processing lawful?



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

a. consent

The data subject has given consent to the processing of his or her personal data for one or more specific purposes

Attention to the definition of consent!

b. performance or conclusion of a contract

Processing is necessary:

- the performance of a contract to which the data subject is party, or
- in order to take steps at the request of the data subject prior to entering into a contract

c. legal obligation

Processing is necessary for compliance with a legal obligation to which the controller is subject

Apart from public sector, there also other cases where data controllers are obliged by law to process data: ex. doctors and hospitals, employers, companies (customers data for tax purposes)



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

d. vital interest

Processing is necessary for the **vital interest** of data subject or of another natural person

e. public
interest

Processing is necessary for the performance of a task carried out :
in the **public interest** or
in the exercise of **official authority vested in the controller**



Processing is necessary:

for the purposes of the *legitimate interests* pursued by the controller or a third party

except where such interests are *overridden* by the *interests* or *fundamental rights* and *freedoms* of the data subject which require protection of personal data, *in particular where the data subject is a child*.



- ✓ It's often used in private sector (ex. for financial purposes)
- ✓ Where consent can't be the legal base (ex. video surveillance)

Attention!

It can not be implemented in processing held by **public authorities** in the performance of their duties.



When is processing of *special categories* is lawful?

Prohibition!

Processing of special categories is prohibited.

There are still few exceptions in GDPR!

a. consent

the data subject has given explicit consent to the processing of those personal data for one or more specified purposes

Attention! The contractual relationship with the data subject is not considered as a general legal basis for the special categories

- ✓ If an airline passenger, when booking, asks the airline to offer him / her a wheelchair and a kosher meal, the airline is allowed to use this data, even though the passenger has not signed an additional clause expressly giving his or her consent to use these data which provide information about his health and religious beliefs. This action resulting from the choice of the passenger is considered as explicit consent.



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

**b. Employment/
Social Security
and Protection**

Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of *employment* and *social security* and *social protection law* in so far as it is authorized by:

-law **provision** or

-a **collective agreement** pursuant to national law providing for appropriate safeguards for the fundamental rights and the interests of the data subject

c. vital interest

Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is *physically* or *legally incapable* of giving **consent**



d. Foundations /
Associations/
Non profit
bodies

processing is carried out by a foundation, association or any other not-for-profit body with *a political, philosophical, religious or trade union aim*, in the course of its legitimate activities:

- (a) *with appropriate safeguards* and
- (b) on condition that the processing *relates solely to the members or to former members* of the body or to *persons who have regular contact* with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

e. Manifestly
public

processing relates to personal data which are *manifestly made public by the data subject*

f. Legal claims

processing is necessary for the *establishment, exercise or defence of legal claims* or whenever *courts are acting in their judicial capacity*



g. substantial public interest

Processing is necessary for substantial public interest, on the basis of Union or Member State law which:

- shall be *proportionate* to the aim pursued,
- respect the essence* of the right to data protection and
- provide for *suitable* and *specific measures* to safeguard the fundamental rights and the interests of the data subject

h. medical data

Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law provision or pursuant to contract with a health professional

- ✓ **Further safeguards:** processing is being held by a professional or a person subject to an obligation of secrecy under
 - ✓ law provision, or
 - ✓ rules established by national competent parties (ex. professional codes of conduct)



i. Public health

Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which:

provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

j. Research / Archiving

Processing is necessary for **archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**

on the basis of Union or Member State, which :

- shall be *proportionate* to the aim pursued,
- respect the *essence of the right* to data protection and
- provide for *suitable* and *specific measures* to safeguard the fundamental rights and the interests of the data subject



When is processing of data relating to *criminal offenses* and *convictions* is lawful?



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

Official
Authority

Under the control of **Official Authority**
or

Law Provision

Processing is authorised by Union or Member State law providing for **appropriate safeguards** for the rights and freedoms of data subjects.

Any comprehensive register of criminal convictions shall be kept only under the control of official authority

- ✓ Attention!: It doesn't refer to processing by authorities competent for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security . = Directive 680/2016
- ✓ Processing by these authorities for other purposes (ex. employees data) fall within the scope of GDPR



CONSENT



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

Definition: *Consent must be a freely given, specified, informed and unambiguous indication of an individual's wishes* by which he or she, by *a statement* or by *a clear affirmative action*, signifies agreement to the processing of personal data relating to him or her

Consent is only one of the legitimate grounds for processing personal data under the GDPR.

It should only be used where an individual is offered a **genuine choice** to either accept or decline what is being offered. It would not be appropriate to rely on consent if, for example, the individual had no choice but to use the service or to accept the terms:

e.g. access to free wifi only if the user consents to receiving marketing materials would be unacceptable as the two things are unrelated.

There must be some form of **clear affirmative action** – a “positive opt in”.

Consent cannot be inferred from **silence, pre-ticked boxes** or **inactivity**.

Consent must be as **easily revoked** as it is given, and therefore clear processes should be in place for individuals to **withdraw consent**.



Components of *valid* consent



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

Freely given

Free means real choice for the data subject

- Where there is a clear inequality between the data subject and the controller consent cannot be considered as “freely given”
 - In cases, where the controller is public authority consent is really difficult to be considered as free
 - The same applies Blanket consent for a number of processing activities is not valid, there needs to be consent processes **for each separate element of data processing**
 - in the labour sector
- The data subject may always have the right to object or withdraw his/her consent **without suffering any detriment**



Specified

1. **Purpose determination**
2. **Separate consent for each purpose**
 - General purposes should be avoided
 - It may cover more than one processings as long as they have the main purpose
3. **Separate and clear information on processing before consent**

Data controllers should provide data subjects with information on the categories of data processed for each purpose, in order for the data subjects to be able to know the effects or risks of the processing



informed

- **Information** provided should be at least the following:
 - Controller's identity
 - Purpose of each processing for which consent is needed
 - Categories of data collected and processed
 - Existence of the right to withdraw
 - Use of automated decision making, including profiling
 - In case there is a transfer to third countries, information on the risks
- **Ways/Methods** of providing information
 - GDPR doesn't give specific direction, defines though that it should be clear and in simple words
 - Language and text comprehensible by an average citizen
.no legal text or terms



affirmative
declaration of
consent

- GDPR requires declaration or affirmative action of the data subject
 - Not acceptance after simple information with no further action
 - Pre-ticked or opt-out boxes are not considered as valid consent
 - Any means may be used for reception of consent as long as controller can prove that consent is given
 - Ideally in written form!
 - Recording if appropriate prior information has been provided
- By electronic means...
 - Controllers can create their own systems as long as they are based on GDPR rules and principles, ex:
 - Swipe, mobile rotation in 8 etc.
 - A simple scroll in the text doesn't meet the requirement



Child's consent



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



Special child protection in relation to the offer of **information society services** directly to a child

Consent is valid **ONLY** if it is given or authorised by the holder of parental responsibility over the child (parent or guardian)

Especially in the use of personal data for the purpose of marketing or creating a personality profile or user profile

The consent of a parent or guardian should not be required in the case of prevention services or counseling offered directly to a child.

GDPR set an age limitation: *Under 13 =not valid consent =unlawful processing*
Over 16 =valid =lawful processing

In Greece, a child may give its own, valid consent, when she/he is over 15 years old.

Data controller must verify that consent is given or authorized by the parent or the guardian.



Things to do now if you are relying on consent to process data:

Identify where you are relying on consent to process personal data / special categories data:

- Review *how* you collect the consent (information sheets, data collection notices, forms etc.)
- Make sure you are collecting *a freely given, specified, informed* and *unambiguous indication* of an individual's wishes (what are you telling them?);
- Can you offer individuals the opportunity to *consent to certain areas of the processing* and utilise a “positive opt in” – e.g. a tick box process? *This could be useful for research projects.*
- Consider *how individuals can revoke* their consent? Is it *clear* from your documentation / website? It needs to be as clear as the process you utilised to collect the consent, and individuals should be able to notify you through the same medium.
- *What do you do with consent* already collected?



D. Data Subject Rights

- Transparent communication and modalities (art. 12).
- (1) Right to be informed (art. 13, 14).
- (2) Right of access (art. 15).
- (3) Right of rectification (art. 16).
- (4) Right to erasure/ right «to be forgotten» (art. 17).
- (5) Right to restriction of processing (art. 18).
- (6) Right to data portability (art. 20)
- (7) Right to object (αρ. 21).
- (8) Right to non automated decision making, including profiling (art. 22).



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



Transparent information, communication and modalities for the exercise of the rights



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

Information and communication should be provided in the following cases:

- before / during processing,
- exercise of rights and
- data breach.
- Concise, transparent, intelligible and easily accessible form.
- **Way of information:** in *writing* or by other means, inter alia, *by electronic means, where appropriate*.
- **Orally, when requested by the data subject:** provided that the identity of the data subject is proven by other means.
- Information shall be provided **free of charge** (a *reasonable fee* may be charged, if the requests are manifestly unfounded or excessive, in particular because of their repetitive character,).





- **Deadline for the controller to provide information:**
 - without undue delay and in any event within **one (1) month** of receipt of the request.
 - Extension of period by **two (2) further months** taking into account the **complexity** and **number** of the requests.
 - Data subject should be in any case informed of any extension and the reasons for it within **one (1) month**.
- **No action taken by the controller:**
 - the controller shall inform the data subject **without delay** and **at the latest within one (1) month** of receipt of the request:
 - of the **reasons** for not taking action and
 - on the possibility of lodging a **complaint** with a supervisory authority and seeking a judicial remedy.

1a. Right to be informed when data *are being obtained* from the data subject



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



- **Identity/Contact details** of data controller.
- **Contact details** of Data Protection Officer (DPO).
- **Purpose** of processing – **legal base**.
- **Legitimate interest** of data controller or third party.
- **Recipients** or categories of recipients.
- **Transfer** to third country or international organization.
- **Storage period** or criteria of such storage.
- Existence of the **right** to request access to or rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability .
- Right to **withdraw consent**.
- Right to **lodge complaint** with a supervisory authority.
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the **possible consequences** of failure to provide such data.
- Existence of automated decision-making, including profiling.



1b. Right to be informed when data *have not been obtained* from the data subject



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



- **Further** to the previous ones:
 - **Categories** of data
 - From which **source** the personal data originate, and if applicable, whether it came from **publicly accessible sources**.
- **When is the data subject is informed?**
 - within a **reasonable period** after obtaining the personal data,
 - but at the **latest within one (1) month**, having regard to the specific circumstances in which the personal data are processed
 - at the latest at the time of the **first communication** to that data subject, if the personal data are to be used for communication with the data subject,.
 - at the latest **when the personal data are first disclosed**, if a disclosure to another recipient is envisaged.



Exception from the right to be informed *when data are obtained from other sources*



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

- If data subject already has the information.
- the provision of such information proves
 - **impossible** (ex. **there are no contact details of data subject**) or information would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,
 - in so far as the information is likely to render impossible or seriously impair the achievement of the objectives of that processing. (ex: money laundry)
 - data controller makes information publicly available
- obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests (ex. **tax legislation**)
- where the personal data must remain *confidential* subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy (ex. **receipt of medical history of relative**).



2. Right of access

- The data subject shall have the right:
 - a. to obtain from the controller confirmation of processing and, where that is the case, access to the personal data and specific information (*see below*), and
 - b. A copy of his/her data
- **No justification** is required.
- **Verification by any means** of data subject's identity by data controller.
- Providing **remote access to a secure system**.
- **Provision of a copy** of the data also in electronic form (free of charge and for additional copies a reasonable fee for administrative expenses)
- **Facilitating the subject** to exercise the right of access.
- Possibility of electronic submission of requests especially for data in electronic form.
- **Examples:**
 - *Online form on a website.*
 - *Printed form at reception point*





...*access to what information?*



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

- **Purpose of processing.**
- Categories of **data**.
- **Recipients or categories of recipients** to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations.
- the envisaged **period** for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- Existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- Existence of the right to lodge a complaint with a supervisory authority.
- Where the personal data are not collected from the data subject, any available information as to their source.
- The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.



3. Right to rectification



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

- The data subject has the right :
 - **to obtain Rectification of inaccurate personal data,**
 - to have **incomplete personal data completed,** including by means of providing a supplementary statement.



Examples: the indication that someone is married while he is not, the non-updating of the TIREZIA database.

- It's up to the data subject to determine which data need correction ex. wrong name.



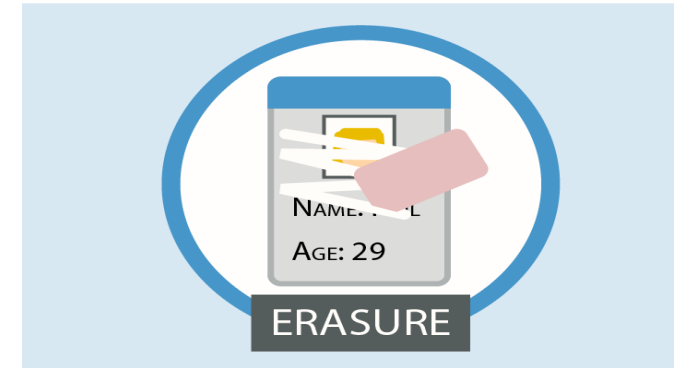
4. Right to erasure /right 'to be forgotten'



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

Only when:

- Data are ***no longer necessary*** for the purpose of processing.
- ***Withdrawal of consent*** and of any other legal base.
- The data subject ***objects*** to the processing and there are no overriding legitimate grounds for the processing.
- ***Unlawful*** processing.
- Compliance of data controller with legal obligation for erasure.
- Personal data have been collected in relation to the offer of information society services directly to the ***child***.





Exceptions!



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

When processing is necessary for:

- exercising the right of freedom of expression and information,
- compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,
- reasons of public interest in the area of public health,
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,
- the establishment, exercise or defence of legal claims.



5. Right to restriction of processing



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

Only where:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data,
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead,
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims,
- the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Possible ways:

- *Temporary move of data to another system.*
- *Remove accessibility of selected data by users.*
- *Temporarily remove data from a web page.*





6. Right to portability



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



The data subject shall have the right to:

- a) **receive** the personal data concerning him or her, **which he or she *has provided to a controller****, in a structured, commonly used and machine-readable format**, and
- b) have the right to **transmit** those data to another controller **without hindrance** from the controller to which the personal data have been provided

Only where:

- the processing is based on **consent** or on a **contract**, and
- the processing is carried out by automated means
- the processing does not adversely affect rights and freedoms of others

**consciously - actively provided / observed activity, ex. Search history. NO: deduced / produced data, ex. Health assessment, profile.*

*** security measures / costs taken into account*



7. Right to object



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

Only where the legal base of the processing is:

- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, *in particular where the data subject is a child.*

*** Where the data subject objects to processing for **direct marketing purposes**, the personal data shall no longer be processed for such purposes

- **Exception!**

When processing is necessary for the performance of a task carried out in the public interest and the data are processed *for scientific or historical research purposes or statistical purposes*³.

Results: END of processing!

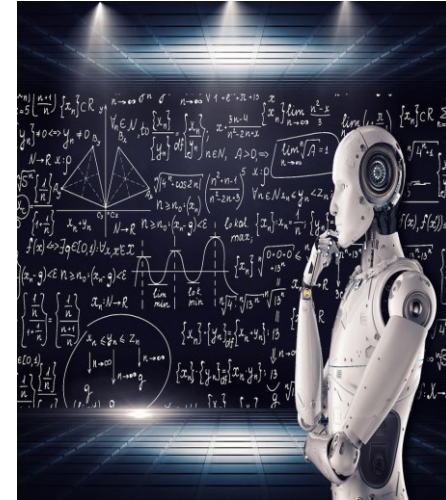


8. Right to non-automated decision making



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

- Data subject's right to:
 - not to be subject to a decision based solely on automated processing, including profiling,
 - which produces legal effects concerning him or her or similarly significantly affects him or her (*ex. automatic denial of an online credit application*)
- It doesn't apply when the decision:
 - (a) is necessary for the entering into, or performance of, a contract between the data subject and a data controller,
 - (b)) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests,
 - (c) is based on the data subject's explicit consent.
- In cases (a) and (c) the controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.





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

Thank you for your attention!

Appendix 2

ICT organizational GDPR roles - DPIA



Funded by European Union's
Rights, Equality and
Citizenship Programme (REC)



ICT organizational GDPR roles – DPIA – examples

dates

byDesign: Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services

www.bydesign-project.eu





The DPO – role and responsibilities

- The controller and the processor shall designate a data protection officer (DPO) when:
 - the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
 - the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
 - the core activities of the controller or the processor consist of processing on a large scale of special categories of data (art. 9-10 of the GDPR).
- A group of undertakings may appoint a single data protection officer
 - provided that a data protection officer is easily accessible from each establishment.
- For public authority or body: A single DPO may be designated for several authorities or bodies
 - taking account of their organisational structure and size.
- The DPO shall be designated on the basis of professional qualities
 - Expert knowledge of data protection law and practices and the ability to fulfil the tasks (see next).
- The DPO may be a staff member or fulfil the tasks on the basis of a service contract.
- The controller or the processor shall publish the contact details of the DPO and communicate them to the supervisory authority.



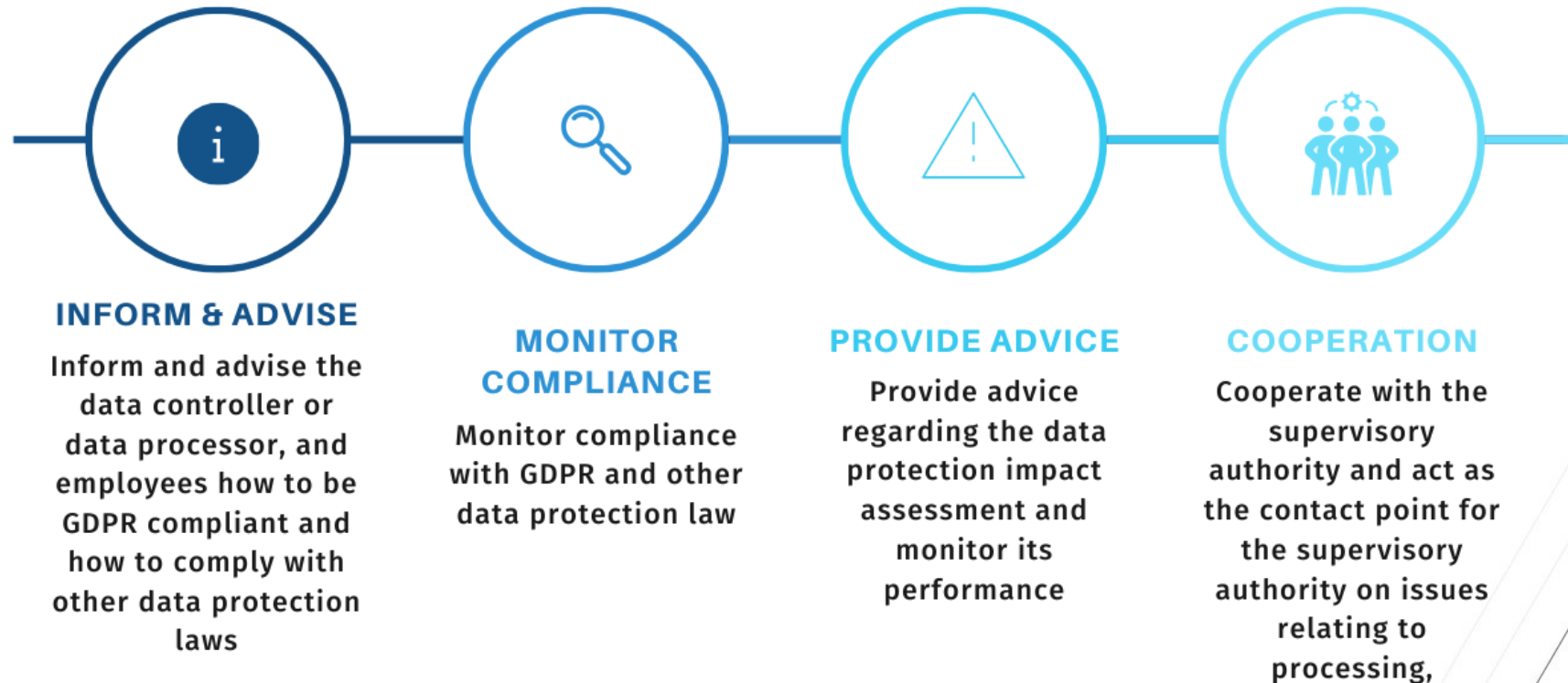
The DPO – role and responsibilities

- The controller and the processor shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- The controller and processor shall support the DPO in performing the tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
- The controller and processor shall ensure that **the DPO does not receive any instructions regarding the exercise of those tasks**. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The DPO shall directly report to the highest management level of the controller or the processor.
- Data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under GDP.
- The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
- The DPO may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties **do not result in a conflict of interests**.



The DPO – role and responsibilities

TASKS OF THE DATA PROTECTION OFFICER





The DPO – role and responsibilities

- The DPO shall have at least the following tasks:
 - to **inform and advise** the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
 - to **monitor compliance** with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
 - to **provide advice** where requested as regards the data protection impact assessment and monitor its performance;
 - to **cooperate** with the supervisory authority;
 - to act as the **contact point** for the supervisory authority on issues relating to processing, including the prior consultation for a data protection impact assessment, and to consult, where appropriate, with regard to any other matter.



The DPO – role and responsibilities

You should position the DPO in line with the following criteria:

- DPO reports directly to your highest level of management and is given the required independence to perform their tasks
- DPO is involved in all issues relating to the protection of personal data
- DPO is sufficiently well resourced to perform tasks
- DPO is not penalized for performing their duties
- Any other tasks or duties do not result in a conflict of interest with their role as a DPO



Chief Information Security (CISO) responsibilities¹



Funded by European Union's
Rights, Equality and
Citizenship Programme (REC)

- *Act as the organization's representative* with respect to inquiries from customers, partners, and the general public regarding the organization's security strategy.
- *Act as the organization's representative* when dealing with law enforcement agencies while pursuing the sources of network attacks and information theft by employees.
- *Balance security needs* with the organization's strategic business plan, identify risk factors, and determine solutions to both.
- *Develop security policies* and procedures that provide adequate business application protection without interfering with core business requirements.
- *Plan and test responses to security breaches*, including the possibility for discussion of the event with customers, partners, or the general public.
- *Oversee the selection, testing, deployment, and maintenance* of security hardware and software products as well as outsourced arrangements
- *Oversee a staff of employees* responsible for organization's security, ranging from network technicians managing firewall devices to security guards

(1. *Mixing Technology and Business: The Roles and Responsibilities of the Chief Information Security Officer*, Matthew Cho, SANS GSEC Certification, Practical Assignment Option 1.4 – Research on Topics in Information Security, 2021 SANS Institute)



DPO and CISO relationship and possible conflict of interest

- Initial position of the Belgian DPA (BDPA): very strict delineation
 - BDPA's Litigation Chamber: "the role of head of a department is [...] incompatible with the role of DPO" because the DPO cannot carry out any independent supervision of such a department, even though the departments in question (e.g. Risk) had an advisory function
- DPA changes course: new insights following a decision of April 26, 2021
 - the DPO at the financial institution could combine the role of DPO with a role as CISO
 - the CISO "presents to the Management of the company the risks and their importance and [...] it befalls Management to decide whether the measures put in place are sufficient to mitigate the risks";
"in case of disagreement between [the CISO] and Management regarding the measures taken and notwithstanding the comments submitted to [Management], it is not [the CISO]'s decision to make";
"security measures fall within the scope of the IT department, not that of the CISO"
- DPO and CISO roles may be compatible if purely advisory



Privacy team

- team should be familiar with the operations and privacy needs of
 - Chief privacy officer
 - Privacy manager
 - Privacy analyst
 - Business line privacy leaders
 - First responders- incident response and security computer incident response team
 - Data Protection Officers
- no particular qualifications or certifications specified in the GDPR, but organizations should consider the *necessary skills and expertise* to include:
 - expertise in national and European data protection laws and practices, including an **in-depth understanding of the GDPR**
 - the apprehension of the **processing operations** carried out;
 - understanding of **information technologies** and data security;
 - insight into the **business sector** and the organization; ability to **promote a data protection culture** within the organization.



Relationship between personal data protection and security

- Principles related to personal data processing (Article 5(1) GDPR):
 - “(a) **lawfulness, fairness and transparency**
 - (b) **purpose limitation**
 - (c) **data minimisation**
 - (d) **Accuracy**
 - (e) **Storage limitation**
 - (f) processed in a manner that ensures appropriate *security* of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“**integrity and confidentiality**”).”
- Article 5(2) GDPR adds that:
 - “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (“**accountability**”).”
- Security is present in several other provisions of the GDPR



The notion of risk in data protection

- The GDPR adopts a risk-based approach for data protection and security
 - Not a new concept – already known from the current Directive 95/46/EC
 - The Article 29 Working Party already was in favor of the inclusion of a risk-based approach in the EU data protection legal framework.
 - The Working Party recognizes that some of the provisions in the proposed Regulation may pose a burden on some controllers which may be perceived as *unbalanced* and has therefore in earlier opinions already expressed the view that all obligations must be *scalable* to the controller and the processing operations concerned. Compliance should never be a box-ticking exercise, but should really be about ensuring that personal data is *sufficiently* protected. How this is done, may differ per controller..... Data subjects should have the *same level* of protection, regardless of the size of the organisation or the amount of data it processes. Therefore the Working Party feels that all controllers must act in compliance with the law, though this can be done on in a scalable manner.” (WP29 statement, 2013)
- There is no question of the rights of individuals being weakened in respect of their personal data
 - Those rights must be just as strong even if the processing in question is relatively ‘low risk’. Rather, the scalability of legal obligations based on risk addresses compliance mechanisms. This means that a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk.



The notion of risk in data protection

- Recital 74 of the GDPR states unambiguously that measures of controllers should take into account the risk to the rights and freedoms of natural persons.
- Various provisions in Chapter IV of the GDPR on the obligations of the controller and the processor specifically refer to “risk”, “high risk” and risk assessment (including data protection impact assessment).
- Organisations are required to assess the “likelihood and severity of risk” of their personal data processing operations to the fundamental rights and freedoms of individuals.
 - This does not affect the fulfillment of data subjects rights
- Consequently, processing operations which raise lower risks to the fundamental rights and freedoms of individuals may generally result in fewer compliance obligations, whilst “high-risk” processing operations will raise additional compliance obligations, such as data protection impact assessments (DPIAs).
- In effect, this also links to the notion of “scalability” which envisages that the required compliance and accountability measures should take into account the nature, scope, context and purposes of the processing.
 - Scalability and the risk-based approach are closely linked mechanisms incentivising accountability, based on the specificities of a particular processing operation.
- The GDPR requires DPAs to create lists of the kinds of high-risk processing operations requiring a DPIA
- The GDPR also requires the European Data Protection Board (“EDPB”) to issue guidelines, recommendations and best practices on data breaches that may result in “high risk” to individuals.



The notion of risk in data protection

- The GDPR adopts a coherent risk based approach throughout its provisions
 - in Articles 24, 25, 32, 33, 34 and 35 with a view to identify appropriate technical and organisational measures to protect individuals, their personal data and comply with the requirements of the GDPR.
 - The risk and the assessment criteria are the same: the assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights and freedoms), taking into account the same conditions (nature, scope, context and purposes of processing).
- The risk based approach does not exclude the use of baselines, best practices and standards.
 - These might provide a useful toolbox for controllers to tackle similar risks in similar situations (nature, scope, context and purpose of processing).
 - Nevertheless, the obligation in Article 25 (as well as Articles 24, 32 and 35(7)(c) GDPR) to take into account "risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing" remains.
 - Therefore, controllers, although supported by such tools, must always carry out an assessment of data protection risks for the processing activity at hand and verify the effectiveness of the measures and safeguards proposed.



Personal Data Protection Risks Vs Security Risks

- Risk Definition (Recital 75)
 - The risks to the rights and freedoms of individuals of “varying likelihood and severity” may result from personal data processing which could lead to “physical, material or non-material damage”
- Non-exhaustive list of examples of such “physical, material or non-material damage” and of processing activities that could result in such damage (Recital 75)
 - Discrimination
 - Identity theft / fraud, financial loss
 - Reputation damage
 - Loss of confidentiality of personal data protected by professional secrecy
 - Unauthorised reversal of pseudonymisation
 - Any other significant economic or social disadvantage
 - Individuals deprived of rights and freedoms, or prevented from exercising control over their data
 - Processing sensitive data, including data on racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership; genetic data; health data; data concerning sex life; or data on criminal convictions and offences or related security measures
 - Profiling (personal aspects are evaluated [e.g. analyse or predict work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements] to create or use personal profiles)
 - Processing children’s and vulnerable persons’ data
 - Processing large amounts of data affecting large numbers of individuals
- Additional examples of risks (Article 32.2)
 - Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data



Personal Data Protection Risks Vs Security Risks

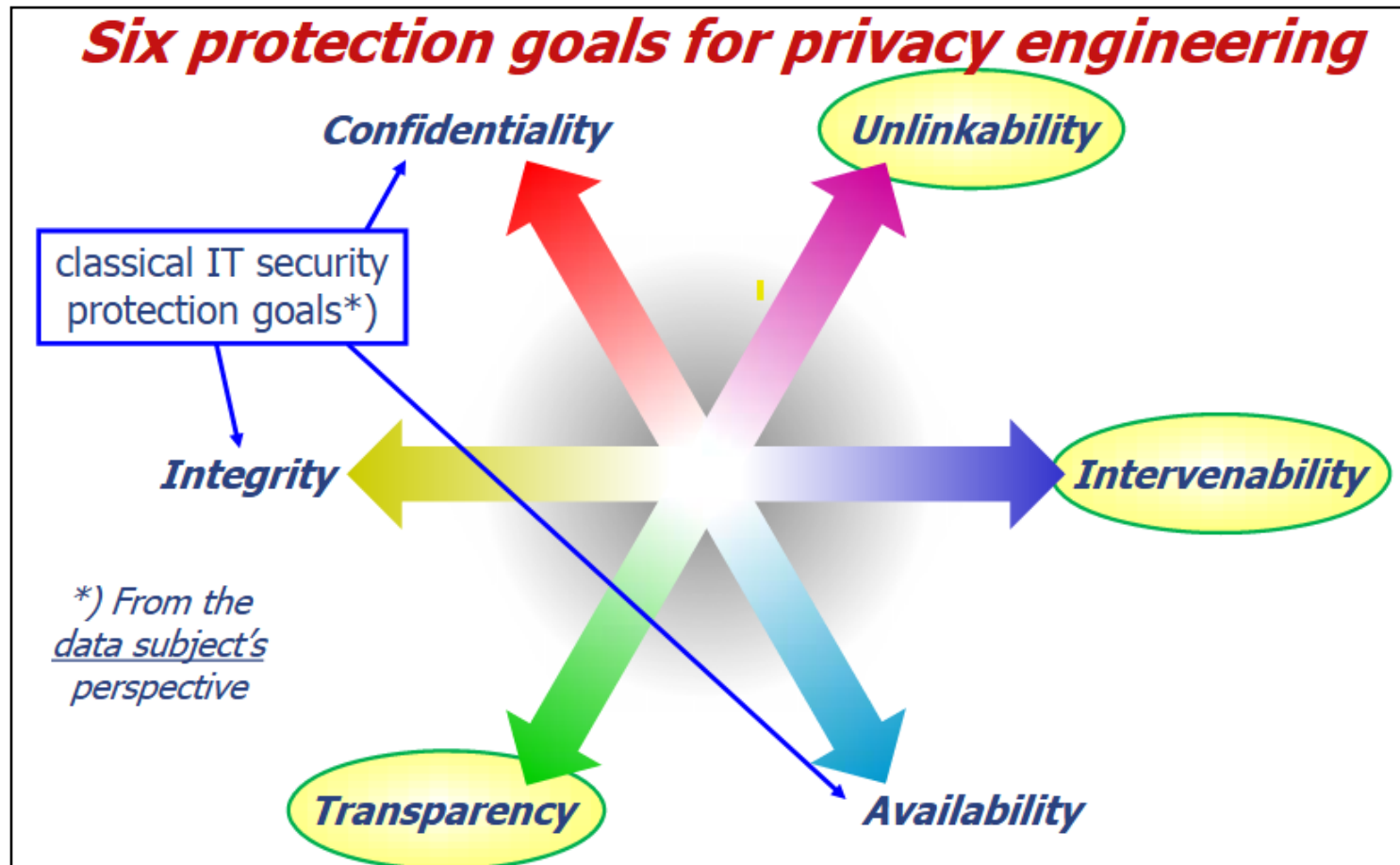
- Factors to take into account when determining risk level (i.e. likelihood and severity of risk) (Recital 76)
 - Nature;
 - Scope;
 - Context; and
 - Purposes of processing.
- What types of processing may result in “high risk”?

Each of the risks above can become “high risk”, depending on the “likelihood and severity” of the risks as determined in a risk assessment process by reference to the nature, scope, context and purpose of processing;

 - Processing, “particularly using new technologies”, might result in “high risk”, depending on “nature, scope, context and purposes of the processing” (“high risk” processing requires an “assessment of the impact” [a DPIA] of the proposed processing operation);
 - New “kind” of personal data processing operation where no DPIA has been conducted or where a DPIA has become necessary over time on the basis of the time elapsed since initial processing; and
 - Large-scale processing operations at regional, national or supranational level and which could affect a large number of data subjects
- Examples of “high risk processing” [Article 35(3)]
 - “Systematic and extensive evaluation of personal aspects ... based on automated processing, including profiling, on which decisions are based that produce legal effects ...”
 - Large-scale processing of sensitive personal data as well as criminal conviction and criminal offence data
 - Large-scale and systematic monitoring of a publicly accessible area.



Data protection goals (Transparency, unlinkability, intervenability)



*PROTECTION GOALS FOR PRIVACY ENGINEERING, Marit Hansen, Meiko Jensen, and Martin Rost, International Workshop on Privacy Engineering, 2015



Data protection goals (Transparency, unlinkability, intervenability)

- Unlinkability
 - privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context
- Transparency
 - all privacy-relevant data processing – including the legal, technical, and organisational setting – can be understood and reconstructed at any time
- Intervenability
 - intervention is possible concerning all ongoing or planned privacy-relevant data processing.
- Intervenability is not prominent in privacy engineering literature
 - Reasons for that:
 - Hard to formalise and to measure
 - Compared with data minimisation research, far less proposed techniques and technologies
 - Can often not be solved within the IT system alone
 - Needs a running system with clear responsibilities (operator, users) – not on prototype level
 - Not one fixed solution, but process-oriented, taking into account the full lifecycle of system evolution



Data protection goals: Transparency

- Related to
 - Openness
 - Accountability
 - Documentation
 - Reproducibility
 - Notice (and Choice)
 - Auditability
 - Full-Disclosure
- Implemented by
 - Logging and Reporting
 - User Notifications
 - Documentation
 - Status Dashboards
 - Privacy Policies
 - Transparency Services for Personal Data
 - Data Breach Notifications

See next seminars...



Data protection goals: Unlinkability

- **Related to**

- Data Minimization
- Necessity / Need-to-Know
- Purpose Binding
- Separation of Power
- Unobservability
- Undetectability

- **Implemented by**

- Data Avoidance / Reduction
- Access Control Enforcement
- Generalization
- Anonymization/Pseudonymization
- Abstraction
- Derivation
- Separation / Isolation
- Avoidance of Identifiers

See next seminars...



Data protection goals: Intervenability

- Related to
 - Self-determination
 - User Controls
 - Rectification or Erasure of Data
 - (Notice and) Choice
 - Consent Withdrawal
 - Claim Lodging / Dispute Raising
 - Process Interruption
- Implemented by
 - Configuration Menu
 - Help Desks
 - Stop-Button for Processes
 - Break-Glass / Alert Procedures
 - System Snapshots
 - Manual Override of Automated Decisions
 - External Supervisory Authorities (DPAs)

See next seminars...



DPIA as a GDPR accountability tool and ICT role

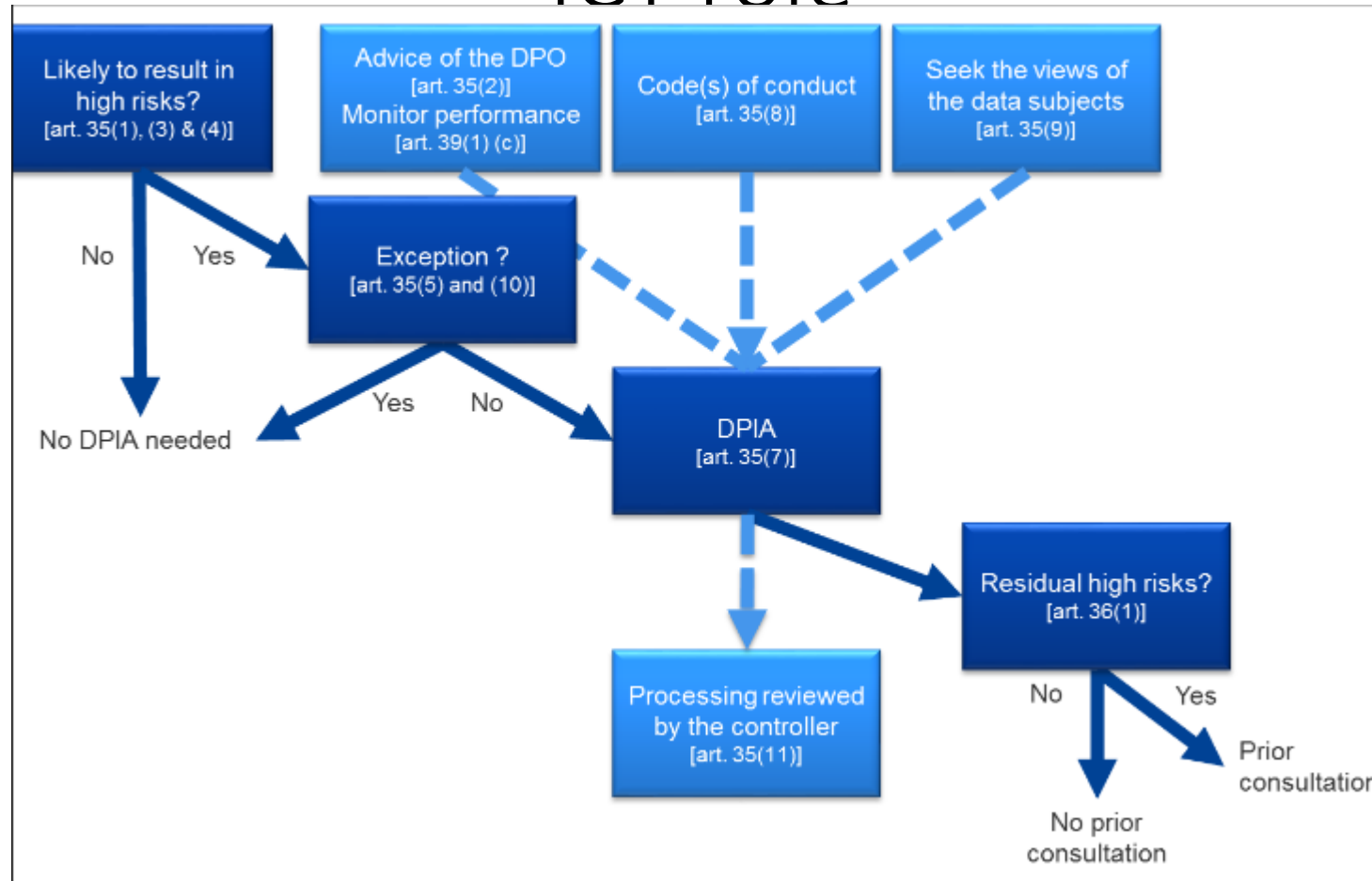
- Accountability Principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities

| | Responsible | Accountable | Consulted | Informed |
|------------------------------|-------------|-------------|-----------|----------|
| Top Management | | X | | |
| Business owner | X | | | |
| DPO | | | X | |
| IT department | | | X | |
| Processors, where relevant | | | X | |
| Data subject representatives | | | (X) | |

[Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation, EDPS, 2018]



DPIA as a GDPR accountability tool and ICT role



DPIA is further analysed in next seminars...

[Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP29, 2017]



DPIA as a GDPR accountability tool and ICT role



| | <i>Fairness</i> | <i>Transparency</i> | <i>Purpose limitation</i> | <i>Data minimisation</i> | <i>Accuracy</i> | <i>Storage limitation</i> | <i>Security</i> |
|-----------------------------------|-----------------|---------------------|---------------------------|--------------------------|-----------------|---------------------------|-----------------|
| <i>Collection</i> | X | X | X | X | X | | X |
| <i>Merging datasets</i> | X | X | X | X | X | | X |
| <i>Organisation/structuring</i> | | | X | X | X | | |
| <i>Retrieval/consultation/use</i> | X | X | X | | X | X | X |
| <i>Editing/alteration</i> | | X | | X | X | | X |
| <i>Disclosure/Transfer</i> | X | X | X | X | X | | X |
| <i>Restriction</i> | | | X | X | X | X | X |
| <i>Storage</i> | X | X | X | | | X | X |
| <i>Erasure/destruction</i> | | | X | | | X | X |

[Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation, EDPS, 2018]



Role of the DPO with respect to DPIA and records of processing activities

- What is the role of the DPO with respect to data protection impact assessment?
- The controller should seek the advice of the DPO, on the following issues, amongst others:
 - whether or not to carry out a DPIA
 - what methodology to follow when carrying out a DPIA
 - whether to carry out the DPIA in-house or whether to outsource it
 - what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects
 - whether or not the data protection impact assessment has been correctly carried out and
 - whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with data protection requirements

[Guidelines on Data Protection Officers ('DPOs'), WP29, 2017]



Funded by European Union's
Rights, Equality and
Citizenship Programme (REC)

Thank you for your attention!

Appendix 3

Data Protection By Design and By Default in GDPR



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



Data Protection by Design and by Default in GDPR

DATES

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





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

Agenda of the Seminar

- Relevant Challenges, Main elements, Importance
- Roles and stakeholders
- Software development with Data Protection by Design and by Default
- DPbD (early) approaches
- By default vs. by design



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

Data Protection by Design (DPbD)

Art. 25(1) of the GDPR



What the GDPR says...

- “Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, **implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing** in order to meet the requirements of this Regulation and protect the rights of data subjects”.
- This also has to do with system producers/developers (see Recital 78)



Relevant Challenges

- A “generic” obligation: No specific measures are implied
 - The chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question
- Decisions should be based on:
 - *State of the art*
 - *Cost of implementation*
 - *Nature, scope, context and purpose of processing*
 - *Risks for rights and freedoms*
- *Time aspect*
 - *From the beginning and during the processing*

Implementation of data protection principles
(in an effective way)

By Design!!



Main elements

- Proactive – not reactive
- Embed privacy into the design process
- Not only security aspects!
 - Much broader than “security-by-design”





Effectiveness - heart of DPbD

- Implement the principles in an “effective manner”
 - implement measures and safeguards to protect data protection principles
 - Each implemented measure should produce the intended results for the processing
 - The measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk
- Controllers should be able to **demonstrate that the principles have been maintained.**
- Documentation of the implemented technical and organizational measures.
 - Appropriate key performance indicators (KPI) to demonstrate the effectiveness.
 - Quantitative, such as the percentage of false positives or false negatives, reduction of complaints, reduction of response time when data subjects exercise their rights; or
 - Qualitative, such as evaluations of performance, use of grading scales, or expert assessments.
 - Alternatively, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards



Why is DPbD important?

- If not implemented or implemented incorrectly:
 - “Wrong” decisions on the processing may be taken
 - Yielding issues in terms of (effectively) fulfilling personal data protection principles
 - Mitigating measures may be impossible or with high cost
 - A (total?) re-design may be necessary



Non only for data controllers...

- Processors and producers - Key enablers for DPbDD
 - Should be aware that controllers are required to only process personal data with systems and technologies that have built-in data protection
 - Should use their expertise to build trust and guide their customers, including SMEs, in designing /procuring solutions that embed data protection into the processing
 - The design of products and services should facilitate controllers' needs
 - Should play an active role in ensuring that the criteria for the “state of the art” are met, and notify controllers of any changes to the “state of the art” that may affect the effectiveness of the measures they have in place.
 - Producers should strive to demonstrate DPbDD in the life-cycle of their development of a processing solution.
 - Controllers, processors and producers, should consider their obligations to provide children under 18 and other vulnerable groups with specific protection in complying with DPbDD

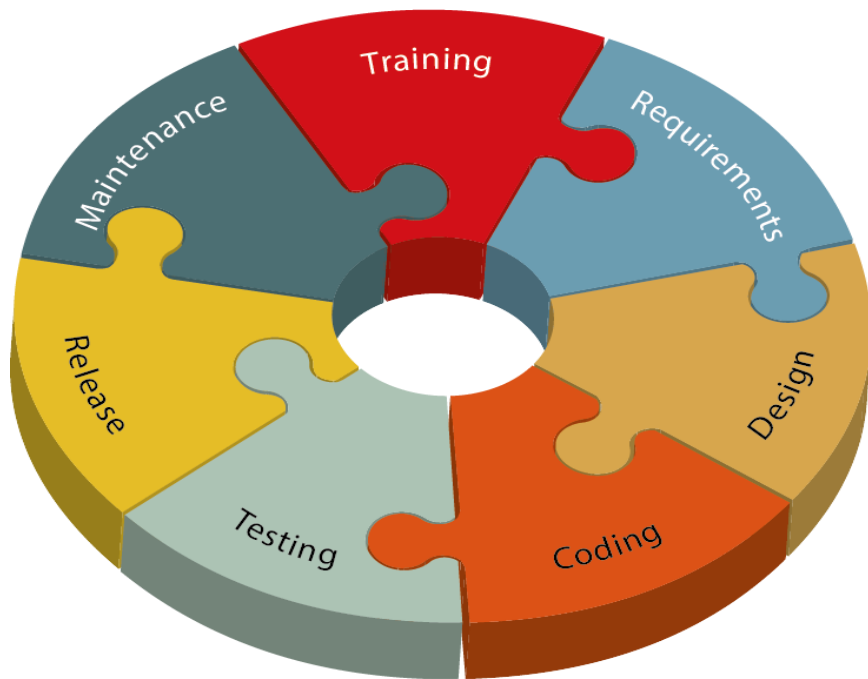


Possible stakeholders and roles

- System engineers: In charge of design and development
- Security managers/officers: In charge of network and systems/applications security
- Data Protection Officer: Independent consulting from a data protection point of view
- Project managers: Senior executive in charge of development
- End users: Users of the system performing personal data processing
- Data subjects



Software development with Data Protection by Design and by Default



Training: Important data protection topics

Requirements: measures needed to ensure data protection and security, the tolerance levels the organisation should set for data protection and security, and the need to assess both security risks and data protection implications.

Design, data oriented and process oriented design requirements. Threat modelling and an analysis of the attack surfaces.

Coding : use of approved tools and frameworks, disabling unsafe functions and modules, and regularly carrying out static code analysis and code review.

Testing: test whether data protection and security requirements are implemented properly

Release, incident response plan, security review, release approval

Maintenance: prepared to respond to incidents, personal data breaches, faults and attacks, and be capable of issuing updates, guidelines, and information to users and those affected by the software

<https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true>



Some (early) approaches

- Kung, 2014

Depending on the context/purpose

| Strategy | | Tactics Examples |
|-----------------------------------|--|---|
| 1 Minimization | Collection of personal information should be kept to a strict minimum | <ul style="list-style-type: none">• Anonymize credentials (e.g. Direct anonymous attestation)• Limit processing perimeter (e.g. client processing, P2P processing) |
| 2 Enforcement | Provide maximum protection of personal data during operation | <ul style="list-style-type: none">• Enforce data protection policies (collection, access and usage, collection, retention)• Protect processing (e.g. storage, communication, execution, resources) |
| 3 Transparency and accountability | Maximum transparency provided to stakeholders on the way privacy preservation is ensured | <ul style="list-style-type: none">• Log data transaction• Log modifications (policies, crypto, protection)• Protect log data |
| 4 Modifiability | Cope with evolution needs | <ul style="list-style-type: none">• Change Policy• Change Crypto Strength and method• Change Protection Strength |



Some (early) approaches

Depending on the context/purpose

- Hoepman, 2014

| Strategy | | Patterns Examples |
|----------------|--|--|
| 1 Minimization | Amount of processed personal data restricted to the minimal amount possible | <ul style="list-style-type: none">• select before you collect• anonymisation / pseudonyms |
| 2 Hide | Personal data, and their interrelationships, hidden from plain view | <ul style="list-style-type: none">• Storage and transit encryption of data• mix networks• hide traffic patterns• attribute based credentials• anonymisation / pseudonyms |
| 3 Separate | Personal data processed in a distributed fashion, in separate compartments whenever possible | <ul style="list-style-type: none">• Splitting data bases (e.g. through pseudonyms) |
| 4 Aggregate | Personal data processed at highest level of aggregation and with least possible detail in which it is (still) useful | <ul style="list-style-type: none">• aggregation over time (used in smart metering)• dynamic location granularity (used in location based services)• k-anonymity• differential privacy |
| 5 Inform | Transparency | <ul style="list-style-type: none">• Platform for privacy preferences• Layered approach for information (no large texts) |
| 6 Control | Data subjects provided agency over the processing of their personal data | <ul style="list-style-type: none">• User centric identity management• End-to-end encryption support control |
| 7 Enforce | Privacy policy compatible with legal requirements to be enforced | <ul style="list-style-type: none">• Access control• Sticky policies and privacy rights management |
| 8 Demonstrate | Demonstrate compliance with privacy policy and any applicable legal requirements | <ul style="list-style-type: none">• privacy management systems• use of logging and auditing |



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

Data Protection by Default

Art. 25(2) of the GDPR



Why is data protection by default important?

- When designing IT systems or IT-based services, the default settings, are of vital importance
- Recognizing the role of the default settings, the GDPR introduces a relevant obligation to data controllers: *“The controller shall implement appropriate technical and organisational measures for ensuring that, **by default**, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons”*.



By default vs. by design

- The obligation for data protection by default is closely interlinked with the one on data protection by design
- It might be perceived only as a substantiation of data protection by design
- However, the task of selecting and implementing the default settings has its own specific significance and challenges.
 - Choosing the defaults is not trivial, even with security and data protection by design in mind
 - It requires an assessment of the necessity for each purpose of the processing, balanced with other equally important requirements, such as usability and expected behaviour of the system or service



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

Thank you for your participation!

Appendix 4

Handling data breaches under the GDPR



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

Handling Data Breaches under the GDPR

byDesign: Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services

www.bydesign-project.eu





GDPR – the need for appropriate measures



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

- **Article 24:** *“1. 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, the controller shall implement **appropriate technical and organisational measures** to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be **reviewed and updated** where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include **the implementation of appropriate data protection policies** by the controller.”*
- Explicit reference to a General Responsibility of the data controller
- Review and update => Personal Data “legality” Management System (corresponding to an Information security management system - ISMS)
- Provision for appropriate (e.g. individual) data protection policies



GDPR and Information Security

- **Article 32:** 1. (...) 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.
- 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing,(...)



What's new?

- ✓ Explicit reference to the obligation of processors for security measures
- Proposal of "appropriate" technical and organizational measures:
 - pseudonymisation and encryption
 - ensure the ongoing confidentiality, integrity, availability and resilience
 - restore the availability and access to personal data in a timely manner
 - a process to test and evaluate security measures
- ✓ Use of an approved code of conduct or certification mechanism to demonstrate compliance
- ✓ **Data protection incident handling procedures**



What is a GDPR Data Breach

“...a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”

- The GDPR is applied when information is personal data

Personal Data Breaches \subset Security Incidents

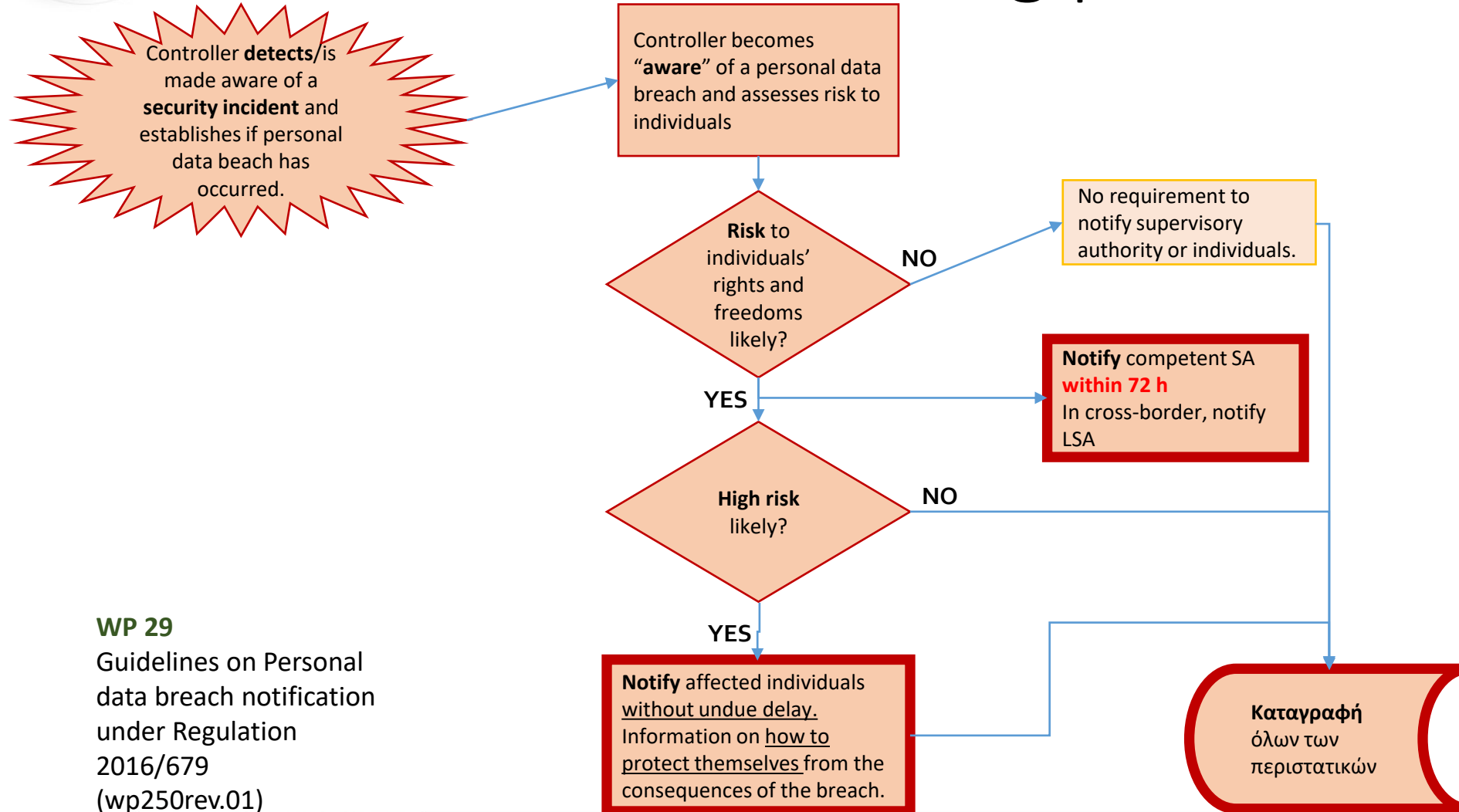
Infringement: { **Confidentiality**
Integrity
Availability } or a combination

GDPR Novelties – Data controller responsibility:

- Recording of all incidents.
- Notification of incidents entailing risk to the Supervisory Authority.
- Informing affected persons about high risk.



Incident handling process



WP 29
Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)



When does a controller become “aware”?

- There's **no objective definition** of the moment that the controller becomes aware
- Emphasis on **immediate action** to assess whether an incident report is a breach of personal data
 - Investigation time does not "count", as long as the controller's reaction is immediate.
 - One can argue about timing, but is it a good policy?
 - When there's a significant degree of certainty that a breach has occurred => the 72h "timer" starts.
- **Points of attention** (and control):
 - Internal investigation and handling procedures.
 - Reporting findings to the appropriate persons within the controller.
 - Procedures that are also applied to Processors.
- If the Processor identifies a breach, the Controller should be informed **without undue delay!**
 - 72h start from the moment the Controller is informed, however, processor is responsible
 - Safer stance: an immediate, basic notification, followed by updates.
 - A Processor may notify on behalf of the controller only if this is provided for in their agreement.



Providing information to the SA

- a) the **nature** of the data breach
 - categories and the approximate number of data subjects affected
 - categories and the approximate number of affected files
- b) name and **contact details** of **DPO** or other point of direct contact
- c) possible **consequences** of the breach
- d) **measures** taken or proposed to be taken by the controller
 - to handle the data breach (the cause of it)
 - to mitigate any adverse effects to data subjects (where appropriate)
- It is also useful to identify any Processors
 - especially since there may be other similar incidents.
- A specific justification of the delay is needed, if exceeding 72 hours.
- **Purpose of the provision:** limiting damage to individuals, by informing them on how to mitigate themselves the consequences of the breach. The Supervisory Authority is informed in order to supervise the actions of the controller
- In complex cases the notification can be done in phases.
 - However, the controller should be able to demonstrate the necessity of partial notification.



When notification is not required?

- When the personal data breach is **unlikely** to result in a risk to the rights and freedoms of natural persons
 - While under directive 2002/58/EC all breaches are notified to the SAs

❖ When is a personal data breach unlikely to result in a risk?

All 3 parameters of security should be satisfied:

- **Confidentiality**: personal data have been made essentially unintelligible to unauthorised parties
 - Encryption, tokenization
- **Integrity**: Data have not been altered
- **Availability**: Backup is existing and data can be restore within reasonable time

Sometimes the assessment may change over time, due to the state-of-the-art and the risk would have to be re-evaluated



Communication to the data subject

- *When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*
- Obligation to inform only for **high-risk** breaches
 - While every breach entailing risk is notified to the SAs
- **Without undue delay**: The aim is to protect data subjects, so they need to be informed as soon as possible to be able to take measures by themselves
 - Without undue delay < 72 hours !!! (ideally)
 - Communication may be delayed if there is a need to address other risks (e.g. to mitigate issues that caused the incident or due to immediate investigation by LEAs)
- Information provided is practically the same as the notification to the SA.
 - Emphasis on recommendations to data subjects on mitigating potential adverse effects



Contacting data subject

- Through **individual communication**, for the specific breach
 - Not as part of other information
 - Selection of the medium (s) by maximizing the possibility of receiving the information (email, SMS, Instant messages, banners, mail, media announcements, etc.).
 - Comprehensible and clear, in the language of the data subjects (or at least in the same language as the data collection)
 - See also WP260 - "Guidelines on transparency under Regulation 2016/679"
- Collaborate (informally) with SA for the selection of the appropriate medium

When is direct communication to the subjects not required?

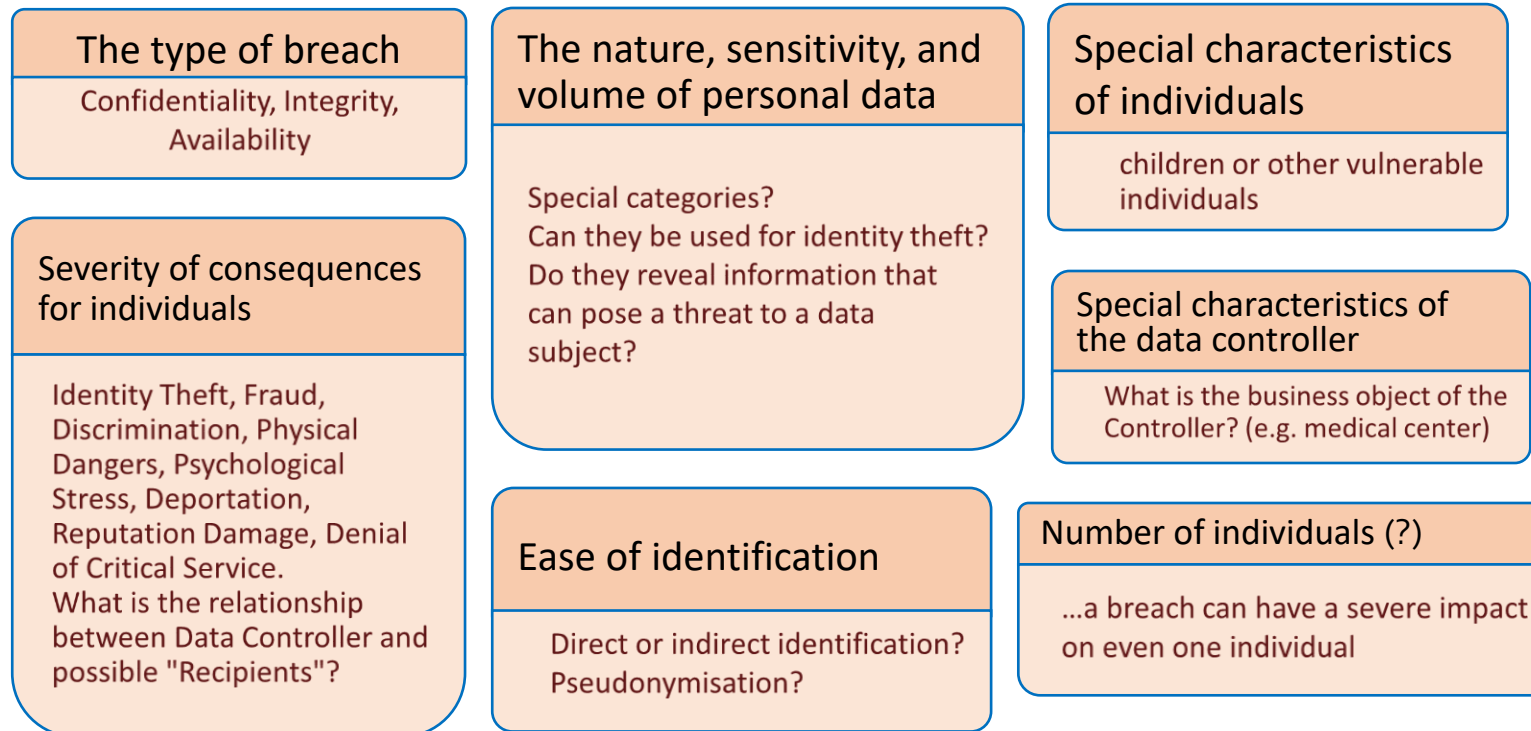
1. When notification to the Authority is not required
 - Unintelligible data, low risk
 2. When the controller took action immediately after the incident and a high risk **is no longer likely**
 3. When providing individual information requires disproportionate efforts.
 - A public announcement or similar measure is required
- The Supervisory Authority may order the Controller to communicate the breach to the affected data subjects



Risk Assessment

- The breach has already occurred, so the focus is wholly about the resulting risk of the impact of the breach on individuals
 - the potential level of impact on individuals
 - how likely is that this risk will materialise

Factors



ENISA has produced recommendations for a methodology of assessing the severity of a breach



Accountability and record keeping

- GDPR ar. 33 para 5 – The principle of accountability in practice

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

- Controllers are obliged to keep an **internal register of data breaches**, regardless of whether a breach should be notified to the Authority.
- This register is used, inter alia, **to demonstrate compliance** in case of an audit.
 - Therefore, all evidence proving compliance must be recorded (e.g. any risk assessment that led to a decision not to communicate the incident)
- Controllers should investigate each incident, without burdening SAs with information about low risk incidents.



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

Thank you for your attention!

Appendix 5

Data protection policies and notices



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

Data Protection Policies and Notices

byDesign: Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services

www.bydesign-project.eu





Transparency under GDPR

- The first principle of the GDPR requires you to process data in a transparent manner in relation to the data subject (Article 5(1)(a))
- The GDPR emphasises the need for transparency over how you use personal data. This can be achieved by providing individuals with privacy information (typically through a privacy notice) such as how their data will be processed, who it will be shared with and what their rights are with respect to it (Article 13 and 14)
- If individuals know this information from the outset, they will be able to make informed decisions in relation to their personal data
- Any information you supply relating to the processing of personal data should be easily accessible, easy to understand and written in clear and plain language



Privacy notices under GDPR

- Presented to data subject whenever new processing is undertaken
- Consider a layered approach to notification
- Must explain:
 - personal data being processed,
 - purpose of processing,
 - legal base of processing, including an analysis of legitimate interest
 - intended retention periods,
 - data subject rights and where they can lodge a complaint
 - source of data,
 - conditions of processing,
 - intended recipients and international transfers
 - existence of automated decision making, including profiling



Privacy notices under GDPR

In particular Article 12 requires that the information or communication in question must comply with the following rules:

- it must be concise, transparent, intelligible and easily accessible (Article 12.1);
- clear and plain language must be used (Article 12.1);
- the requirement for clear and plain language is of particular importance when
- providing information to children (Article 12.1);
- it must be in writing *“or by other means, including where appropriate, by electronic means”* (Article 12.1);
- where requested by the data subject it may be provided orally (Article 12.1); and
- it generally must be provided free of charge (Article 12.5).



Privacy notices under GDPR

“Concise, transparent, intelligible and easily accessible”

- “concise and transparent” manner means that data controllers should present the information/communication efficiently and succinctly in order to avoid information fatigue.
- The requirement that information is “intelligible” means that it should be understood by an average member of the intended audience.
- A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used.
- The “easily accessible” element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed



Privacy notices under GDPR

- Every organization that maintains a website should publish a privacy statement/ notice on the website. A direct link to this privacy statement/ notice should be clearly visible on each page of this website under a commonly used term (such as “Privacy”, “Privacy Policy” or “Data Protection Notice”).
- Positioning or color schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.
- For apps, the necessary information should also be made available from an online store prior to download. Once the app is installed, the information still needs to be easily accessible from within the app.
- One way to meet this requirement is to ensure that the information is never more than “two taps away” (e.g. by including a “Privacy”/ “Data Protection” option in the menu functionality of the app).
- Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public.
- Best practice: the point of collection of the personal data in an online context
 - a link to the privacy statement/ notice is provided or
 - that this information is made available on the same page on which the personal data is collected.



Privacy notices under GDPR

- the use of digital layered privacy statements/ notices is not the only written electronic means that can be deployed by controllers. Other electronic means include “Justin-time” contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards.
- Non-written electronic means which may be used *in addition* to a layered privacy statement/notice might include videos and smartphone or IoT voice alerts.²⁵ “Other means”, which are not necessarily electronic, might include, for example, cartoons, infographics or flowcharts.
- Where transparency information is directed at children specifically, controllers should consider what types of measures may be particularly accessible to children (e.g. these might be comics/ cartoons, pictograms, animations, etc. amongst other measures).
- Another possible way of providing transparency information is through the use of “push” and “pull” notices. Push notices involve the provision of “just-in-time” transparency information notices while “pull” notices facilitate access to information by methods such as permission management, privacy dashboards and “learn more” tutorials.
- A privacy dashboard
- A just-in-time notice
- **Guidelines on transparency under Regulation 2016/679** <https://ec.europa.eu/newsroom/article29/items/622227>



Examples

WHAT WE DO WITH PERSONAL DATA WHEN YOU...

MAKE A COMPLAINT

To investigate and take regulatory action in line with our statutory duties

Information from you to investigate your complaint properly

Necessary to perform our public tasks as a regulator

MAKE AN ENQUIRY

To fulfil our regulatory responsibilities

Enough information to respond to your enquiry

Necessary to perform our public tasks as a regulator

REGISTER FOR A WEBINAR

To facilitate the event and provide access to it

Contact information

Consent

MAKE AN INFORMATION REQUEST

Fulfil your information request

Contact information and enough information

Necessary to comply with a legal obligation to which we are subject

SUBSCRIBE TO OUR E-NEWSLETTER

So we can email information to you

Name and address

Consent

ARE BEING INVESTIGATED BY THE ICO

To establish whether a criminal offence has occurred and take any appropriate legal action

Information compiled during our investigation of an alleged offence

Necessary to perform our public tasks as a regulator

PAY A FEE

To communicate with you about the fee and any related issue

Contact and address information for your business, and DPO name if relevant

Necessary to perform our public tasks as a regulator

REPORT A NUISANCE CALL OR MESSAGE

Investigate and take regulatory action in line with our statutory duties

Phone number you received the call on and the first part of your postcode, contact information is optional

Necessary to perform our public tasks as a regulator

ATTEND AN EVENT

To facilitate the event and provide you with a good service

Contact information, organisation name. If offered a place, dietary requirements or access provisions. We may also ask for payment if there is a charge to attend.

Consent

REQUEST OUR PUBLICATIONS

So we can post information to you

Name and address

Consent



PURPOSE OF PROCESSING PERSONAL DATA

the INFO WE NEED

LAWFUL BASIS for USING YOUR DATA

For further information on how and why we use your personal data, including how long we keep it, your rights, who we share it with, and how you can contact us, please read our full privacy notice at:

ico.org.uk/privacy-notice





Example: layered approach

> **How will we use the information about you?** 

⌵ **How will we use the information about you?**

Process your order, manage your account, personalise your use of the website and post offers of other products and services we offer to you (if you agree).

May be shared with – members of our group of companies (if you agree). Won't be shared – for marketing purposes outside of our group. [Please follow this link for further information.](#) 

Privacy > How will we use the information about you?

How will we use the information about you?

We collect information about you to process your order, manage your account and , if you agree, post offers of other products and services that we offer.


We use your information collected from the website to personalise your repeat visits to the website.





If you agree, we shall pass on your personal information to our group of companies so that they may offer you their products and services.

We will not share your information for marketing purposes with companies outside of our group.




Example: dashboards

My Account Dashboard 

| | |
|---|---|
|  Account settings My account details My devices My display preferences |  My preferences Who can see my details? Who can share my info What ads do I want? |
|  Security View and manage your security settings |  Privacy Privacy notice Manage my consent preferences How to access my personal data |

[My Account Dashboard](#) / [My preferences](#)

 **Who can see my details?**

| | |
|--|-------------------------------------|
| People who I am connected to | <input type="checkbox"/> |
| People who are connected to my connections | <input checked="" type="checkbox"/> |
| Anyone with an account | <input type="checkbox"/> |
| I don't want anyone to see my details | <input type="checkbox"/> |

[Back to My Account Dashboard](#)



Example: dashboards

juro Your privacy at a glance

Hello. We are Juro Online Limited (known by humans as Juro). Here's a summary of how we protect your data and respect your privacy.

- Types of data we collect**
 - Contact details
 - Financial information
 - Data from your contracts
 - Data that identifies you
 - Data on how you use Juro
- When and how we collect data**
 - You browse any page of our website
 - You request a demo of Juro
 - We call you
 - You use Juro
 - You receive emails from us
 - You view and sign contracts
 - You chat with us for customer support
 - You connect integrations (like Slack)
 - You opt-in to marketing messages
- How we use your data**
 - To keep Juro running
 - To help us improve Juro
 - To give personalised customer support
 - To send you marketing messages (but only if you tell us to)
- Third parties who process your data**
 - Infrastructure: Algolia, AWS, MongoDB
 - Analytics: Heap, Mixpanel, Metabase
 - Integrations: (by your request) Salesforce, Slack, Google
 - Comms: Hubspot, Intercom, Sendgrid, Sumo
 - Payments: Stripe
- We use cookies**
 - We use only necessary cookies to run and improve the service
 - Our third party service providers use cookies too, which they control
 - You can turn off cookies but this will mean for example that we can't recognise you in in-app messaging or we can't resolve issues so efficiently
- Know your rights**
 - Access information we hold on you
 - Opt-out of marketing comms
 - Port your data to another service
 - Be forgotten by Juro
 - Complain about us

Read the full policy (no legalese, we promise)

Types of data we collect

Contact details

Your name, address, telephone number, email address...

Financial information

Your bank account number, sort code, credit/debit card details...

Data from your contracts

Your contract templates, smart fields, data integrated into contracts from third party providers, counterparty names and email addresses, comments, activity on contracts, signatures...

Data that identifies you

Your IP address, login information, browser type and version, time zone setting, browser plug-in types, geolocation information about where you might be, operating system and version...

Data on how you use Juro

Your URL clickstreams (the path you take through our site), products/services viewed, page response times, download errors, how long you stay on our pages, what you do on those pages, how often, and other actions...

What about really sensitive data?

We don't collect any "sensitive data" about you (like racial or ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, genetic data, biometric data, health data, data about your sexual life or orientation, and offences or a legal offences) except when we have your specific consent, or when we have to to comply with the law.

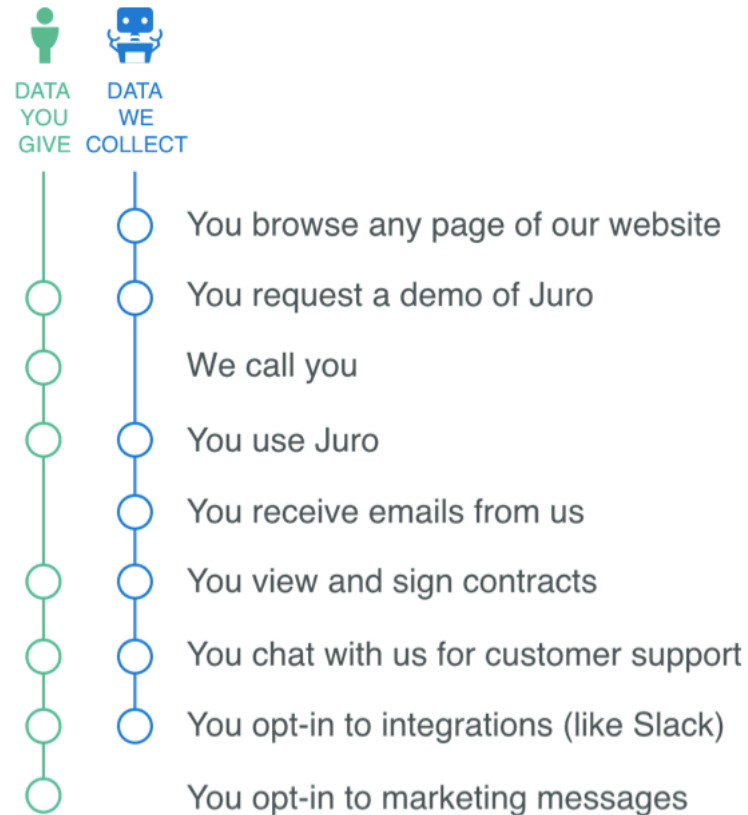
What about children's data?

Juro is a business-to-business service directed to and intended for use only by those who are 18 years of age or over. We do not target Juro at children, and we do not knowingly collect any personal data from any person under 16 years of age.

[Read more](#)



Example: Privacy timeline



Thank you for your attention!

Appendix 6

Online marketing and advertising - Cookies and trackers



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



Online marketing and advertising – Cookies and trackers

**byDesign: Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT
products and services**

www.bydesign-project.eu

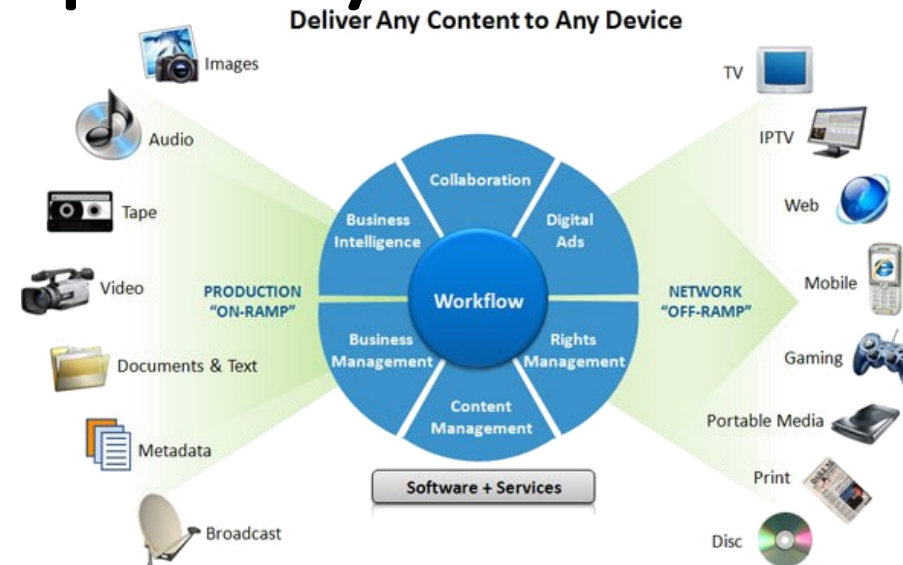




Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Why e-privacy?

ICT is increasingly overturning traditional market structures by creating a single, global infrastructure for providing a wide range of online services

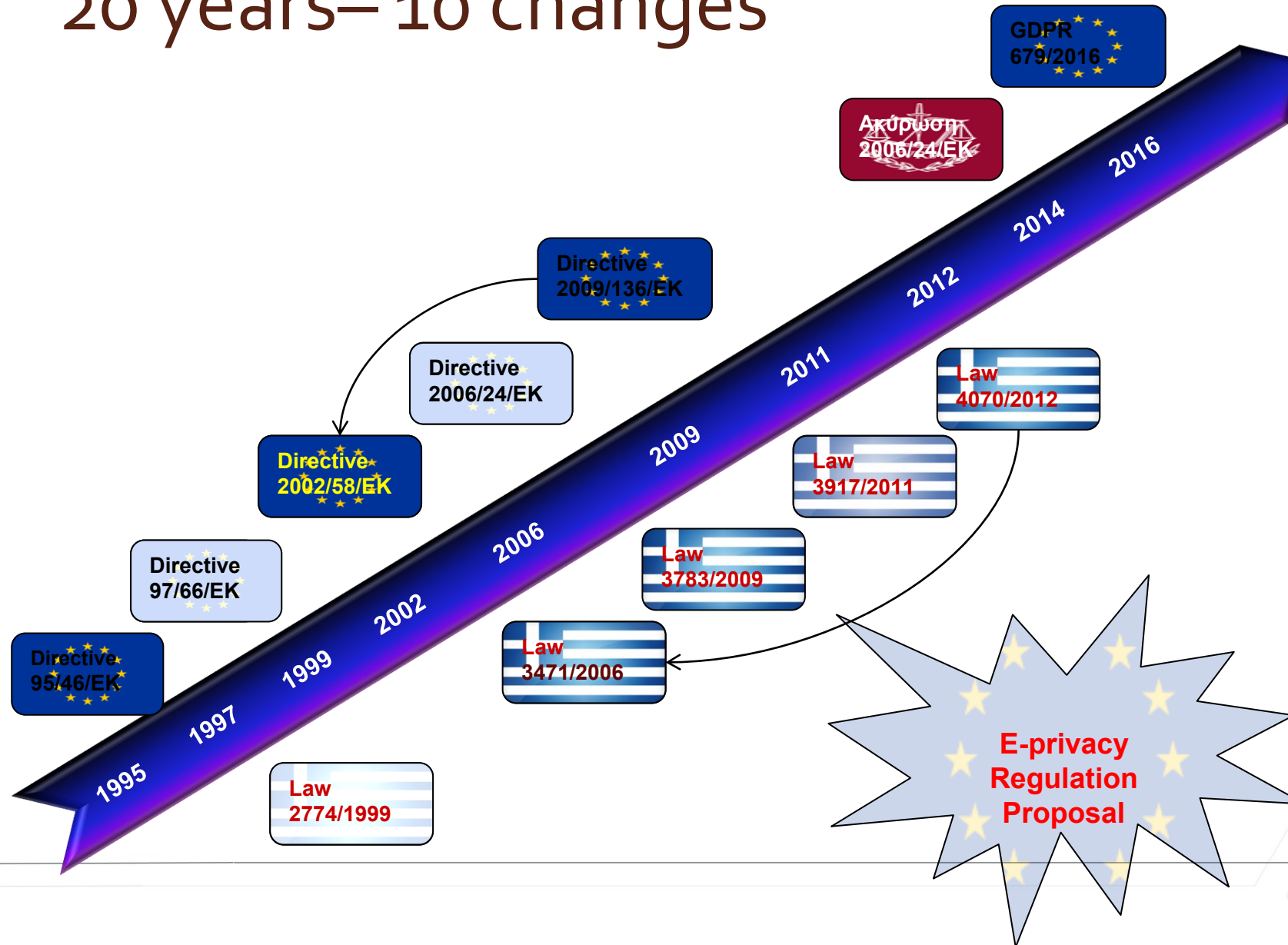


- **Requires:** Protection of fundamental rights and freedoms of natural persons and legal interests of legal persons
- Protection of personal data in conjunction with the Protection of privacy of electronic communication
- **Goals:**
- The same level of protection of personal data and privacy for all users of communications services available to the public, regardless of the technologies used
- Harmonize legislation to avoid barriers to the internal market for electronic communications



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

20 years– 10 changes





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

Scope of e-privacy Directive(2002/58/EK) & Law 3471/2006

Includes: Traditional providers of electronic communications services (telephony, internet, e-mail, etc.) in the territory of the Member State

Recently included (ECC, from 12/2020): "Competitive" communication services (e.g. chat, VoIP applications)

Does not include: Private or not, open to the public (e.g. corporate networks, academic networks, public WiFi, WiFi provided to customers / store visitors)



- Roles of subscribers and users
- *Additional application in specific areas:*
 - *Unsolicited communication*
 - *Terminal equipment*





e-Privacy Regulation

Scope changes

- Complements GDPR
- Includes:
 - **OTT providers** (π.χ. Messaging apps και VoIP) - already included (although an amendment of Law 3471/06 is needed)
 - Communication “**machine to machine**” when linked to personal data (IoT).
 - As in GDPR, providers establishment does not matter.
- Subscriber and user replacement by "end user"
- The proposed regulation might introduce settings for S / W and Browsers that are essentially considered terminal devices and must have settings in the direction of privacy by design and privacy by default



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

Direct marketing via phone

- Article 13 Directive 2002/58/EK
- Greece: Law 3471/2006, article 11, par. 2
 - Opt-outs system:
 - Unsolicited human intervention communications (calls) may not be made if the subscriber has stated to the publicly available service provider that he or she generally does not wish to receive such calls.
 - The provider is obliged to register these statements free of charge in a special directory ("opt-out" register).





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

Marketing via electronic messages

- Article 13 law. 3471/2006 (according to article 11 of Directive 2002/58/EK).
- Opt-in
 - Consent, prior notification
 - Ability to revoke consent with each message
 - It also includes legal entities
- Exception - opt-out
- The data was legally obtained in the context of the sale of a product or service to the supplier
- Promotion of similar products / services
- During the collection of this information but also with each sending of a message the recipient has the opportunity to express his objection



Electronic messages include e-mails, SMS and messages in messaging platforms



Opt-in/Opt-out effectiveness*

The data subject is presented with one of the following options, during the collection of his/hers personal data

Table 1. Formats and Participation Rates, Experiment 1

| Question | Percent Participating | |
|---|-----------------------|---|
| (1) <input type="checkbox"/> Notify me about more health surveys. | 48.2 | Valid consent (with appropriate information) |
| (1) <input type="checkbox"/> Do NOT notify me about more health surveys. | 96.3 | Valid legitimate interest (with appropriate information) |
| (3) <input checked="" type="checkbox"/> Notify me about more health surveys. | 73.8 | Questionable legitimate interest |
| (4) <input checked="" type="checkbox"/> Do NOT notify me about more health surveys. | 69.2 | Valid legitimate interest (with appropriate information), more privacy friendly |

*Johnson, E.J., Bellman, S. & Lohse, G.L. Defaults, Framing and Privacy: Why Opting In-Opting Out¹. *Marketing Letters* 13, 5–15 (2002). <https://doi.org/10.1023/A:1015044207315>



e-Marketing examples

Opt-in example (good practice)

Tick if you would like to receive information about our products and any special offers:

- by post
- by email
- by telephone
- by text message
- by recorded call

Opt-out example (bad practice)

By submitting this registration form, you indicate your consent to receiving email marketing messages from us.

If you do not want to receive such messages, tick here:

Soft Opt-in example (acceptable practice)

Tick here if you **do not** want to hear about the latest offers and news from

Email SMS Post Phone

We'll use your contact details for **legitimate business purposes**

to tell you about our **latest holiday offers, products and**

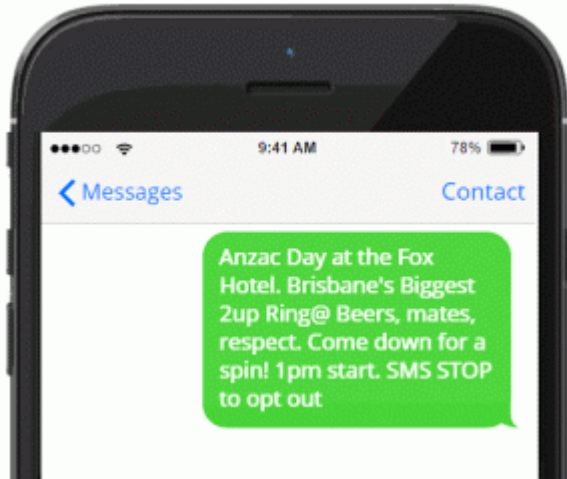
services. If you would like further information on how we

process your personal data please click on our [privacy policy](#). If

you opt out of receiving marketing information from us, we'll

still send you important service messages about your booking.

e-Marketing examples



- ✓ Consent from the recipient (or existing customer relationship)
- ✓ Accurate identification of the sender (business name)
- ✓ Clear unsubscribe function e.g.
 - SMS Reply Number
 - Opt-out Keyword on specific number
 - Opt-out URL Link
 - Even manually



LEGAL INFORMATION ABOUT THIS EMAIL: This e-mail cannot be considered as spam as long as the **senders contact info** and **unsubscribe options** are valid according to the EU Directiva 2002/58/EC, Relative as A5-270/2001. We are firmly committed to respecting your privacy. We do not share your information with anyone, for any reason. If you don't wish to receive newsletters please **click here**.

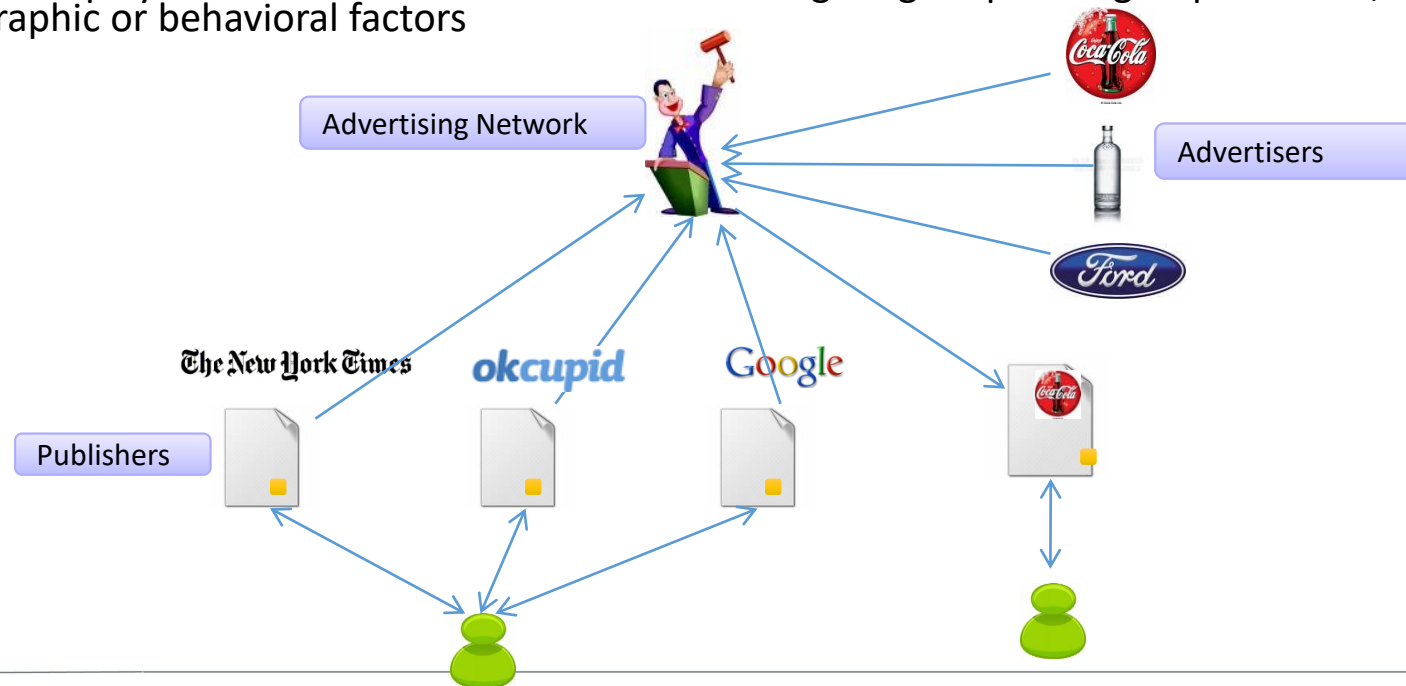


Targeted/Behavioral ads, Real time bidding: A kind of "auction": which advertiser will "win"



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

- **Advertising Network:** Links websites and media owners to advertisers
- **User Profile:** Information about Internet browsing. Advertising networks collect and use information from visits to websites participating in that network
- **Tools:** Cookies, Device Fingerprinting, ...
- **Behavioural/targeted advertisement techniques:** Use information about the user's browsing in order to display ads tailored to their interests or targeting a specific group of users, based on demographic or behavioral factors

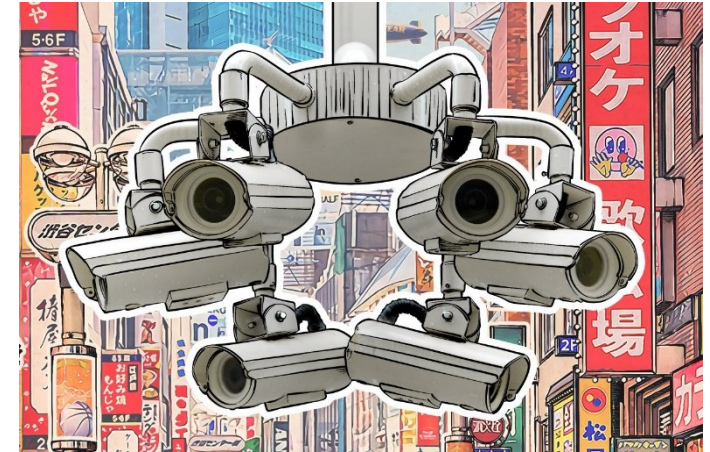




Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Tracking technologies

- HTTP Cookies
- HTTP Auth
- HTTP Etags
- Content cache
- IE userData
- HTML5 protocol and content handlers
- HTML5 local storage
- Flash cookies
- Silverlight storage
- TLS session ID & resume
- Browsing history
- window.name
- HTTP STS
- DNS cache





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

Tracking is widespread

64 independent site tracking mechanisms from the top-50 in traffic...



Advertisers

Content Providers



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

How is this regulated?



- Article 5 of Directive 2002/58/EK,
- Article Article4 par. 5 of law 3471/2006

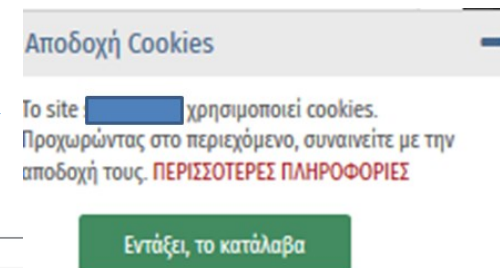
- The storage of information or access to information already stored on the subscriber or user terminal equipment is allowed only with the consent of the explicit notification.
- Exceptionally, without the consent but always with information, the storage or access is allowed if it is necessary for the transmission of a communication through an electronic communications network or for the provision of an information society service, which has been expressly requested by the user.

- Cookies fall into this category
 - Also MAC and IP address, browser header data and anything locally stored.
- If the user's browser is configured to accept all cookies, this cannot be construed as special consent!



Cases of cookies

- It is allowed to install cookies on the user's terminal equipment (e.g. computer), without his consent, only if they are absolutely necessary for the provision of the service
 - E.g. Session cookies,
For other cases of cookies, there must be explicit consent of the user
Π.χ. Cookies for targeted ads, stats, visitor counts, etc.
- Consent must be obtained with clear user action (clear, explicit and specific consent)
- Choose an appropriate selection button that agrees, from which it must be clear that it is adequately informed about what its selection means
- It is not considered clear, explicit and specific consent of the user if she/he simply continues to navigate after being first informed (e.g. with a pop-up "window") about the existence of cookies





Cases of cookies

Only information- par. 5 art. 4 law. 3471/2006

Shopping cart - content retention

Security, online payments

'load balancing' , 'reverse proxying'

...

Consent
art. 4 I. 3471/2006

Analytics

Ads presented from site owner

Ads presented from third party

Content adaptation to revisiting customer

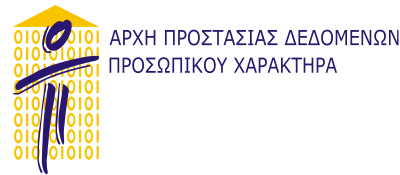
Social media plugins

Behavior tracking in social media



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

HDPA– requirements



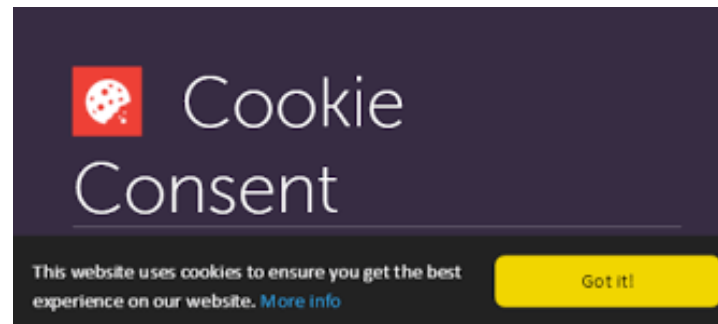
- No “cookie walls”
- Information for all cookies
- By default not checked
- Different purposes– different consents
- Active behavior with clear information
- Ease to withdraw consent
- Same number of actions to accept/reject



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

Bad practices

- Incomplete information / pre-checked consent options
- "Cookie wall" effect (if the user does not accept cookies without exception, can not proceed)



Examples

The image displays three different styles of cookie consent banners. The top banner is a small, semi-transparent white box with a green 'Accept' button. The middle banner is a large white box with a green 'Accept' button and a 'More information' link. The bottom banner is a light blue box with three buttons: 'ACCEPT', 'REJECT', and 'MORE INFORMATION'. A blue 'X' icon is visible in the top right corner of the bottom banner's background.

Example 1 (Top): A small, semi-transparent white box with a green 'Accept' button. The text inside reads: "This site uses functional and analytical cookies to offer you an optimal visitor experience. This also enables us to record and analyze visitor behavior and thereby improve our site and display relevant advertisements. By clicking on agree below you agree with this. [Read more about our privacy policy](#)".

Example 2 (Middle): A large white box with a green 'Accept' button. The text inside reads: "We need your consent to set cookies on your device. To agree, click 'Accept below.'". Below the button is a link: [More information](#).

Example 3 (Bottom): A light blue box with three buttons: 'ACCEPT', 'REJECT', and 'MORE INFORMATION'. The text inside reads: "We use cookies. The EDPB website uses cookies to collect data in order to create statistics to improve the quality of our website. You can accept or refuse our cookies by clicking on the buttons below or by visiting our [Cookie policy page](#). A default 'no consent' option applies in case no choice is made and a refusal will not limit your user experience. If you would like to know more about our cookie policy, please click on the 'More information' button below."

Examples (CNIL)

Some features of this site are based on services offered by third party sites (twitter feed, video).

If you give your consent, third party websites will place cookies that will allow you to display in the content of our website hosted by these third parties and share our content.

They will collect your browsing data and use the data collected through their cookies for purposes they have determined in accordance with their privacy policy (link below).

You can give or withdraw your consent on this page. You can express your choice as a whole or purpose

Managing your preferences about cookies

Some features of this website rely on services offered by third-party sites (twitter feed, videos). If you give your consent, these third-party sites will drop cookies that will allow you to visualize on our site content hosted by these third-parties, and share our contents. They will collect your browsing data and use the data collected via their cookies for purposes they have determined in accordance with their privacy policy (link below). You can give or withdraw your consent on this page. You can express your choice globally or purpose by purpose

Preference for all services

Allow Deny

Audience measurement

The audience measurement services used to generate useful statistics attendance to improve the site.

Piwik

> See their privacy policy

Allow Deny

Social networks

The cookies that are dropped via social networks buttons are intended to allow users to facilitate the sharing of content and to improve the user experience.

Facebook

> See their privacy policy

Allow Deny

Twitter

> See their privacy policy

Allow Deny

Twitter (cards)

> See their privacy policy

Allow Deny

Twitter (timelines)

> See their privacy policy

Allow Deny

Videos

The cookies dropped via video sharing services are intended to allow the user to view the multimedia content directly on the site.

Prezi

> See their privacy policy

Allow Deny

SlideShare

> See their privacy policy

Allow Deny

Vimeo

> See their privacy policy

Allow Deny

YouTube

> See their privacy policy

Allow Deny

To exercise your rights on the data collected via the cookies dropped by the third parties or for any questions on the processing, you can contact them directly.
[More information on the processing of personal data carried out by the CNIL.](#)

Examples (EDPB)

The screenshot shows the homepage of the European Data Protection Board (EDPB). The browser address bar displays 'https://edpb.europa.eu'. The website header includes the EDPB logo and navigation links: HOME, ABOUT EDPB, NEWS, and OUR WORK & TOOLS. A search bar is located on the right. The main content area is divided into 'Latest news' and 'Agenda'. Under 'Latest news', there are three articles: '13th Plenary Agenda' (10 September 2019), 'EDPB Stakeholder Event' (02 October 2019), 'Polish DPA imposes €645,000 fine' (20 September 2019), and 'Belgian DPA imposes a fine of' (partially visible). The 'Agenda' section lists upcoming plenary sessions: 'Fourteenth Plenary Session of the EDPB - 8 & 9 October 2019', 'EDPB Stakeholder Event on Data Subject Rights' (04 November 2019), 'Fifteenth Plenary Session of the EDPB - 12 & 13 November 2019', and 'Sixteenth Plenary Session of the EDPB - 2 & 3 December 2019'. At the bottom, a cookie consent banner is displayed with the text: 'We use cookies. The EDPB website uses cookies to collect data in order to create statistics to improve the quality of our website. You can accept or refuse our cookies by clicking on the buttons below or by visiting our "Cookie policy page". A default 'no consent' option applies in case no choice is made and a refusal will not limit your user experience. If you would like to know more about our cookie policy, please click on the "More information" button below.' The banner contains three buttons: 'ACCEPT', 'REJECT', and 'MORE INFORMATION'. An orange arrow points to the 'MORE INFORMATION' button.

If the user does not take any action or select "reject", none of the unnecessary cookies are installed (case of "opt-in" consent)

If the user selects here, he can choose which cookie to install



Funded by European Union's
Rights, Equality and
Citizenship Programme (REC)

Thank you for your attention!

Appendix 7

Risk Assessment – DPIA



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



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)*





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



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?

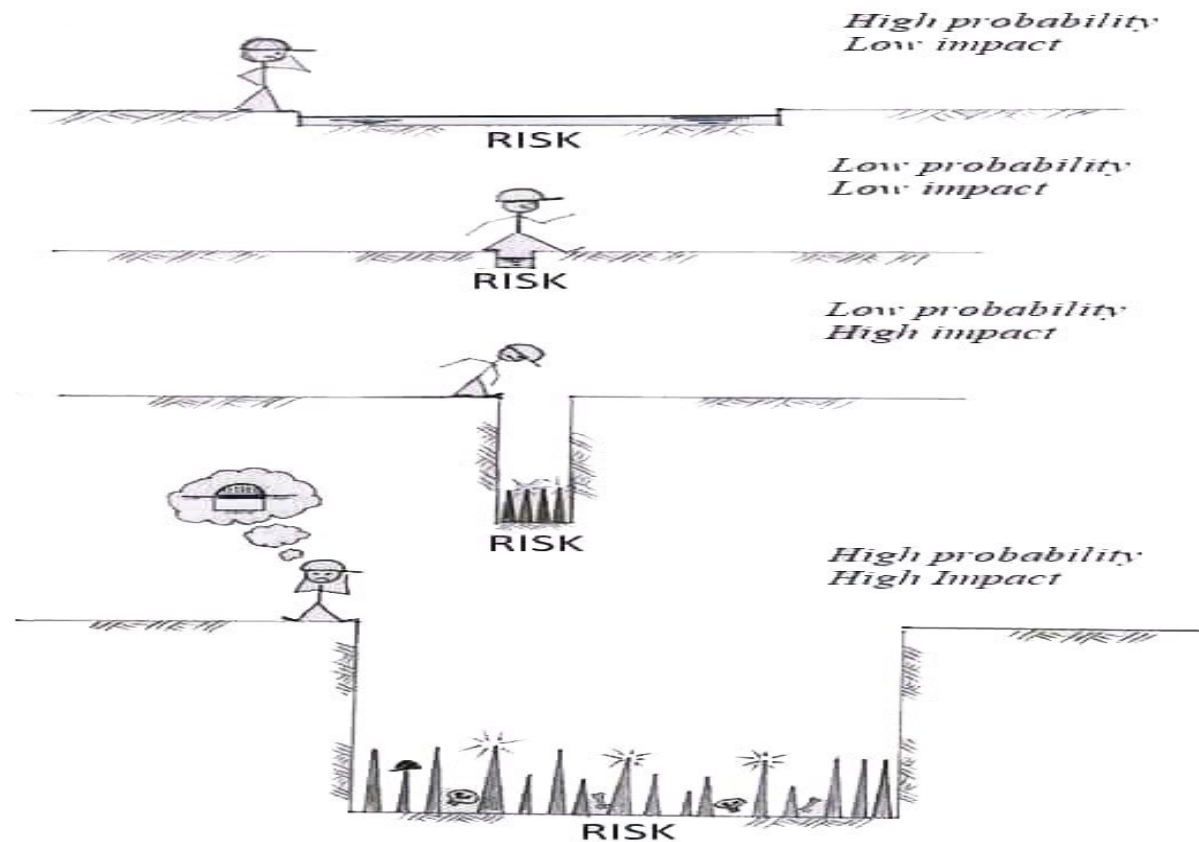


The Concept of Risk

- 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



The Concept of Risk





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

Information Security Risk Assessment



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



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



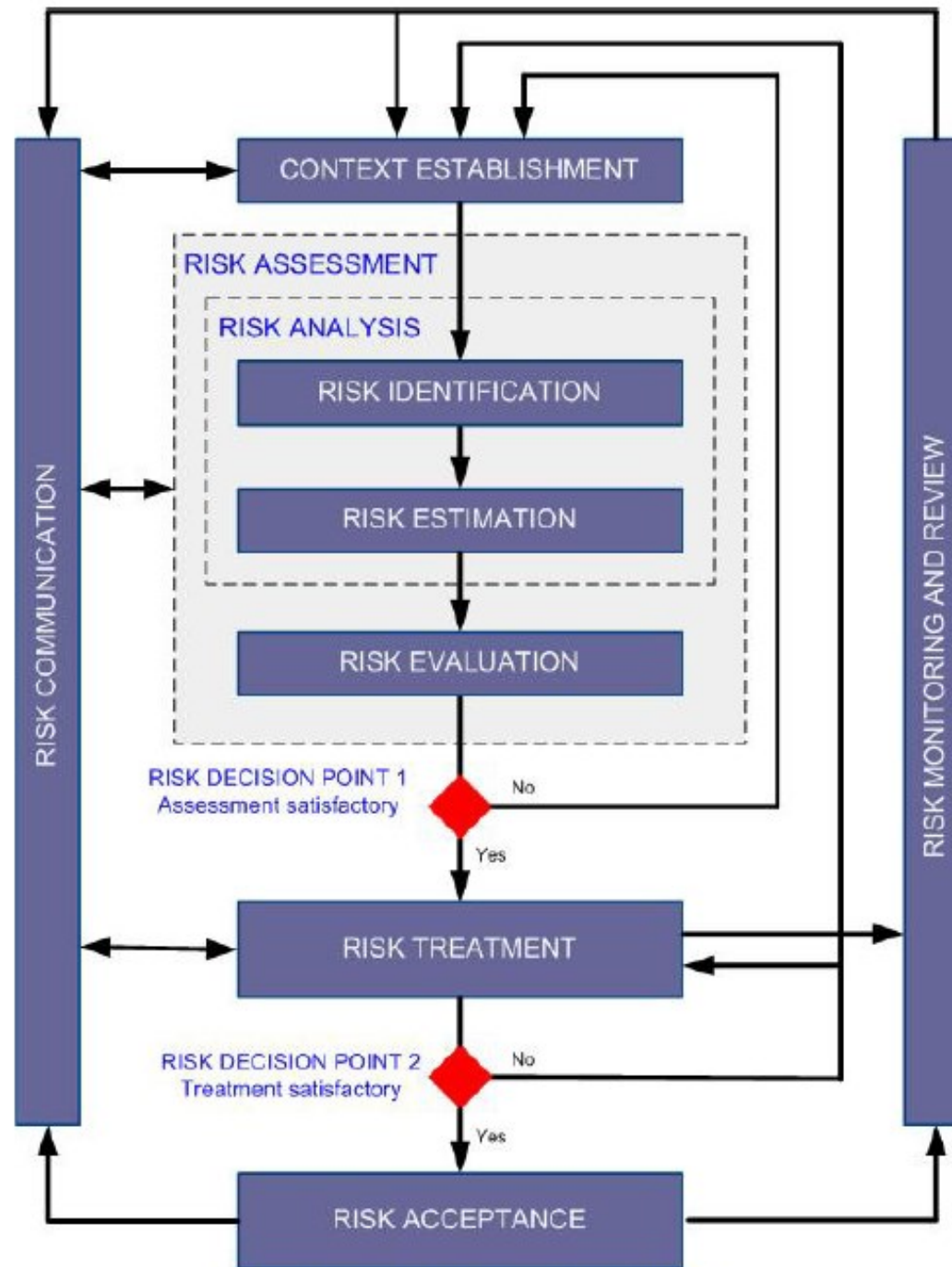
ISO 27005:2018 Guidelines for information security risk management

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





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



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.



Risk identification – Identification of Assets



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

- 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



Risk identification – Identification of Assets



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

Primary assets:

- Business processes & activities
- Information

Supporting assets of all types:

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



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



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



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



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



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



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



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



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



Risk identification – Identification of threats

Example of threats and
respective types of threats



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

| 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 |



Risk identification – Identification of threats

Example of human threats
sources



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

| 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



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

- 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



Risk identification – Identification of vulnerabilities



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

- 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

| 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 |

Risk identification – Identification of vulnerabilities



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



Risk identification – Identification of consequences



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

- This step 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



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



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



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 presented in the Figure

| | Likelihood of occurrence – Threat | Low | | | Medium | | | High | | |
|-------------|-----------------------------------|-----|---|---|--------|---|---|------|---|---|
| | | 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 |



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

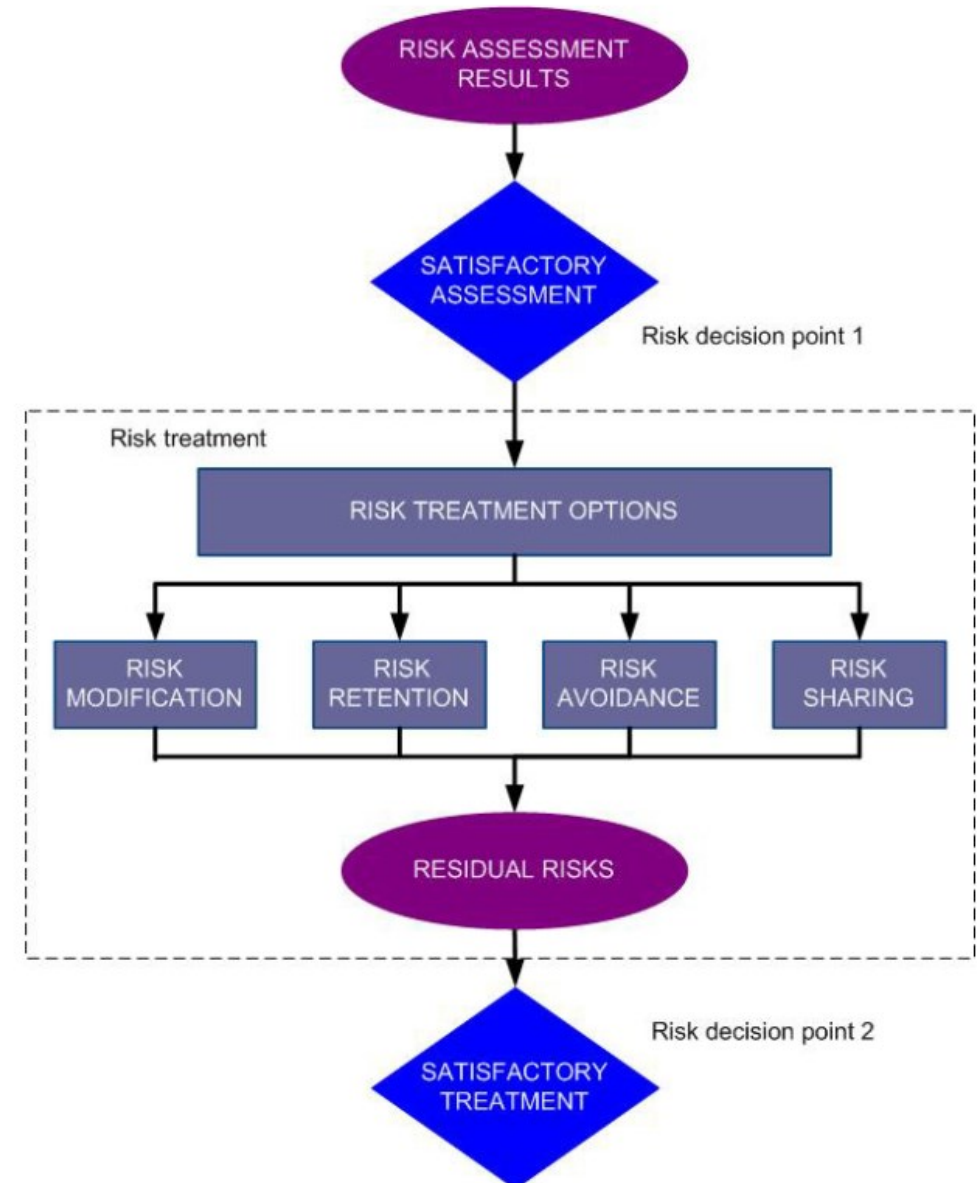


Information security risk treatment

- 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





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

Data Protection Impact Assessment



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





Data Protection Impact Assessment in the General Data Protection Regulation



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

- 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



Data Protection Impact Assessment in the General Data Protection Regulation



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

- 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



Data Protection Impact Assessment in the General Data Protection Regulation



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

- 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



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



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

Privacy Impact Assessment (PIA)

METHODOLOGY





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





The Steps of the CNIL DPIA Methodology



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

- 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



The Steps of the CNIL DPIA Methodology



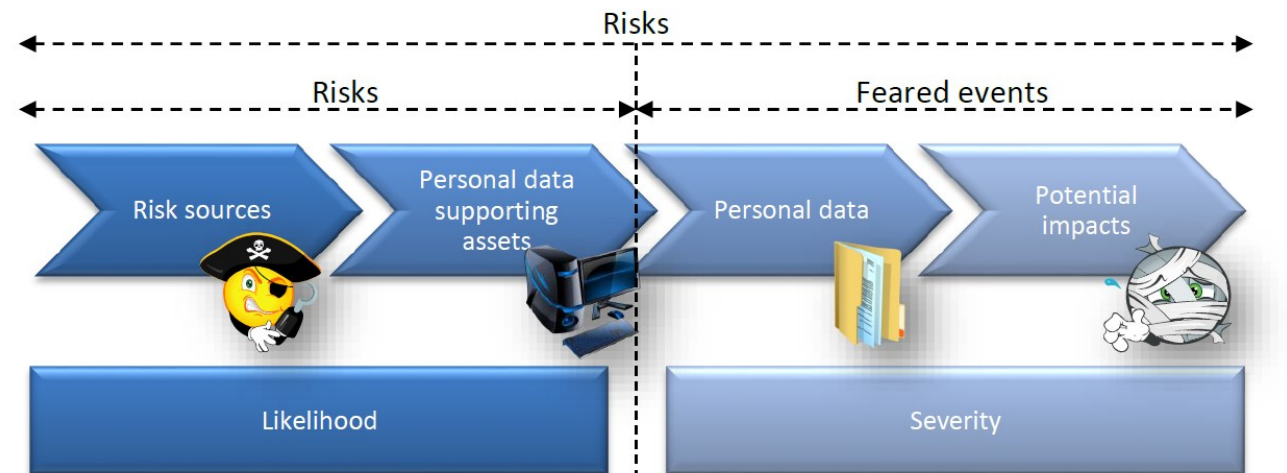
- DPIA is a continuous improvement process
- It may require several iterations to achieve an acceptable privacy protection system
- It requires a monitoring of changes over time (in context, controls, risks, etc.), for example, every year, and updates whenever a significant change occurs



The Concept of Risk in DPIA

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

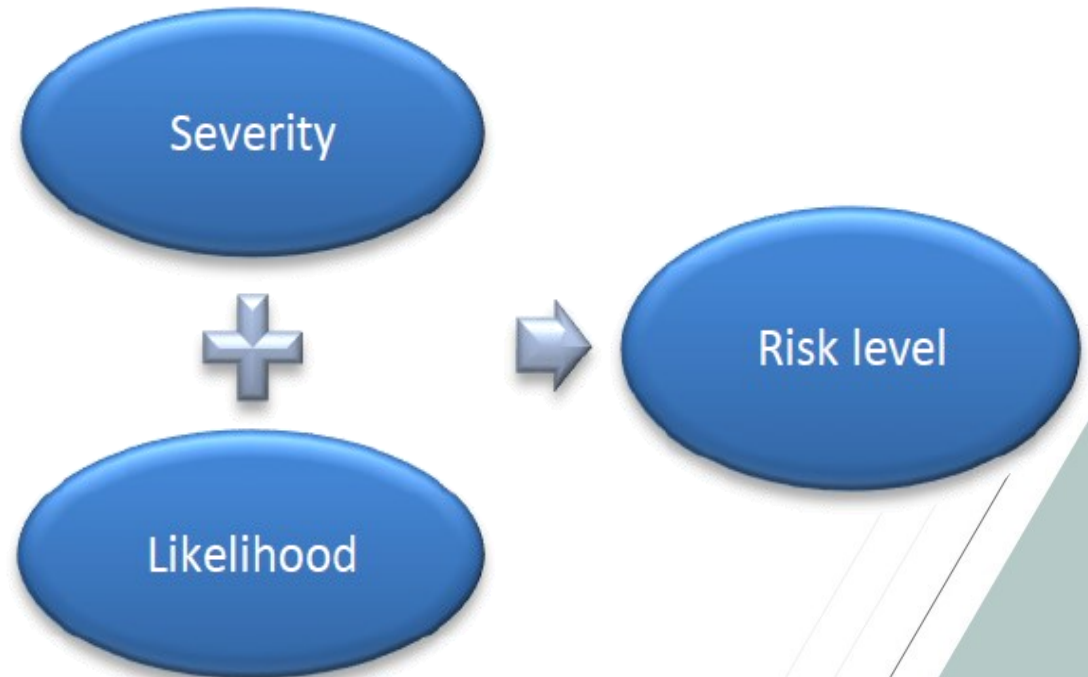
- how **Risk Sources** (e.g., an employee bribed by a competitor)
- could exploit the vulnerabilities in **personal data supporting assets** (e.g., the file management system that allows the manipulation of data)
- in a context of **threats** (e.g., misuse by sending emails)
- and allow **feared events** 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.)





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





Step 1: Context of personal data processing



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

- 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)



Step 2: Controls - Study of the fundamental principles



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

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



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



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

- 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.



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



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

- 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)



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



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



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



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



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

- 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



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



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



Variations regarding Data in Consideration



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

- 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



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



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



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.



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



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 |



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 |



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!

Appendix 8

Privacy by Design - Requirements Elicitation and Data Subjects' Rights



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



Privacy By Design Requirements Elicitations and Data Subjects' Rights

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





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

Agenda of the Seminar

- Introduction
- Privacy Requirements Elicitation Methodologies
- Personal Data Retention
- Data Subjects' Rights Management



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

Introduction



Legislation and Current Challenges

- Article 25 of the General Data Protection Regulation ‘Data protection by design and by default’
 - How can the system analysts and designers integrate in the software technical measures that are designed to implement data-protection principles in order to meet the regulatory requirements and protect the rights of data subjects?
 - How can the system analysts and designers integrate in the software measure ensuring that by default, only personal data which are necessary for each specific purpose of the processing are processed?
 - How can they integrate measures ensuring that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons?



The Concept of Privacy Requirements

- Privacy requirements are statements that reflect key privacy principles and objectives and specify capabilities and functions that a system must be able to perform
- Privacy requirements address privacy concerns and preferences, ensuring that users' privacy needs are met by introducing adequate control features
- Privacy requirements are generally in compliance with legislation or data privacy rules existing in a country



The Concept of Privacy Requirements

- Privacy requirements may differ depending on the requirements' elicitation methodology
- Privacy requirements elicitation methodologies are relevant to:
 - Requirements' analysts who specify privacy requirements and want to carry out the elicitation of these requirements in an easy way, avoiding ambiguities
 - Software developers who implement those requirements and should be able to understand them to discuss alternative options with the requirements analysts, especially if a particular privacy requirement is not possible to be implemented as it has been specified



The Concept of Privacy Requirements

- Despite the different approaches there is a consensus on the common privacy requirements, which are:
 - **Anonymity:** Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set. For example, an entity is non-identifiable within a set of entities when using system's resources and services
 - **Unlinkability:** An attacker cannot distinguish if two or more items of interest are related or not. For example, an entity can use system's resources and services without being associated with them
 - **Unobservability:** Undetectability of the item of interest against all subjects uninvolved in it and anonymity of the subjects involved in the item of interest even against the other subjects involved in that item of interest.
 - **Pseudonymity:** The function of using pseudonyms as user identifiers
 - **Undetectability:** An attacker cannot sufficiently distinguish if an item of interest exists or not. Undetectability ensures that an attacker cannot identify which user in a set of users is accessing the service
 - **Personal Data Protection:** The protection of personal data in accordance with regulation and standards



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

Privacy Requirements Elicitation Methodologies



Privacy Requirements Elicitation Methodologies



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

- Several techniques, methodologies, methods and tools have been introduced the past years
- Among the most popular ones are:
 - LINDUUN
 - SQUARE for Privacy
 - PriS
 - RBAC
 - STRAP
 - The i* method
 - Privacy Requirements Elicitation Technique (PRET)
 - Preparing Industry to Privacy by Design by supporting its Application in Research (PRIPARE)
 - Modelling and Analysis of Privacy-aware Systems (MAPaS Framework)
 - Goal-Based Requirements Analysis Method (GBRAM)



Privacy Requirements Elicitation Methodologies: LINDDUN



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

LINDDUN is threat-driven and classifies privacy requirements into hard and soft requirements:

- Hard privacy requirements: unlinkability, anonymity, pseudonymity, plausible deniability, undetectability, unobservability, confidentiality
- Soft privacy requirements: user content awareness and policy and consent compliance



Privacy Requirements Elicitation Methodologies: LINDDUN



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

- LINDDUN includes the identification of a list of potential privacy risks and the mapping of potential privacy risks with the components of the system
- LINDDUN considers seven categories of privacy requirements: Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance



Privacy Requirements Elicitation Methodologies: LINDDUN



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

- **Linkability:** Refers to an adversary being able to link two items of interest without knowing the identity of the data subject(s) involved
- **Subject Identifiability:** Refers to an adversary being able to identify a data subject from a set of data subjects through an item of interest
- **Non-Repudiation:** Refers to the data subject being unable to deny a claim (e.g., having performed an action, or sent a request)
- **Detectability:** Refers to an adversary being able to distinguish whether an item of interest about a data subject exists or not, regardless of being able to read the contents itself



Privacy Requirements Elicitation Methodologies: LINDDUN



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

- **Disclosure of information:** Refers to an adversary being able to learn the content of an item of interest about a data subject
- **Unawareness:** Refers to the data subject being unaware of the collection, processing, storage, or sharing activities (and corresponding purposes) of the data subject's personal data
- **Non-compliance:** The processing, storage, or handling of personal data is not compliant with legislation, regulation, and/or policy



Privacy Requirements Elicitation Methodologies: LINDDUN



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

LINDDUN consists of six distinct steps:

- Creating a system data-flow diagram
- Mapping privacy risks per component of the system data-flow diagram
- Extraction of misuse cases from the identified system privacy risks. Each case of system abuse includes a set of privacy risk scenarios.
- Risk assessment to assess identified privacy risks according to severity.
- Extraction of privacy requirements from the analysis of misuse cases
- Selection of Privacy Enhancing Technology (PET) per system misuse case



Privacy Requirements Elicitation Methodologies: SQUARE for Privacy

- The SQUARE (Security Quality Requirements Engineering) method was originally introduced to provide a framework for determining security requirements
- SQUARE focuses on identifying a system risk to deliver a set of security requirements
- SQUARE was adapted to meet the risk-based identification of system privacy requirements
- Introduces the terms: privacy goals, threat, risk, system assets



Privacy Requirements Elicitation Methodologies: SQUARE for Privacy

SQUARE comprises the following activities:

- Agreement on the definition of privacy between the stakeholders
- Identification of system assets and privacy objectives
- Collection of items that can describe the system, such as system architecture diagrams, use case scenarios, misuse cases, attack trees, user-roles hierarchies), etc.
- Preparation of risk assessment
- Selection of a technique for extracting privacy requirements, such as structured / semi-structured interviews, usage / mismanagement scenarios, application of variable systems methodology, the PRET technique, etc.



Privacy Requirements Elicitation Methodologies: SQUARE for Privacy

SQUARE comprises the following activities:

- Determination of the set of system privacy requirements (a questionnaire supported by the PRET technique is suggested)
- Categorization of privacy requirements in order to separate requirements from project constraints
- Classification of privacy requirements in order of priority to meet time constraints, resources, acceptable costs
- Inspection of the final set of requirements to address any ambiguities or ambiguities in the requirements



Privacy Requirements Elicitation Methodologies: PriS



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

- PriS is a security requirements engineering method, which incorporates privacy requirements early in the system development process
- PriS considers privacy requirements as organizational goals that need to be satisfied and adopts the use of privacy process patterns to:
 - (a) describe the effect of privacy requirements on business processes
 - (b) facilitate the identification of the system architecture that best supports the privacy-related business processes



Privacy Requirements Elicitation Methodologies: PriS



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

- Privacy requirements are considered a special type of goal, the privacy goal, which constraints the causal transformation of organizational goals into processes.
- There are eight types of privacy goals:
 - Authentication
 - Authorization
 - Identification
 - Data protection
 - Anonymity
 - Pseudonymity
 - Unlinkability
 - Unobservability



Privacy Requirements Elicitation Methodologies: PriS



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

- PriS comprises of the following activities:
 - Elicitation of the privacy goals that are relevant to the specific organization: Identification of the basic privacy concerns and interpretation of the general privacy requirements with respect to the specific context
 - Impact identification: Identification of the impact of privacy goals on organizational goals and on the relevant processes that realize these goals. Identification of privacy related processes that realize privacy goals
 - Modeling of privacy processes based on the relevant privacy process patterns
 - Definition of a system architecture that supports the privacy processes: Process patterns are used to identify the proper implementation technique(s) that best implement the corresponding processes



Privacy Requirements Elicitation Methodologies: PriS



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

- PriS assists in the application of privacy requirements in the organizational context
- PriS provides a systematic method to locate system architectures that can realize the privacy requirements.
- PriS comprises:
 - a formal definition model
 - graphical representation
 - a software tool



Privacy Requirements Elicitation Methodologies: RBAC



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

- RBAC is an agent-oriented framework for modelling privacy requirements
- Connects privacy requirements to organizational access control policies
- RBAC includes a context-based data model for representing roles that have permissions to access data objects and privacy elements linked to these objects
- Three privacy elements:
 - Purpose
 - Conditions
 - Obligations



Privacy Requirements Elicitation Methodologies: RBAC



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

- RBAC also provides a goal-driven role engineering process for eliciting and modelling privacy elements:
 - Role Permission Analysis
 - Identification of task by each role based on goal-oriented, scenario analysis and association of the tasks with RBAC permissions
 - The events of each scenario are modeled as RBAC permissions, and the actors of the events are modelled as RBAC roles
 - Role Permission Refinement
 - Refinement of identified set of roles and permissions
 - Identification of associated privacy elements
- RBAC is not supported by formal models
- RBAC is partially supported by a software tool



Privacy Requirements Elicitation Methodologies: STRAP



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

- STRAP (STRuctured Analysis of Privacy) aims to elicit and analyze privacy requirements during system design phase
- In STRAP privacy requirements are represented as vulnerabilities
- STRAP builds a goal-model that represents all functional requirements
- Vulnerabilities have the form of obstacles between the goals and the subgoals in the goal-model
- STRAP is not supported by formal models or software tool



Privacy Requirements Elicitation Methodologies: STRAP



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

- STRAP comprises the following activities:
 - Analysis:
 - Analysis of all system goals
 - The result of this phase is the identification of all goals, the active entities and the basic system components
 - Identification of information regarding the context and development of the first set of privacy requirements
 - Identification of system vulnerabilities regarding privacy protection
 - Vulnerabilities are recorded as obstacles between the goals and the subgoals



Privacy Requirements Elicitation Methodologies: STRAP



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

- STRAP comprises the following activities:
 - Refinement:
 - Elimination of the set of vulnerabilities by deleting all vulnerabilities for which a solution is easy to implement
 - Evaluation:
 - Assessment of system design scenarios based on how the design scenario overcomes the vulnerability. The best scenario is the one that eliminates the most vulnerabilities
 - Iteration:
 - Repetition of the previous steps to identify possible alterations
 - Re-examination of the goal structure
 - Identification of alterations
 - Re-definition of vulnerabilities
 - Generation of new system design scenarios
 - Stops when no alterations are identified



Privacy Requirements Elicitation Methodologies: The i^* method



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

- The i^* method is agent-oriented in the sense that it focus on systems agents and their social interdependencies
- The method was originally designed as tool for modelling, analyzing and redesigning organization processes
- It has been used for modelling security and privacy requirements
- The i^* method focuses on individual goals of system actors
- System actors are interdependent



Privacy Requirements Elicitation Methodologies: The i* method



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

- The i* method comprises the following activities:
 - Initial construction of a domain model, in terms of the actors involved and their dependencies
 - Security analysis:
 - Attacker analysis to identify potential system abusers and their malicious intents
 - Dependency vulnerability analysis to detect vulnerabilities in terms of organizational relationships among stakeholders
 - Countermeasure analysis to support the dynamic decision-making process of addressing vulnerabilities and threats
 - Refinement of the domain model
 - Evaluation regarding if the impact of threats and vulnerabilities has been eliminated to an acceptable level
 - Role-based access control analysis to specify actor roles
- The i* method is supported by formal meta-model and the OME software tool



Privacy Requirements Elicitation Methodologies: PRET



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

- The Privacy Requirements Elicitation Technique (PRET) was developed to support the identification and classification of privacy requirements in a system
- PRET uses a database that records the privacy requirements arising from various privacy laws and policies
- PRET uses a questionnaire and creates a list of prioritized privacy requirements



Privacy Requirements Elicitation Methodologies: PRET



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

- The technique is supported by a software tool (PRET tool) which uses a questionnaire to extract information about the system to be developed
- Software engineers and project stakeholders complete a second questionnaire on privacy requirements
- The tool correlates the given privacy requirements with its database and displays the results so that engineers can adapt the privacy requirements to those of the system under development



Privacy Requirements Elicitation Methodologies: MAPaS



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

- Modeling and Analysis of Privacy-aware Systems (MAPaS) is model-based method
- MAPaS is based on the concept of purpose, which is the reason for the collection and use of data of a system
- MAPaS uses a privacy-aware Modeling Language (PaML) and a set of functions that assist analysts in identifying privacy requirements from the system design phase
- MAPaS also uses the Atlas Transformation Language (ATL) toolkit



Privacy Requirements Elicitation Methodologies: MAPaS



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

- ATL supports two functions for MAPaS:
 - Creation of target models from a set of source models, using transformation rules
 - Creation of queries in order to extract properties from models
- The MAPaS modeling includes three activities:
 - Creation of editing and visualizing models with PaML (using the IBM RSA editing tool)
 - Validation of the PaML model or its key components (using the graphical interface of MAPaS)
 - Analysis of PaML models through a set of analysis queries (using the ATL toolkit)



Privacy Requirements Elicitation Methodologies: GBRAM



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

- GBRAM is goal-oriented that provides a systematic approach for identifying and refining the goals that software systems must achieve, managing trade-offs among the goals, and converting them into operational requirements
- GBRAM includes a process called ‘goal mining’:
 - Analysis of privacy policies to systematically extract privacy requirements and goals underlying organizations’ privacy practices
 - Classification of privacy requirements based on a privacy taxonomy into either protection goals or vulnerabilities
 - Protection goals express the effort declared by an organization to honor/respect its customers’ privacy
 - Vulnerabilities reflect potential threats to customer privacy as derived from current organization practices such as information collection, storage and transfer



Privacy Requirements Elicitation Methodologies: GBRAM



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

- GBRAM includes a process called ‘goal mining’:
 - Analysis of privacy policies to systematically extract privacy requirements and
 - Operationalization of privacy goals into system requirements, using:
 - scenario analysis
 - identification of goal obstacles and constraints
 - refinement strategies via heuristics, guidelines and recurring question types
 - Alignment of privacy requirements to privacy policies: assessment of the degree of compliance between requirements and policy statements, resolution of conflicts and ambiguities
- GBRAM is not supported by formal models.
- GBRAM is supported by a software tool called SMaRT (Scenario Management and Requirements Tool)



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

Personal Data Retention



Data Retention

- When developing an Information System or establishing a processing activity, and while the purpose of data processing is set, the organisation must check / determine the retention period for the processed data.
 - It is necessary to record the criteria used for determining the retention period
- It is necessary to establish a notification procedure (preferably automatic) that signals the expiration of the retention period
- A methodology for secure deletion of the data should be in place



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

Data Subjects' Rights Management



Data Subjects' Rights Management

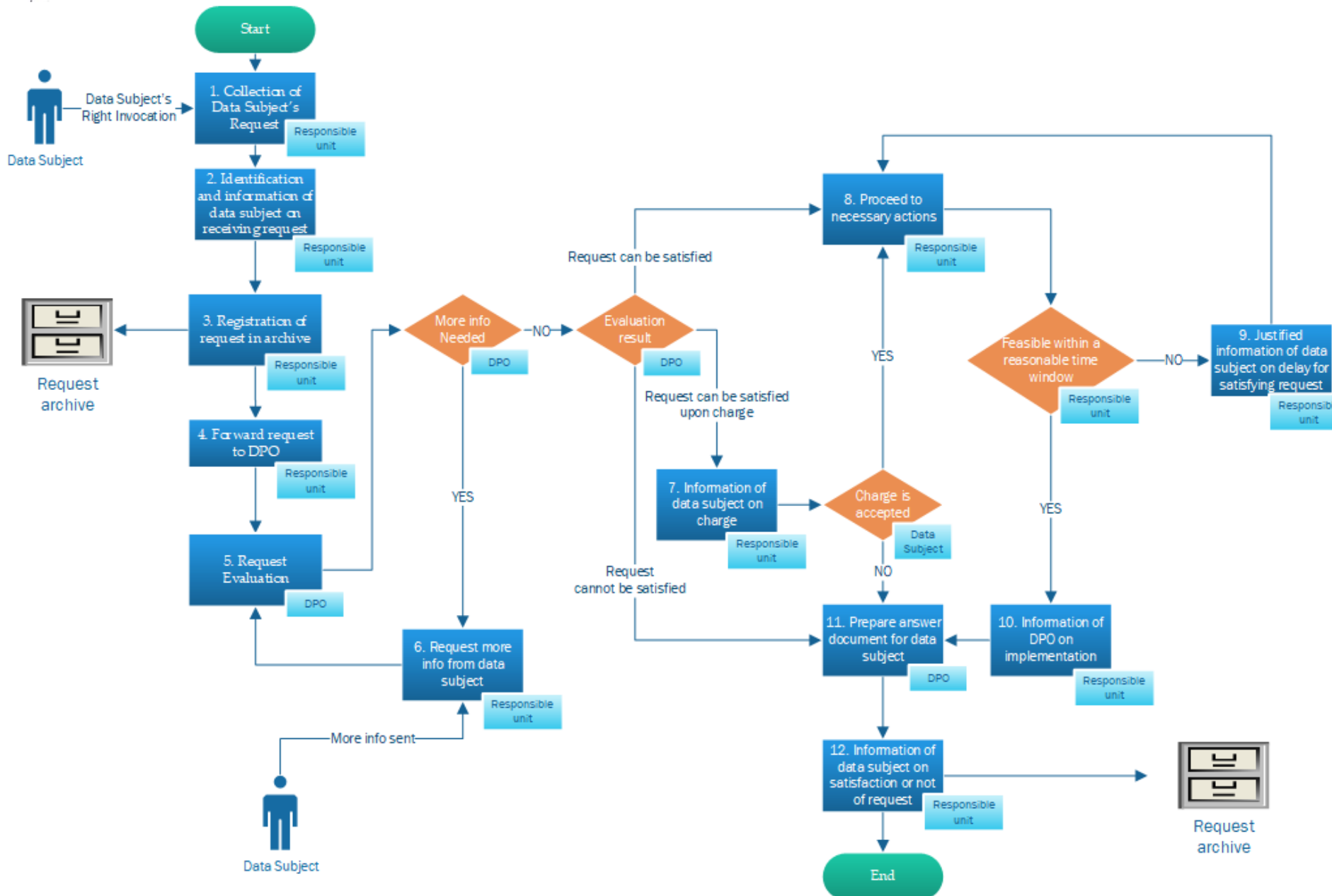
- In order for an organization to be able to manage the requests of the Data Subjects who use their services, concerning the exercise of their rights, it must follow a specific procedure.
 - Initially, it should identify the details of the Data Subjects, then
 - evaluate their requests and finally,
 - decide whether to satisfy them or not, while also informing them.



Data Subjects' Rights Management



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





Data Subjects' Rights Management:



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

Step 1: Collection of Data Subject's Request

- The Data Subject submits, via the available channels, his/her request regarding his/her personal data, in order to exercise his/her corresponding right(s). The communication channels that the Data Subjects can use are (indicatively):
 - Physical Presence: The Data Subject completes a standardised form on the premises of the organization.
 - Website: The Data Subject, after visiting the website of the organization, completes an online form.
 - Mail (physical or electronic): The Data Subject can exercise one of its rights by writing free text and sending it to the organization via mail (postal address) or via e-mail.



Data Subjects' Rights Management:



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

Step 2: Identification and information of the Data Subject for the reception of the request

- Upon reception of the request, the responsible department / person must, within a reasonable time, proceed to identify the Data Subject who filed the request.
- Indicative required information for the identity of the Data Subject is:

| Communication channel | Identification data |
|---------------------------------|--|
| Physical presence | Identity card, passport, etc. |
| Website | Phone communication and identification based on the existing identification process via phone. |
| Mail (postal address or e-mail) | Phone communication and identification based on the existing identification process via phone. |

- Once the Data Subject has been identified, the organization must manage the request and respond within thirty (30) days, with the possibility of extending additional sixty (60) days.



Data Subjects' Rights Management:



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

Step 3: Registration of the request in the requests record

- The department / responsible person who received the request of the Data Subject, registers it in the "Requests record". For each request, the following information must be recorded:
 - Identification of the Data Subject (identity card, passport, driving license, etc.).
 - The type of the exercised right (right of access, right of rectification, erasure, etc.).
 - The channel through which the request was received.
 - If the Data Subject wishes to receive the answer to its request through a specific communication channel.
 - Useful details and information about the request of the Data Subject.
 - If the Data Subject's request has been assessed as excessive or without appropriate legal basis/ grounds, the reasons that led to this result.
 - The date of receipt of the request.
 - The date the Data Subject was identified.
 - The date of the response.
 - The channel through which the response was sent to the Data Subject.



Data Subjects' Rights Management:

Step 4: Forwarding the request to the Data Protection Officer



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

- All requests of the Data subjects, regardless of the channel through which they were submitted and of the responsible department / person who received it, must be sent to the Data Protection Officer so that his/her assessment is carried out and the necessary further actions are taken.



Data Subjects' Rights Management:



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

Step 5: Evaluation of the Request

- At this stage of the process, the Data Protection Officer, upon receipt of the request of the Data Subject, is responsible for thoroughly assessing the request to decide whether to proceed with its satisfaction or whether he/she needs additional information from the Data Subject in order to effectively assess the request.
- If the available information is considered incomplete and additional information from the Data Subject is required, the procedure continues to Step 6.
- For the assessment, the Data Protection Officer must seek the necessary information through the available information systems and / or to get in contact with the departments of the organization which may be related to the request of the Data Subject.



Data Subjects' Rights Management:



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

Step 5: Evaluation of the Request

- After the Data Protection Officer has assessed the subject's request she/he can classify it as "Request can be settled", "Request can be settled but a charge is raised for the subject", or "Request cannot be settled".

| REQUEST ASSESSMENT TABLE | | |
|--|---|--|
| Request | Description | Examples of requests |
| Request can be settled | Request that can be implemented within the foreseen timeframe (30 days). | <ul style="list-style-type: none">• Data rectification• Data access• Limitation of data processing |
| Request can be settled but a charge is raised for the data subject | Request that is excessive (e.g., due to its repetitive character). | <ul style="list-style-type: none">• Multiple copies of data (X times over Y months) |
| Request cannot be settled | Unjustified request or request that is excessive (e.g., due to its repetitive character). | <ul style="list-style-type: none">• The subject has access to his data, but this will result in the disclosure of personal data of a third party.• The subject has exercised the right to the portability of his data but has previously requested the erasure of the data.• See followingTable: Legal basis and Exercise of rights of Data Subjects |



Data Subjects' Rights Management:



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

Step 5: Evaluation of the Request

- The following table shows the ability to exercise the rights of the subjects, which arises in relation to the legal basis of processing. The requests which cannot be met for this reason are considered unjustified.

| LEGAL BASIS | RIGHT OF ACCESS | RIGHT TO RECTIFICATION | RIGHT TO ERASURE | RIGHT TO RESTRICTION | RIGHT TO PORTABILITY | RIGHT TO OBJECT | RIGHT TO OBJECT (DIRECT MARKETING) |
|---------------------------|-----------------|------------------------|------------------|----------------------|----------------------|-----------------|---------------------------------------|
| Consent | √ | √ | √ | √ | √ | x | √ (withdrawal of consent) |
| Performance of a contract | √ | √ | √ | √ | √ | x | √ |
| Legal obligation | √ | √ | x | √ | x | x | √ |
| Legitimate interest | √ | √ | √ | √ | x | √ | √ |
| Vital interest | √ | √ | x | √ | x | x | √ |
| Public interest | √ | √ | √ | √ | x | √ | √ |

- If the request is assessed as “Request can be settled but a charge is raised for the subject”, the procedure continues to Step 7 of this procedure. If the Data Subject's request is assessed as “Request can be settled”, the process continues to Step 8. Finally, if the request is assessed as “Request cannot be settled”, the procedure continues to Step 11 of the procedure.



Data Subjects' Rights Management:



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

Step 6: Requesting additional information from the Data Subject

- If the available information when assessing the request is incomplete, then the competent department of the organization requests additional information from the Data Subject. Once the Data Subject provides the necessary information, the procedure continues to Step 5.



Data Subjects' Rights Management:



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

Step 7: Informing the Data Subject of a charge to process the request

- The competent department of the organization informs the Data Subject that their request will be processed only if they pay a reasonable amount corresponding to the complexity of their request. If the Data Subject accepts the charge, the process continues to Step 8. Otherwise, the procedure continues to Step 11.



Data Subjects' Rights Management:



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

Step 8: Performing the required actions

- The organization must be able to satisfy the rights of the Data Subjects via printed or electronic media.
- In order to satisfy the right to information and the right of access, the organization should employ specific templates.
- In order to satisfy the rights of rectification, erasure, objection, limitation of processing, data portability, the organization, in cooperation with the Data Protection Officer, should develop technical mechanisms to support these requests.
- The organization should maintain a “Requests record” where details of how each data subject’s request has been satisfied can be found.



Data Subjects' Rights Management:

Step 9: Justified information to the Data Subject for delaying the satisfaction of their request



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

- The competent department is responsible for informing the Data Subject in case that their request cannot be satisfied within the period of thirty (30) days specified by the GDPR. This update must contain documented reasons regarding the delay of the satisfaction of the Data Subject's request.
- The procedure continues to Step 8.



Data Subjects' Rights Management:



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

Step 10: Informing the DPO regarding the implementation

- Once the competent department or departments have completed all the required actions for the satisfaction of the Data Subject's request, they must inform the Data Protection Officer that the request has been served and that no further actions are required from their part.
- The process continues to Step 11.



Data Subjects' Rights Management:

Step 11: Prepare the response document for the Data Subject



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

- The Data Protection Officer must analyse all available information, whether the source is the Data Subject or deriving from the actions of the competent departments of the organization, and prepare the response to the Data Subject. These actions are carried out in any case; fulfilment of the request or not.
- The process continues to Step 12.



Data Subjects' Rights Management:

Step 12: Informing the Data Subject regarding the fulfilment or not of the request



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

- The competent department of the organization must inform the Data Subject appropriately for the fulfilment or not of his/her request. The response can be communicated:
 - By letter to the designated postal address of the Data Subject
 - Electronically, either if the Data Subject has requested so or if the request has been submitted by electronic means.
 - Orally, if the Data Subject has requested so.
- Finally, the competent department updates the requests record, so that the request is properly marked as fulfilled. It is noted that this record proves that the Data Subject's request has been investigated promptly and the necessary actions have been taken.



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

Thank you for your participation!

Appendix 9

Encryption – Anonymization – Pseudonymization



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

Encryption- Anonymization – Pseudonymization

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





Agenda of the Seminar

- Symmetric Encryption
- Asymmetric Encryption
- Hash - MAC - Digital Signatures - TLS
- PGP and Deriving Pseudonyms
- VPN and IPSec
- Anonymization - Pseudonymization



Cryptography is present in...

- Surfing the Internet (see <https>)
- Mobile communications
- Wireless networks (802.11x, Bluetooth, ...)
- Electronic payments
- Electronic mail
- Enterprise security
- Military networks
- E-voting
- Teleconferences (VoIP applications)
- Virtual Private Networks (VPN)
- Cryptocurrency (Bitcoin,...) – Distributed Ledger Technology
- Internet of Things – IoT
- eHealth applications



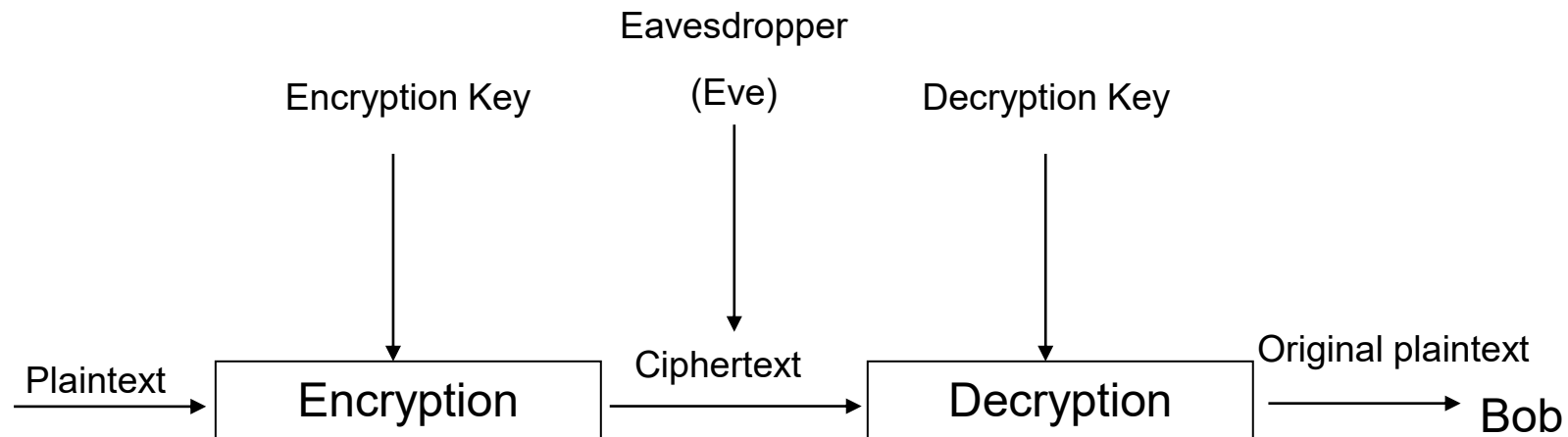
Basic Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext without knowing key
- **cryptology** - the field of both cryptography and cryptanalysis



Key-based ciphers

- Ciphers use one (or more) keys.



- The security rests with the secrecy of the key – the encryption and decryption algorithms can be publically known (Kerchoff's principle).



Types of Cryptographic Algorithms

- Symmetric (or private) key algorithms
 - The same key is being used for both encryption and decryption
 - Examples: AES, DES, 3DES, RC4, ...
- Asymmetric (or public key) algorithms
 - The decryption key is different from the encryption key
 - A totally different underlying idea from the symmetric cryptography
 - Examples RSA, Elliptic curve cryptography, ...



A Mathematical Formulation

If E and D denote the encryption and decryption respectively, then:

- $E_{K_1}(m) = c$
- $D_{K_2}(c) = m$

where m and c are the plaintext and the ciphertext respectively.

The indexes K_i imply that the results are dependent on the key each time.

The following property holds:

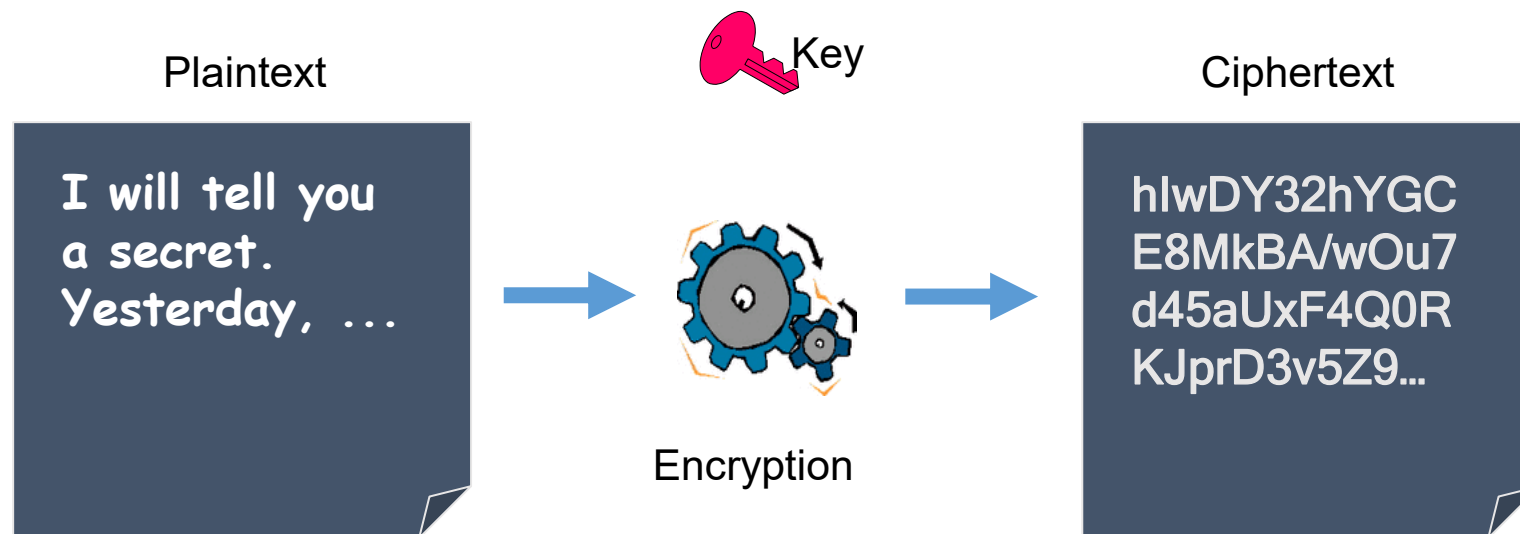
$$D_{K_2}(E_{K_1}(m)) = m$$

In symmetric-key ciphers, we have $K_1 = K_2$



Symmetric encryption

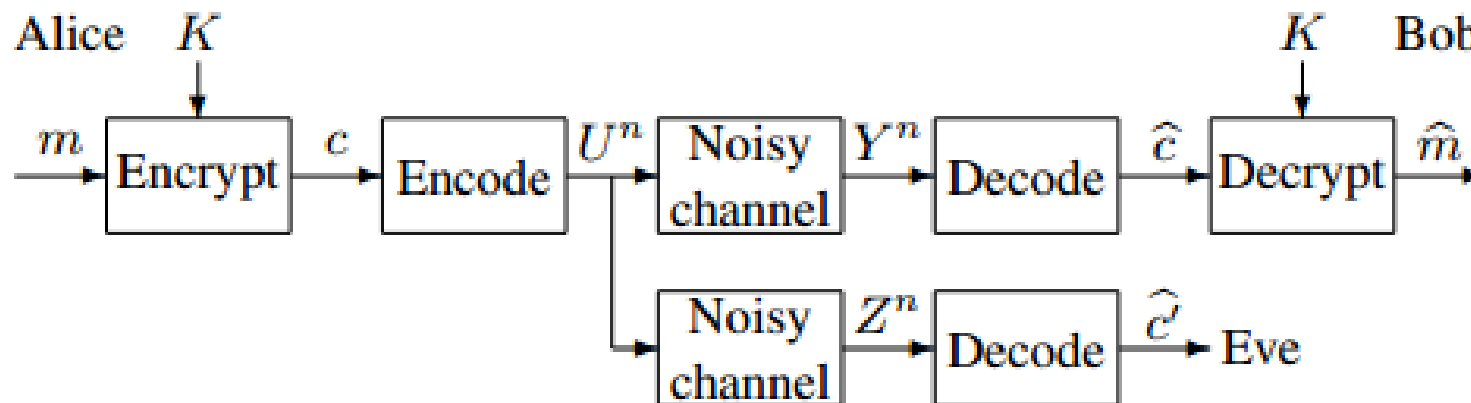
- The security rests with the secrecy of the key – the encryption and decryption procedures (algorithms) are public!





Encryption in a telecommunications channel

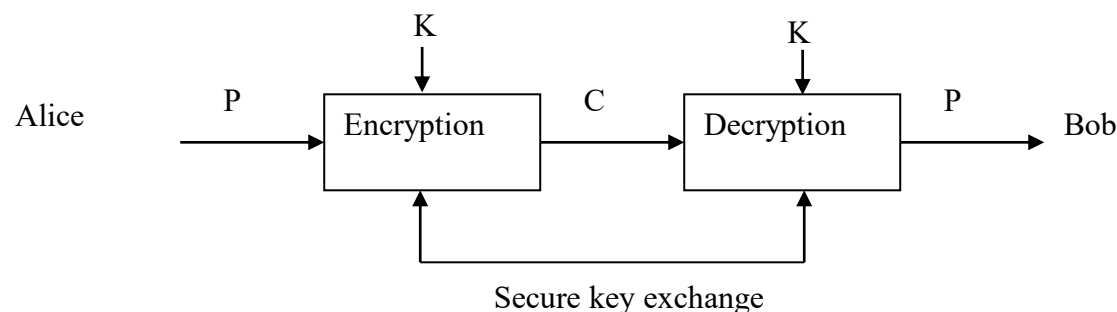
- Typical case: the message is encrypted and subsequently encoded (error-control coding), to detect/correct errors introduced by the channel
- However, there are also other options:
 - Encryption after the error control coding
 - Simultaneous encryption and error-control coding
 - Physical-layer encryption





How to securely exchange the secret key?

- A «secure channel» is needed for performing key exchange
 - Great challenge – if a secure channel was in place, then we would not need encryption at all





Defining the strength of a cipher

- **Unconditional security**

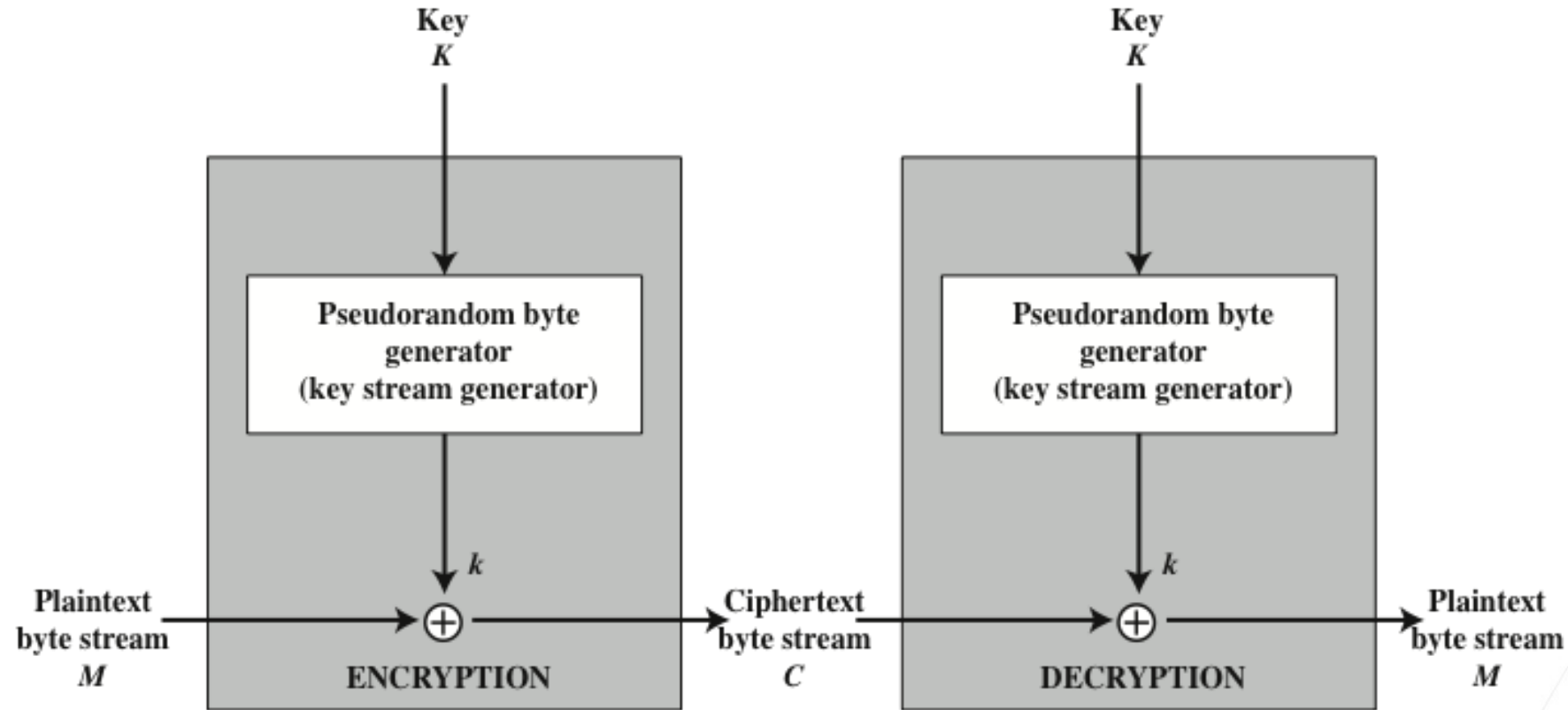
- no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext

- **Computational security**

- given limited computing resources (e.g. time needed for calculations is greater than age of universe), the cipher cannot be broken



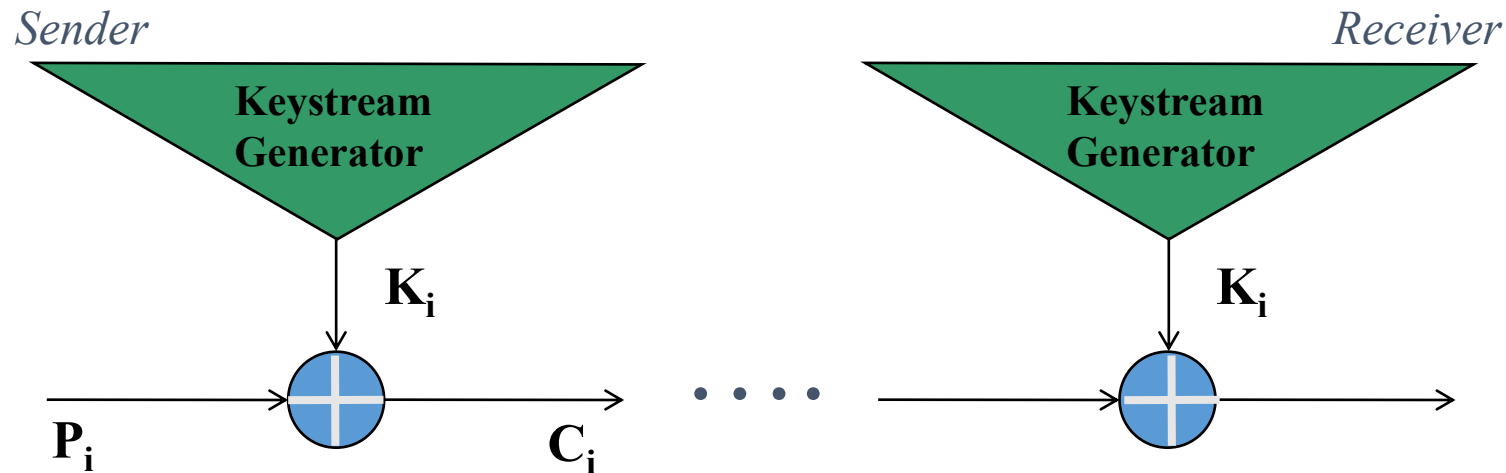
Stream Ciphers



They try to resemble the one-time pad



A typical case of a stream cipher



- Encryption is being performed bit-by-bit (or byte-by-byte)
 - A keystream generator is being used, to produce a “random” sequence (keystream)
 - Keystream bits are being XOR-ed with the bits of the plaintext, so as to produce the ciphertext
 - Encryption: $C_i = P_i \oplus K_i$
- The decryption is similarly performed (the recipient has the same keystream generator, producing the same keystream):
 - Decryption: $P_i = C_i \oplus K_i$
- Example: For keystream 00110010..... and plaintext 11000110, the ciphertext will be 11110100



Applications of stream ciphers

- Suitable in applications with memory and power restrictions, as well as with requirements for high speed
- Examples
 - WiFi networks
 - (Older) Mobile communications (GSM, 3G)
 - Bluetooth
 - RFID networks
 - IoT
- Also used in Web (RC4, ChaCha20)



Known stream ciphers

- Probably the most known is RC4
- Used for more than 2 decades in several applications
 - WEP, WPA, TLS, ...
- However, some weaknesses were known
 - Some non-random properties of the keystream, etc.
 - For vulnerabilities of RC4 in Microsoft Office products, see https://www.schneier.com/blog/archives/2005/01/microsoft_rc4_f.html
- RC4 found insecure in 2013, with regard to the security protocol SSL/TLS
 - For more information: <http://www.isg.rhul.ac.uk/tls/>
- Later on, several other weaknesses have been found out (<https://www.rc4nomore.com/>)
- Not is it well-known that RC4 should not be used
- RFC 7465 (February 2015): RC4 is considered to be “on the verge of becoming practically exploitable...[and] can no longer be seen as providing a sufficient level of security for TLS sessions.”
- In TLS 1.3 (latest version), RC4 has been replaced by Chacha20



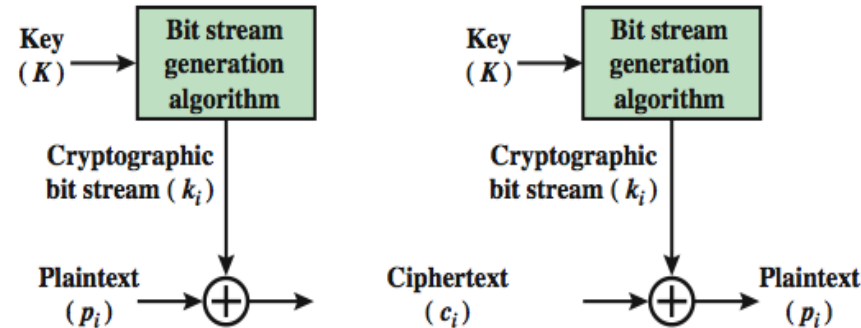
The RC4 cipher

- Variation in key sizes
 - From 40 up to 256 bits
- The keystream generator is mainly based on a register S with 256 entries, which initially contains the numbers from 0 to 255 in an ordered fashion (each entry corresponds to 1 byte = 8 bits)
- Based on the key, the entries of S are being permuted
- The keystream is being obtained by a specific rule (described next), based on this permuted version of the register

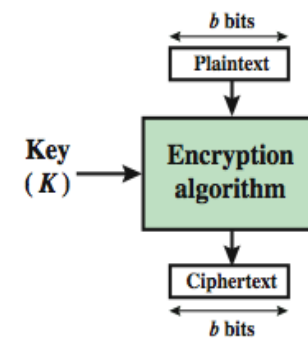


From stream ciphers to block ciphers

- Block ciphers perform encryption on a block (and not on a bit) basis
- Encryption is much more complex than a simple XOR addition



(a) Stream Cipher Using Algorithmic Bit Stream Generator

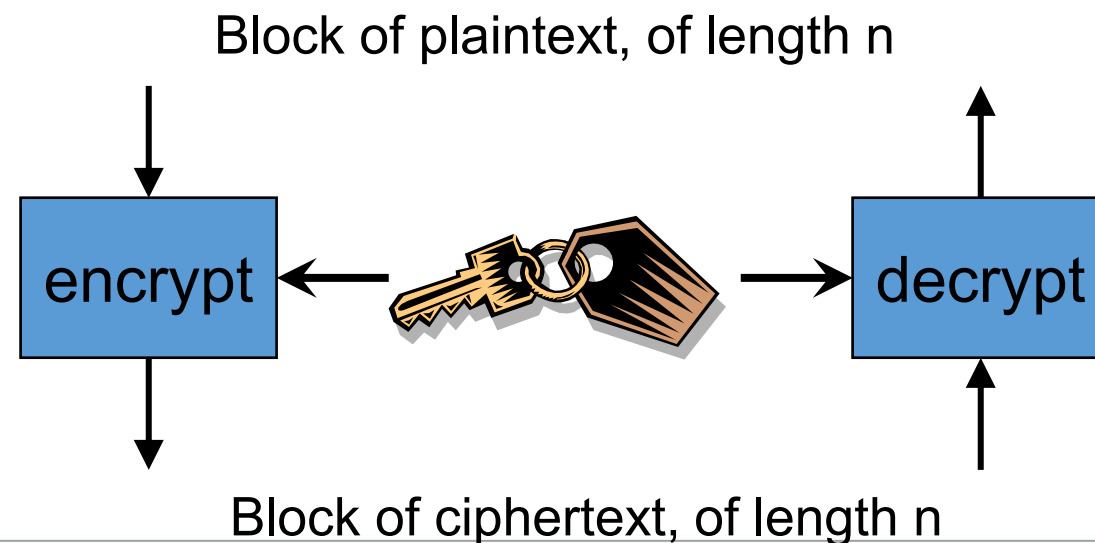


(b) Block Cipher



Block ciphers

- The initial message is being “splitted” into blocks of fixed size, whereas each block is being encrypted separately
 - Typical size of block: 128 bits
- Encryption (and decryption) is a complex operation over the input block





Motivation

- A block cipher operates on a block of n bits.
- It produces a ciphertext block of n bits.
- There are 2^n possible different plaintext/ciphertext blocks.
- The encryption must be reversible. i.e.
 - decryption to be possible.
 - each plaintext must produce a unique ciphertext block. (one-to-one correspondence)



Reversible vs. Irreversible

Reversible Mapping

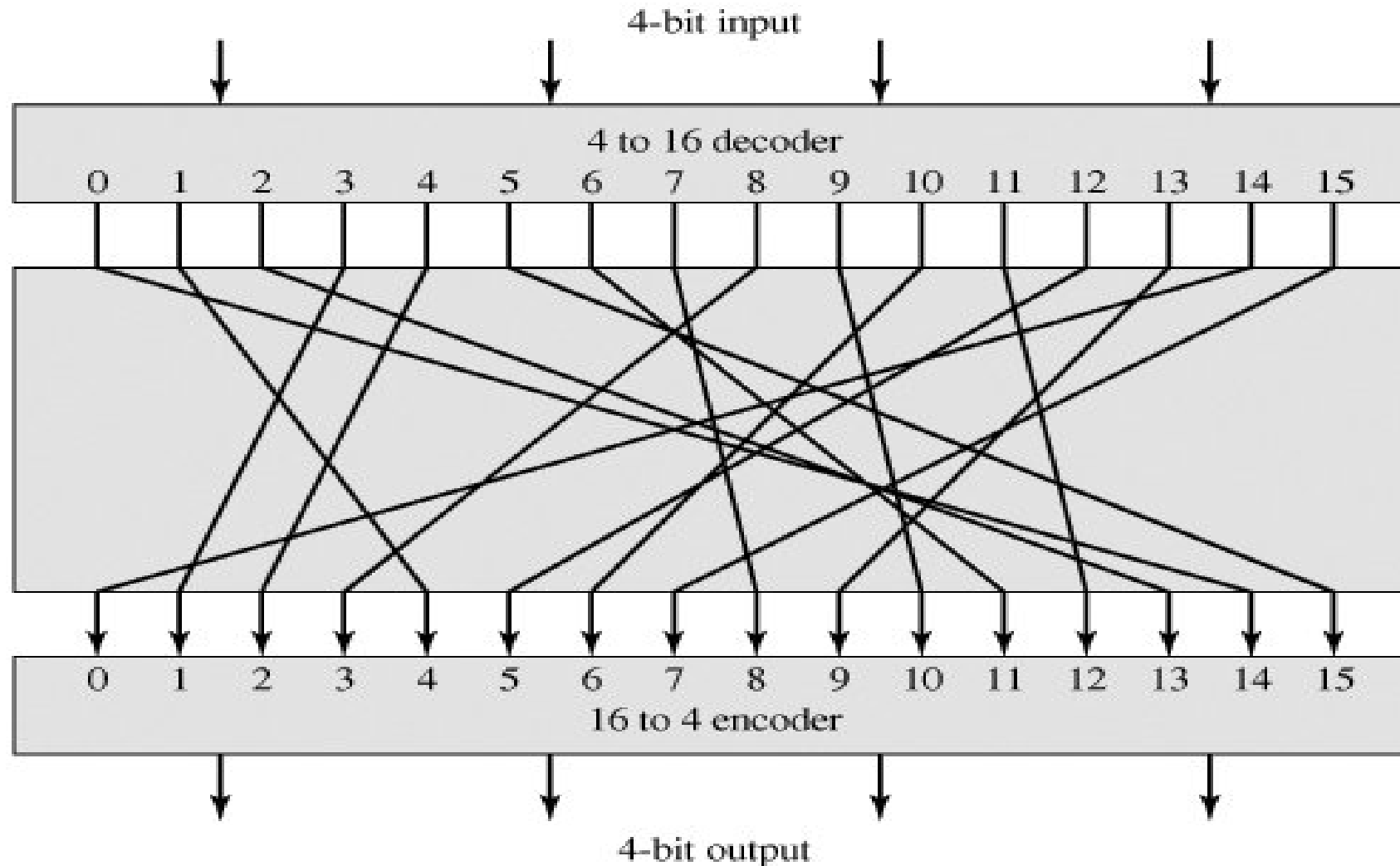
| Plaintext | Ciphertext |
|-----------|------------|
| 00 | 11 |
| 01 | 10 |
| 10 | 00 |
| 11 | 01 |

Irreversible Mapping

| Plaintext | Ciphertext |
|-----------|------------|
| 00 | 11 |
| 01 | 10 |
| 10 | 01 |
| 11 | 01 |



Ideal Block Cipher (a general substitution cipher)





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

Encryption/Decryption Table for Substitution Cipher

| Plaintext | Ciphertext |
|------------------|-------------------|
| 0000 | 1110 |
| 0001 | 0100 |
| 0010 | 1101 |
| 0011 | 0001 |
| 0100 | 0010 |
| 0101 | 1111 |
| 0110 | 1011 |
| 0111 | 1000 |
| 1000 | 0011 |
| 1001 | 1010 |
| 1010 | 0110 |
| 1011 | 1100 |



Problems with Ideal Cipher

- If a small block size, such as $n = 4$, is used, then the system is equivalent to a classical substitution cipher
→ Easy attack (statistical analysis of the plaintext)
- If large block size is used → not practical (for implementation and performance)
 - Huge encryption/decryption tables
 - → Huge key:
 - for $n = 4$, key size = 4 bits x 16 rows = 64 bits
 - for $n = 64$, key size = $64 \times 2^{64} = 2^{70} = 10^{21}$ bits



Block ciphers in practice

- Aim: Easily implementable structures that resemble somehow the ideal cipher
- A key of size k bits is being used
 - Hence, the possible mappings are 2^k είναι οι πιθανές αντιστοιχίσεις (less than $2^n!$ which is the number of all possible mappings)
- The encryption process is being iterated many times
- Key-dependent permutations and substitutions are involved in this process



Data Encryption Standard (DES)

- most widely used block cipher in world for almost two decades
- adopted in 1977 by NBS (now NIST)
 - as FIPS PUB 46
- encrypts 64-bit data using 56-bit key
- has widespread use
- has been considerable controversy over its security
- Now deprecated due to short key

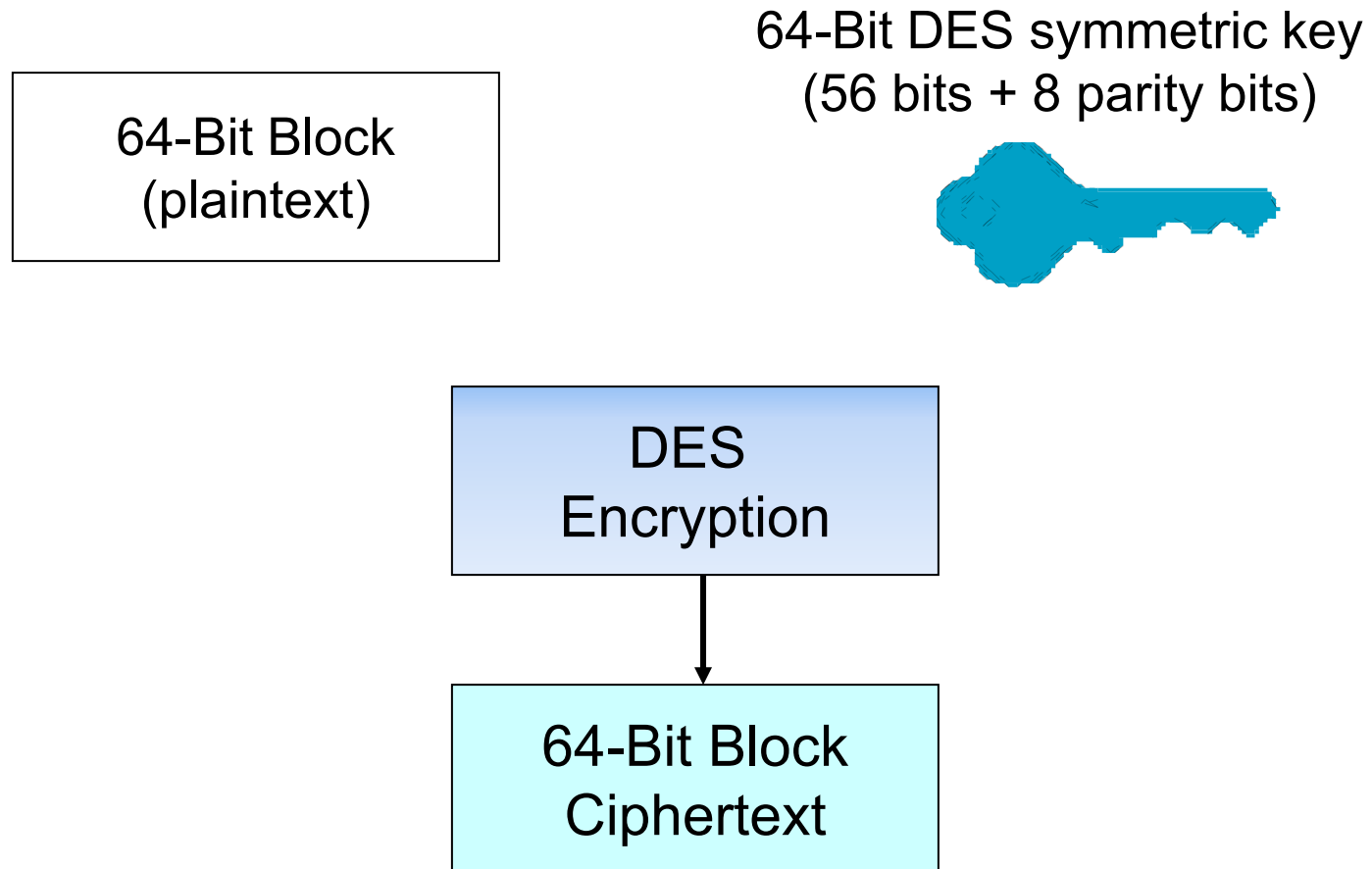


DES History

- IBM developed Lucifer cipher
 - by team led by Feistel
 - used 64-bit data blocks with 128-bit key
- then redeveloped as a commercial cipher with input from NSA and others
- in 1973 NBS issued request for proposals for a national cipher standard
- IBM submitted their revised Lucifer which was eventually accepted as the DES
 - Accepted as standard by NIST in 1976
 - Renew every five years



Data Encryption Standard (DES)



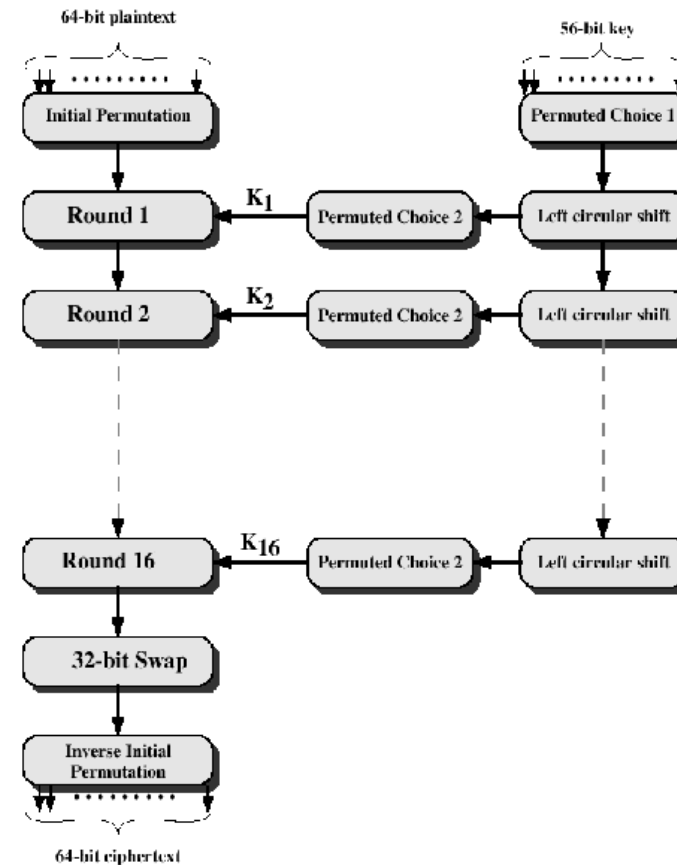


Data Encryption Standard (DES)



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

- Feistel networks
- 64-bit blocks
- 56-bit key
- 16 rounds
- An initial permutation at the beginning (and the reverse permutation at the end)
- At each round, a 48-bit subkey is being used



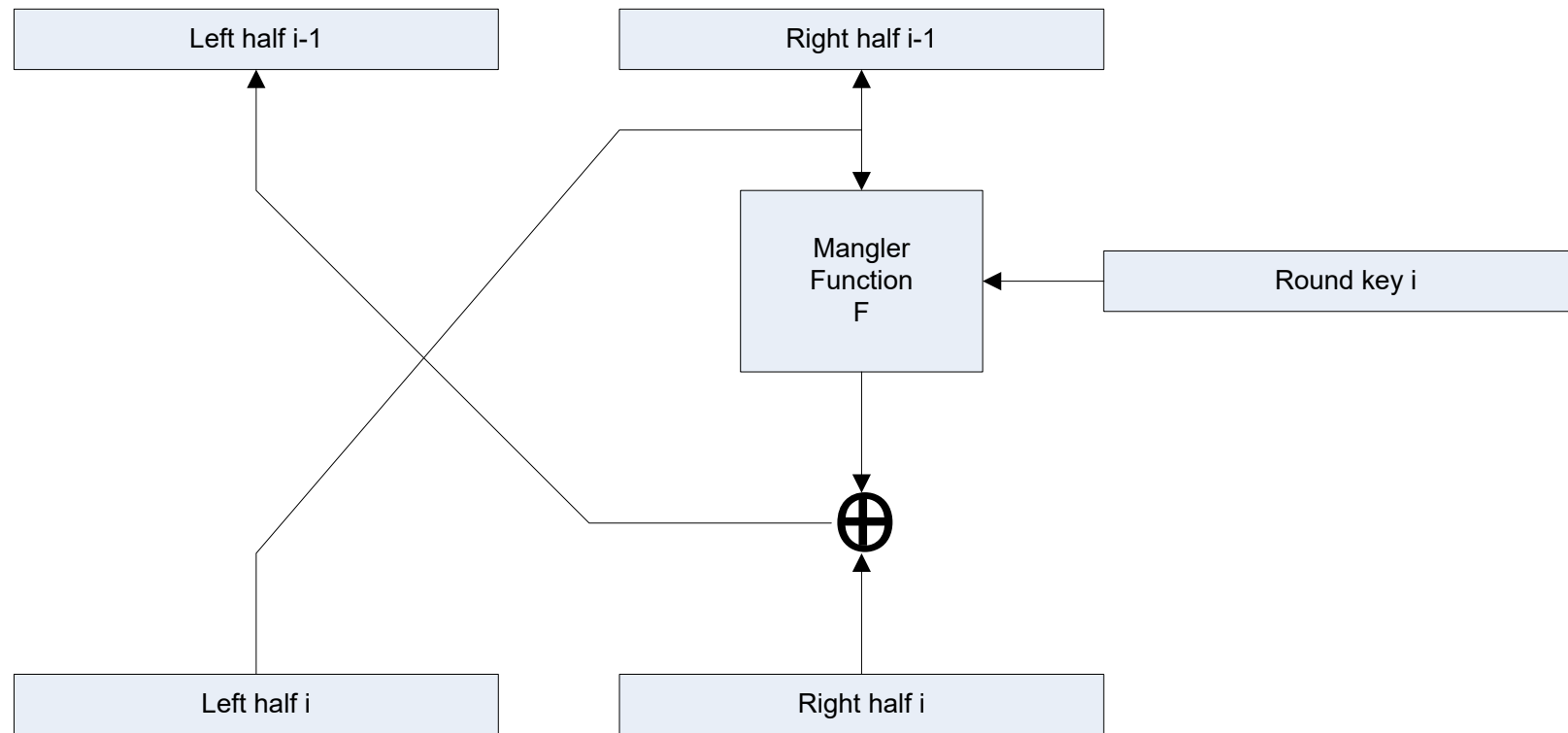


DES Decryption

- decrypt must unwind steps of data computation
- with Feistel design, do encryption steps again using subkeys in reverse order (SK16 ... SK1)
 - IP undoes final FP step of encryption
 - 1st round with SK16 undoes 16th encrypt round
 -
 - 16th round with SK1 undoes 1st encrypt round
 - then final FP undoes initial encryption IP
 - thus recovering original data value



DES Round Decryption



Decryption



DES Example

| Round | K_i | L_i | R_i |
|------------------|------------------|----------|----------|
| IP | | 5a005a00 | 3cf03c0f |
| 1 | 1e030f03080d2930 | 3cf03c0f | bad22845 |
| 2 | 0a31293432242318 | bad22845 | 99e9b723 |
| 3 | 23072318201d0c1d | 99e9b723 | 0bae3b9e |
| 4 | 05261d3824311a20 | 0bae3b9e | 42415649 |
| 5 | 3325340136002c25 | 42415649 | 18b3fa41 |
| 6 | 123a2d0d04262a1c | 18b3fa41 | 9616fe23 |
| 7 | 021f120b1c130611 | 9616fe23 | 67117cf2 |
| 8 | 1c10372a2832002b | 67117cf2 | c11bfc09 |
| 9 | 04292a380c341f03 | c11bfc09 | 887fbc6c |
| 10 | 2703212607280403 | 887fbc6c | 600f7e8b |
| 11 | 2826390c31261504 | 600f7e8b | f596506e |
| 12 | 12071c241a0a0f08 | f596506e | 738538b8 |
| 13 | 300935393c0d100b | 738538b8 | c6a62c4e |
| 14 | 311e09231321182a | c6a62c4e | 56b0bd75 |
| 15 | 283d3e0227072528 | 56b0bd75 | 75e8fd8f |
| 16 | 2921080b13143025 | 75e8fd8f | 25896490 |
| IP ⁻¹ | | da02ce3a | 89ecac3b |



Undesirable properties of DES

- 4 weak keys
 - (e.g. 00....011...1)
 - They produce identical subkeys
- 12 semi-weak keys
 - Key pairs that encipher a plaintext into the same ciphertext
- Complementary property
 - $DES_k(m) = c \Rightarrow DES_{k'}(m') = c'$
- NIST had changed the initial S-boxes as submitted by the IBM, and this raised some concerns (for possible trapdoors)
 - However, the subsequent research analysis indicated that S-boxes have nice cryptographic properties



Cryptanalysis in DES

- Being international standard for almost two decades, many researchers focused on fully analysing the cryptographic strength of DES
- Two important cryptanalytic techniques occurred (they will not be studied here):
 - Differential cryptanalysis – Biham and Shamir (1990)
 - Linear cryptanalysis – Matsui (1993)
- Any new cipher should be examined against these techniques
 - DES proved to be secure against them
 - DES designers stated that differential cryptanalysis had been already considered when designing their cipher, almost 15 years before Biham and Shamir come up with it!
 - But linear cryptanalysis was something new



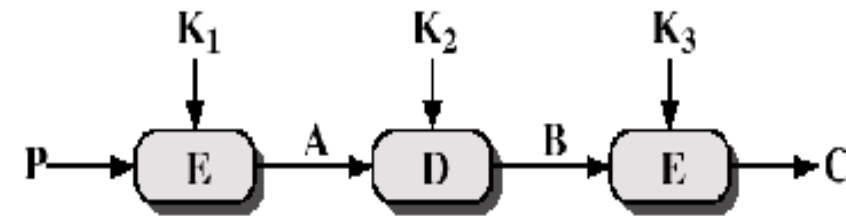
Strength of DES today – Insecure

- 56-bit keys have $2^{56} = 7.2 \times 10^{16}$ values
- brute force search looked hard in 1976, but:
 - in 1997 on Internet in a few months
 - in 1998 on dedicated h/w (EFF) in a few days
 - in 1999 above combined in 22hrs!
- NIST officially announced the end of DES in 2004
 - See also Bruce Schneier's blog:
http://www.schneier.com/blog/archives/2004/10/the_legacy_of_d.html

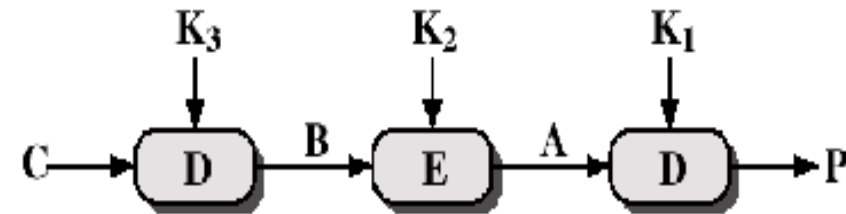


Triple DES (3DES) - 168

- 3 encryptions, with 3 distinct keys
- Hence, the key size in 3DES είναι $3 \times 56 = 168$ bits.
- The middle stage performs decryption and not encryption, so as to ensure that 3DES can decrypt a message that has been encrypted by simple DES
- Encryption:
 - $C = E_{k_3}(D_{k_2}(E_{k_1}(P)))$
- Decryption:
 - $P = D_{k_1}(E_{k_2}(D_{k_3}(C)))$
- If $K_1 = K_2$, then 3DES = DES



(a) Encryption

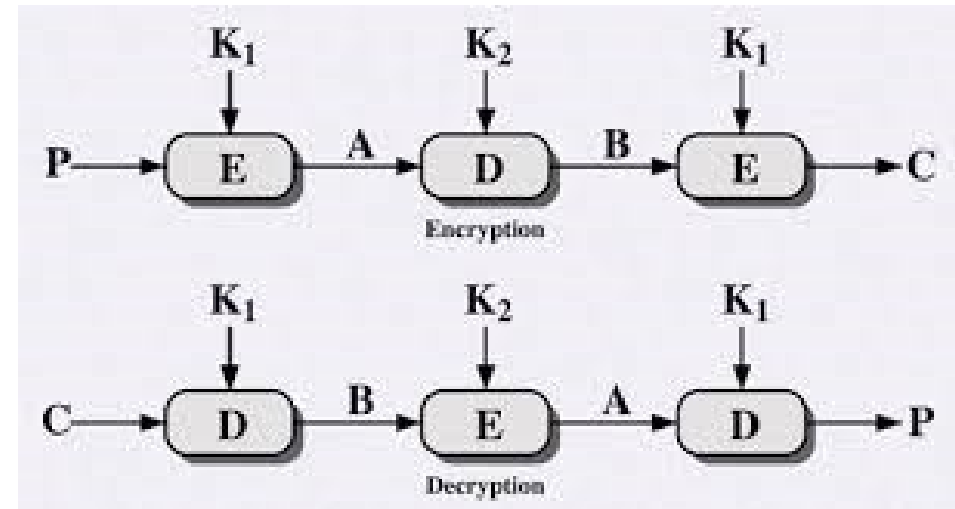


(b) Decryption



Triple DES (3DES) - 112

- The same 56-bit key can be used at the first and third stage
- In this case, the key size is $2 \times 56 = 112$ bits.
- Again, 3DES can decrypt ciphertexts that have been produced the simple DES
- Encryption:
 - $C = E_{k_1}(D_{k_2}(E_{k_1}(P)))$
- Decryption:
 - $P = D_{k_1}(E_{k_2}(D_{k_1}(C)))$
- Again, if $K_1 = K_2$, then 3DES = DES





AES (Advanced Encryption Standard) Requirements



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

- Private key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- stronger & faster than Triple-DES
- active life of 20-30 years (+ archival use)
- provide full specification & design details
- both C & Java implementations
- NIST have released all submissions & unclassified analyses



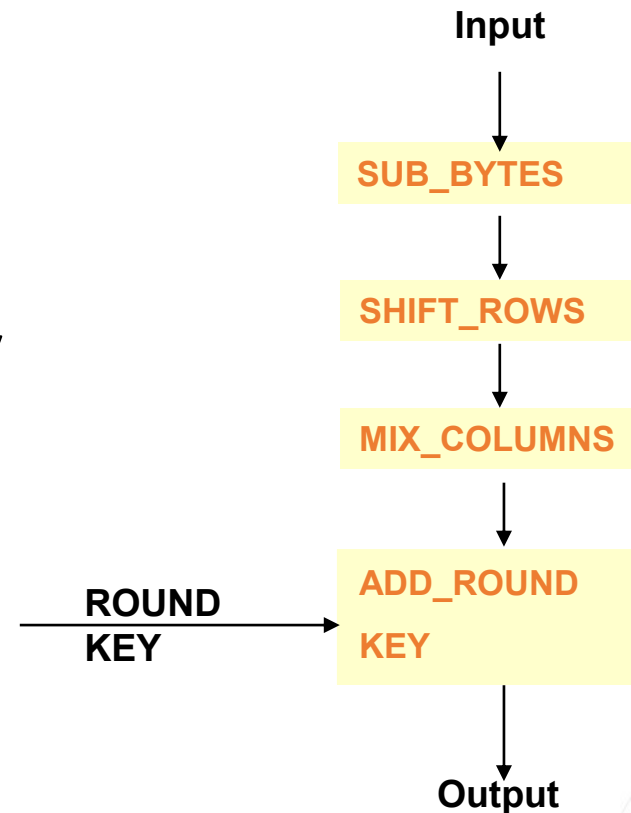
AES parameters

| | AES-128 | AES-192 | AES-256 |
|------------------------------|----------------|----------------|----------------|
| Key size (bits) | 128 | 192 | 256 |
| Plain text block size (bits) | 128 | 128 | 128 |
| Number of rounds | 10 | 12 | 14 |
| Round key size (bits) | 128 | 128 | 128 |
| Expanded key size (bytes) | 176 | 208 | 240 |



A typical AES encryption round

- SUB_BYTES: Substitution of bytes
 - SHIFT_ROWS: Shifting of bytea
 - MIX_COLUMNS: “Mixing”
 - ADD_ROUND_KEY: XOR addition with key
-
- Basic assumption: Each block is being considered as a 4x4 array of bytes (8 bit): $4 \times 4 \times 8 = 128$ bits in total.
 - The inputs and outputs of each round are such types of blocks



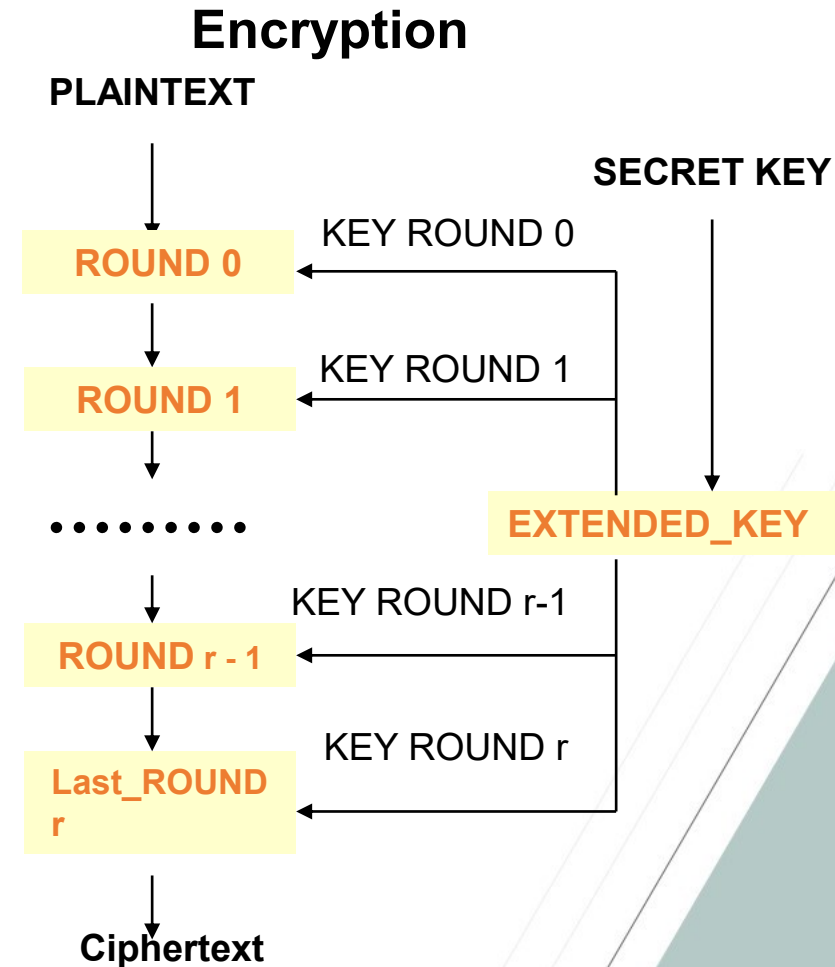


A typical AES encryption round



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

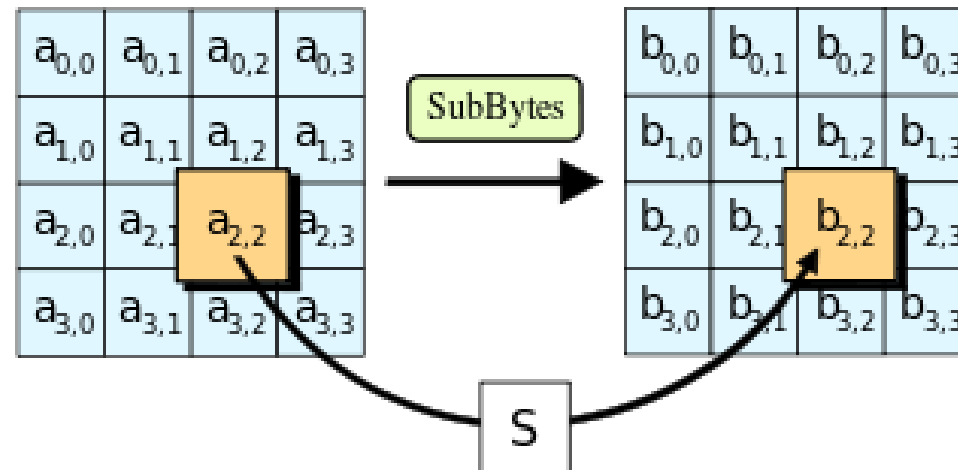
- Round 0 is simply an XOR addition with the round key
- The next $r-1$ rounds are identical, consisting of the four stages
- The last round r is slightly different, as discussed next.
- The secret key is being extended (with a well-determined procedure); from this extended key, a key scheduling procedure derives the sub-keys for each round





Byte substitution

- Plaintext is usually 128 bits, or 16 bytes

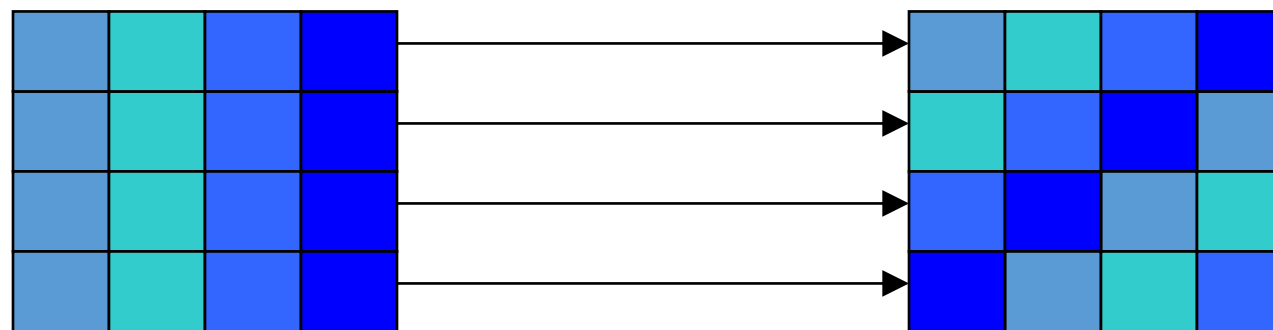


- Each byte (out of 16) is being substituted by another byte, under a highly nonlinear transformation (function S) with nice mathematical properties from a cryptographic point of view



Shift rows and mix columns

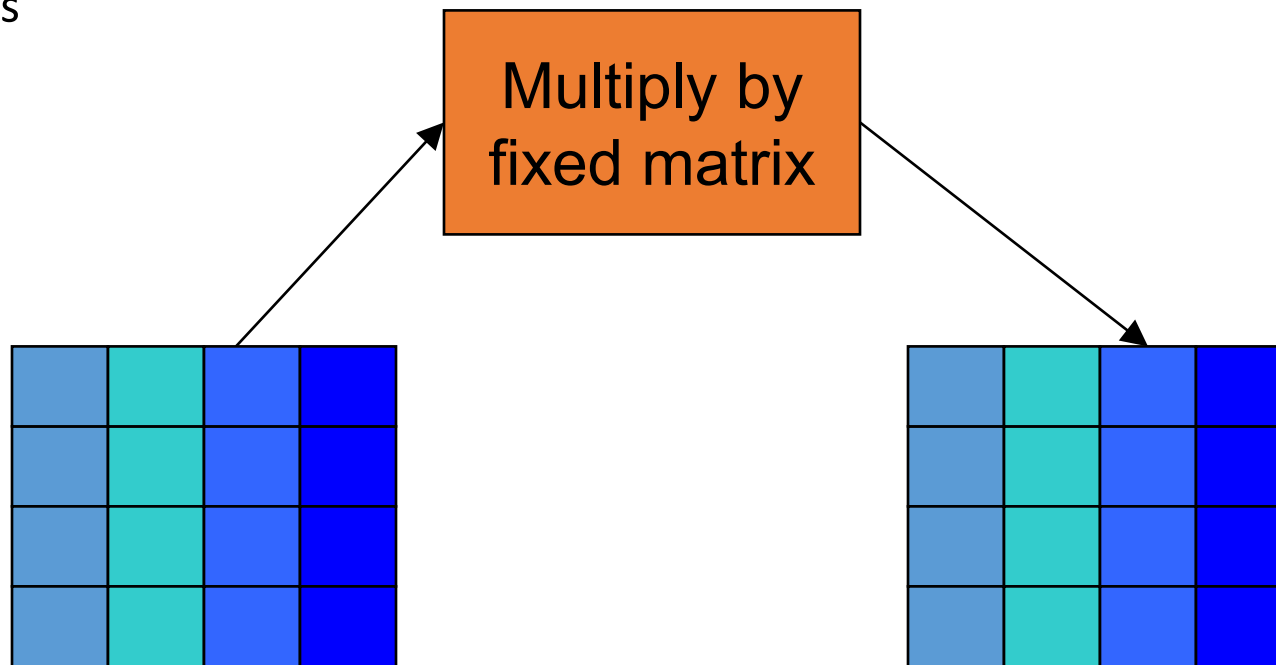
- Diffusion is reached in two steps
 - Shift rows





Shift rows and mix columns

- Diffusion is reached in two steps
 - Mix columns

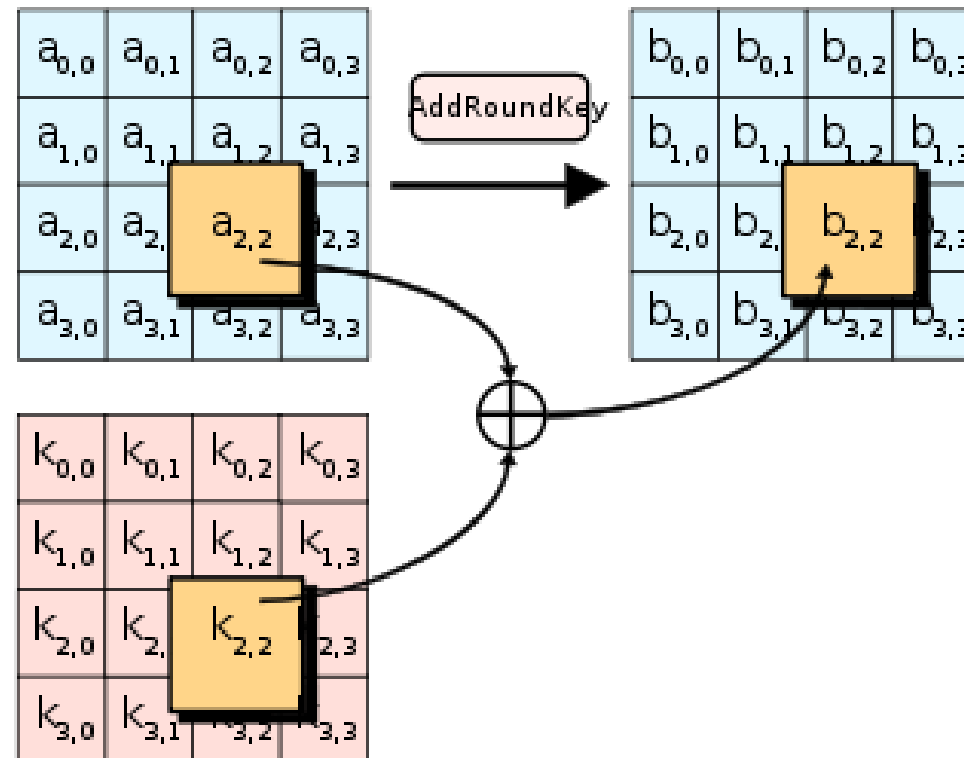


- Each column (4 bytes) is being transformed into another column (of 4 bytes)
- This is not performed in the last round



Round key addition

- Finally, the round key is XOR-ed with the state
- It is the only stage that key is being used!



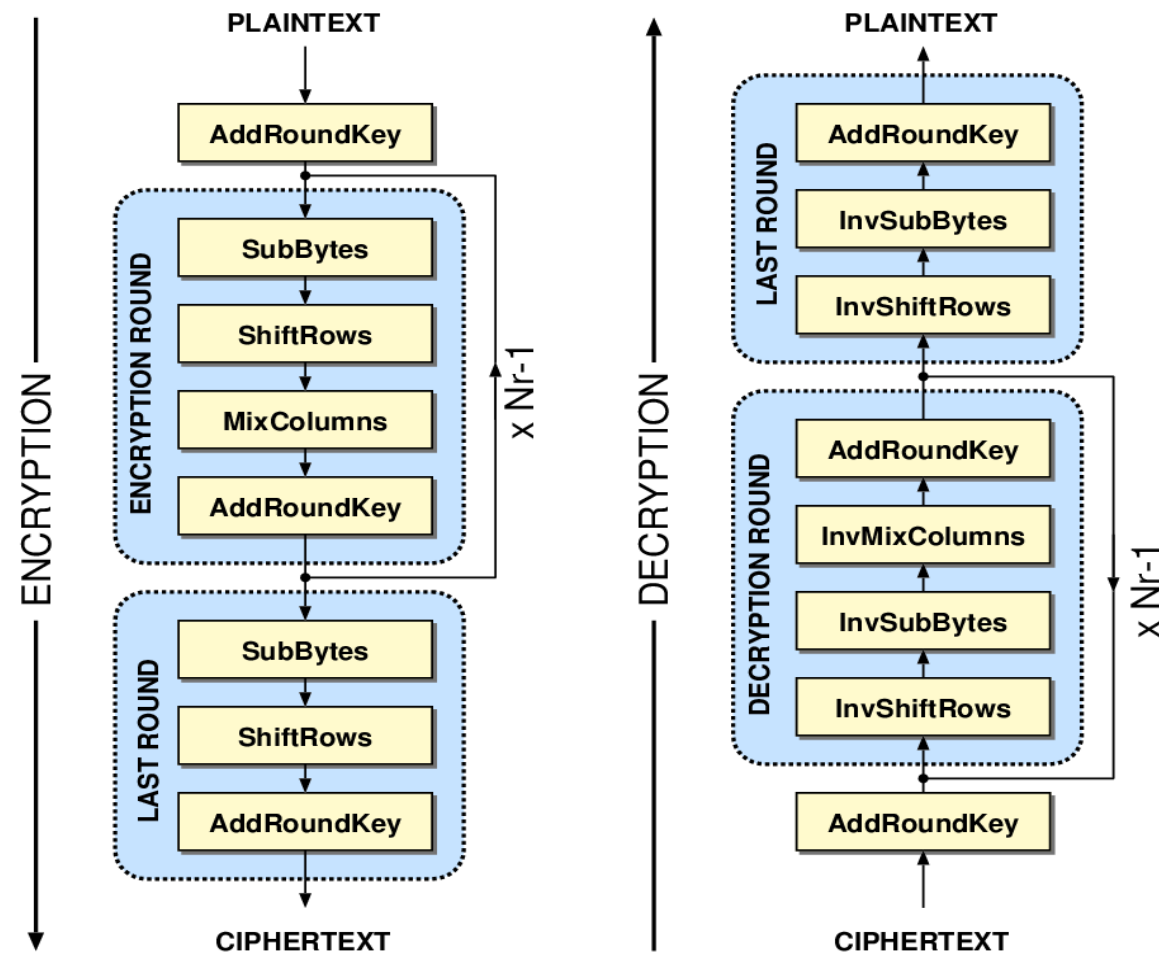


Decryption

- The inverse transformations are employed (Inv_Mix_Columns, Inv_Shift_Rows κτλ.)
- Only the Inv_Add_Round_Key is (obviously) the same with the Add_Round_Key
- AES decryption is slower than AES encryption. However:
 - The decryption is still fast, compared to other block ciphers
 - The speed in encryption is more important than the speed in decryption, as discussed next



Encryption vs. Decryption





A security comparison

- "Assuming that one could build a machine that could recover a DES key in a second (i.e., try 255 keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key."
- AES remains secure today
 - And it will remain secure even in the era of post-quantum computing (for key size 256 bits)



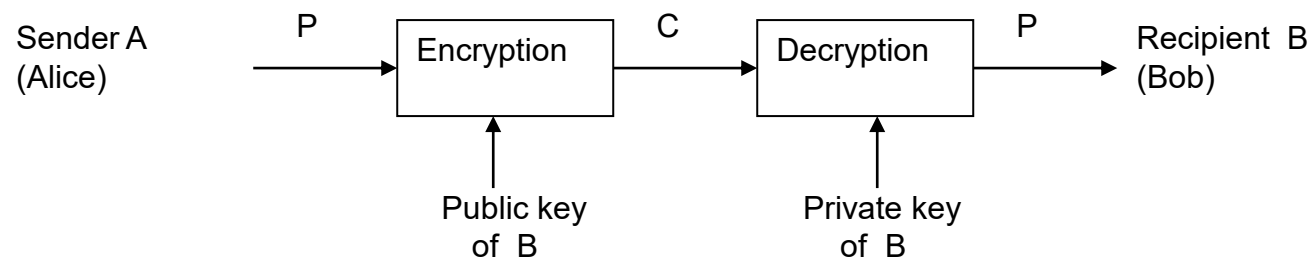
Public-Key Cryptography

- Probably most significant advance in the 3000 year history of cryptography
- uses two keys – a public & a private key
- Asymmetric since parties are not equal
- uses clever application of mathematical (mainly number theoretic) concepts to function
- Note: complements rather than replaces symmetric key crypto



Public key encryption - operation

- Public-key (or asymmetric) encryption/decryption involves the use of two keys:
 - a public-key, which may be known by anybody (including adversaries), and can be used to encrypt messages,
 - a related private-key, known only to the recipient, used to decrypt messages,
 - infeasible to determine private key from public
- is asymmetric because
 - those who encrypt messages cannot decrypt these messages – only the legitimate recipient can





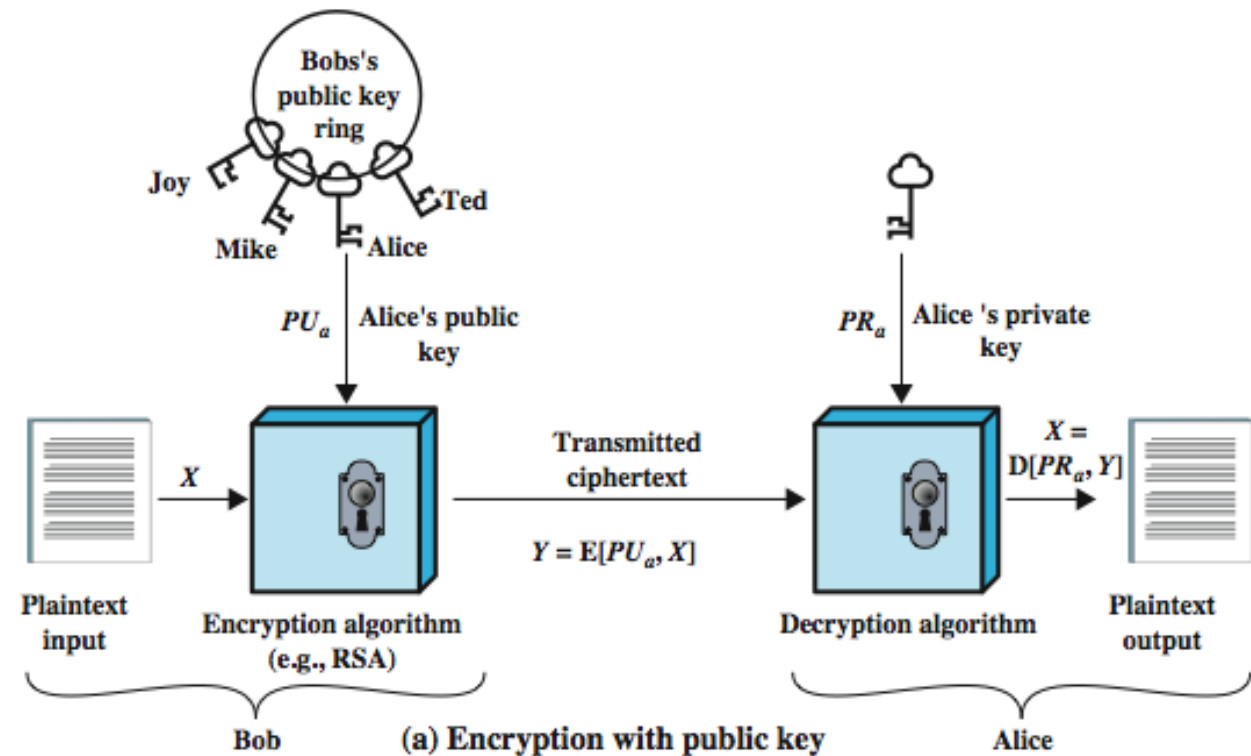
Why Public-Key Cryptography?

- The sender may start encryption without any prior “secret” communication with the recipient
 - The secure key distribution problem is being solved
 - As it will be shown next, public-key cryptography also suffices to generate digital signatures – used to verify a message comes intact from the claimed sender
- Public invention due to Whitfield Diffie & Martin Hellman at Stanford University in 1976
 - Seems though to be known earlier in classified community
 - Diffie and Hellman, received the 2015 Turing award - <http://awards.acm.org/about/2015-turing>



Public-Key Cryptography – a more generalized view

- The sender has a ring of public keys, (at least) one for each potential recipient
- Of course, the sender has also his own public-private key pair...





Symmetric vs Public-Key

| Conventional Encryption | Public-Key Encryption |
|---|---|
| <p><i>Needed to Work:</i></p> <ol style="list-style-type: none">1. The same algorithm with the same key is used for encryption and decryption.2. The sender and receiver must share the algorithm and the key. <p><i>Needed for Security:</i></p> <ol style="list-style-type: none">1. The key must be kept secret.2. It must be impossible or at least impractical to decipher a message if no other information is available.3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key. | <p><i>Needed to Work:</i></p> <ol style="list-style-type: none">1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.2. The sender and receiver must each have one of the matched pair of keys (not the same one). <p><i>Needed for Security:</i></p> <ol style="list-style-type: none">1. One of the two keys must be kept secret.2. It must be impossible or at least impractical to decipher a message if no other information is available.3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key. |



Some widely known public key cryptographic schemes



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

- Diffie-Hellman (protocol)
 - RSA
 - El Gamal
 - Rabin
 - McEliece
 - Elliptic curve cryptography
 - And others...
-
- Not all of them are being used for the same purposes



Public-Key Applications

- can be classified into 3 categories:
 - encryption/decryption (provide secrecy)
 - digital signatures (provide authentication)
 - key exchange (of session keys)
- some algorithms are suitable for all uses, others are specific to one

| Algorithm | Encryption/Decryption | Digital Signature | Key Exchange |
|----------------|-----------------------|-------------------|--------------|
| RSA | Yes | Yes | Yes |
| Elliptic Curve | Yes | Yes | Yes |
| Diffie-Hellman | No | No | Yes |
| DSS | No | Yes | No |



RSA

- by Rivest, Shamir & Adleman of MIT in 1977
- best known & widely used public-key scheme
- based on exponentiation in a finite field over integers modulo a prime
- uses large integers (eg. 2048 bits today)
- security due to cost of factoring large numbers



Which is the difficult mathematical problem for RSA?

- Any positive integer n can be represented in exactly one way as a product of primes (Fundamental Theorem of Arithmetic)
 - e.g. $140 = 2 \cdot 2 \cdot 5 \cdot 7$
 - There is no other product of primes which gives rise to 140
 - Finding out the unique such product of primes, for given number n , is being called factorization of n
 - Factorization is known to be computationally hard
 - The security of RSA is based on the difficulty of the factorization problem



Length of an RSA modulus

- It is hard to compare the equivalent security parameters for symmetric key cipher systems and RSA, however it is roughly believed that factorising a 512 bit number is about as hard as searching for a 56 bit symmetric key.
- Today, 2048 bits provide security (NIST suggests 2048 bits for RSA modulus size) – corresponds to 112-bit key security



RSA Security

- Possible approaches to attacking RSA are:
 - brute force key search
 - infeasible given the large size of numbers
 - mathematical attacks
 - based on difficulty of computing $\varphi(N)$, by factoring modulus N , or on not properly chosen parameters
 - timing attacks
 - on running of decryption
 - chosen ciphertext attacks
 - given properties of RSA



Elliptic curve cryptography (ECC)

- A general class of public key algorithms that are based on a special mathematical structure, being called elliptic curve
 - Similarly to the DLP problem, there is a known difficult problem that is being called Elliptic Curve Discrete Logarithm Problem (ECDLP)
 - Any cipher whose security rests with the difficulty of the ECDLP, is being called an elliptic curve cryptographic algorithm
 - ECC and RSA constitute the most common implementations of the public key algorithms
 - ECC will not be discussed in this course...



The major advantage of the ECC

- Smaller key sizes to achieve the same level of security

| ECC KEY SIZE (Bits) | RSA KEY SIZE (Bits) | KEY SIZE RATIO | AES KEY SIZE (Bits) |
|------------------------|------------------------|-------------------|------------------------|
| 163 | 1024 | 1 : 6 | |
| 256 | 3072 | 1 : 12 | 128 |
| 384 | 7680 | 1 : 20 | 192 |
| 512 | 15 360 | 1 : 30 | 256 |



General advantages of public key cryptographic algorithms



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

- No previous negotiation is needed
- The key pair can remain unchangeable for many years
 - In contrast to the symmetric key
- In a network, a much smaller number of keys is needed to be distributed with respect to the symmetric key
 - In symmetric encryption, we need a different key for each pair of users!
 - If we have N users, we actually need $N(N-1)/2$ symmetric keys



General disadvantages of public key cryptographic algorithms

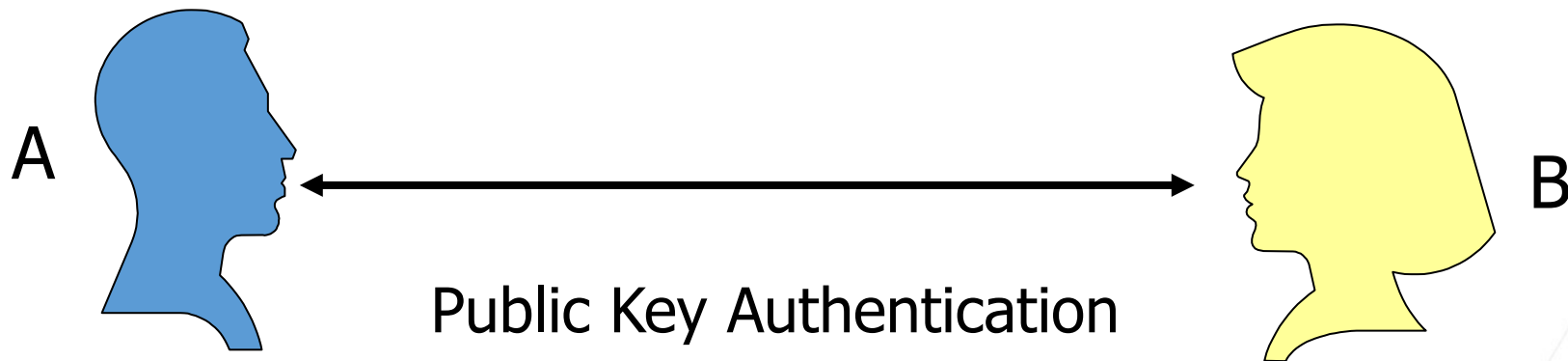
- Much smaller throughput
 - Actually, we cannot encrypt real time communication with public key encryption
- Keys of large sizes are difficult to be handled
- Their security rests with difficult mathematical problems which are known to be difficult but they have not proved to be “unsolvable”.
 - What if we find a “solution” for such a problem?
- In a post-quantum world, most public key algorithms will be no longer secure any more!!



Combining symmetric with public key algorithms (1/3)

First, a mutual authentication needs to be performed,

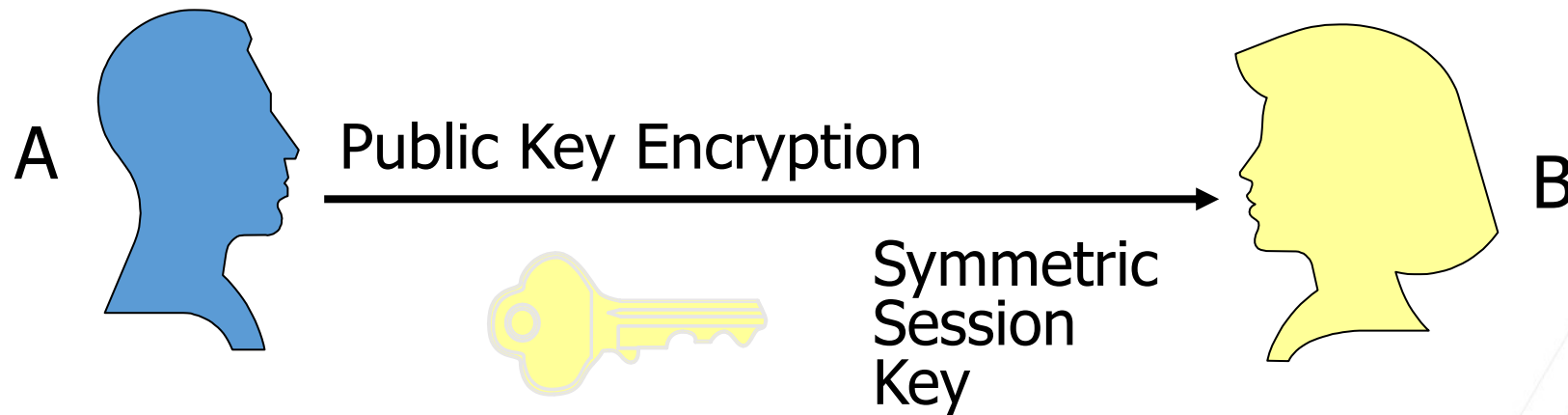
- Public key cryptographic structures are being used





Combining symmetric with public key algorithms (2/3)

- Next, a user generates a symmetric key
- This key is being encrypted with the public key of the other user and is being transmitted to her
 - Hence, they both have the same secret key, being securely interchanged





Combining symmetric with public key algorithms (3/3)

- Now they communicate securely, with symmetric key encryption





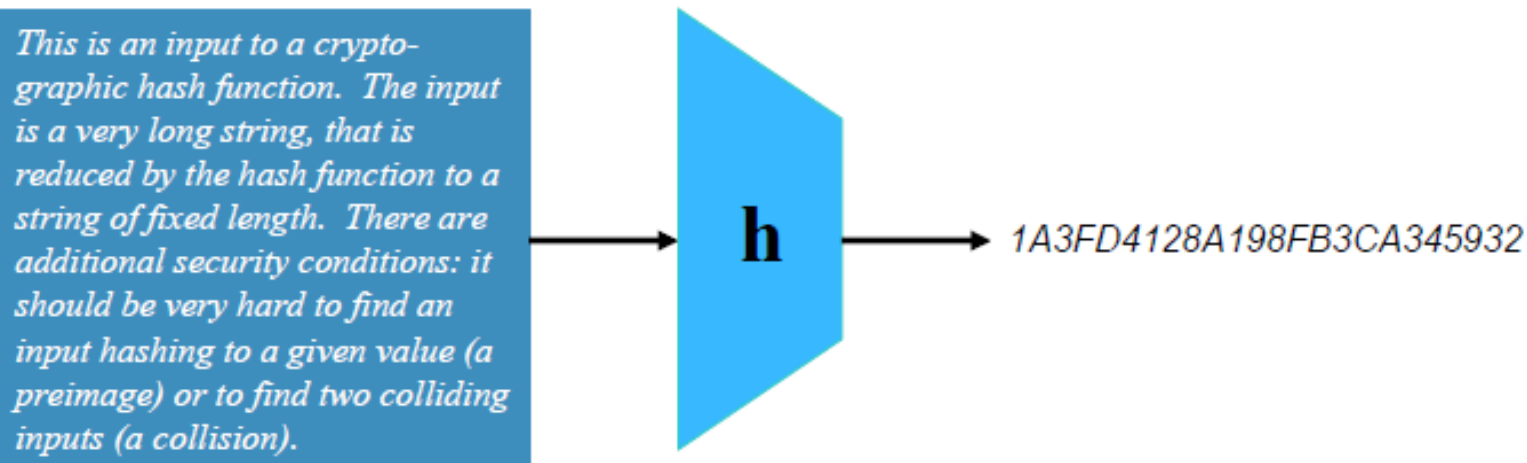
Further security requirements

- Entity authentication: Need to ensure that the identity of a user is genuine (there is no masquerading)
- Data integrity: Need to ensure that the data themselves have not been altered
- Cryptography also examines these goals
- Several cryptographic primitives
 - Cryptographic hash functions have a crucial role



Cryptographic hash functions

- A cryptographic primitive which maps any input to an output of fixed length, relatively small, satisfying some specific properties
 - This output is being called fingerprint or digest of the message





Properties of hash functions in simple words (informal..)



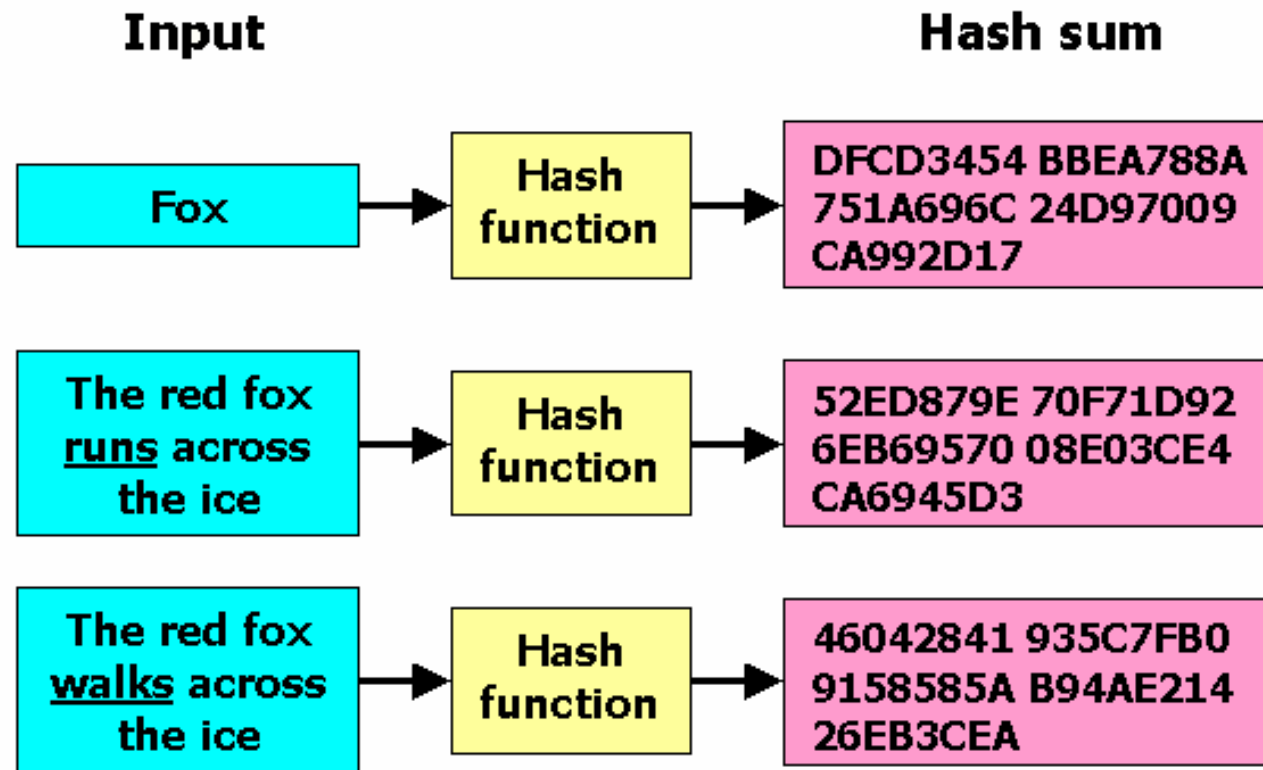
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

- condenses arbitrary message to fixed size
- It is not possible to obtain a message from its fingerprint (non-reversible function)
- It is practically impossible to find two distinct messages with the same digest
- They are commonly used to detect changes to message
 - Can be used in various ways with message
 - most often to create a digital signature, as shown next



An example

- The output is of fixed length, regardless the size of the input





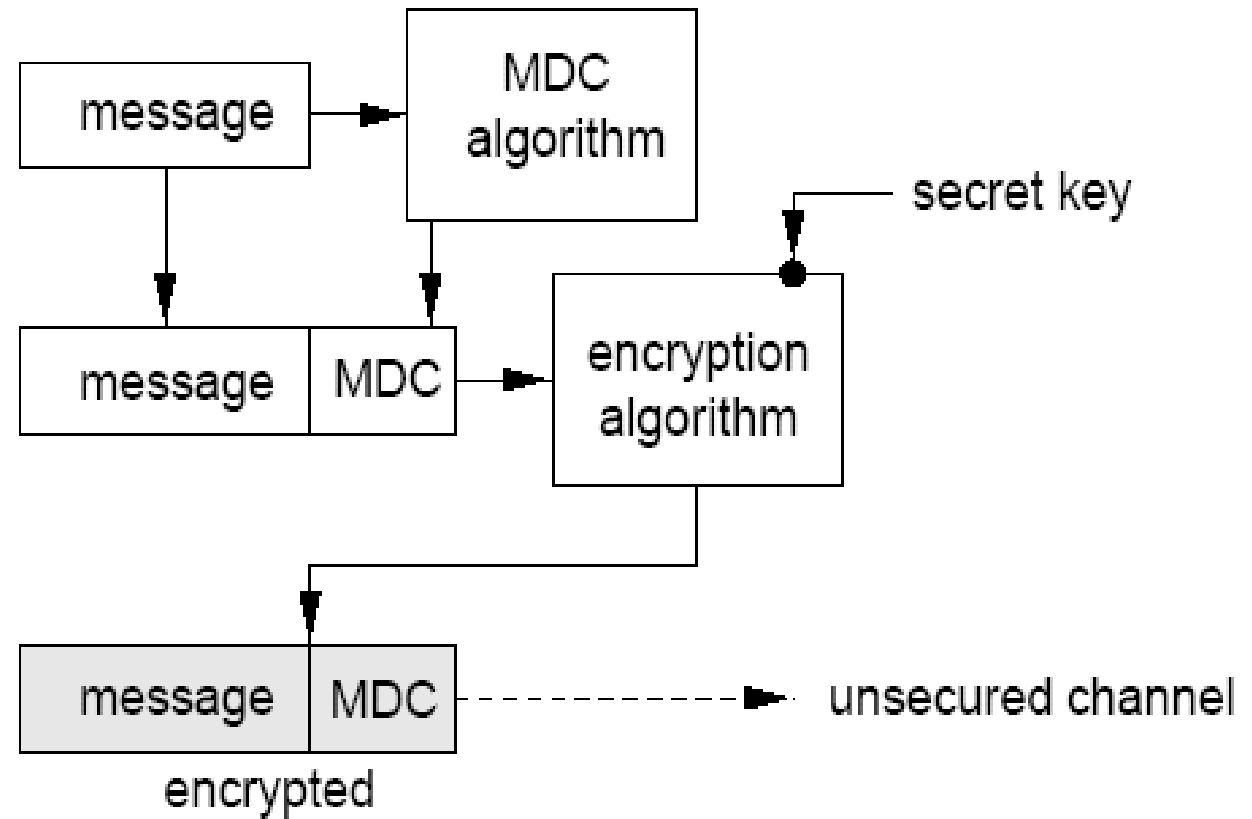
Requirements for Hash Functions

- MDC (Modification Detection Code)
 - Simple hash function without the usage of any key.
- MAC (Message Authentication Code)
 - A keyed hash function



Message Detection Code (MDC)

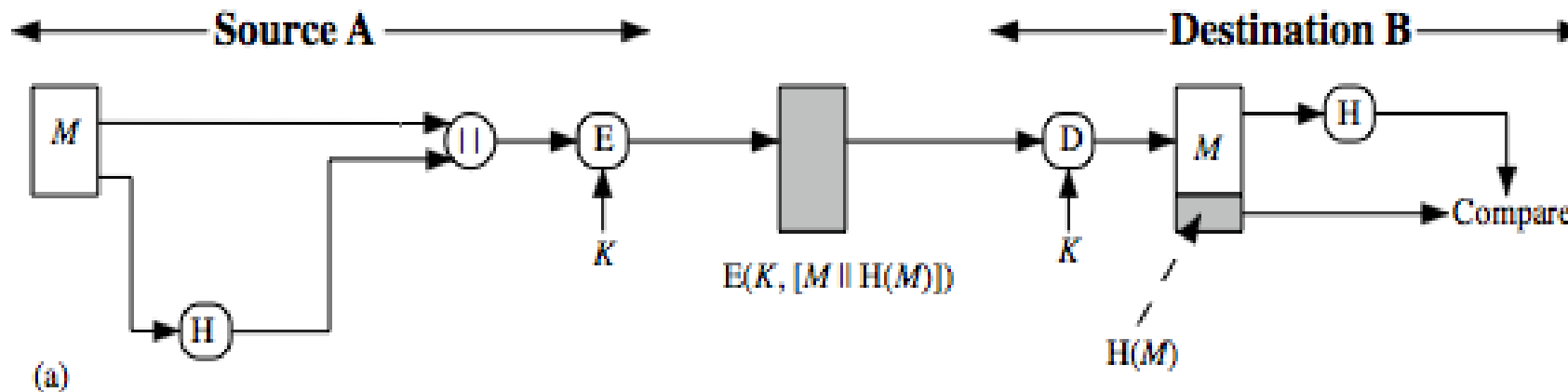
- It is the classical notion of a simple hash function
 - The term MDC is not so commonly used nowadays
- The message is augmented by its fingerprint, before its transmission
- The whole augmented message is being encrypted, towards achieving confidentiality
 - The message digest should not be computed over the encrypted (simple) message (why?)





Use of a hash function for message integrity

- If the encrypted message is being modified/alterred during the transmission, the receiver will be able to detect this!!
 - Recall the properties of hash functions...





Gains

- Message integrity
- Can be used for creating digital signatures for entity authentication (described in the sequel)
- Some common uses of hash functions
 - Secure processing of users passwords
 - Passwords are not stored in plaintext
 - In forensics analysis, to check/verify the validity of a file (see, e.g. https://gnupg.org/download/integrity_check.html)



MD2, MD4 and MD5 hash functions

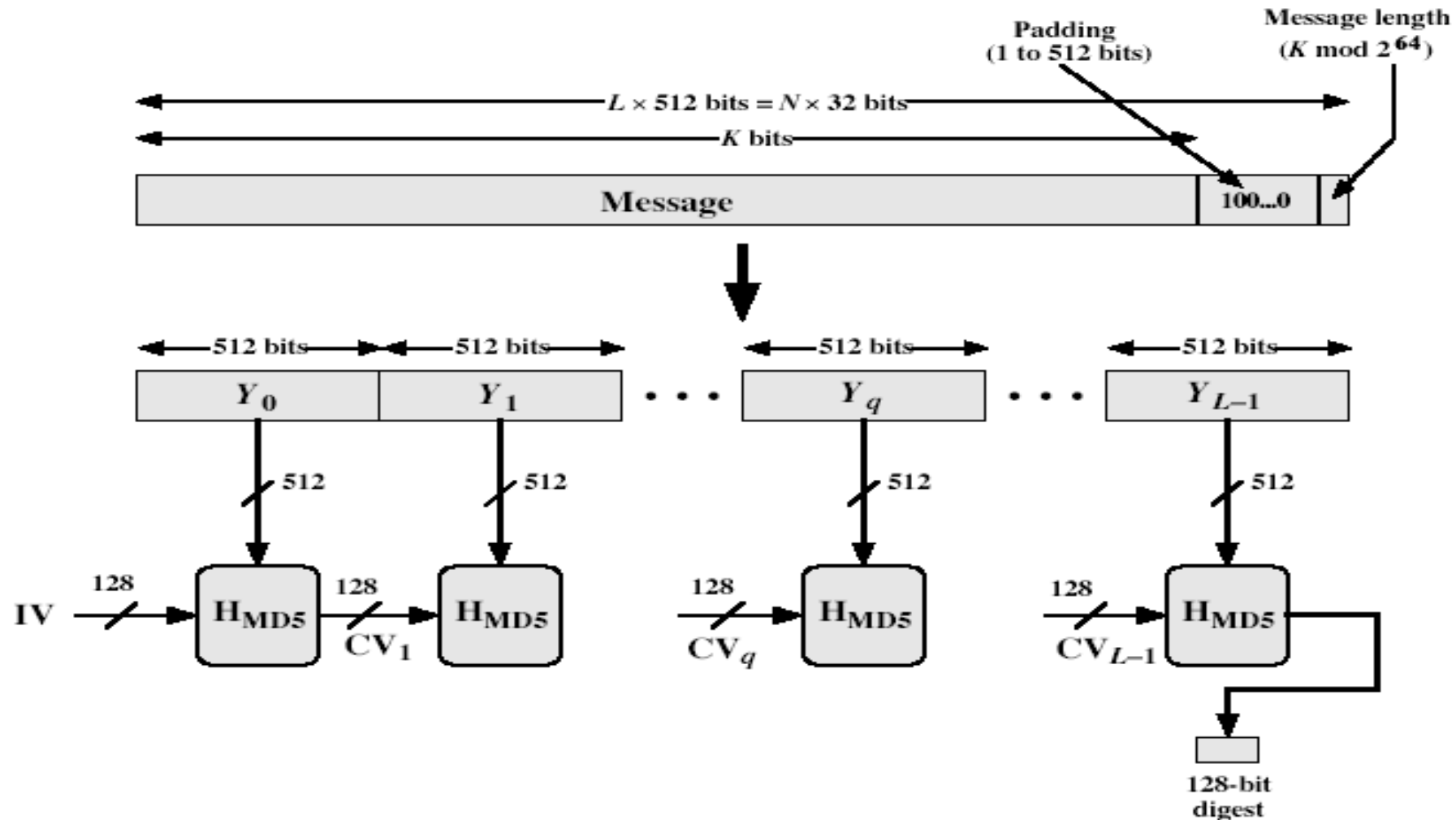


Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

- A family of hash functions invented by Ronald Rivest
 - They all generate 128 bit as output
- MD2: 1989
 - A collision found in 1995
- MD4: 1990
 - A collision found in 1995
- MD5: 1992
 - Internet standard (RFC 1321)
 - Since 1997 it was believed that collisions could be found – this came true in 2004
 - Nowadays, it is not considered as secure
 - 2012: According to Microsoft, a collision in MD5 was exploited by attackers to launch the malicious software Flame



MD5 – General description





A collision in MD5

- These two messages:

```
d131dd02c5e6eec4 693d9a0698aff95c 2fcab58712467eab 4004583eb8fb7f89  
55ad340609f4b302 83e488832571415a 085125e8f7cdc99f d91dbdf280373c5b  
d8823e3156348f5b ae6dacd436c919c6 dd53e2b487da03fd 02396306d248cda0  
e99f33420f577ee8 ce54b67080a80d1e c69821bcb6a88393 96f9652b6ff72a70
```

```
d131dd02c5e6eec4 693d9a0698aff95c 2fcab50712467eab 4004583eb8fb7f89  
55ad340609f4b302 83e4888325f1415a 085125e8f7cdc99f d91dbdf7280373c5b  
d8823e3156348f5b ae6dacd436c919c6 dd53e23487da03fd 02396306d248cda0  
e99f33420f577ee8 ce54b67080280d1e c69821bcb6a88393 96f965ab6ff72a70
```

which are different at 6 (hexadecimal) places, have the same MD5
digest: 79054025255fb1a26e4bc422aef54eb4



Secure Hash Algorithm (SHA)

- Developed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standard (FIPS 180) in 1993
- A revised version was issued as FIPS 180-1 in 1995 and is generally referred to as SHA-1
- Based on the hash function MD4 and its design closely models MD4
- SHA-1 produces a hash value of 160 bits
- In 2005, a research team described an attack in which two separate messages could be found that deliver the same SHA-1 hash using 2^{69} operations
 - This result has hastened the transition to newer, longer versions of SHA.



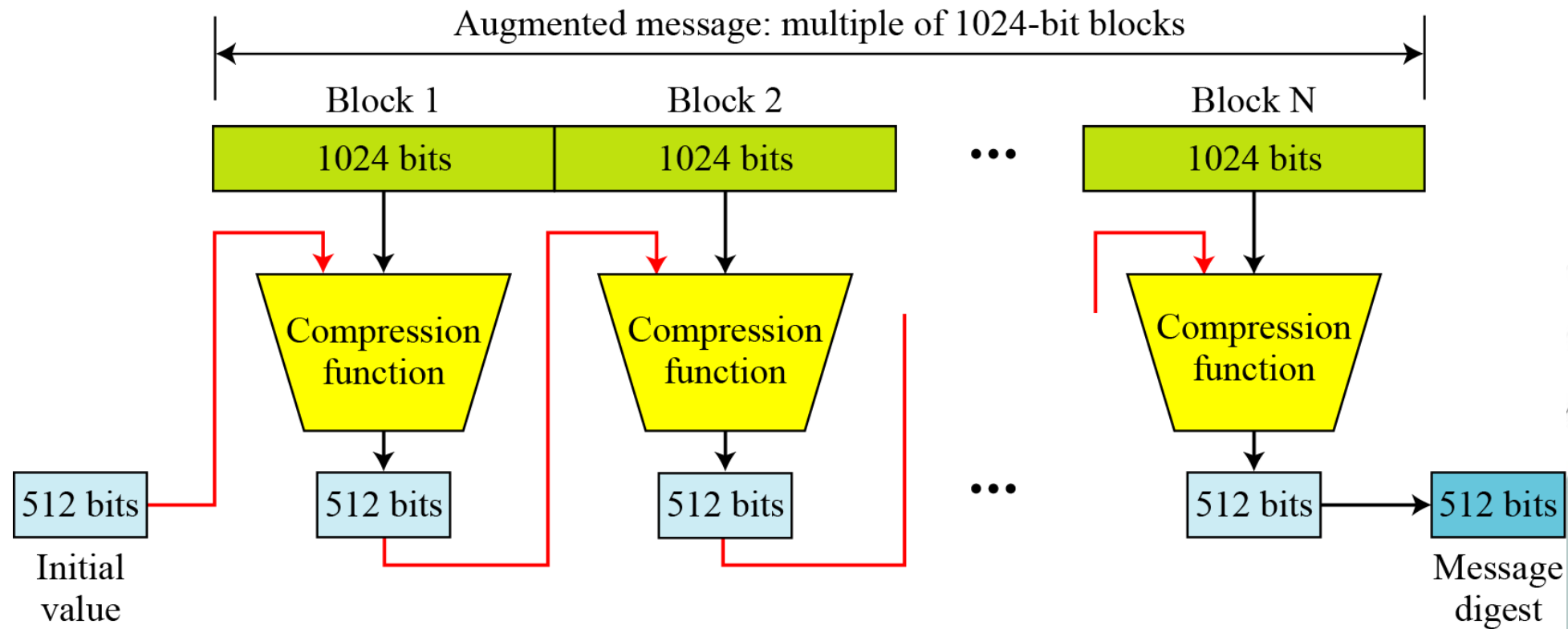
Revisions on SHA

- In 2002, NIST produced a revised version of the standard, FIPS 180-2, that defined three new versions of SHA, with hash value lengths of 256, 384, and 512 bits,
 - Known as **SHA-256, SHA-384, and SHA-512.**
- Collectively, these are known as SHA-2
- Same underlying structure with SHA-1
- In 2005, NIST announced the intention to phase out approval of SHA-1 and move to a reliance on the other SHA versions by 2010.



An overview of SHA-512

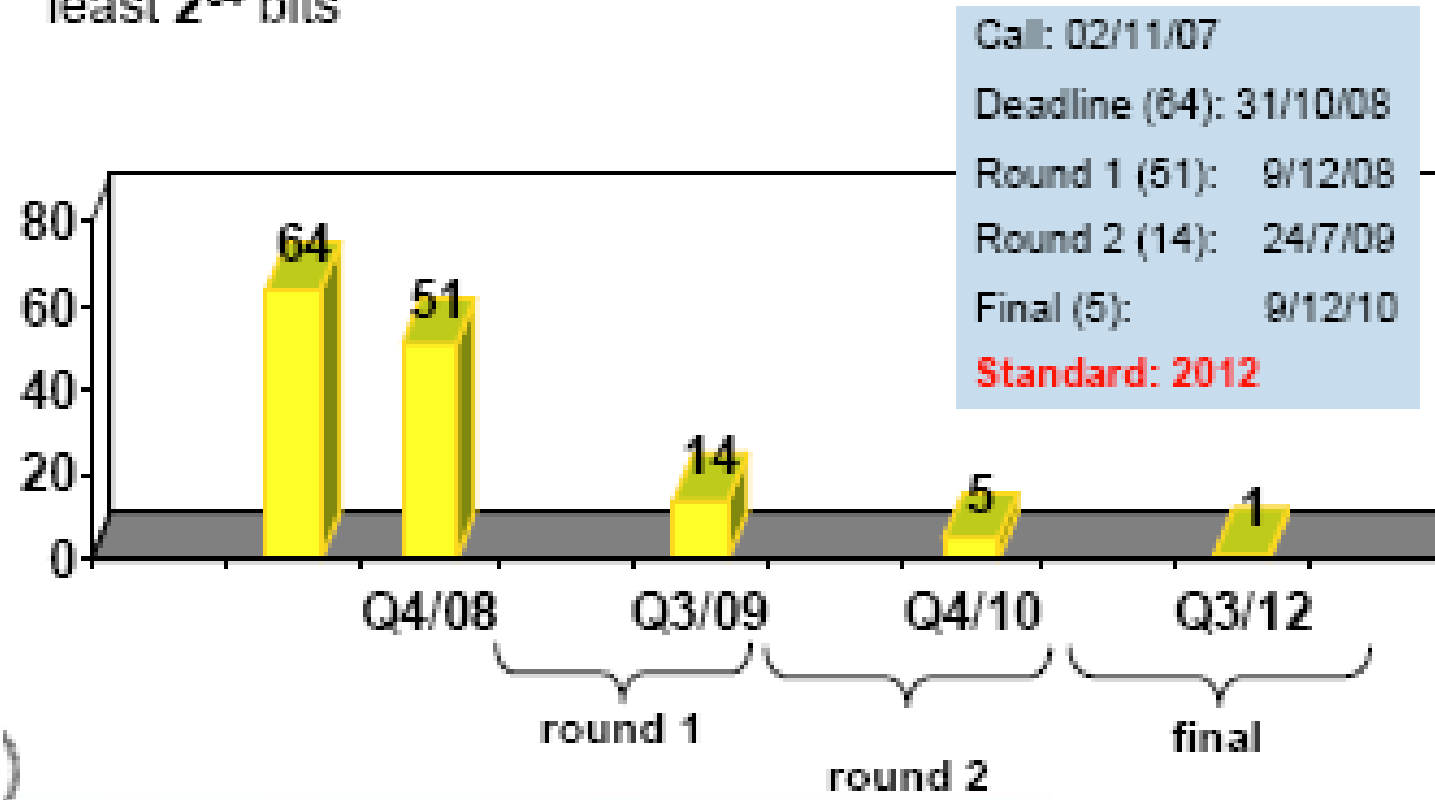
- The compression function is the “heart” of the algorithm





New standard: SHA-3

- SHA-3 must support 224, 256, 384, and 512-bit message digests, and must support a maximum message length of at least 2^{64} bits





Collisions in SHA-1

- It was known for year that it was simply a matter of time to practically find collisions in SHA-1
- February 2017: Researchers managed to break SHA-1 in practice
- See <https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html>
 - <https://shattered.io/> (two different .pdf files with the same SHA-1 fingerprint)
 - Online tool: <https://alf.nu/SHA1>
- More recent and powerful attacks (collisions) on SHA-1:
- <https://portswigger.net/daily-swig/researchers-demonstrate-practical-break-of-sha-1-hash-function>



Limitation of Using Hash Functions for Authentication

- Require an authentic channel to transmit the hash of a message
 - Without such a channel, it is insecure, because anyone can compute the hash value of any message, as the hash function is public
 - Such a channel may not always exist
- How to address this?
 - use more than one hash functions
 - use a key to select which one to use

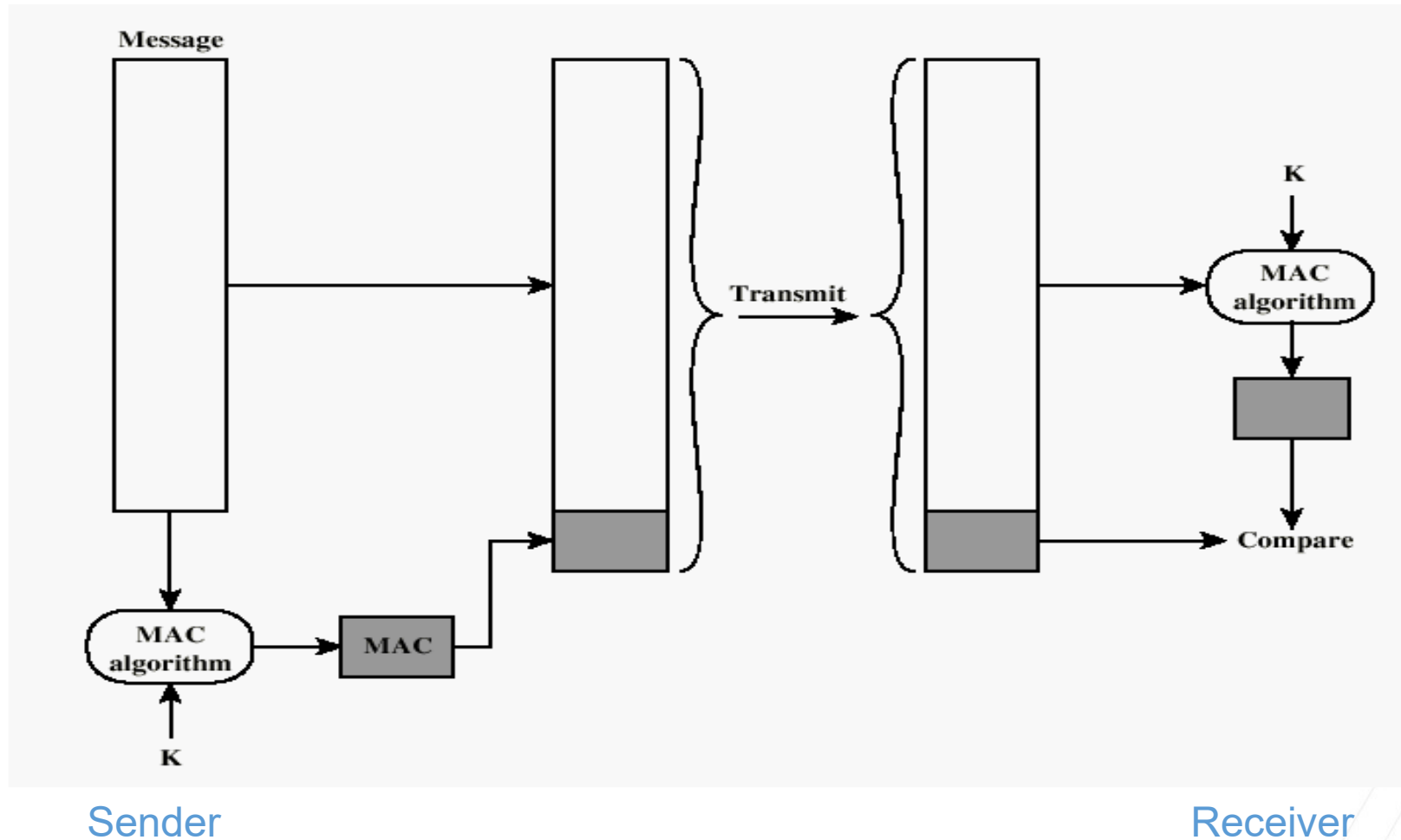


Message Authentication Code (MAC)

- A hash algorithm that produces, for any arbitrary message, a fixed-length output
 - The output is dependent on both the message and a secret key (keyed-hash function)
 - It resembles encryption, but it is not reversible!!
 - The output of a MAC is also called, for simplicity, MAC
 - Also being called as keyed hash function
- The MAC is added at the end of the message
- The recipient, who knows the secret key, checks the MAC with regard to its validity
 - Any modification in the message or in the MAC during the transmission will be identifiable (see next slide)



MAC for message integrity





Message Authentication Code

- A MAC scheme is actually a hash family, used for message authentication
- $\text{MAC}(K,M) = H_K(M)$
- The sender and the receiver share secret K
- The sender sends $(M, H_K(M))$
- The receiver receives (X,Y) (where X is the message and Y its MAC value) and verifies that $H_K(X)=Y$, if so, then accepts the message as from the sender
- To be secure, an adversary shouldn't be able to come up with (X',Y') such that $H_K(X')=Y'$.
 - Recall that the adversary does not know the key K



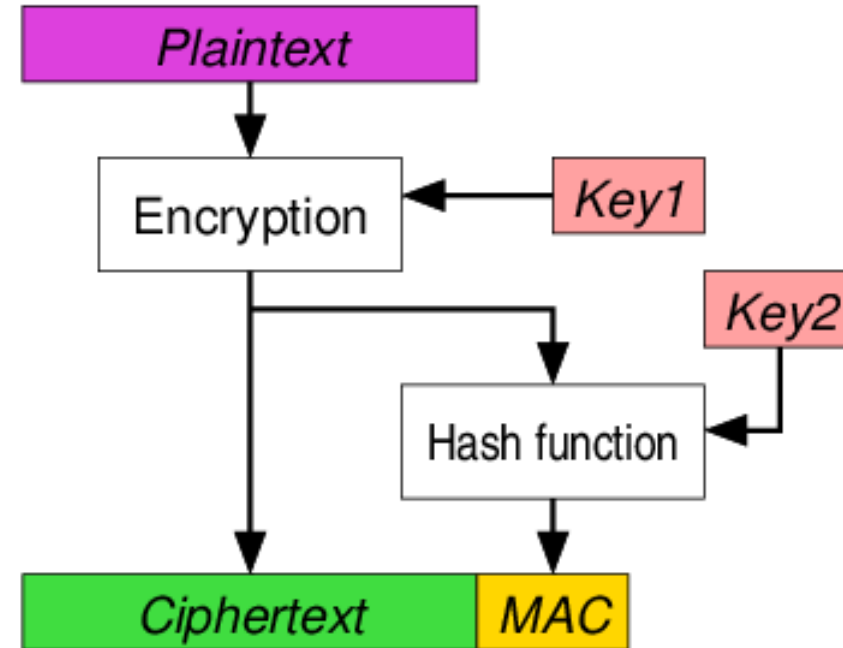
Properties of a MAC

- It is a many-to-one function
 - There always exist different messages with the same MAC but, despite their existence, they cannot be found in practice
- If confidentiality is also a goal, then the message needs to be additionally encrypted (possibly with another key)
 - MAC can be computed over the initial message or the encrypted message (see next slide)



Encrypt-then-MAC (EtM)

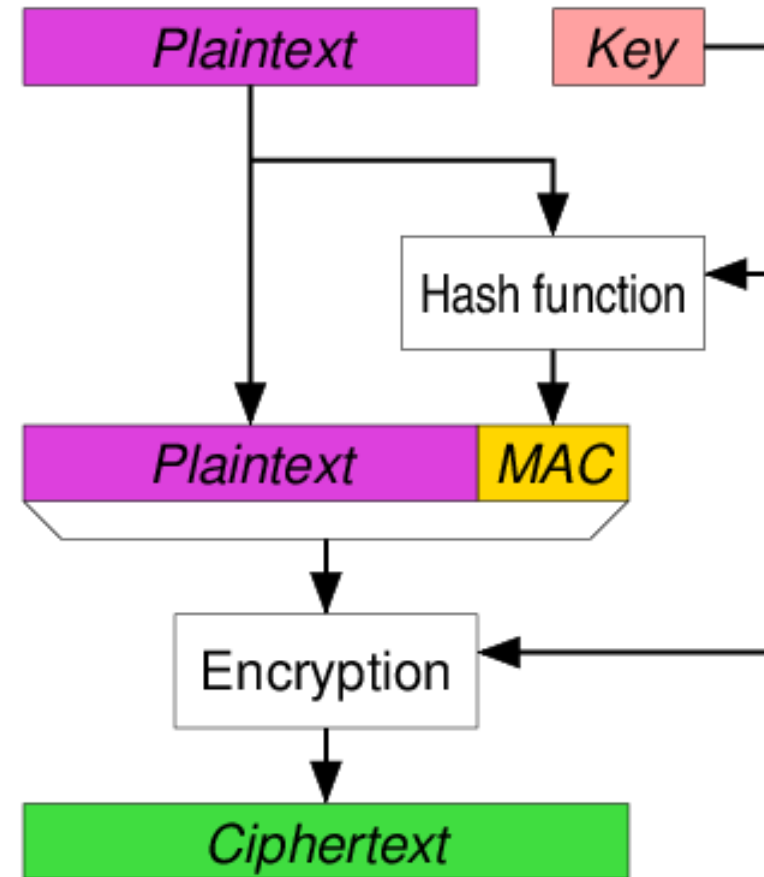
- Many security protocols support it – e.g. the IPsec





MAC-then-Encrypt (MtE)

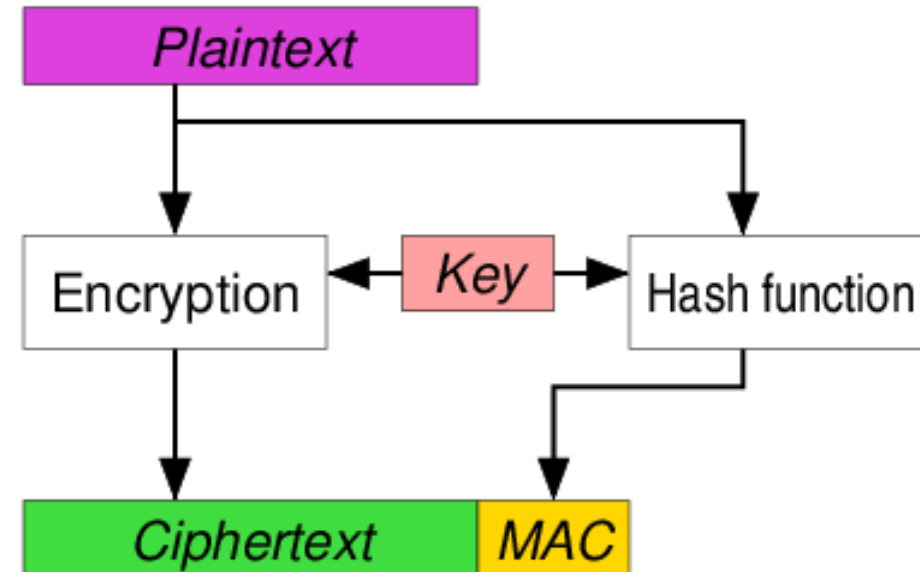
- Many security protocols support it – e.g. SSL/TLS (the versions until 1.2 – not in the most recent version 1.3)





Encrypt-and-MAC (E&M)

- Some block ciphers modes of operation compute simultaneously with the ciphertext and a MAC (being called “tag” in this context).
 - It is a special case of E&M
 - The most prominent one: The Galois Counter Mode (GCM)





Gains

- MAC ensures the following:
 - The message has not been modified (message integrity)
 - If an attacker alters the message or its MAC, this will be detectable from the receiver
 - He could produce a valid pair of a message and its MAC, only if he/she knew the secret key
 - The source of the message is genuine (sender authentication)
 - Provided that nobody else has the key that has been used for the MAC



Digital Signatures

- Data that are being attached to a message, aiming to verify the identity of the sender as well as the integrity of the data
- A digital signature has the following properties:
 - Only the signer can create his signature (e.g. none can create Bob's signature)
 - It allows others to verify the validity of the signature (e.g. that indeed Bob is the signer)
 - It is uniquely associated with the message ("bound with a message") so as to ensure its integrity; a valid signature for a message cannot be moved to sign another message
 - The signer cannot deny that he signed (non-repudiation property)



Digital signature vs. Hand-made signature

- Actually, the same meaning in terms of verifying the signer
- However, hand-made signature is always the same (for the same signer), whereas digital signatures are different for each possible message, even for the same signer
 - And, thus, message integrity is also ensured



Digital Signature Requirements

- must depend on the message signed
- must use information unique to sender
 - to prevent both forgery and denial
- must be relatively easy to produce
- must be relatively easy to recognize & verify
- be computationally infeasible to forge
 - with new message for existing digital signature
 - with fraudulent digital signature for given message
- be practical
- Cryptographic primitives for the “typical” digital signatures
 - Public key ciphers
 - Hash functions



How a Digital Signature is created?

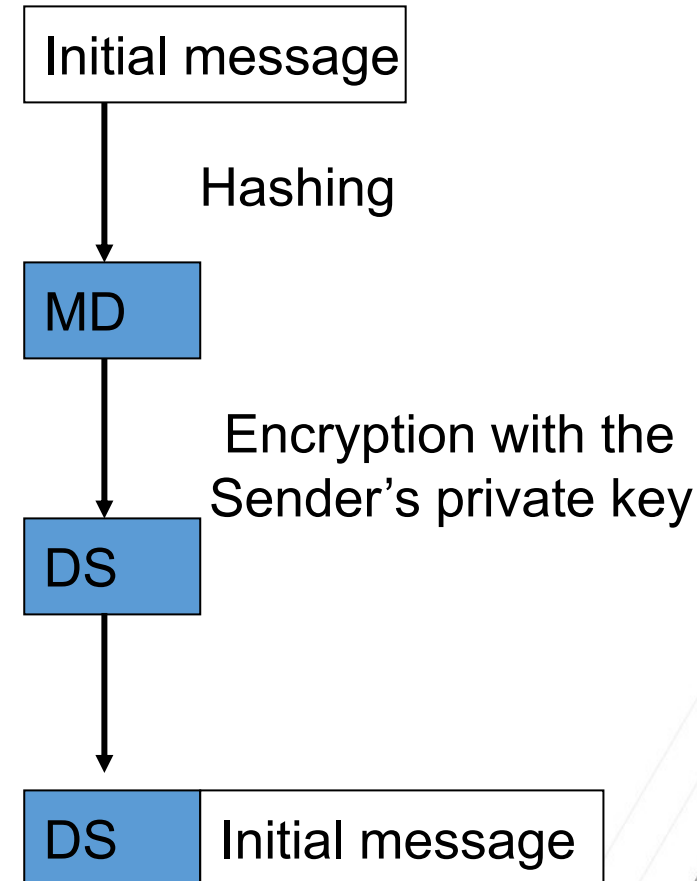
- A Digital Signature is the result of **encrypting** the Hash of the data to be exchanged.
- Recall that the Hash uniquely represents the original data.
- The probability of producing the same Hash with two sets of different data is negligible
- Signature Process is opposite to Encryption Process
 - Private Key is used to Sign (encrypt) Data
 - Public Key is used to verify (decrypt) Signature



A generic model of creating digital signatures

To create a digital signature:

1. Hash (digest) the data using one of the supported Hashing algorithms, e.g., SHA-2, SHA-3. We get the digest MD.
2. Encrypt the hashed data using the sender's private key. We get the digital signature DS
3. Append the signature to the end of the data that was signed (a copy of the sender's public key is also generally attached)

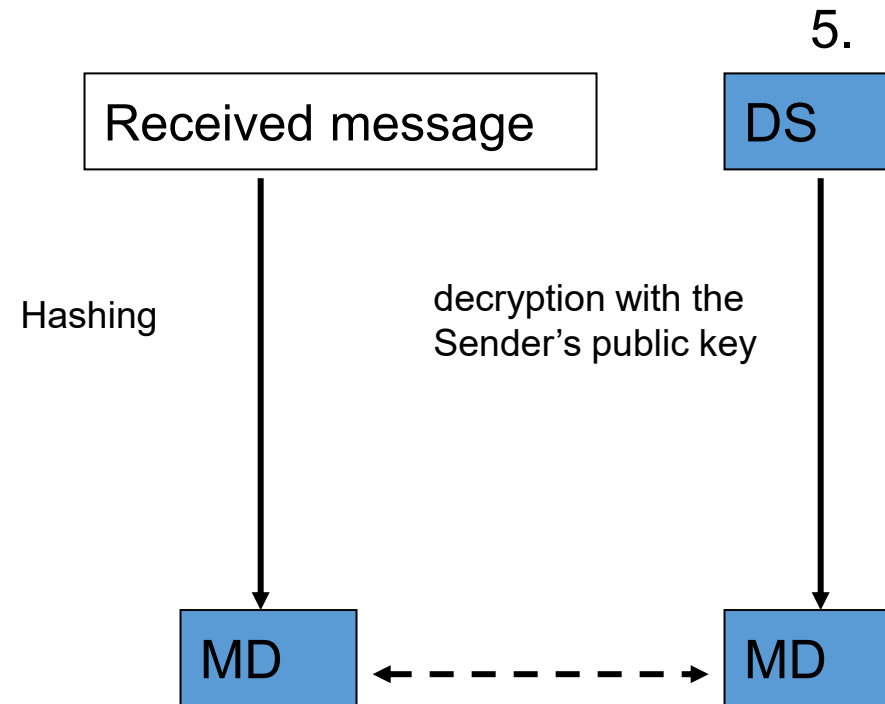




A generic model of verifying a digital signature

To verify the signature:

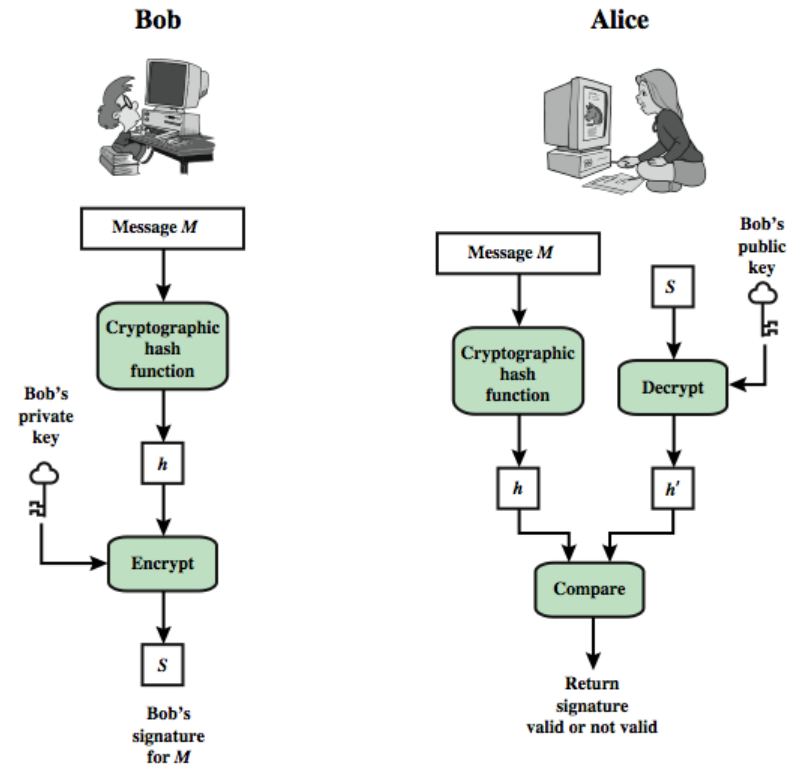
4. Hash the original data using the same hashing algorithm. Its digest MD is computed
5. Decrypt the digital signature using the sender's public key.
6. Compare the results of the hashing and the decryption. If the values match then the signature is verified. If the values do not match, then the data or signature was probably modified in transit.





Digital Signature Model (with data confidentiality)

- Note the difference between public key encryption and signatures:
- In encryption, the sender uses the recipient's public key
- In digital signatures, the sender (signer) uses its own private key





Digital signatures algorithms

- Most of the known public key ciphers can be used to create digital signatures
- Most commonly used:
 - RSA
 - Elliptic curve
- DSA (Digital Signature Algorithm)
 - An adaptation of a known public key encryption algorithm, being called El Gamal
 - Most commonly used is its Elliptic Curve variant (ECDSA)
- It is being used in the Digital Signature Standard (DSS)
 - NIST Standard - FIPS 186 (not discussed here)



RSA Signatures

- Public key is (n,e) , private key is d
- To **sign** message m : $s = (\text{hash}(m))^d \bmod n$
 - Signing and decryption are the same mathematical operation in RSA
- To **verify** signature s on message m :
 $s^e \bmod n = (\text{hash}(m)^d)^e \bmod n = \text{hash}(m)$
 - Verification and encryption are the same mathematical operation in RSA
- PKCS #1 (Public Key Cryptography Standard)



Digital signatures

- Sender authentication is in place
- Verification of a sender's identity (and the integrity of message) can be performed by anyone, since anyone has access to sender's public key
- Any user can produce a digital signature that suffices to authenticate her identity and the message integrity, whilst any other user can proceed with such a verification (i.e. to check the validity of the signature).
- Note that computing a MAC is usually much faster than producing a digital signature



An overall comparison

- Note that MACs do not support the non-repudiation property: Any user who can verify a MAC is also capable of generating MACs for other messages (because he knows the secret key)

| Security Goal | Hash | MAC | Digital Signature |
|-----------------|------------------|-----------|-------------------|
| Integrity | Yes | Yes | Yes |
| Authenticity | No | Yes | Yes |
| Non-repudiation | No | No | Yes |
| Key used | Normally no keys | Symmetric | *Asymmetric |



Trusted third parties and Digital Certificates



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

- Before B accepts a message with A's Digital Signature, B wants to be sure that the public key belongs to A and not to someone masquerading as A on an open network
- One way to be sure, is to use a trusted third party to authenticate that the public key belongs to A. Such a party is known as a Certification Authority (CA)
 - The analogue to a “solicitor” in a digital world
- Once A has provided proof of identity, the Certification Authority creates a message containing A's name and public key. This message is known as a Digital Certificate.



Certification Authority – CA

- A trusted authority (Trusted Third Party – TTP) which issues digital certificates for entities, containing their public keys
- Since they are trusted, we are ensured for the validity of the certificates – that is for the validity of the public key of the certificate's owner



Actions of a CA

- Certificate issuance
- Certificate renewal
- Certificate revocation
- Certificate suspension/activation
- and others...(including generation of public-private keys, timestamping procedures etc.)

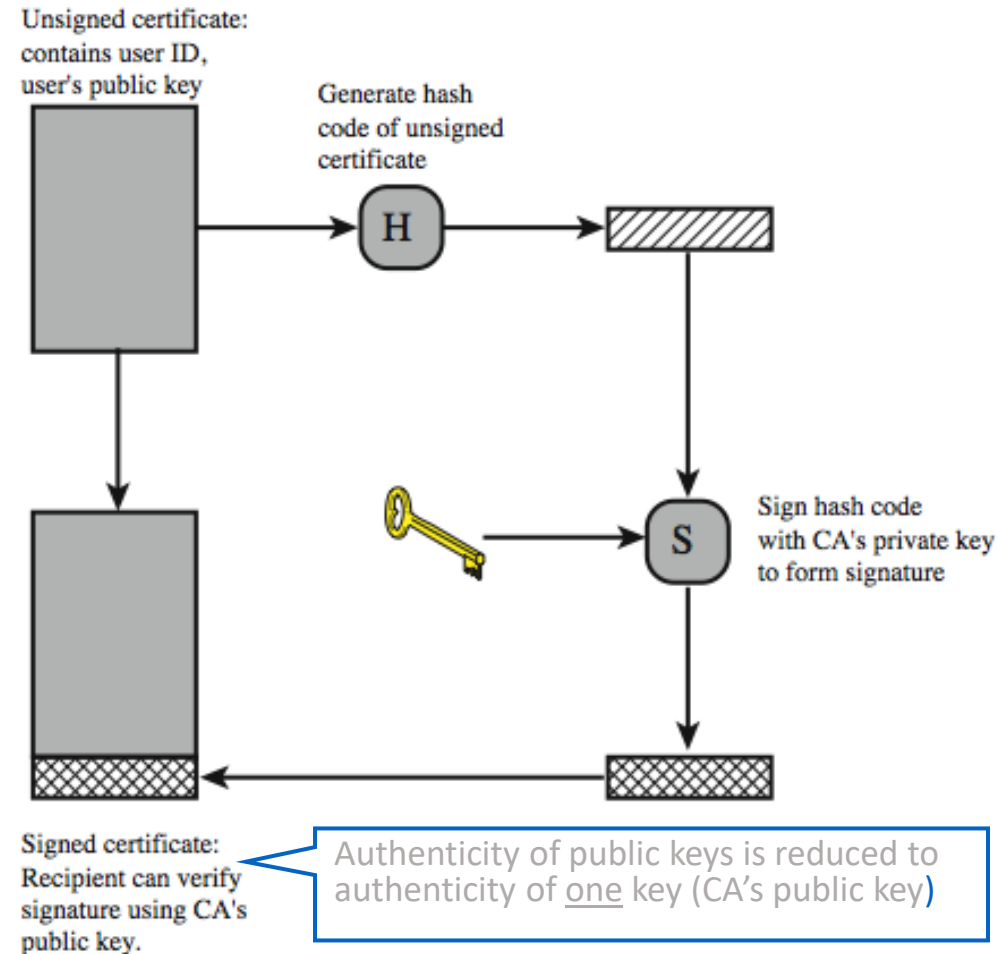


Digital Certificates

- A certificate is being issued and digitally signed by a C
 - The signature ensures the genuineness of the certificate (since the CA is trusted; equivalently, anyone can verify the CA's signature, whereas nobody can create a CA's signature)
- By these means, it is ensured that an entity indeed has a public key (the one that is being “written” within the corresponding certificate)
- The owner of a certificate is able to provide digital signatures
- Common standard: X.509



Using Public-Key Certificates





X.509 Authentication Service

- Internet standard (1988-2000)
- Specifies certificate format
 - X.509 certificates are used in widely used protocols such as IPsec and SSL/TLS
- Specifies certificate directory service
 - For retrieving other users' CA-certified public keys
- Specifies a set of authentication protocols
 - For proving identity using public-key signatures
- Does not specify crypto algorithms
 - Can use it with any digital signature scheme and hash function, but hashing is required before signing



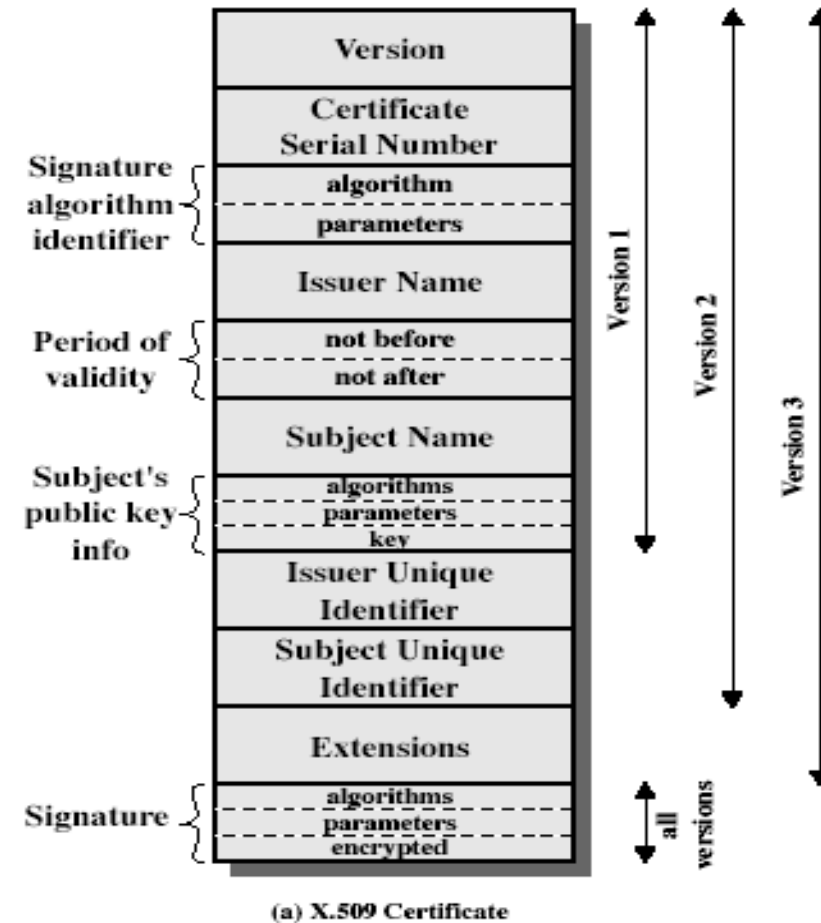
Digital Certificates - structure

- Digital Certificate is the secure binding between an entity and his/her public key, such that we have data integrity, authentication and non-repudiation.
- The secure binding is done by a trusted third party, known as Certificate Authority.
- They overcome the short comings of *public key cryptography*, which is that anyone can purport to be the owner of public key.
- Contains
 - The name of an issuer, a CA that issued the certificate.
 - Name of the entity, who is issued this certificate.
 - The dates between which the certificate is valid.
 - The certificate's serial number, which is guaranteed by the CA to be unique.
 - Public key
 - The uses of the key-pair (the public key and the associated private key) identified in the certificate.



X.509 certificate

- User A obtains user's B public key via getting the digital certificate of B, which contains his public key
- This certificate is digitally signed by a CA, which is a trusted third party
- A is ensured for the validity of the certificate because she trusts the CA which has signed it (whereas A can validate CA's signature)
 - Hence, by these means, A is ensured for obtaining the genuine public key of B



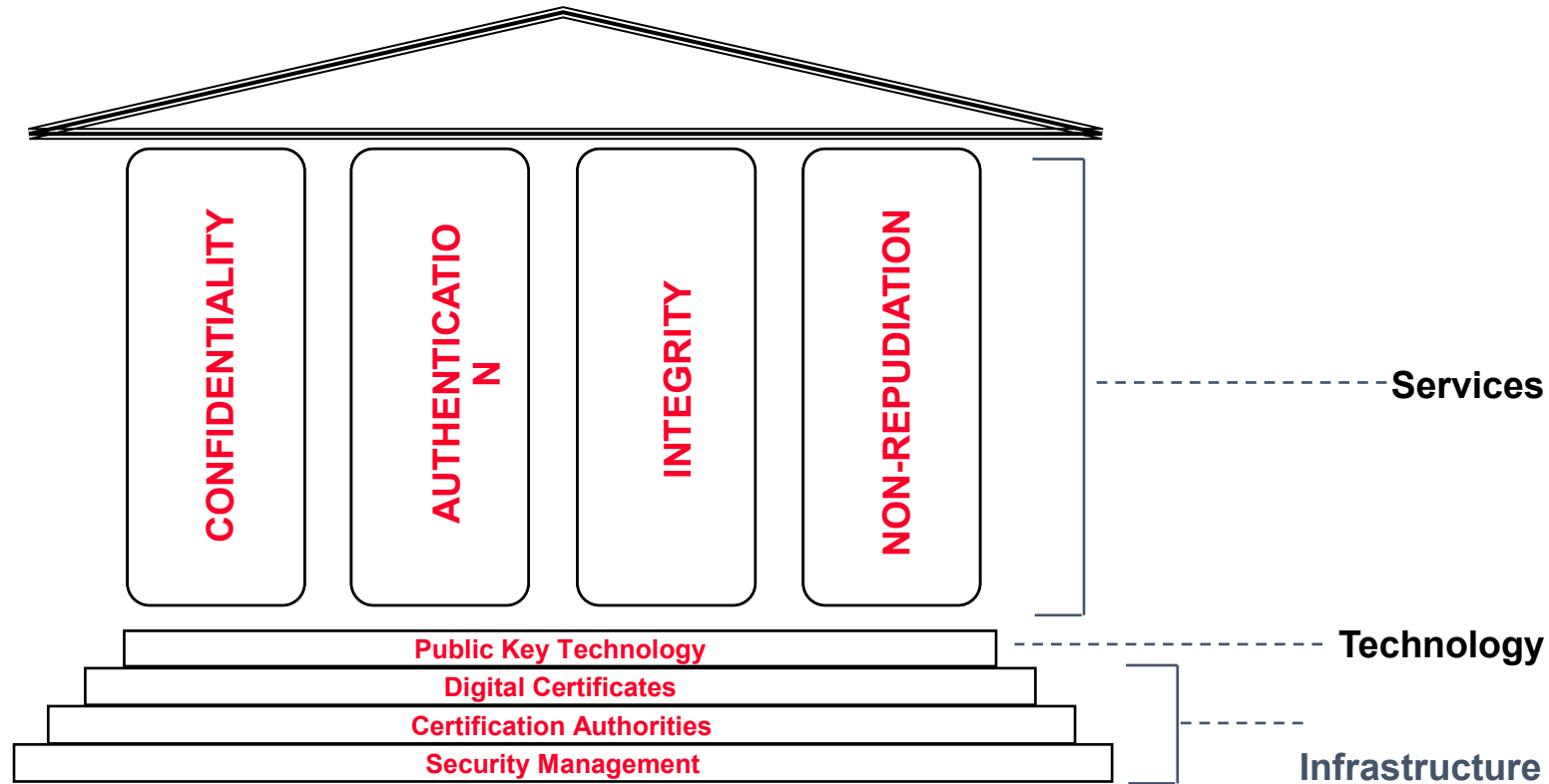


TLS protocol

- **Transport Layer Security (TLS):** Security protocol for establishing a secure connection between a client and a server
- Server's authentication is ensured by using digital certificates
 - Signed by a trusted CA
- Data between server and client are encrypted through a symmetric cipher
 - A MAC is being also used for message authentication
 - Or an authenticated encryption
- For securely exchanging the keys for the symmetric cipher and the MAC, a public key algorithm is being used
 - The server's public key lies inside the server's certificate
 - Since the certificate is signed by a CA, man-in-the-middle attacks are efficiently addressed*
- **TLS provides security services to higher protocols**
 - HTTP over TLS: HTTPS



Public Key Security



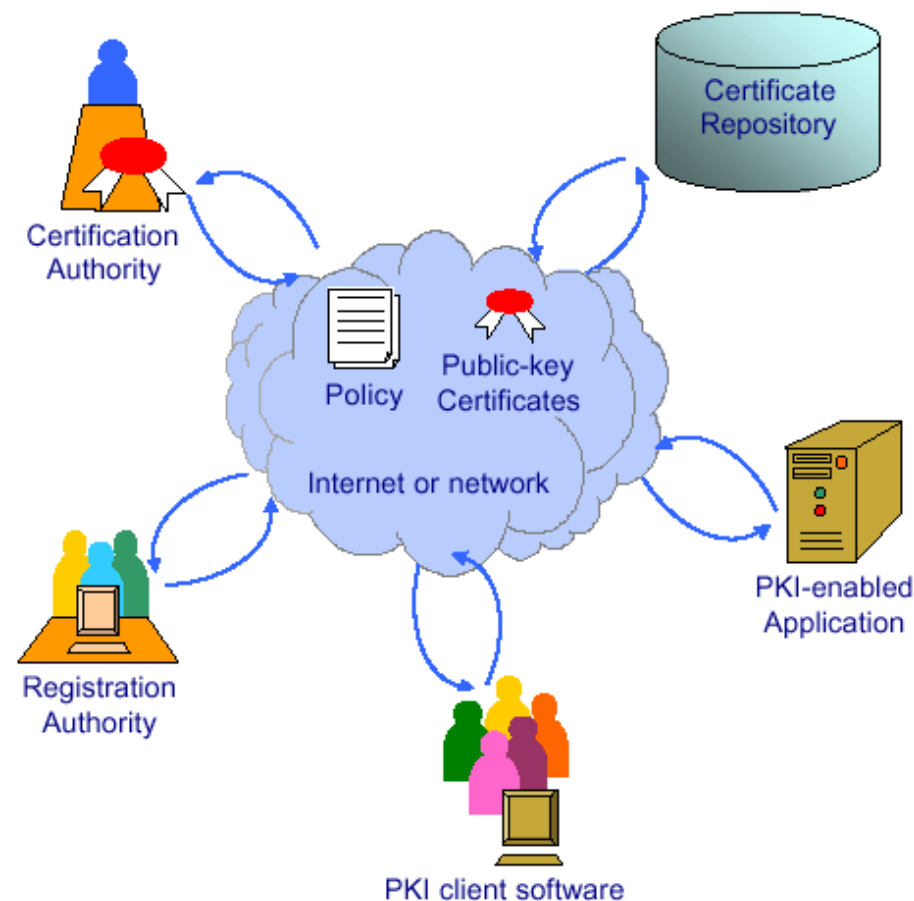
- Public Key Technology Best Suited to Solve Business Needs
- Infrastructure = Certification Authorities – known as Public Key Infrastructure (PKI)



X. 509 certificate

Public Key Infrastructure (PKI):
the set of protocols, services,
standards, entities etc.
regarding the handling of digital
certificates

- Main certification providers
 - Entrust, Verisign, RSA Security, Equifax ...





In practice

- Platforms like Windows, macOS, Android, maintain a system root store that is used to determine if a certificate issued by a particular Certificate Authority (CA) is trusted
- In Android (versions larger than 8.0), follow these steps:
 - Open Settings
 - Tap “Security & location”
 - Tap “Encryption & credentials”
 - Tap “Trusted credentials.” This will display a list of all trusted certs on the device.



Pretty Good Privacy (PGP)

- Invented by Phil Zimmerman
- Available for any platform
 - GPG: <http://www.gpg4win.org/> (Gnu Privacy Guard)
 - The same design principles with the GPG
- Implements several known cryptographic algorithms (AES, RSA etc.)



PGP

- PGP (Pretty Good Privacy)
 - The users are able to “sign” the public keys of the other users, once they are sure for their identities
 - Hence, each user is a CA
 - Users trust a public key that is being found on a public PGP key server if it has been signed by another user who is trusted
- The PGP software is a nice option for encrypting files or e-mails
 - Its main version it not currently free
 - Provided by Symantec
 - Instead: GPG (free application), OpenPGP



PGP Operation – Authentication

- Sender creates a message
- SHA-2 used to generate the hash code of message
- The hash code is encrypted with RSA using the sender's private key, and result is attached to message
- The receiver uses RSA with sender's public key to decrypt and recover hash code
- Receiver generates new hash code for message and compares with decrypted hash code, if match, message is accepted as authentic



PGP Operation – Confidentiality

- The sender generates message and random 256-bit number to be used as session key for this message only
 - uses random inputs taken from previous uses and from keystroke timing of user
- The message is encrypted, using AES with session key
- The session key is encrypted using RSA with recipient's public key, then attached to message
- The receiver uses RSA with its private key to decrypt and recover session key
- The session key is used to decrypt message



PGP Operation – Confidentiality & Authentication

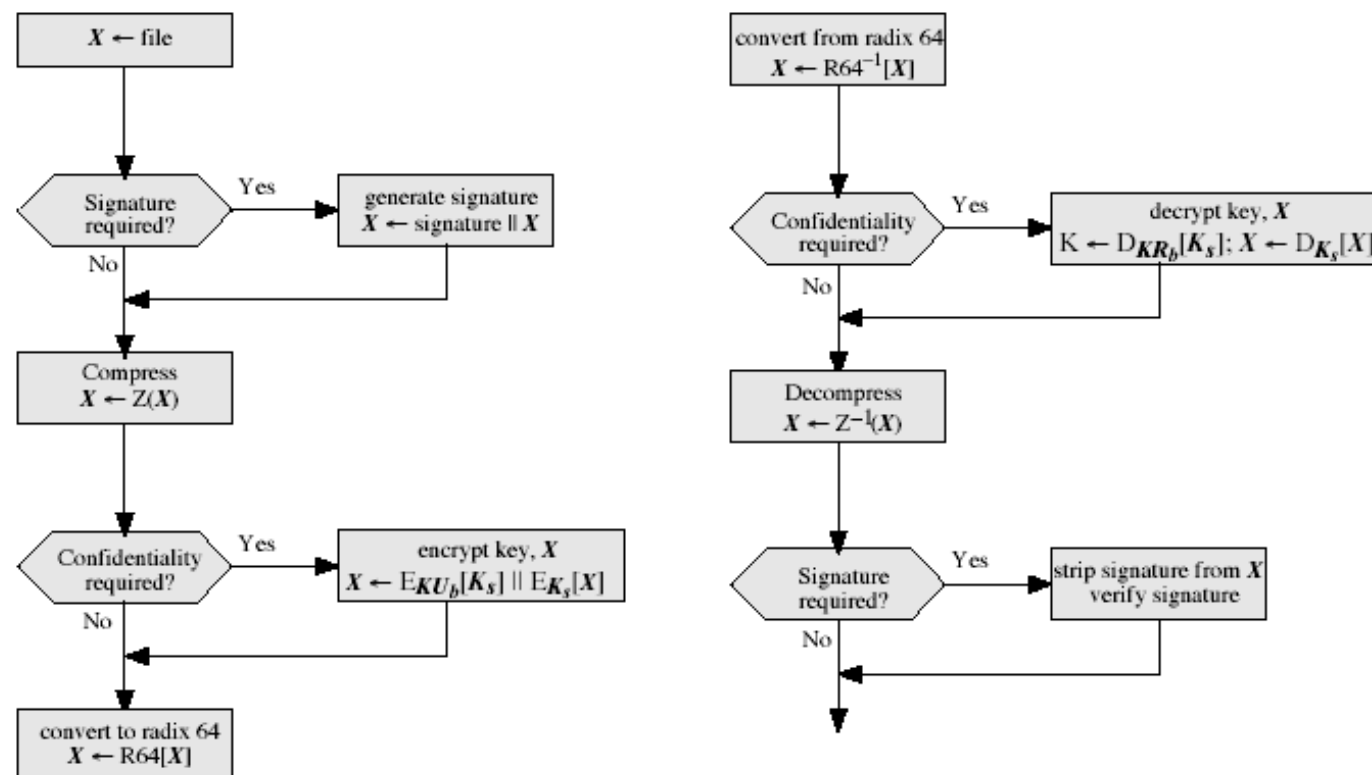


Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

- uses both services on same message
 - create signature & attach to message
 - encrypt both message & signature
 - attach RSA encrypted session key
- By default, PGP compresses message after signing but before encrypting
 - uses ZIP compression algorithm



A diagram of PGP operation



(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

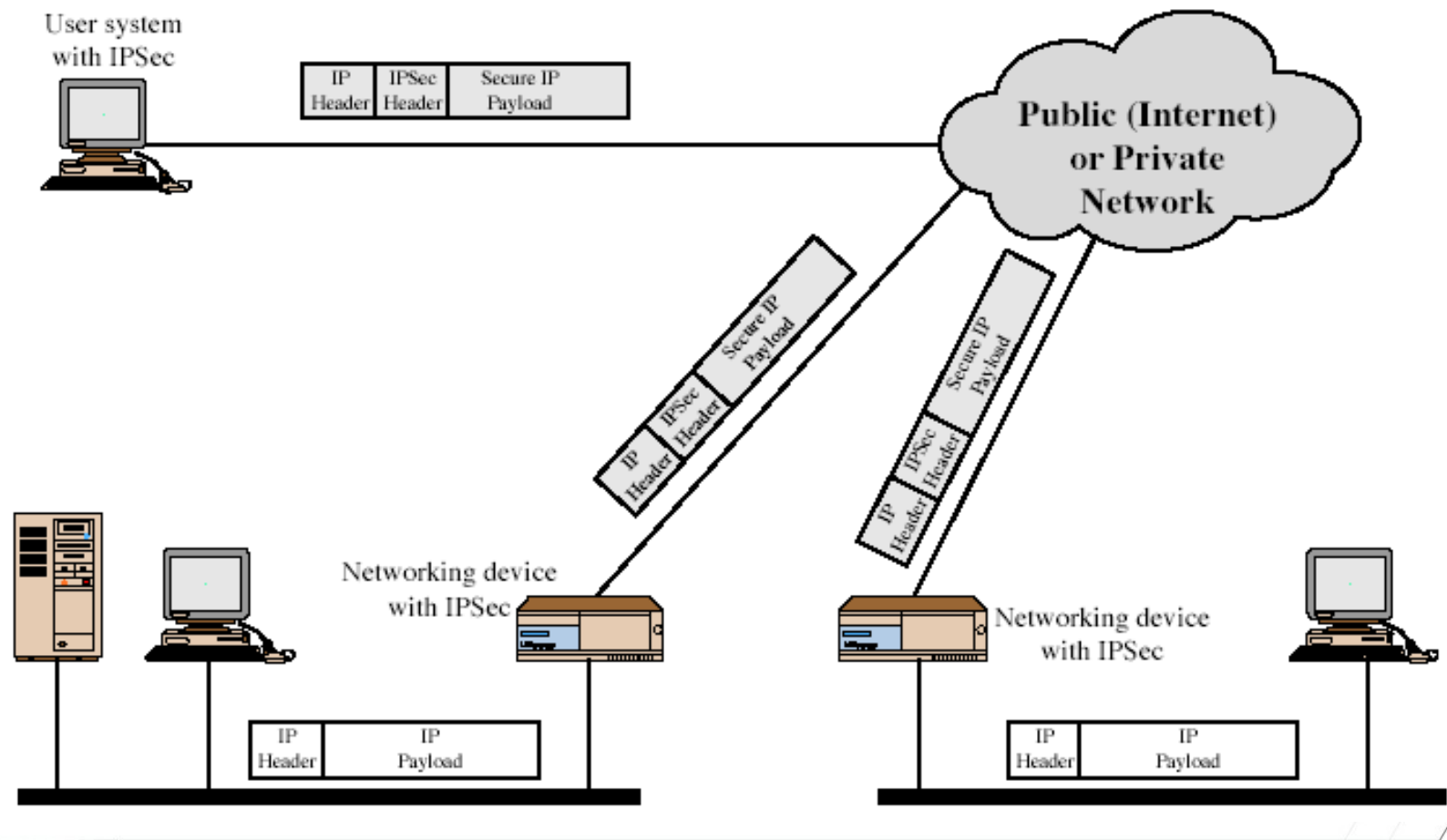


IPSec

- Protocol for “forcing” security in the Internet Protocol (IP) level
- Being determined in a set of RFCs (2401/2402/2406/2408)
- Ensures
 - Authentication
 - Confidentiality
 - Key management
- All these are being implemented into the IP packets, so any higher-level applications (mail, file transfer) may rely on this lower-level security
- Applications
 - Setting up a secure Virtual Private Network (VPN) over the Internet or over a public WAN
 - Less cost for the organization than using leased lines for a private network
 - Remote users (employees / external workers) may securely connect to the organization’s network



An IPSec case



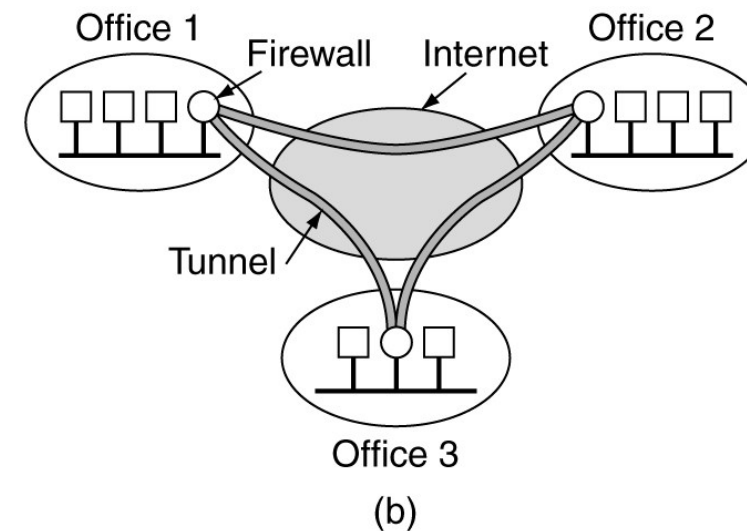
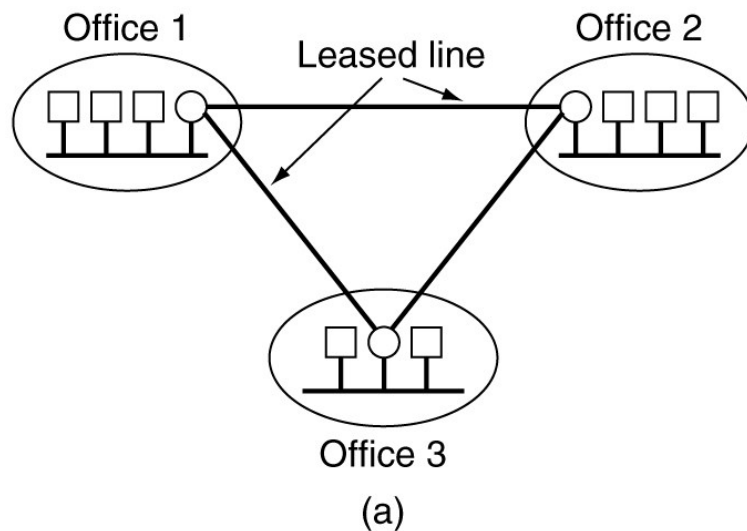


Virtual Private Networks – VPNs

- A safe and encrypted connection over a less secure **network**, such as the public internet.
- A **VPN** works by using the shared public infrastructure while maintaining security features (confidentiality, integrity, authentication) through security procedures and tunneling protocols
- Desired goals
 - Security
 - No degradation in QoS



Virtual Private Networks

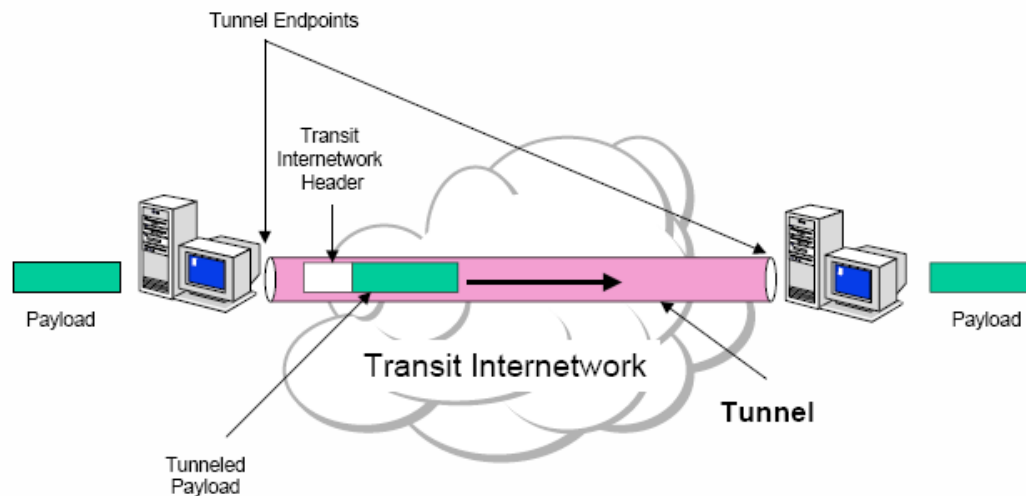


(a) A leased-line private network. (b) A virtual private network



What is a tunnel

- The virtual connections are being implemented by creating “special” IP packets. By these means, a so-called tunnel is being built (the network in which these special secure packets are being sent)



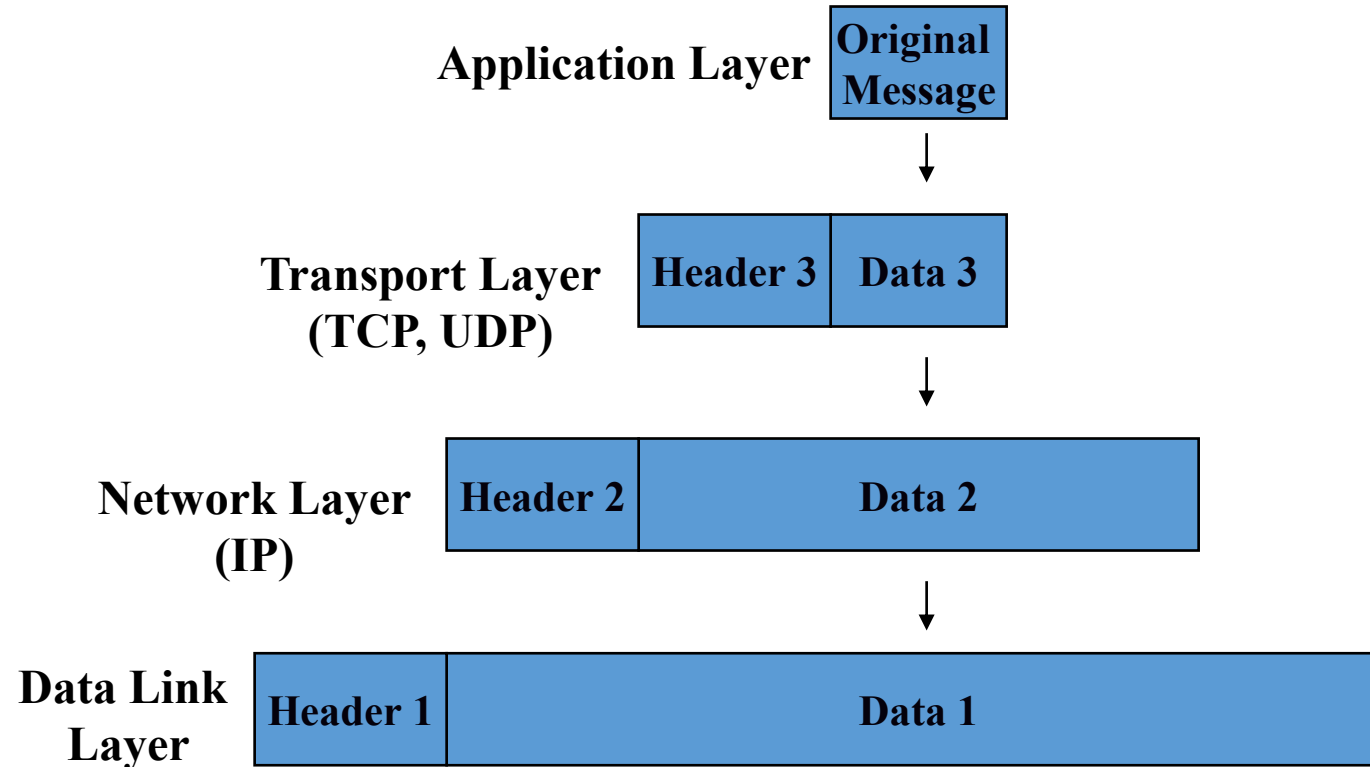


Benefits of IPSec

- IPSec provides strong security that can be applied to all traffic crossing the network perimeter
- IPSec is below the transport layer (TCP/UDP) and, thus, is transparent to applications
 - There is no need to change software on a user's system when IPSec is implemented in a router
- IPSec can be transparent to end users
 - There is no need to train users on security mechanisms or revoke material when users leave the organisation
- IPSec can provide security for individual users if needed
 - Useful for offsite workers



Encapsulation in TCP/IP



- IPsec defines a new set of headers, which are being attached to the original IP packets, thus producing "new" IP packets in such a way that security requirements are met



Basic IPSec functionalities

- Two protocols (each of them has its own headers):
 - **The Authentication Header (AH) Protocol,**
 - **The Encapsulating Security Payload (ESP)**
- The AH protocol provides source authentication and data integrity, but not confidentiality.
- The ESP protocol was designed after the AH protocol was already in use. ESP does whatever AH does with an additional functionality: confidentiality.
- IPSec supports both IPv4 and IPv6
- Known cryptographic primitives are also used:
 - Diffie-Hellman key exchange algorithm
 - AES or other block ciphers for encryption
 - Hash functions for message integrity
 - Digital certificates for validating the public keys



IPSec modes of operation

- Transport Mode:

Initial IP packet

| | | |
|------------------|-------------------|-------------|
| IP Header | TCP Header | Data |
|------------------|-------------------|-------------|

Transport Mode protected packet

| | | | |
|------------------|---------------------|-------------------|-------------|
| IP Header | IPSec Header | TCP Header | Data |
|------------------|---------------------|-------------------|-------------|

protected

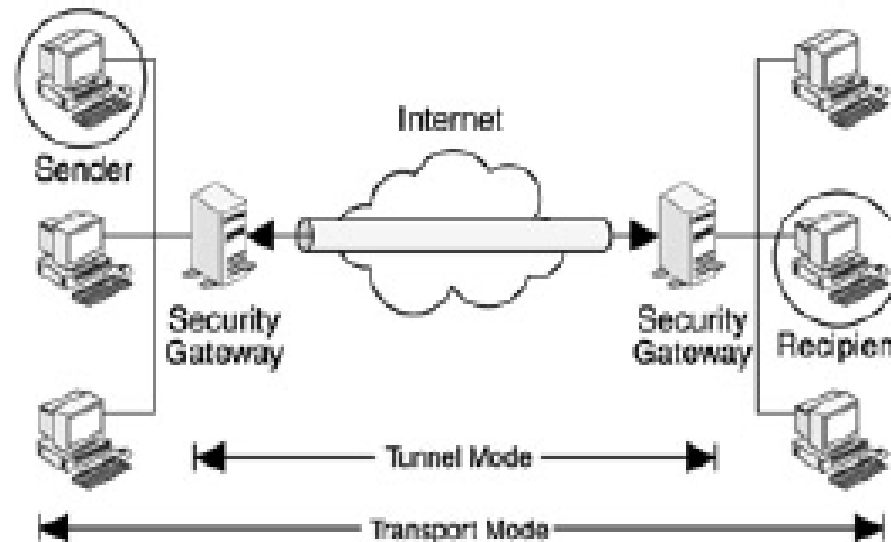
- Tunnel Mode (especially in VPN set-ups):

Tunnel Mode protected packet

| | | | | |
|----------------------|---------------------|---------------------------|-------------------|-------------|
| New IP Header | IPSec Header | Original IP Header | TCP Header | Data |
|----------------------|---------------------|---------------------------|-------------------|-------------|

protected

Basic IPSec functionalities

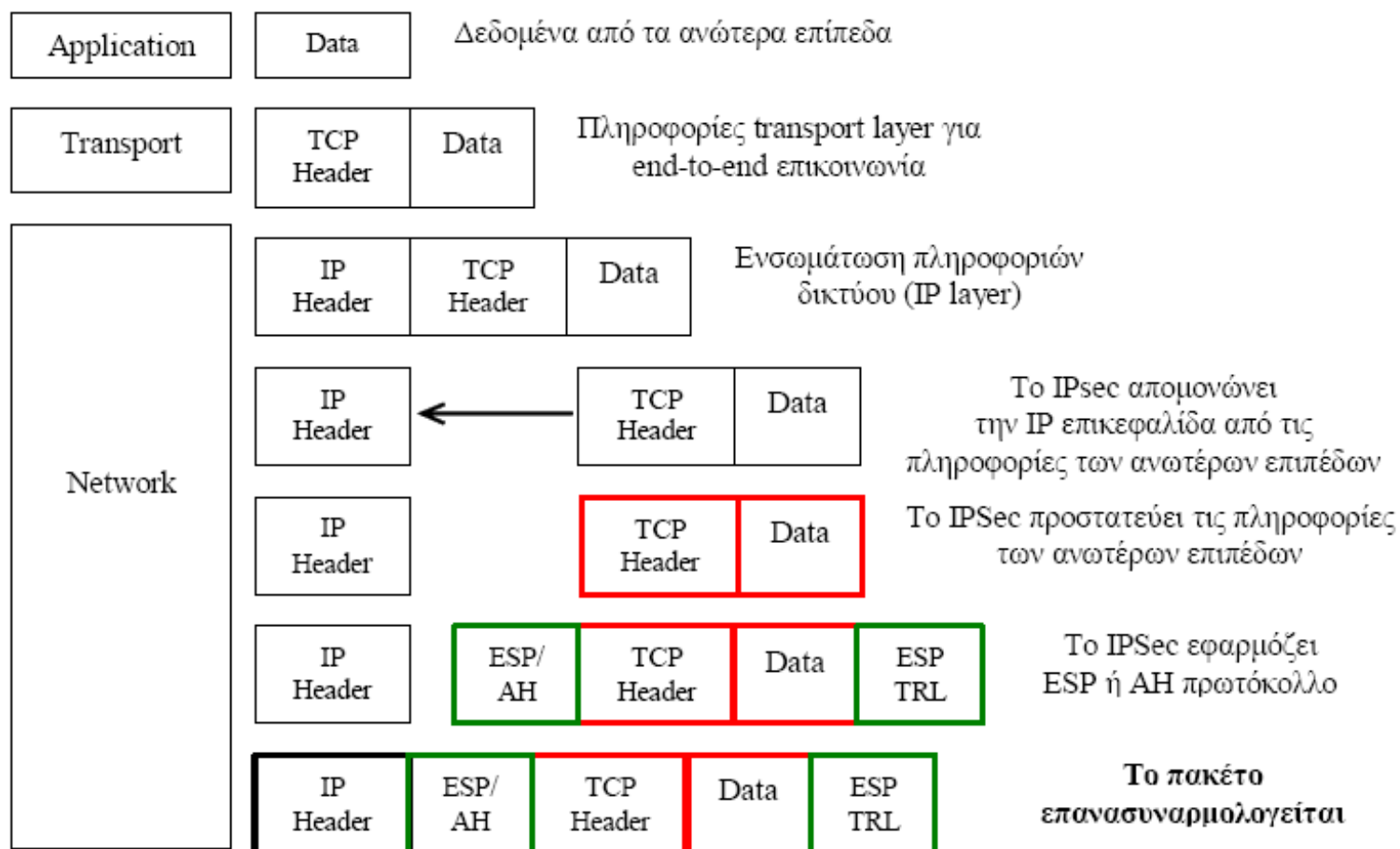


- Tunnel mode:
 - Between gateways (routers/firewalls)
- Transport mode:
 - For end-to-end security (e.g. Client-server applications).

In both modes, either AH or ESP can be used (thus resulting in 4 possible combinations)

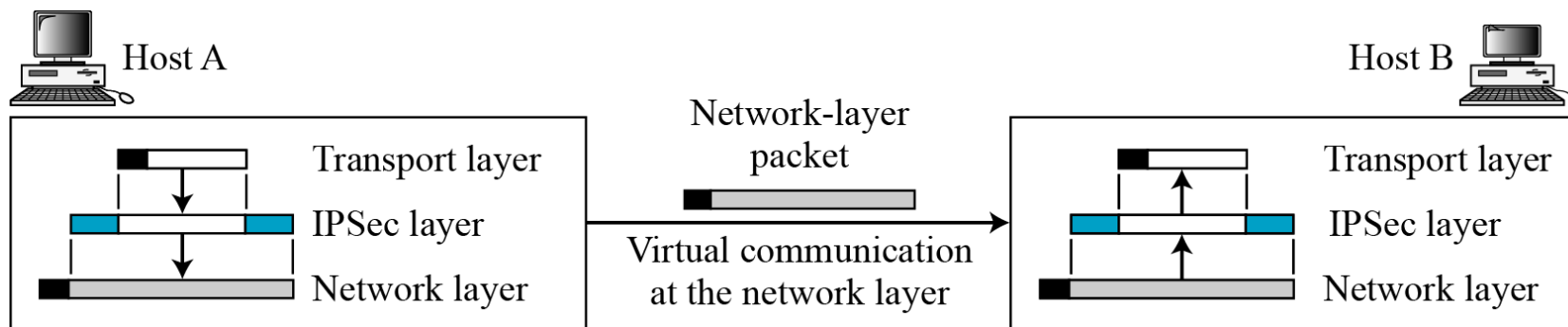
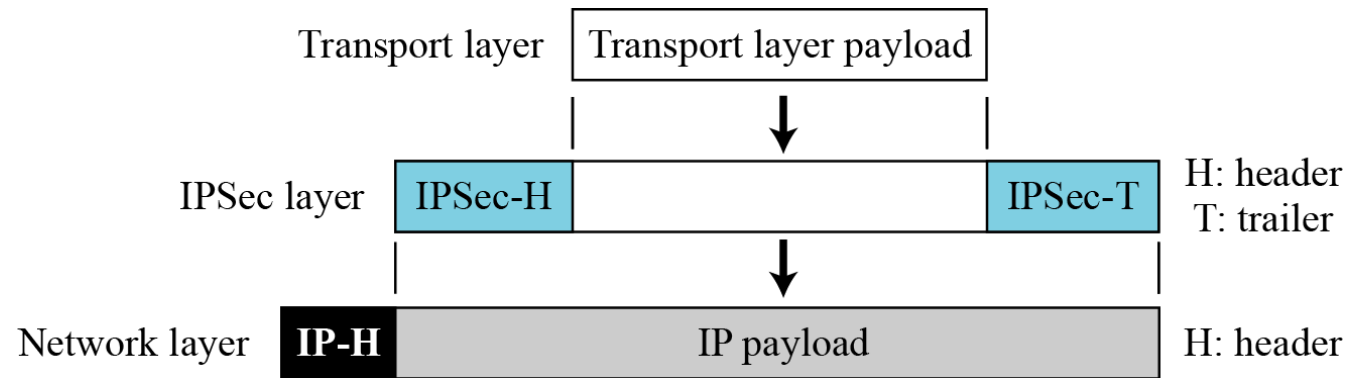


IPSec in transport mode



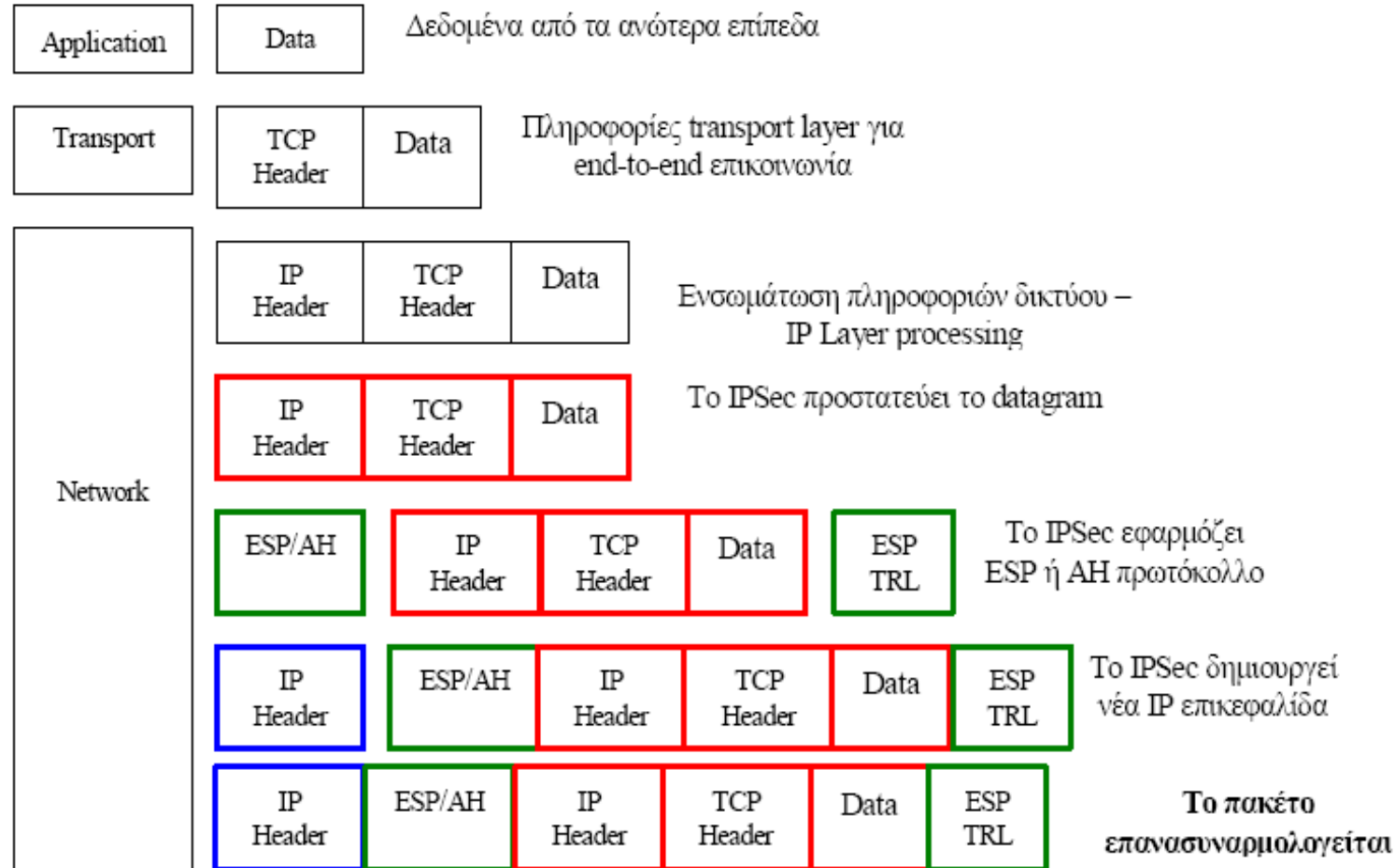


Transport mode



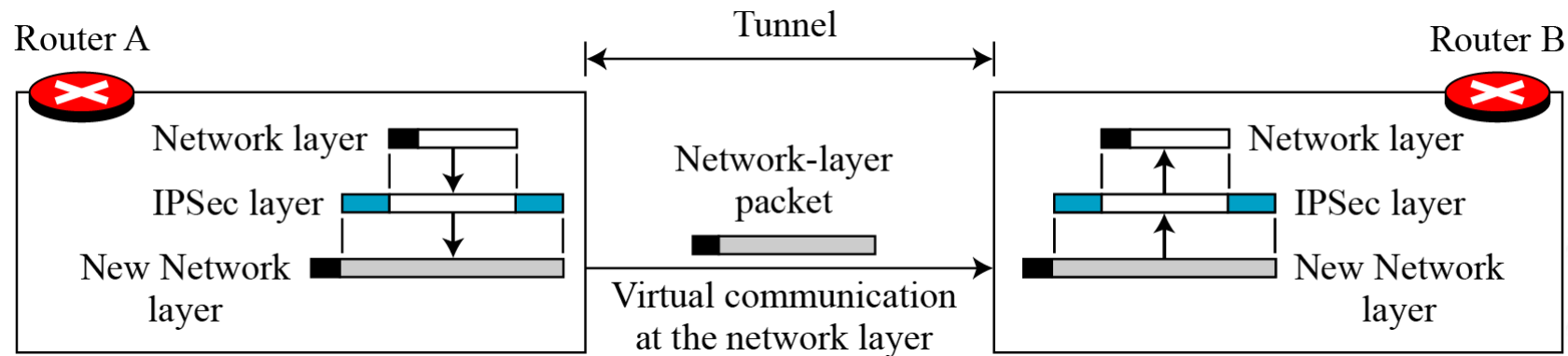
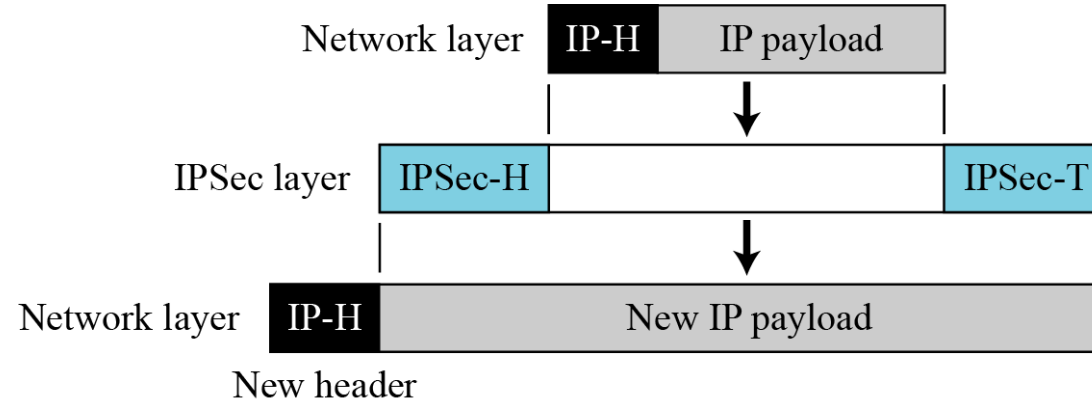


IPSec in tunnel mode



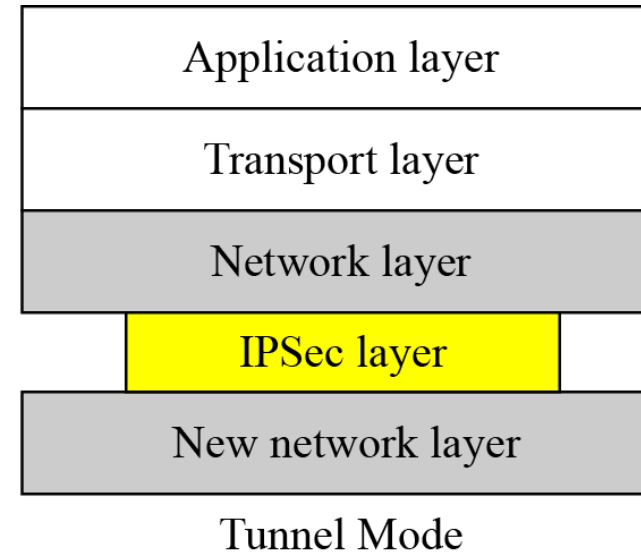
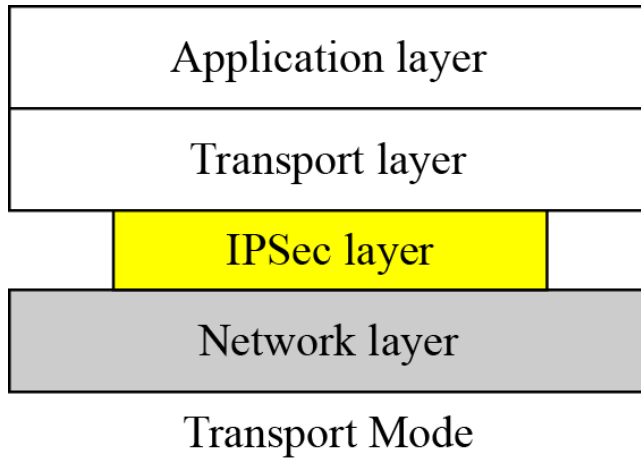


Tunnel mode





Transport mode vs. tunnel mode





A comparison

- Tunnel mode: Gateways (routers) act as IPSec proxies, namely the user's operating system does not need any special software. Moreover, it provides security against traffic analysis, since the initial IP addresses are encrypted. However, it requires more computational cost than the transport mode.
- Transport mode: Less computation cost, since only a few more bytes are being added. Moreover, since the gateways “see” the initial source/destination IP addresses, routings based on desired QoS can be performed. A drawback is that traffic analysis is now achievable.

Personal and anonymous data

Definitions (GDPR)



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



- The term “**personal data**” refers to any information relating to an **identified** or **identifiable** natural person
- The data protection principles do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person
- However, to determine whether a natural person is identifiable, account should be taken **of all the means reasonably likely to be used**, such as singling out, by any person to identify – directly or indirectly – the natural person
 - Objective factors, such as the costs of and the amount of time required for identification, should be taken into account
- *In simple words, we should be very careful when characterizing data as anonymous data*
- *Have we thoroughly examined whether identification is practically fully impossible?*
 - *Identification in which context?*

The famous AOL incident (2006)



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

August 2006: research.aol.com

AOL is embarking on a new direction for its business making its content and products freely available to all consumers. To support those goals, AOL is also embracing the vision of an open research community. To get started, we invite you to visit us at <http://research.aol.com>, where you will find:

- ...
- ***Query streams for 500,000 users over 3 months (20 million queries)***
-
- A random ID was associated to each user
 - The same (meaningless) ID, for the same user
- However, a combination of the published information with other available data could allow identification!



The user #4417749



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

HOME PAGE MY TIMES TODAY'S PAPER VIDEO MOST POPULAR TIMES TOPICS

The New York Times

Technology


WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION

CAMCORDERS CAMERAS CELLPHONES COMPUTERS HANDHELDS HOME VIDEO MUSIC PERIPHERALS

A Face Is Exposed for AOL Searcher No. 4417749

By MICHAEL BARBARO and TOM ZELLER Jr.
Published: August 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.



No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from “numb fingers” to “60 single men” to “dog that urinates on everything.”

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for “landscapers in Lilburn, Ga.,” several people with the last name Arnold and “homes sold in shadow lake subdivision gwinnett county georgia.”

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. “Those are my searches,” she said, after a reporter read part of the list to her.

AOL removed the search data from its site over the weekend and apologized for its release, saying it was an unauthorized move by a team that had hoped it would benefit academic researchers.

But the detailed records of searches conducted by Ms. Arnold and 657,000 other Americans, copies of which continue to circulate online, underscore how much people unintentionally reveal about themselves when they use search engines — and how risky it

Multimedia

[Graphic: What Revealing Search Data Reveals](#)

ERIK S. LESSER FOR THE NEW YORK TIMES
Thelma Arnold's identity was betrayed by AOL records of her Web searches, like ones for her dog, Dudley, who clearly has a problem.

SIGN IN TO E-MAIL THIS

PRINT

SINGLE PAGE

REPRINTS

SAVE

ARTICLE TOOLS SPONSORED BY HISTORY BOYS

- The characterization of anonymous data is not an easy task
- Simply removing “obvious identifiers” is not adequate
- In other words, the notions of identifiers or “identifying data” is wide
 - Identifier in which context?

The notion of pseudonymisation



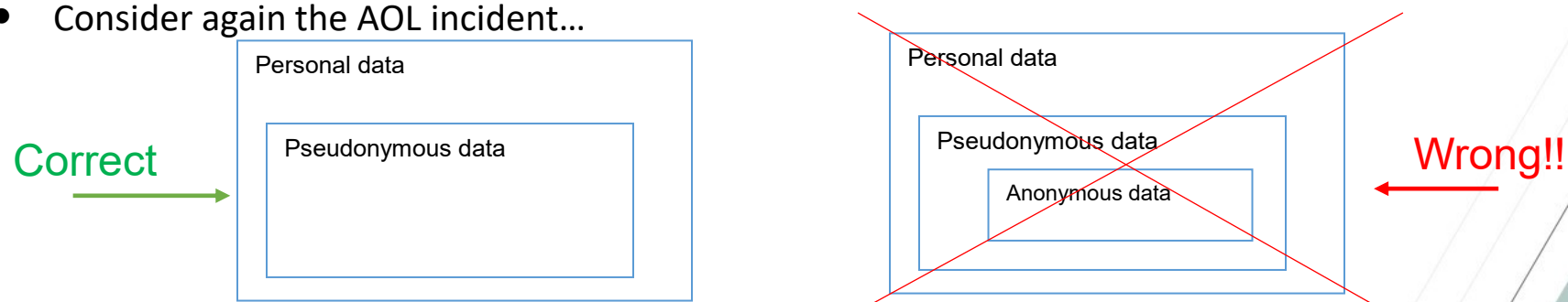
- According to ISO/TS 25237:2017 standard:
- *“Pseudonymisation is a particular type of de-identification that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms”*
- *De-identification is a general term for any process of reducing the association between a set of identifying data and the data subject.*
- A *pseudonym* a personal identifier that is different from the normally used personal identifier and is used with pseudonymized data to provide dataset coherence linking all the information about a data subject, without disclosing the real world person identity’.
- As a note to the latter definition, it is stated in ISO/TS 25237:2017 that pseudonyms are usually restricted to mean an identifier that does not allow the direct derivation of the normal personal identifier. They can either be derived from the normally used personal identifier in a reversible or irreversible way or be totally unrelated.



The notion of pseudonymisation in the GDPR



- “Pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information, **provided that such additional information is kept separately and is subject to technical and organisational measures** to ensure that the personal data are not attributed to an identified or identifiable natural person
- Personal data which have undergone pseudonymisation should be considered to be information on an identifiable natural person.
- That is pseudonymization does not result in anonymous data
 - Additional information to allow re-identification does exist (somewhere...)
 - Consider again the AOL incident...



Benefits of pseudonymisation on personal data protection



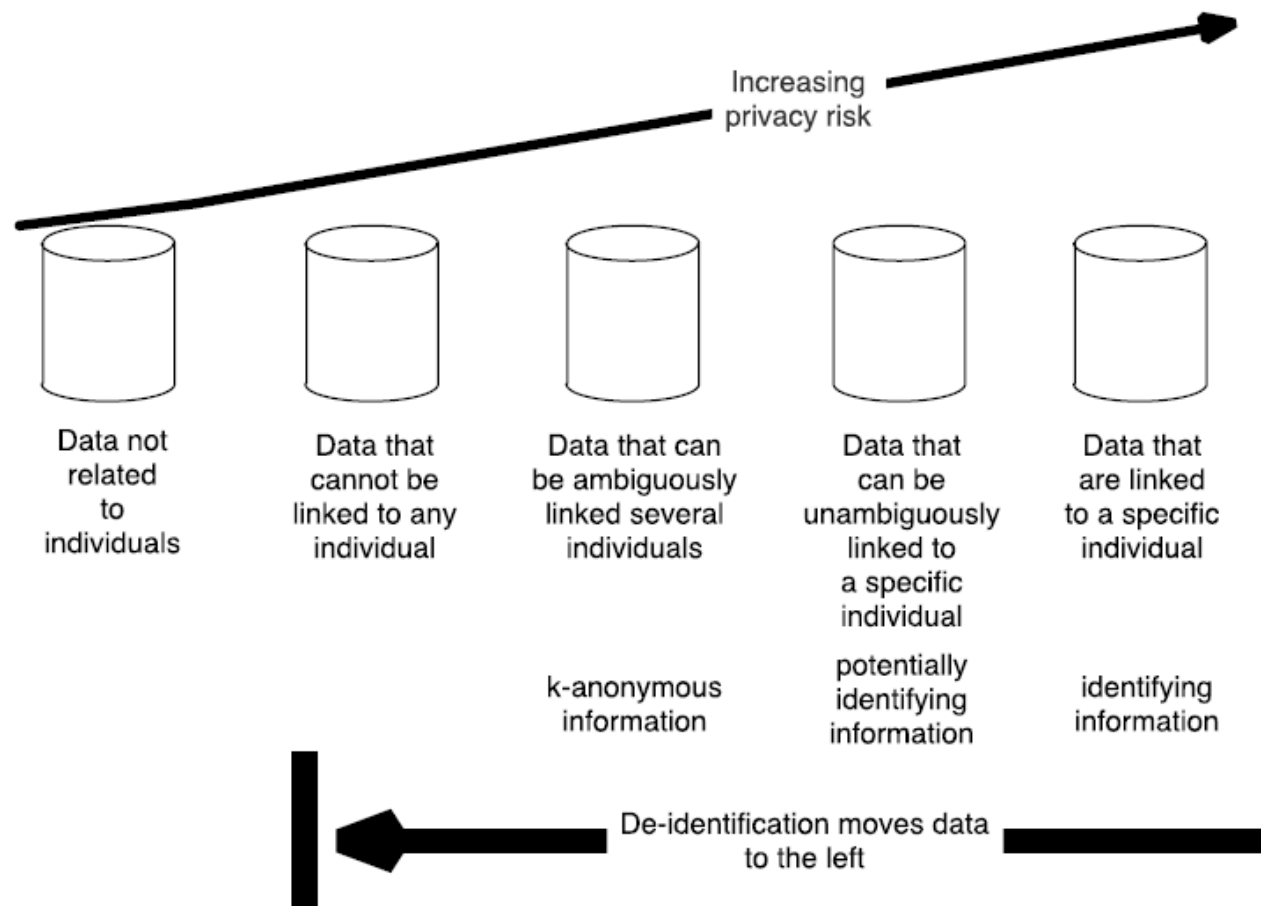
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης



- The GDPR makes about 15 references to pseudonymisation
 - Possible appropriate safeguard for:
 - *“purpose limitation balancing test” (art. 6, par. 4)*
 - *Data protection by design and by default (art. 25)*
 - *Security of processing (art. 32)*
 - *Processing of personal data for public interest, scientific or historical research purposes or statistical purposes (art. 89)*
- Pseudonymisation is also implied in several other places within GDPR
 - When the controller is able to demonstrate that is not in a position to identify the individual (data subject), Art. 15-20 shall not apply – i.e. right of access, right to rectification/erasure/restriction/portability (*art. 11*)
 - *Unless the data subject provides additional information enabling his/her identification*
 - Appropriately-implemented pseudonymisation can reduce the likelihood of individuals being identified in the event of a personal data breach



«Phases» of Anonymization



S. L. Garfinkel, “De-Identification of Personal Information”, NIST Internal Report 8053, 2015



When a Person can be Identified?



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

- In addition to the **identifiers**, there are the **quasi-identifiers** which when combined can lead to the identification of a person!

| Identifier | Quasi-identifier | | | Sensitive attribute |
|------------|------------------|--------|---------|---------------------|
| Name | DOB | Gender | Zipcode | Disease |
| Andre | 1/21/76 | Male | 53715 | Heart Disease |
| Beth | 4/13/86 | Female | 53715 | Hepatitis |
| Carol | 2/28/76 | Male | 53703 | Brochitis |
| Dan | 1/21/76 | Male | 53703 | Broken Arm |
| Ellen | 4/13/86 | Female | 53706 | Flu |
| Eric | 2/28/76 | Female | 53706 | Hang Nail |

Removal of Identifiers cannot guarantee anonymity



An example of «Bad Anonymization»

(a) Patient table

| Job | Sex | Age | Disease |
|----------|--------|-----|-----------|
| Engineer | Male | 35 | Hepatitis |
| Engineer | Male | 38 | Hepatitis |
| Lawyer | Male | 38 | HIV |
| Writer | Female | 30 | Flu |
| Writer | Female | 30 | HIV |
| Dancer | Female | 30 | HIV |
| Dancer | Female | 30 | HIV |

- Assume that a Hospital provides the above “anonymized” table (after removal of all data that could lead to the identification of a person (Name, ID number, VAT number, Social security number etc)).



An example of «Bad Anonymization»

(a) Patient table

| Job | Sex | Age | Disease |
|----------|--------|-----|-----------|
| Engineer | Male | 35 | Hepatitis |
| Engineer | Male | 38 | Hepatitis |
| Lawyer | Male | 38 | HIV |
| Writer | Female | 30 | Flu |
| Writer | Female | 30 | HIV |
| Dancer | Female | 30 | HIV |
| Dancer | Female | 30 | HIV |

(b) External table

| Name | Job | Sex | Age |
|--------|----------|--------|-----|
| Alice | Writer | Female | 30 |
| Bob | Engineer | Male | 35 |
| Cathy | Writer | Female | 30 |
| Doug | Lawyer | Male | 38 |
| Emily | Dancer | Female | 30 |
| Fred | Engineer | Male | 38 |
| Gladys | Dancer | Female | 30 |
| Henry | Lawyer | Male | 39 |
| Irene | Dancer | Female | 32 |

Source: B. Fung et.al., Privacy-Preserving Data Publishing: A Survey of Recent Developments, ACM Computing Surveys, 2010

- Assume that somebody knows that the list provided by the Hospital includes some specific persons (e.g. residents of a small village)
- For these persons data can be easily found from publicly available sources (Table b)
- By combining the two Tables we can identify some persons
 - E.g. (Job, Sex, Age) = (Laywer, Male, 38) reveals that Doug suffers form HIV



Addressing the Problem – «Generalization»

- To avoid this type of attacks we can appropriately modify the values of quasi-identifiers, through generalization:
 - E.g. we do not release the precise age but, instead, an age range (for instance 30-40)
 - The greater the Generalization the better the anonymity, although we may miss useful information
 - The aim is to achieve the best possible anonymization with the least possible loss of information



«Generalizing» the previous table

(a) Patient table

| Job | Sex | Age | Disease |
|----------|--------|-----|-----------|
| Engineer | Male | 35 | Hepatitis |
| Engineer | Male | 38 | Hepatitis |
| Lawyer | Male | 38 | HIV |
| Writer | Female | 30 | Flu |
| Writer | Female | 30 | HIV |
| Dancer | Female | 30 | HIV |
| Dancer | Female | 30 | HIV |

«Generalization»



| Job | Sex | Age | Disease |
|--------------|--------|---------|-----------|
| Professional | Male | [35-40] | Hepatitis |
| Professional | Male | [35-40] | Hepatitis |
| Professional | Male | [35-40] | HIV |
| Artist | Female | [30-35] | Flu |
| Artist | Female | [30-35] | HIV |
| Artist | Female | [30-35] | HIV |
| Artist | Female | [30-35] | HIV |

| Job | Sex | Age | Disease |
|--------------|--------|---------|-----------|
| Professional | Male | [35-40] | Hepatitis |
| Professional | Male | [35-40] | Hepatitis |
| Professional | Male | [35-40] | HIV |
| Artist | Female | [30-35] | Flu |
| Artist | Female | [30-35] | HIV |
| Artist | Female | [30-35] | HIV |
| Artist | Female | [30-35] | HIV |

(b) External table

| Name | Job | Sex | Age |
|--------|----------|--------|-----|
| Alice | Writer | Female | 30 |
| Bob | Engineer | Male | 35 |
| Cathy | Writer | Female | 30 |
| Doug | Lawyer | Male | 38 |
| Emily | Dancer | Female | 30 |
| Fred | Engineer | Male | 38 |
| Gladys | Dancer | Female | 30 |
| Henry | Lawyer | Male | 39 |
| Irene | Dancer | Female | 32 |

??





Generalization Criteria



- k-anonymity – (Samarati-Sweeney, 1998):
In an anonymous table the number of records with the same quasi-identifiers values is at least k
- Clearly, the bigger k is, the better the anonymity
- For the previous example: Anonymous with $k = 3$

| Job | Sex | Age | Disease |
|--------------|--------|---------|-----------|
| Professional | Male | [35-40) | Hepatitis |
| Professional | Male | [35-40) | Hepatitis |
| Professional | Male | [35-40) | HIV |
| Artist | Female | [30-35) | Flu |
| Artist | Female | [30-35) | HIV |
| Artist | Female | [30-35) | HIV |
| Artist | Female | [30-35) | HIV |



Alternative Approach

- Suppression: Some fields or entire records are deleted

| # | Zip | Age | Nationality | Condition |
|---|-------|------|-------------|-----------------|
| 1 | 130** | < 40 | * | Heart Disease |
| 2 | 130** | < 40 | * | Heart Disease |
| 3 | 130** | < 40 | * | Viral Infection |
| 4 | 130** | < 40 | * | Flu |

Generalization

Suppression

- Maximum Generalization is equivalent to Suppression



Is k-anonymity enough ?



- Let us assume the following:

| | <i>Zip</i> | <i>Age</i> | <i>National</i> |
|---------|-------------------|-------------------|------------------------|
| Bob → | 13053 | 31 | American |
| Akira → | 13068 | 21 | Japanese |

- and that someone makes public the following data:



Data Set



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

| | <i>Non-Sensitive Data</i> | | | <i>Sensitive Data</i> |
|----------|---------------------------|------------|--------------------|-----------------------|
| # | ZIP | Age | Nationality | Condition |
| 1 | 13053 | 28 | Russian | Heart Disease |
| 2 | 13068 | 29 | American | Heart Disease |
| 3 | 13068 | 21 | Japanese | Viral Infection |
| 4 | 13053 | 23 | American | Viral Infection |
| 5 | 14853 | 50 | Indian | HIV |
| 6 | 14853 | 55 | Russian | Heart Disease |
| 7 | 14850 | 47 | American | Viral Infection |
| 8 | 14850 | 49 | American | Viral Infection |
| 9 | 13053 | 31 | American | HIV |
| 10 | 13053 | 37 | Indian | HIV |
| 11 | 13068 | 36 | Japanese | HIV |
| 12 | 13068 | 35 | American | HIV |



k-anonymity with k=4



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

| | <i>Non-Sensitive Data</i> | | | <i>Sensitive Data</i> |
|-------|---------------------------|------------|--------------------|-----------------------|
| # | ZIP | Age | Nationality | Condition |
| Akira | 130** | < 30 | * | Heart Disease |
| | 130** | < 30 | * | Heart Disease |
| | 130** | < 30 | * | Viral Infection |
| | 130** | < 30 | * | Viral Infection |
| Bob | 1485* | > = 40 | * | HIV |
| | 1485* | > = 40 | * | Heart Disease |
| | 1485* | > = 40 | * | Viral Infection |
| | 1485* | > = 40 | * | Viral Infection |
| | 130** | 3* | * | HIV |
| | 130** | 3* | * | HIV |
| | 130** | 3* | * | HIV |
| | 130** | 3* | * | HIV |



k-anonymity with k=4



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

| | Non-Sensitive Data | | | Sensitive Data |
|-------|--------------------|------|-----------------|-----------------|
| # | ZIP | Age | Nationality | Condition |
| Akira | 130** | < 30 | * | Heart Disease |
| | 130** | < 30 | * | Heart Disease |
| | 130** | < 30 | * | Viral Infection |
| | 130** | < 30 | * | Viral Infection |
| 1485* | > = 40 | * | HIV | |
| 1485* | > = 40 | * | Heart Disease | |
| 1485* | > = 40 | * | Viral Infection | |
| 1485* | > = 40 | * | Viral Infection | |
| Bob | 130* | | | HIV |
| | 130* | | | HIV |
| | 130** | 3* | * | HIV |
| | 130** | 3* | * | HIV |

Bob has HIV!!



k-anonymity with k=4



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

| | Non-Sensitive Data | | | Sensitive Data |
|-------|--------------------|--------|-------------|-----------------|
| # | ZIP | Age | Male/Female | Condition |
| Akira | 130* | < 30 | * | Heart Disease |
| | 130* | < 30 | * | Heart Disease |
| | 130** | < 30 | * | Viral Infection |
| | 130** | < 30 | * | Viral Infection |
| Bob | 1485* | > = 40 | * | HIV |
| | 1485* | > = 40 | * | Heart Disease |
| | 1485* | > = 40 | * | Viral Infection |
| | 1485* | > = 40 | * | Viral Infection |
| | 130* | > = 40 | * | HIV |
| | 130* | > = 40 | * | HIV |
| | 130** | 3* | * | HIV |
| | 130** | 3* | * | HIV |

If we know that heart diseases are extremely rare in Japan, then it is highly likely that Akira has been infected by a virus

Bob has HIV!!



Anonymity with l -diversity

- The total number of non-distinct records (have same QID values) form an **equivalence class**
- **Distinct l -diversity** (Machanavajjhala et al., 2006): Every equivalence class should include at least l distinct values of the sensitive field.



Distinct 3-diversity

| | <i>Non-Sensitive Data</i> | | | <i>Sensitive Data</i> |
|----------|---------------------------|------------|--------------------|-----------------------|
| # | ZIP | Age | Nationality | Condition |
| 1 | 1305* | <= 40 | * | Heart Disease |
| 2 | 1305* | <= 40 | * | Viral Infection |
| 3 | 1305* | <= 40 | * | HIV |
| 4 | 1305* | <= 40 | * | HIV |
| 5 | 1485* | >= 40 | * | HIV |
| 6 | 1485* | >= 40 | * | Heart Disease |
| 7 | 1485* | >= 40 | * | Viral Infection |
| 8 | 1485* | >= 40 | * | Viral Infection |
| 9 | 1306* | <= 40 | * | Heart Disease |
| 10 | 1306* | <= 40 | * | Viral Infection |
| 11 | 1306* | <= 40 | * | HIV |
| 12 | 1306* | <= 40 | * | HIV |

Bob and Akira
Belong
here



Is Distinct I-Diversity enough ?

- Probabilistic inference attacks are still possible

10 records -
Equivalence class

| ... | Disease |
|-----|------------|
| ... | ... |
| | HIV |
| | HIV |
| | ... |
| | HIV |
| | pneumonia |
| | bronchitis |
| | ... |

8 out of 10 have HIV



Anonymization Tools



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

- ARX (<https://arx.deidentifier.org/>)
- Amnesia (<https://amnesia.openaire.eu/>)
- UTD Anonymisation toolbox (<http://cs.utdallas.edu/dspl/cgi-bin/toolbox/index.php?go=home>)
- Anonimatron (<https://realrolfje.github.io/anonimatron/>)

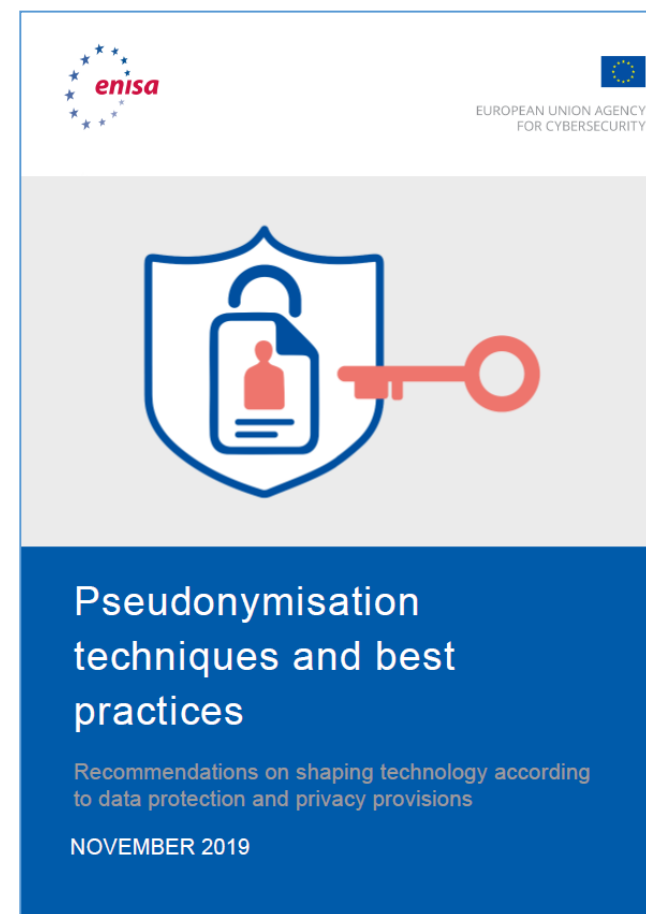


ENISA Report: Pseudonymisation techniques and best practices



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

- Result of ENISA Project (March – October 2019)
 - **Editors:** Athena Bourka (ENISA)
Prokopios Drogkaris (ENISA)
Ioannis Agrafiotis (ENISA)
 - **Contributors:** Meiko Jensen (Kiel University)
Cedric Lauradoux (INRIA)
Konstantinos Limniotis (HDPa)
- Continuation of previous ENISA report
 - “An overview on data pseudonymisation”, 2018



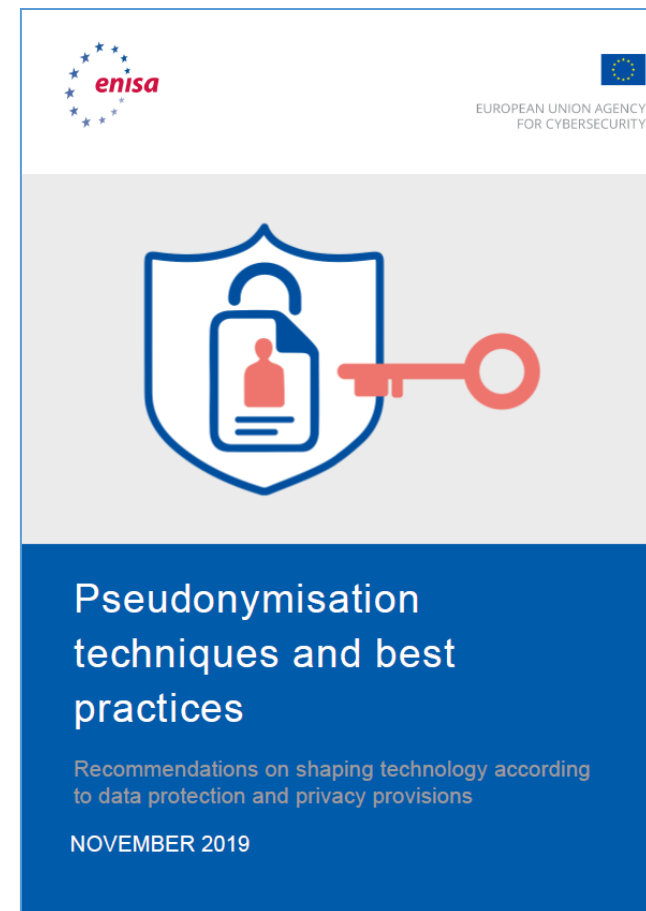


ENISA Report: Pseudonymisation techniques and best practices



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

- Focus on Techniques and Best Practices in Real-World Application Scenarios
 - Terminology
 - Scenarios
 - Adversary Models
 - Techniques
 - Application Scenarios
 - IP Address pseudonymization
 - E-Mail Address pseudonymization
 - Pseudonymization in practice (discussion of complex cases)
- } → In relation with the desired «goals» of the pseudonymisation



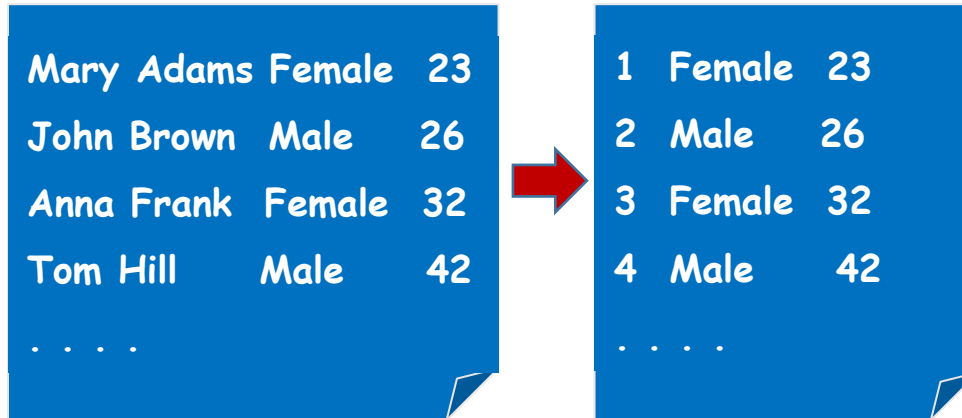


General pseudonymisation goals



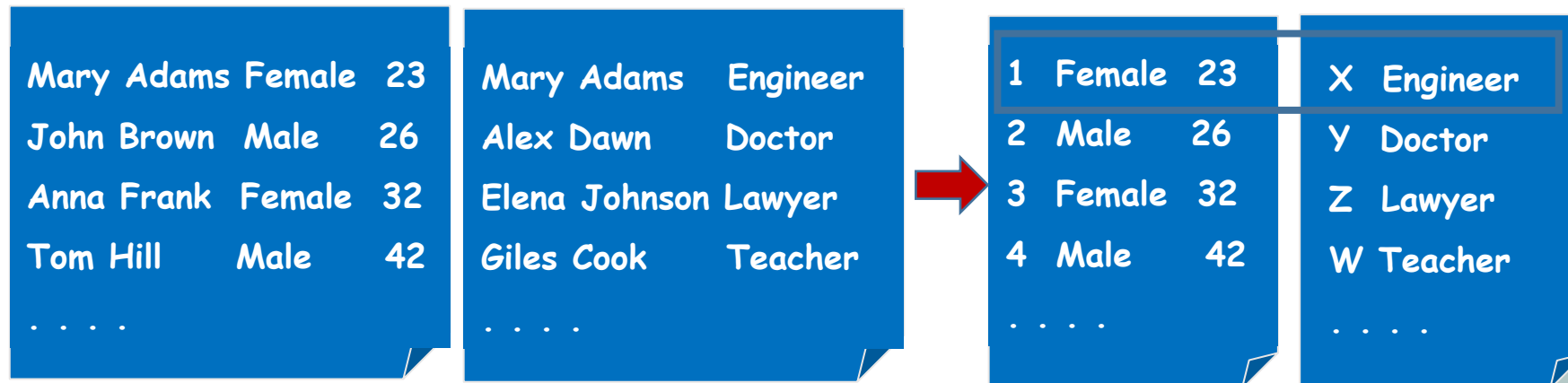
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

1. Hiding identities (related to confidentiality)



- Both goals are actually also related to the **data minimization principle**
- Be careful with the “confidentiality”: The pseudonymised data are not encrypted data (see next)
- Note that, in some cases, pseudonyms need to “carry” some information (i.e. increasing **usability** – see next), despite the fact that the identities should remain hidden

2. Unlinkability





General pseudonymisation goals (Cont.)

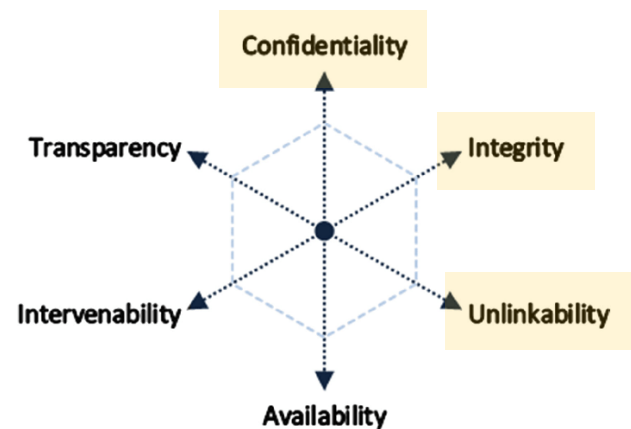


Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

3. Verification of the identity (related to integrity)



Summarizing: Pseudonymisation in relation to general data protection goals



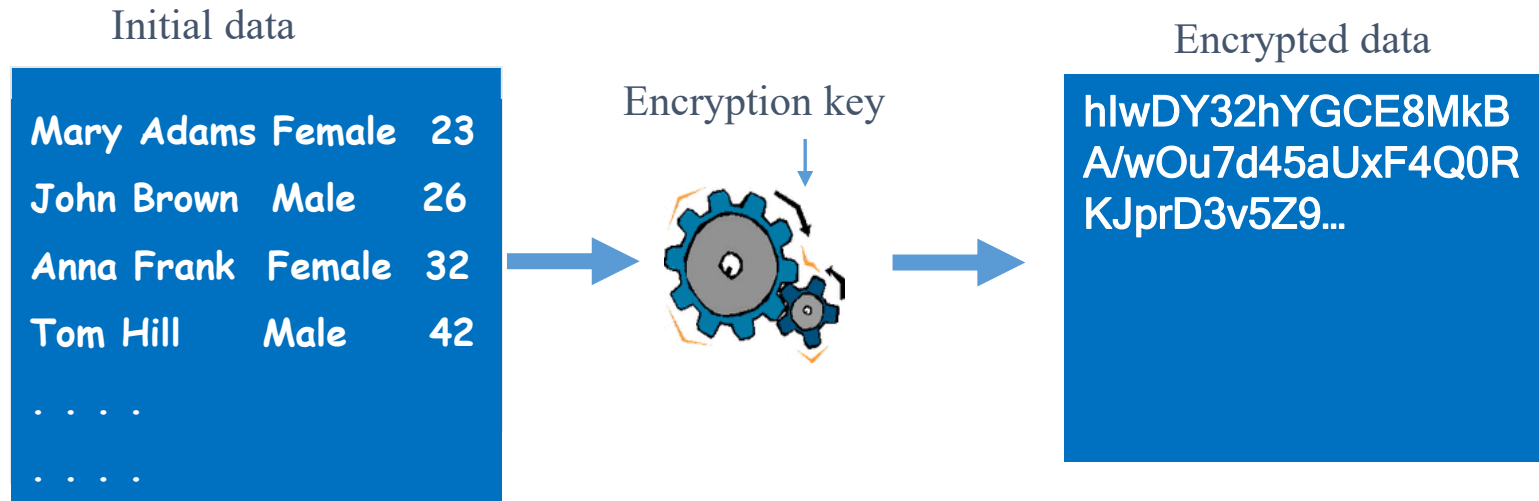
M.Hansen, M. Jensen, and M. Rost, "Protection goals for privacy engineering", 2015



Pseudonymisation ≠ Encryption



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



- Encrypted data are unintelligible to anyone not having the decryption key (which inverses the encryption)
 - Not even statistical analysis can be performed on encrypted data
 - In general this is not the case in pseudonymisation
- Hence, the difference between pseudonymisation and encryption is obvious
 - However, appropriate use of cryptography may give rise to “good” pseudonymisation techniques...
 - The **secret key** could coincide with the “**additional information needed for re-identification**”



Terminology - Roles

- What roles are involved in a classic pseudonymization scenario?
How are they named?
 - ➔ «**Pseudonymization Entity**», «**Adversary**»
- How do these roles relate to the roles of GDPR?
 - ➔ «**Data controller**», «**Data subject**», «**Data processor**»
- **Encryption** is associated with a «secret key», but what is the «secret thing» of **pseudonymization**?
 - Related with the additional information needed for re-identification
 - ➔ «**Pseudonymization secret**»

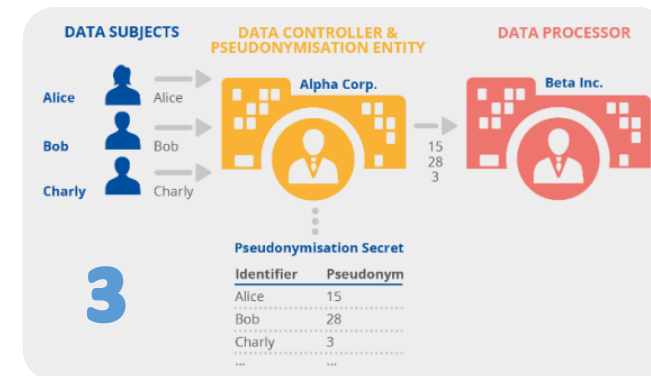
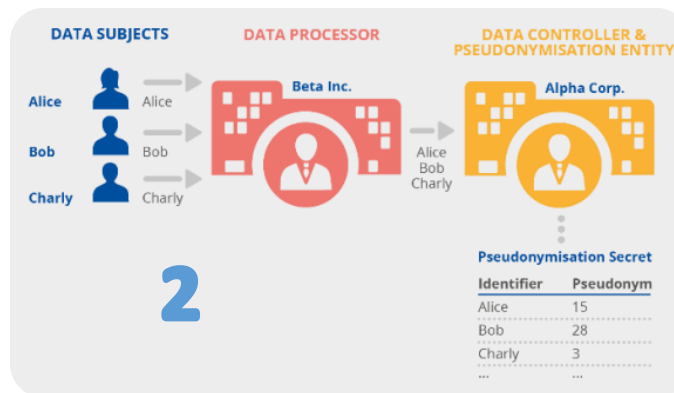
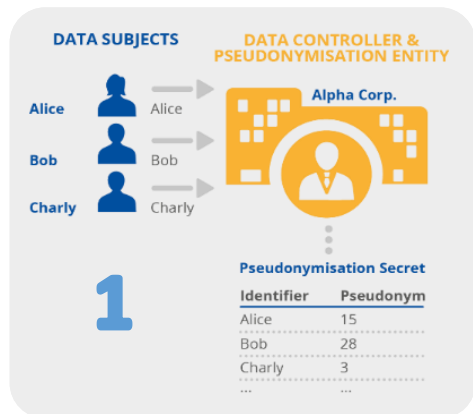


Scenarios

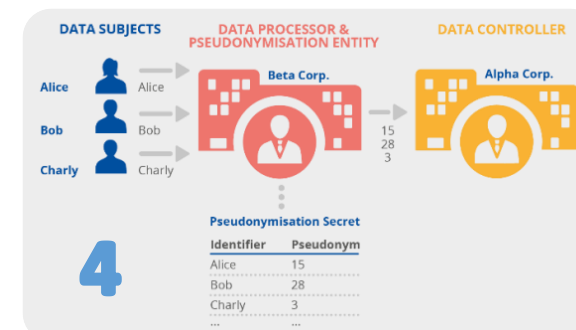
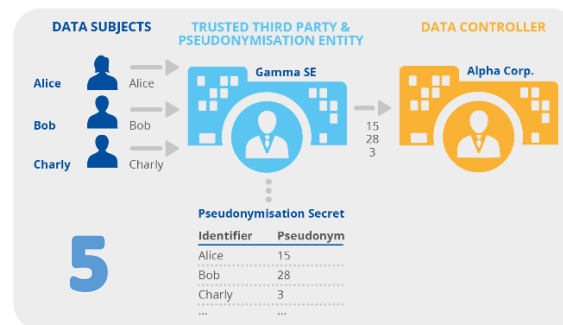
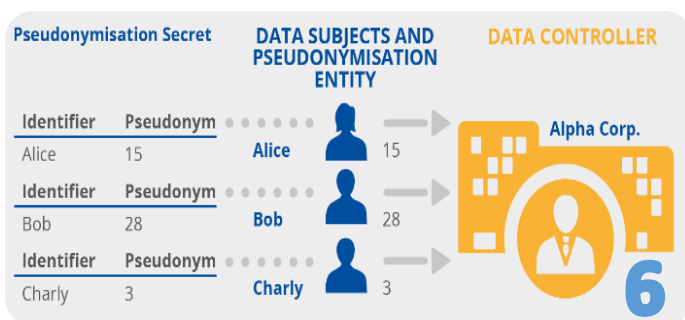


Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Scenarios 1-3: Data controller coincides with the pseudonymisation entity – i.e. the entity that actually performs pseudonymisation

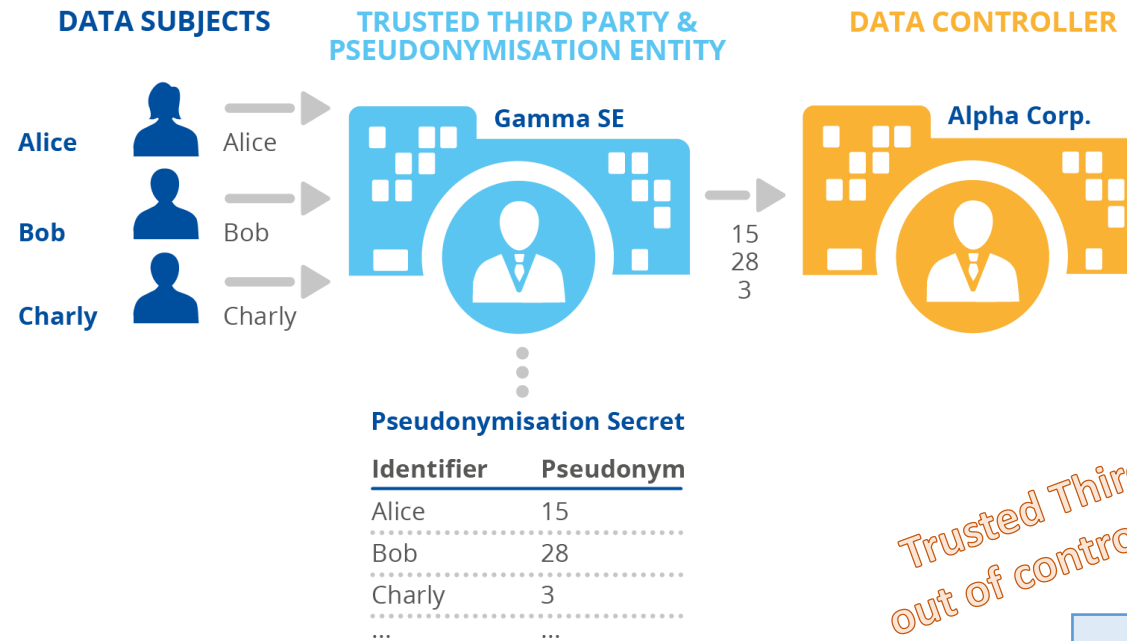


Scenarios 4-6: Data controller does **not** coincide with the pseudonymisation entity





«Special» scenarios: Scenario 5



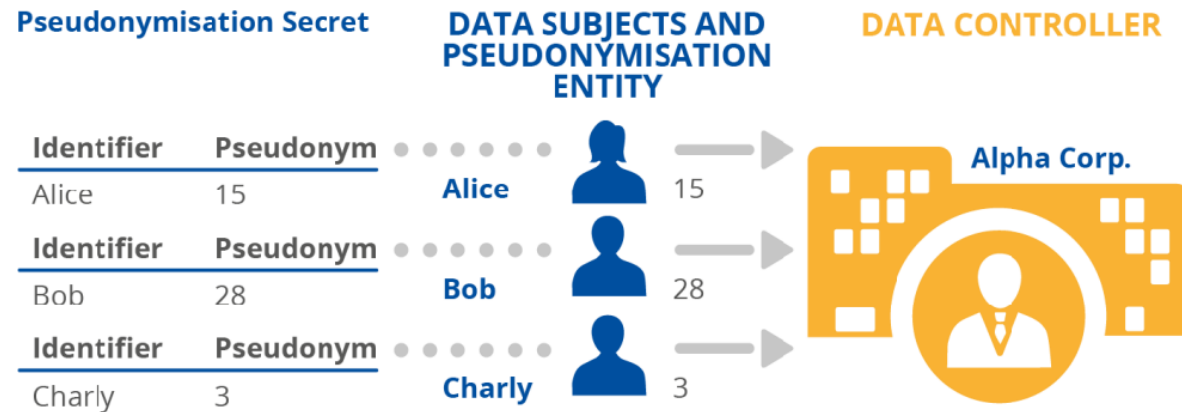
Trusted Third Party is always out of control of data controller!

Scenario 5

- *Preceding Trusted Third Party*
- *Trusted Third Party = Pseudonymization Entity*
- *Joint controllers??*



«Special» scenarios: Scenario 6



Do not confuse with the case that the data subjects simply choose their pseudonyms

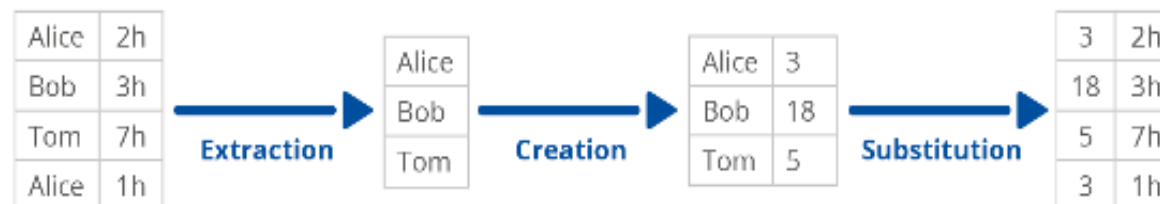
Scenario 6

- The whole process is «governed» by the data controller
- Useful in cases that the data controller **should not know the original identities**
- E.g.: The ID of an electronic ticket for public transportation, uniquely constructed by a owner's passphrase (only the owner of the ticket knows the passphrase)

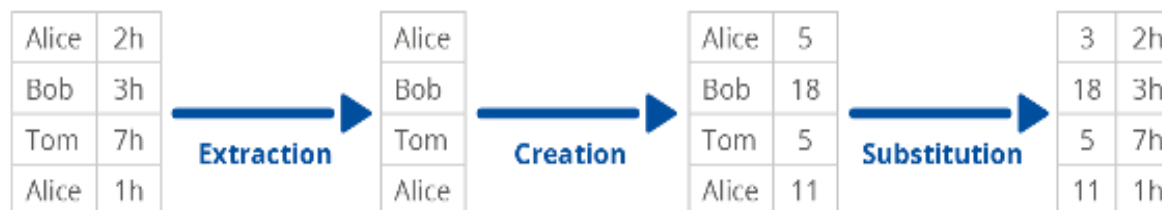


Pseudonymisation policies

1. Deterministic pseudonymisation



2. Randomized pseudonymisation



- The desired purpose of the pseudonymisation actually determines the policy that is preferable
- Deterministic pseudonymisation allows “tracking” of an individual within a database (more usability but also, probably, more data protection risks)

Pseudonymisation techniques



1. Counter / Random Number Generator (RNG)

“Hiding” everything

| E-mail address | Pseudonym (Random number generator) | Pseudonym (counter generator) |
|--|-------------------------------------|-------------------------------|
| alice@abc.eu | 328 | 10 |
| bob@wxyz.com | 105 | 11 |
| eve@abc.eu | 209 | 12 |
| john@qed.edu | 83 | 13 |
| alice@wxyz.com | 512 | 14 |
| mary@clm.eu | 289 | 15 |

Keeping information on domains

| E-mail address | Pseudonym (Random number generator) | Pseudonym (counter generator) |
|--|-------------------------------------|-------------------------------|
| alice@abc.eu | 328@abc.eu | 10@abc.eu |
| bob@wxyz.com | 105@wxyz.com | 11@wxyz.com |
| eve@abc.eu | 209@abc.eu | 12@abc.eu |
| john@qed.edu | 83@qed.edu | 13@qed.edu |
| alice@wxyz.com | 512@wxyz.com | 14@wxyz.com |
| mary@clm.eu | 289@clm.eu | 15@clm.eu |

- Pseudonymisation secret = Mapping table
- Simplicity
- Scalability issues
 - Especially in deterministic pseudonymisation
- The counter-based pseudonyms may generally allow for some information extraction and/or prediction
 - (e.g. consider consecutive University students addresses, stud790@universityA.edu, stud791@universityA.edu etc.)

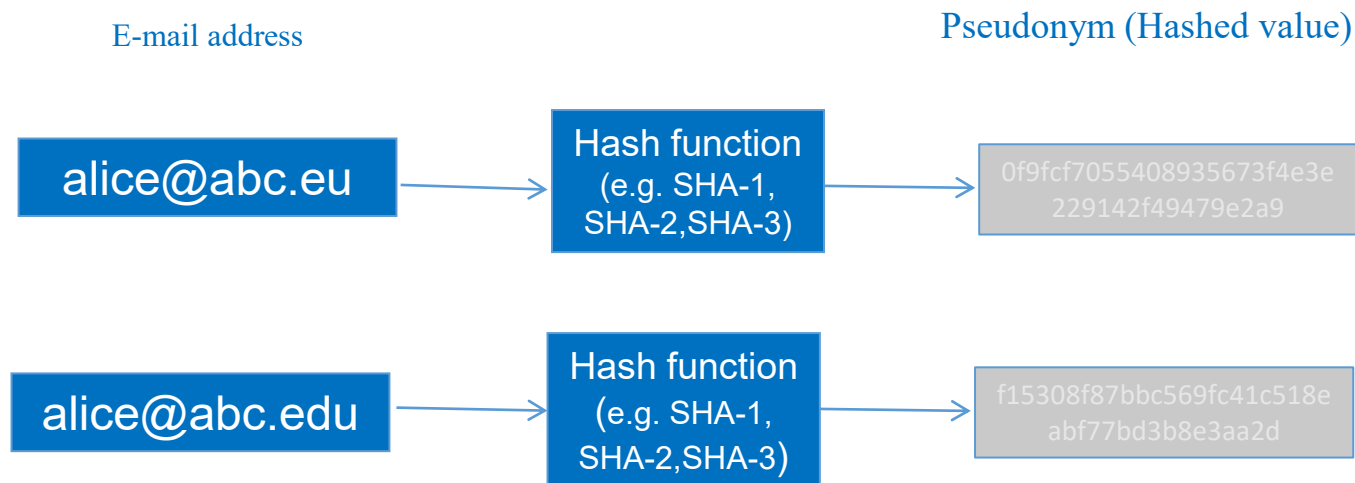


Pseudonymisation techniques



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

2. Cryptographic hash function



People believe that hashing is a nice pseudonymisation technique. **But...**

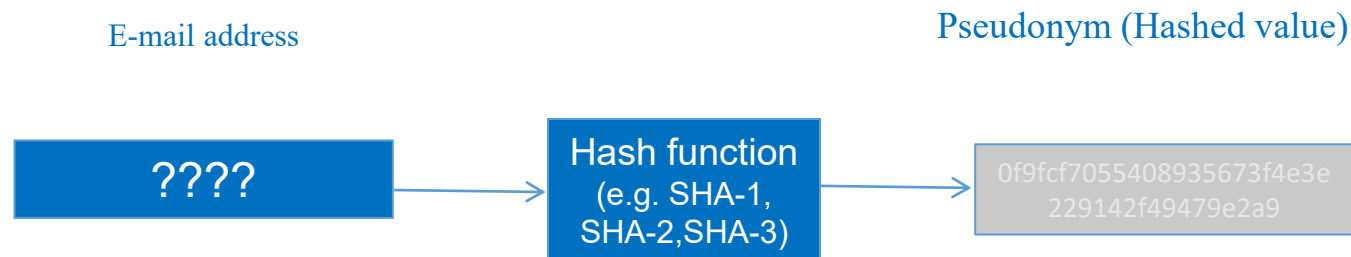


Pseudonymisation techniques



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

2. Cryptographic hash function (Cont.)



The adversary can easily verify whether any of the pseudonyms in the pseudonymised list corresponds to [alice@abc.eu](#)

- Simply computes the hashed value of [alice@abc.eu](#) and checks...
- Actually, in such a scenario there is no pseudonymisation secret...
 - The only “secret” is the input domain
 - The size and the «predictability» of the input domain highly affects the level of protection (identity hiding) that a hash function provides as a pseudonymisation technique

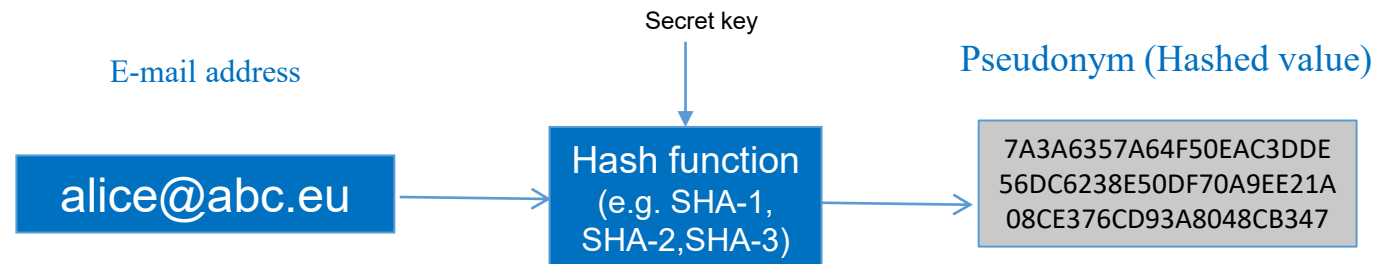


Pseudonymisation techniques



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

3. Cryptographic hash function with key (Message Authentication Code – MAC)



- Pseudonymisation secret = Secret key
- Deterministic or randomised pseudonymisation, based on whether the secret key is fixed or not
- High protection on «hiding» the initial identifier (once the key remains secret)
- High scalability
- But.. restrictions even for the pseudonymisation entity
 - Knowledge of the pseudonym and the pseudonymisation secret does not allow direct estimation of the initial identifier
 - However, given an identifier, it can be easily checked which is its corresponding pseudonym

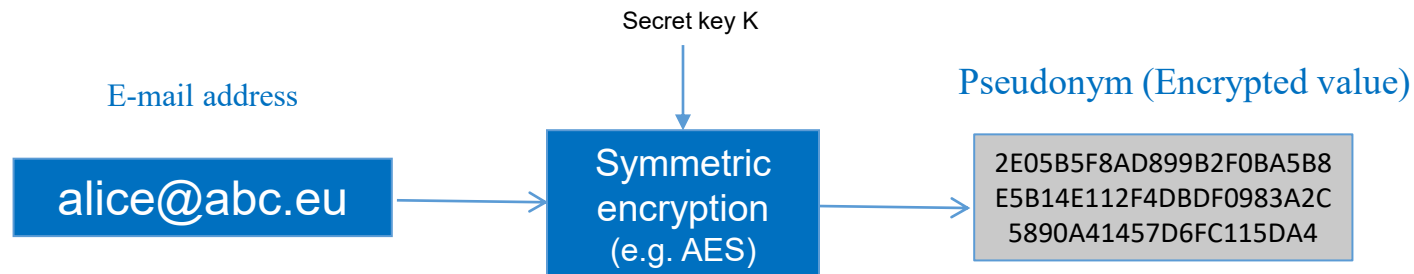


Pseudonymisation techniques



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

4. Encryption – the deterministic case



- Pseudonymisation secret = Secret key (the same for decryption)
- Deterministic pseudonymisation, for fixed secret key
- High protection on «hiding» the initial identifier (once the key remains secret)
- High scalability
- No restrictions for the pseudonymisation entity
 - Knowledge of the pseudonym and the pseudonymisation secret allows direct estimation of the initial identifier

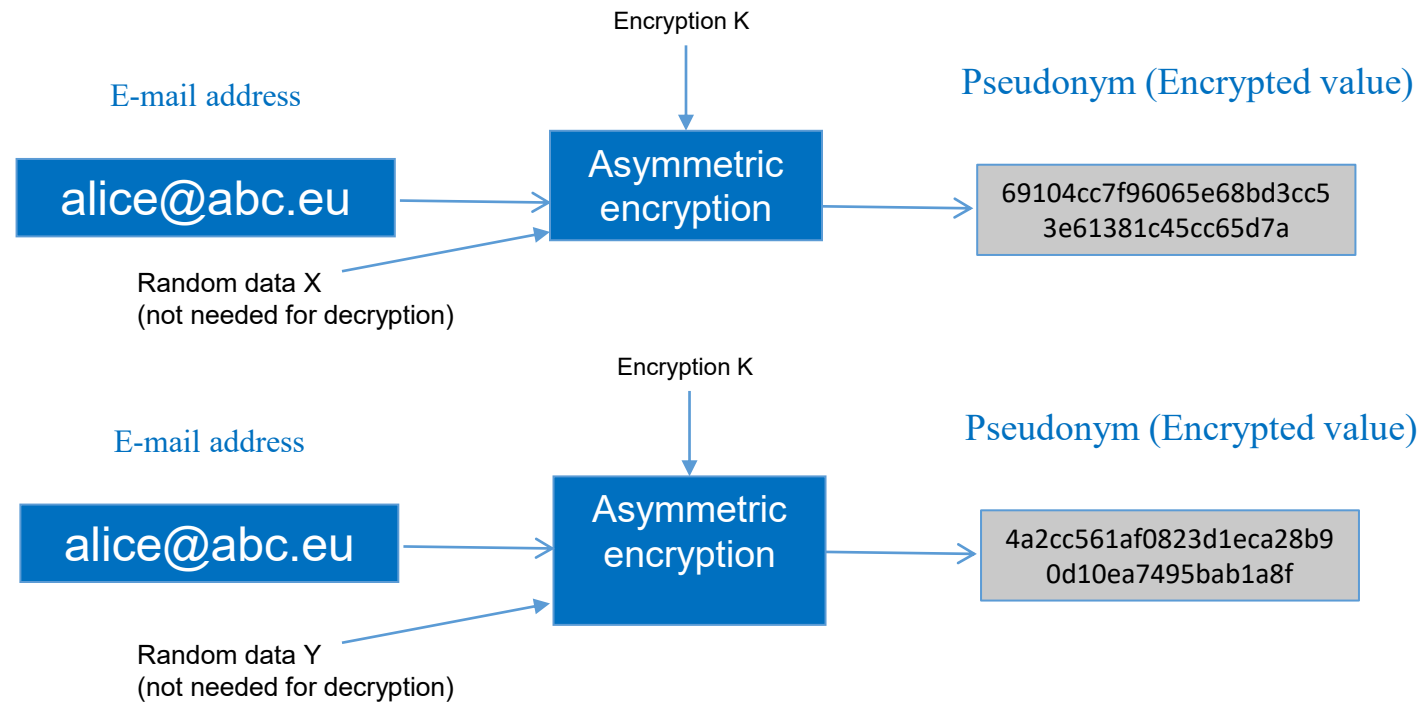


Pseudonymisation techniques



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

4. Encryption – the probabilistic case



- Pseudonymisation secret = Decryption key (different from encryption key)
- Randomised pseudonymisation
- Other pseudonymisation benefits similar to deterministic encryption are also present



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

Thank you for your participation!

Appendix 10

Attacks frequently causing data breaches -
organisational and technical measures for
preventing / mitigating the impacts



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



Attacks frequently causing data breaches - Organisational and technical measures for preventing/mitigating the impacts

byDesign: Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services

www.bydesign-project.eu





Attacks frequently causing data breaches

- **Ransomware attacks**
 - with or without proper backup and with or without exfiltration
- **Data exfiltration attacks**
 - malicious code, SQL injection, with encrypted or not data
- **Internal human risk source**
 - Intentional exfiltration, accidental transmission
- **Lost or stolen devices and paper document**
 - stolen material with encrypted or not data, stolen paper files
- **Mispostal**
 - snail mail mistake, data sent by email by mistake
- **Other cases – social engineering**
 - Identity theft, mail exfiltration



Ransomware attacks

- Malicious code encrypts the personal data.
- Subsequently the attacker asks the data controller for ransom in exchange for the decryption code.
- This kind of attack can usually be classified as a breach of availability, but often also a breach of confidentiality could occur.



Case 1. Ransomware with proper backup and without exfiltration

- **Business:** (computer systems of a) small manufacturing company.
- **Case description:**
 - The company used encryption at rest with *state-of-the-art algorithm*.
 - The decryption key was not compromised.
 - Analyzing available logs and detection systems, ***the attacker only had access to encrypted personal data, without exfiltrating it.***
 - Backup readily available - data restored a few hours after the attack took place.
 - No delay in employee payments or handling client requests or consequences on the day-to-day operation.



Case 1. Ransomware with proper backup and without exfiltration

- **Affected data/subjects:**

- Affected data of employees and clients, a few dozen individuals altogether.
- No special categories of data were affected.

- **Risk assessment:**

- Confidentiality risks reduced to a minimum - cryptanalytic progress can render the encrypted data intelligible in the future.
- The breach was unlikely to result in a risk since:
 - the affected data was effectively restored in a few hours from the backup,
 - the breach did not result in any consequences on the day-to-day operation and
 - had no significant effect on the data subjects (e.g. employee payments or handling client requests).



Case 1. Ransomware with proper backup and without exfiltration

• Mitigation and obligations:

- Resetting all compromised systems to a clean state known to be free of malicious code.
- Fixing the vulnerabilities and restoring the affected data soon after the attack.

| Actions necessary based on the identified risks | | |
|---|------------------|--|
| No risk (internal register) | Risk (notify SA) | High Risk (communicate to data subjects) |
| ✓ | X | X |



Case 2. Ransomware without proper backup



- **Business:** (one of the computers of an) agricultural company.
- **Case description:**
 - Analyzing available logs and other detection systems, *the attacker only encrypted the data, without exfiltrating it.*
 - No backup was available in an electronic form.
 - Most data were restored from paper backups within 5 working days.
 - Minor delays in the delivery of orders to customers.
- **Affected data/subjects:**
 - Affected data of employees and clients, a few dozen individuals altogether.



Case 2. Ransomware without proper backup



Risk assessment:

- Risks from lack of availability as confidentiality is not compromised.
- The likelihood of a confidentiality breach cannot be entirely dismissed
 - sophisticated malware has the functionality to edit log files and remove traces
 - logs are not forwarded or replicated to a central log server,
 - data controller cannot state that the absence of a log entry proves the absence of exfiltration.
- No special categories of personal data affected.
- Low quantity of breached data and number of affected data subjects.
- Absence of a backup database - data still available on paper.



Case 2. Ransomware without proper backup

Obligations:

- Notification to SA necessary:
 - data restoration took some time,
 - could cause some delays in the orders' delivery to customers and
 - a considerable amount of meta-data (e.g. logs, time stamps) might not be retrievable.
- Informing the data subjects may depend on:
 - the length of time the personal data is unavailable,
 - the difficulties it might cause in the operation of the data controller as a result (e.g. delays in transferring employee's payments),
 - financial loss for individuals with compromised data (delays in payments and deliveries),
 - their contribution needed for restoring the encrypted data.

| Actions necessary based on the identified risks | | |
|---|------------------|--|
| No risk (internal register) | Risk (notify SA) | High Risk (communicate to data subjects) |
| ✓ | ✓ | ✗ |



Case 3. Ransomware with backup and without exfiltration in a hospital

- **Business:** (information system of) hospital / healthcare center
- **Case description:**
 - The logs show no outward data flow in the timeframe of the attack.
 - After analyzing logs and detection systems, ***the attacker encrypted significant proportion of the data without exfiltration.***
 - Backups were available in an electronic form.
 - Most of the data were restored but this operation lasted 2 working days.
 - Major delays in treating the patients with surgery cancelled / postponed.
 - Lower level of service due to the unavailability of the systems.



Case 3. Ransomware with backup and without exfiltration in a hospital

- **Affected data/subjects:**
 - thousand employee and patient records.
- **Risk assessment:**
 - high impact of the data unavailability on a substantial part of data subjects,
 - although backup existed and data could be restored in a few days,
 - a high risk still exists due to the consequences from the data unavailability at the moment of the attack and the following days,
 - residual risk of high severity to the confidentiality of the patient data,
 - high quantity of breached data and number of affected data subjects.



Case 3. Ransomware with backup and without exfiltration in a hospital

• Obligations:

- Necessary to notify: special data categories, restoration could take a long time, resulting in major delays in patient care.
- Necessary to inform data subjects: due to the impact for the patients, even after restoring the encrypted data.
- Direct communication of the data breach: to the impacted patients i.e. those scheduled to be treated during when the system was unavailable.
- Public communication or similar equally effective measure: to the other patients (exception of article 34 (3) c).

| Actions necessary based on the identified risks | | |
|---|------------------|--|
| No risk (internal register) | Risk (notify SA) | High Risk (communicate to data subjects) |
| ✓ | ✓ | ✓ |



Case 4. Ransomware without backup and with exfiltration

- **Business:** public transportation company
- **Case description:**
 - The server was exposed to a ransomware attack and data were encrypted.
 - The attacker not only encrypted, but also exfiltrated the data.
 - A backup database existed, but it was also encrypted by the attacker.
- **Affected data/subjects:**
 - Clients, employees and several thousand people using the services of the company (e.g. buying tickets online).
 - Breached data involved basic identity data, identity card numbers and financial data such as credit card details.



4. Ransomware without backup and with exfiltration

- **Risk assessment:**
 - Data availability and confidentiality breach.
 - High number of individuals affected and the overall quantity of affected data.
 - High risk from identity documents and financial data.
 - The backup files were affected by the ransomware.
 - The breach presents high risk because it could likely lead to both:
 - material (e.g. financial loss since credit card details were affected) and
 - non-material damage (e.g. identity theft or fraud since identity card details were affected).



4. Ransomware without backup and with exfiltration

• Obligations:

- Communication to data subjects essential: they can make the necessary steps to avoid material damage (e.g. block their credit cards).
- Communication on a person-by-person basis.
- For individuals where contact data is not available, the controller should do so publicly, e.g. by way of a notification on its website.
- Precise and clear communication is required, in plain sight on the homepage of the data controller, with exact references of the relevant GDPR provisions.

| Actions necessary based on the identified risks | | |
|---|--------------------|--------------------------------|
| Internal documentation | Notification to SA | Communication to data subjects |
| ✓ | ✓ | ✓ |



Ransomware attacks

| | Internal documentation | Notification to SA (risk) | Communication to data subjects (high risk) |
|---|------------------------|---------------------------|--|
| CASE No. 01: Ransomware with proper backup and without exfiltration | YES | X | X |
| CASE No. 02: Ransomware without proper backup | YES | YES | X |
| CASE No. 03: Ransomware with backup and without exfiltration in a hospital | YES | YES | YES |
| CASE No. 04: Ransomware without backup and with exfiltration | YES | YES | YES |



Organizational and technical measures for preventing / mitigating the impacts of ransomware attacks



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

- keeping firmware, operating system and application software on the servers, client machines, active network components, and any other machines on the same LAN (including Wi-Fi devices) **up to date**,
- existence of an up-to-date, secure and tested **backup** procedure,
- appropriate, up-to-date, effective and integrated **anti-malware** software,
- appropriate, up-to-date, effective and integrated **firewall and intrusion detection and prevention system**,
- **training** employees on the methods of recognizing and preventing IT attacks
- forwarding or replication all logs to a **central log server**,
- strong **encryption** and **authentication**,
- **vulnerability** and **penetration testing** on a regular basis,
- establish a Computer Security Incident Response Team (**CSIRT**) or Computer Emergency Response Team (**CERT**) within the organization,
- when assessing countermeasures – **risk analysis** should be **reviewed**



Data exfiltration attacks

- Attacks that exploit vulnerabilities in services offered by the controller to third parties over the internet, e.g. committed by way of injection attacks (e.g. SQL injection, path traversal),
- the risk emanates from the action of an unauthorized third party,
- typically aim at copying, exfiltrating and abusing data for a malicious end,
- they are mainly breaches of confidentiality and, possibly, also data integrity



Case 5. Exfiltration of job application data from a website

- **Business:** employment agency
- **Case description:**
 - a cyber-attack placed malicious code on the website,
 - the malicious code made the data submitted through online job application forms and stored on the webserver accessible to unauthorized person(s),
 - The malware toolkit was discovered only a month after its installation.
 - The toolkit allowed
 - the attacker to remove any history of exfiltration and
 - processing on the server to be monitored and to have personal data captured.



Case 5. Exfiltration of job application data from a website

- **Affected data/subjects:**

- 213 job application forms were possibly affected,
- no special categories of data were affected in the breach.

- **Risk assessment:**

- confidentiality breach with data integrity becoming questionable,
- the accessed data contains considerable information about the individuals from the online forms,
- such data could be misused in a number of ways (targeting with unsolicited marketing, identity theft, etc.).



Case 5. Exfiltration of job application data from a website

- **Mitigation and obligations:**

- compare the database with the one stored in a secure backup,
- return all affected IT systems to a known clean state,
- remedy the vulnerability,
- implement new security measures to avoid similar data breaches in the future e.g. file integrity checks and security audits,
- If personal data were deleted, recover the data in the state they were before the breach,
- apply full backups, incremental changes and then possibly rerun the processing since the last incremental backup.

| Actions necessary based on the identified risks | | |
|---|--------------------|--------------------------------|
| Internal documentation | Notification to SA | Communication to data subjects |
| ✓ | ✓ | ✓ |



Case 6. Exfiltration of hashed password from a website

- **Business:** cooking website
- **Case description:**
 - an SQL Injection vulnerability was exploited to gain access to a server database,
 - users were only allowed to choose arbitrary pseudonyms as usernames,
 - the use of email addresses for this purpose was discouraged
 - passwords stored in the database were hashed with a strong algorithm and the salt was not compromised
 - the controller informed the data subjects about the breach via e-mail and
 - asked them to change their passwords, especially if used for other services.
- **Affected data/subjects:** hashed passwords of 1.200 users



Case 6. Exfiltration of hashed password from a website

- **Risk assessment:**
 - data confidentiality is compromised, but passwords were hashed,
 - no contact data (e.g. e-mail addresses or phone numbers) were compromised,
 - no significant risk for the data subjects of being targeted by fraud attempts (e.g. receiving phishing e-mails or fraudulent text messages and phone calls),
 - no special categories of personal data were involved,
 - user names can be regarded as personal data, but the website's subject does not reveal special categories of data (e.g. as political party website).



Case 6. Exfiltration of hashed password from a website

- **Mitigation and obligations:**

- state of the art encryption could mitigate the adverse effects of the breach,
- limited number of attempts to login will prevent brute force login attacks,
- use of authentication methods obviating the need to process passwords on the server side is preferable,
- correct the vulnerability,
- implement new security measures to avoid similar future data breaches (systematic security audits to the website),
- strongly advisable to communicate a breach involving passwords to data subjects in any case.

| Actions necessary based on the identified risks | | |
|---|--------------------|--------------------------------|
| Internal documentation | Notification to SA | Communication to data subjects |
| ✓ | X | X |



Case 7. Credential stuffing attack on a banking website

- **Business:** online-banking website
- **Case description**
 - cyber-attack aimed to enumerate all possible login user IDs using a fixed trivial (8-digit) password
 - due to a website vulnerability, in some cases data were leaked to the attacker, even if password was incorrect or bank account inactive,
 - all illegitimate log-on attempts were identified,
 - no transactions were performed by these accounts during the attack,
 - the security operations center detected a high number of login requests,
 - the bank switched off the log in and forced password resets of the compromised accounts,
 - the breach was communicated only to the users with the compromised accounts, i.e. to users whose passwords were compromised or whose data was disclosed.



Case 7. Credential stuffing attack on a banking website

- **Affected data/subjects:**

- affected around 100.000 data subjects,
- out of these, the attacker successfully logged into around 2.000 accounts which were using the trivial password tried by the attacker,
- in some cases data were leaked to the attacker: name, surname, gender, date and place of birth, fiscal code, user identification codes.



Case 7. Credential stuffing attack on a banking website

• Risk assessment:

- financial data and identity and user ID information,
- high number of individuals affected,
- the breached data permits the unique identification of data subjects,
- contains other information about them (i.e. gender, date and place of birth),
- can be used to guess the passwords or run a spear phishing campaign,
- the occurrence of material (e.g. financial loss) and non- material damage (e.g. identity theft or fraud) is a conceivable outcome.

| Actions necessary based on the identified risks | | |
|---|--------------------|--------------------------------|
| Internal documentation | Notification to SA | Communication to data subjects |
| ✓ | ✓ | ✓ |



Organizational and technical measures for preventing / mitigating the impacts of hacker attacks



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

- State-of-the-art **encryption** and **key management**
- **Cryptographic hashing and salting** for secret information (passwords) is always preferred over encryption of passwords
- Keeping the system **up to date** (software and firmware)
- Use of **strong authentication methods** like two-factor authentication and authentication servers
- Up-to-date **password policy**
- Strong **user privileges and access control management** policy
- **Secure development standards**: filtering of user input, brute force prevention measures, WAF
- **Firewall, intrusion detection** and other **perimeter defense** systems
- Systematic **IT security audits** and **vulnerability assessments** (penetration testing)
- Regular **reviews** and **testing** to ensure that **backups** can be used to restore any data whose integrity or availability was affected.
- **No session ID in URL** in plain text



Internal human risk source

- Common appearance of human error in personal data breaches
- Can be both intentional and unintentional types of breaches
- Difficult for the data controllers to identify the vulnerabilities and adopt measures to avoid them



Case 8. Accidental transmission of data to a trusted third party

- **Business:** insurance company and insurance agent
- **Case description:**
 - insurance agent accessed data not belonging to his scope - faulty settings of an excel file received by email,
 - he was the sole recipient of the e-mail,
 - he is bound by professional secrecy and an arrangement with the controller,
 - the agent instantly signalled the mistake to the controller,
 - the controller corrected the file and sent it out again, asking the agent to delete the former message
 - the agent confirmed the deletion in a written statement



Case 8. Accidental transmission of data to a trusted third party

- **Affected data/subjects:**

- two dozen customers,
- no special categories of personal data,
- only contact data and data about the insurance itself (insurance type, amount)

- **Risk assessment:**

- confidentiality breach,
- low quantity of data affected – no “sensitive” data,
- immediate detection of the breach and measures taken, deletion of the file



Case 8. Accidental transmission of data to a trusted third party

• Mitigation and obligations:

- reducing file exchange through e-mail,
- double checking files before sending,
- separating the creation and sending of files,
- additional steps in checking documents involving personal data

| Actions necessary based on the identified risks | | |
|---|--------------------|--------------------------------|
| Internal documentation | Notification to SA | Communication to data subjects |
| ✓ | X | X |



Organizational and technical measures for preventing / mitigating the impacts of internal human risk sources



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

- Periodic **training, education** and **awareness** programs for employees
- Effective data protection and privacy **practices and procedures**
- Making proper **access control policies** and forcing users to follow the rules
- **User authentication** when accessing “sensitive” personal data
- **Disabling** user account as soon as the person leaves the company
- **Checking unusual dataflow** between the file server and employee workstations
- Setting up **I/O interface security** in the BIOS or through the use of software controlling the use of computer interfaces (lock or unlock e. g. USB/CD/DVD etc.)
- **Reviewing** employees’ access policy
- **Disabling** open **cloud** services
- **Forbidding** and preventing **access** to known **open mail services**
- **Disabling print screen** function in OS
- Enforcing a **clean desk policy**
- Automated **locking all computers** after a certain amount of inactivity



Lost or stolen devices and paper documents



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

- A frequent case is the loss or theft of portable devices
- measures prior to the breach to ensure an appropriate level of security
- always breach of confidentiality
- If there is no backup, can also be breach of availability and integrity
- the risk assessment might be difficult, as the device is no longer available



Case 9. Stolen material storing encrypted personal data

- **Business:** children's day-care center
- **Case description:**
 - two tablets were stolen during a break-in,
 - the tablets contained an app which held personal data about the children attending the day-care center,
 - both the encrypted tablets which were turned off at the time of the break-in, and the app was protected by a strong password.
- **Affected data/subjects:**
 - name, date of birth, personal data about the education of the children attending the day-care center



Case 9. Stolen material storing encrypted personal data

• Risk assessment

- Data confidentiality on the devices was not compromised due to the strong password protection on tablets and apps.
- Due to the measures taken, data confidentiality was kept intact.
- The backup ensured continuous data availability.

| Actions necessary based on the identified risks | | |
|---|--------------------|--------------------------------|
| Internal documentation | Notification to SA | Communication to data subjects |
| ✓ | X | X |



Case 10. Stolen material storing non-encrypted personal data

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

- **Business:** service provider company
- **Case description:**
 - The electronic notebook device of an employee was stolen.
 - Access to the notebook's hard drive was not protected by any password.
 - Personal data could be restored from daily backups available.
- **Affected data/subjects:**
 - The stolen notebook contained names, surnames, sex, addresses and date of births of more than 100000 customers.



Case 10. Stolen material storing non-encrypted personal data

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

- **Risk assessment:**

- Confidentiality breach of the data stored on the stolen device.
- No password protection or encryption.
- Lack of prior basic security measures enhances the risk level.
- High risk of identity fraud.
- No special categories of personal data.
- Not possible to identify if other data categories were also affected due to the stolen device unavailability.

Case 10. Stolen material storing non-encrypted personal data



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

- **Mitigation and obligation:**

- Turning on device encryption.
- Use of strong password protection of the stored database.

Actions necessary based on the identified risks

| Internal documentation | Notification to SA | Communication to data subjects |
|------------------------|--------------------|--------------------------------|
| ✓ | ✓ | ✓ |



Organizational and technical measures for preventing / mitigating the impacts of loss or theft of devices



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

- Turn on **device's encryption** (such as Bitlocker, Veracrypt or DM-Crypt).
- Use **passcode/password** on all devices. Encrypt all mobile electronic devices requiring complex password for decryption.
- Use **multi-factor authentication**.
- Turn on **location functionalities** of mobile devices to located them in case of loss or misplacement.
- Use **MDM** (Mobile Devices Management) software/app and localization. Use anti-glare filters. Close down any unattended devices. Enable the remote wipe function.
- Save personal data on a **central back-end server** and not on a mobile device.
- Use a **secure VPN** to connect mobile devices to back-end servers.
- Proper **regulation of device usage** inside and outside the company.
- Use **centralized device management** with minimum rights for the end users to install software.
- Install **physical access controls**.
- **Avoid storing sensitive information** in mobile devices or hard drives



Mispostal

- The risk source is an internal human error.
- It is the result of inattentiveness.
- Little can be undertaken by the controller after it happened, so prevention is even more important.



CASE 11. Snail mail mistake

- **Business:** retail company
- **Case description:**
 - Two orders for shoes were packed by the retail company.
 - Due to human error two customers got each other's orders, including the packing bills containing the personal data.
 - After becoming aware of the breach the data controller recalled the orders and sent them to the right recipients.



CASE 11. Snail mail mistake

- **Affected data/subjects:**

- The bills contained the personal data required for a successful delivery (name, address, plus the item purchased and its price).

- **Risk assessment:**

- no special categories of personal data or other data whose abuse might lead to substantial negative effects were involved,
- the breach is not a result of a systemic error,
- only two individuals are concerned,
- no negative effect on the individuals could be identified.



CASE 11. Snail mail mistake

- **Mitigation and obligations:**

- The controller should provide for a free return of the items and the accompanying bills,
- should request the wrong recipients to destroy / delete all eventual copies of the bills containing the other person's data

| Actions necessary based on the identified risks | | |
|---|--------------------|--------------------------------|
| Internal documentation | Notification to SA | Communication to data subjects |
| ✓ | X | X |



Case 12. Sensitive personal data sent by mail by mistake

- **Business:** employment department of a public administration office
- **Case description:**
 - An email message – about upcoming trainings - was sent to the individuals registered in the system as jobseekers.
 - By mistake, a document was attached containing all jobseekers' data.
 - The office contacted all recipients and asked them to delete the previous message and not to use the information contained in it.
- **Affected data/subjects:**
 - Name, e-mail address, postal address, social security number of more than 60000 individuals.



Case 12. Sensitive personal data sent by mail by mistake

- **Risk assessment:**

- considerable number of affected individuals,
- the social security number, along with basic data, increases the high risk,
- the eventual distribution of the data by any of the recipients cannot be contained by the controller

- **Mitigation and obligations:**

- the means to effectively mitigate the risks are limited,
- the controller asked for the deletion of the message but cannot force the recipients to do so,
- as a consequence, cannot be certain that they comply with the request

| Actions necessary based on the identified risks | | |
|---|--------------------|--------------------------------|
| Internal documentation | Notification to SA | Communication to data subjects |
| ✓ | ✓ | ✓ |



Organizational and technical measures for preventing / mitigating the impacts of mispostal



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

- **Setting exact standards** for sending letters / e-mails.
- Adequate **training** for personnel on how to send letters / e-mails.
- When sending e-mails to multiple recipients, they are listed in the '**bcc**' field by default.
- **Extra confirmation** is required when sending e-mails to multiple recipients, and they are not listed in the 'bcc' field.
- **Automatic addressing** instead of manual.
- **Disabling autocomplete** when typing in e-mail addresses.
- **Awareness** sessions on **most common mistakes** leading to a personal data breach.
- **Training sessions** and **manuals** on **how to handle incidents** leading to a personal data breach and who to inform (involve DPO).



Other cases – social engineering

Case 13. Identity theft

- **Business:** telecommunication company
- **Case description:**
 - the contact center receives a telephone call from someone that poses as a client
 - the supposed client asks to change the email address of the billing info
 - the client's identity is validated and the operator makes the requested change
 - the procedure does not foresee any notification to the former email contact
 - the legitimate client asks why he is not receiving billing to his email address,
 - and denies any call asking the change,
 - later, the company realizes that the information has been sent to an illegitimate user and reverts the change



Case 13. Identity theft

- **Risk assessment:**
 - billing data can give information about the data subject's private life (e.g. habits, contacts) and could lead to material damage (e.g. stalking, risk to physical integrity),
 - the data obtained can be used to facilitate account takeover in this organization or exploit further authentication measures in other organizations
 - the “appropriate” authentication measure should meet a high bar, depending on what personal data can be processed as a result of authentication



Case 13. Identity theft

- **Mitigation and obligations:**

- the methods used for authentication were not sufficient,
- use of static knowledge-based authentication is not recommended,
- verify the change demand, by sending a confirmation request to the former contact
- adding extra questions and requiring information only visible on previous bills

| Actions necessary based on the identified risks | | |
|---|--------------------|--------------------------------|
| Internal documentation | Notification to SA | Communication to data subjects |
| ✓ | ✓ | ✓ |



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

Thank you for your attention!

Appendix 11

Implementing DP principles using Data Protection
By Design - By Default



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



Implementing DP principles using Data Protection By Design and By Default

DATES

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





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

DPbD – Transparency, Lawfulness & Fairness



Key design elements for transparency

- **Clarity** – Information shall be in clear and plain language, concise and intelligible.
- **Semantics** – Communication should have a clear meaning to the audience in question.
- **Accessibility** - Information shall be easily accessible for the data subject.
- **Contextual** – Information should be provided at the relevant time and in the appropriate form.
- **Relevance** – Information should be relevant and applicable to the specific data subject
- **Universal design** – Information shall be accessible to all data subjects
- **Comprehensible** – Data subjects should have a fair understanding of what they can expect with regards to the processing of their personal data, particularly when the data subjects are children or other vulnerable groups.
- **Multi-channel** – Information should be provided in different channels and media, not only the textual,
- **Layered** – The information should be layered in a manner that resolves the tension between completeness and understanding



DPdD - Bad practices in transparency

- Common bad formulations in privacy policies:
 - **“We may...”** : Introduces ambiguity
 - **“Personally Identifiable Information”** : This is only a sub-category of personal data
 - **“by <....>, you consent to this processing”**: Consent must be free, informed, specific and unambiguous (and thus, obtaining valid consent necessitates specific implementation)
 - **“administration purposes”**: Needs clarification (maybe in a second-level)
 - **“including, but not limited to....:”** Not clear information – implies non-compliance with the minimization principle
 - **A long page/doc**: Difficult to read.



Key design elements for lawfulness/fairness

- **Relevance** – The correct legal basis shall be applied
- **Differentiation** – The legal basis used for each processing activity shall be differentiated.
- **Specified purpose**
- **Autonomy** – The user should be granted the highest degree of autonomy as possible
- **Gaining consent** – free, specific, informed and unambiguous (“opt-in”)
- **Consent withdrawal** – Withdrawal shall be as easy as giving consent.
- **Cessation** – If the legal basis ceases to apply, the processing stops
- **No deception** – Information and options should be provided in an objective and neutral way, avoiding any manipulation
- **Predetermination** – Establishment of legal basis before the processing takes place.
- **Adjust** – If there is a valid change of legal basis, the actual processing must be adjusted
- **Fair algorithms** – Algorithms functioning in line with the purposes (transparently for users)
- **Interaction** – Users must be able to communicate and exercise their rights
- **Respect rights**



DPdD - Bad practices in lawfulness/fairness



- Common bad practices in implementations:
 - Consent obtained is not valid
 - The user is “forced” to provide consent
 - The actual legal basis is not the user’s consent
 - One for all processes, for several different purposes
 - Etc.
 - Change of legal basis during the process
 - E.g. the user tries to revoke consent but this right is not fulfilled due to “legitimate interests” of the controller
 - The algorithms do much more things than the users think
 - E.g. Profiling of users and making decisions for them



Possible design patterns for transparency

| | Language complexity | Vagueness of terms | Wall of text | Excessive length | Lack of audience-tailoring | Wrong timing | Lack of familiarity | Scattered information |
|-------------------------|---------------------|--------------------|--------------|------------------|----------------------------|--------------|---------------------|-----------------------|
| Illustrative examples | | | | | | | | |
| FAQs | | | | | | | | |
| Timeline | | | | | | | | |
| Swimlane | | | | | | | | |
| Comics | | | | | | | | |
| Meaningful organization | | | | | | | | |
| Companion icons | | | | | | | | |
| Layered notice | | | | | | | | |
| Videos | | | | | | | | |
| Highlighted text | | | | | | | | |
| Alert icons | | | | | | | | |

Table 1 – The design patterns organized per category.

| Explanation | Navigation | Overview | Emphasis |
|-----------------------|-------------------------|----------------|------------------|
| Illustrative examples | Meaningful organization | Layered notice | Highlighted text |
| FAQs | Companion icons | Videos | Alert icons |
| Timeline | | | |
| Swimlane | | | |
| Comics | | | |


Fig. 1 – Matrix illustrating the problem(s) that each design pattern can solve. The different shades of colors indicate the category to which the pattern belongs.

- **Source:** A. Rossi, G. Lenzi, “Transparency by design in data-informed research: A collection of information design patterns”, Computer Law and Security Review, Elsevier, 2020



DPdD - Good and bad examples on information notices

Privacy notices, transparency and control



Date of Birth

Occupation

Address

Post Code

How information about you will be used

We may share your information with credit reference agencies and other companies for use in credit decisions, for fraud prevention and to pursue debtors.

We would like to send you information about our own products and services, by post, telephone, email and SMS. If you agree to being contacted in this way, please tick the relevant boxes.

Post Email Phone SMS Automated phone call

We would also like to share your information with other selected garden products retailers so that they may send you information about their products and services by post. If you agree to your information being shared in this way, please tick the box.

If you need any further information please write to us at 10 Street Name, Town Name, County Name AB123CD.


Customer signature

Date

Simple language, clear font and style.

Clear opportunity to agree to marketing.

Prior consent sought for postal marketing by other companies.



Date of Birth

Occupation

Address

Post Code

LEGAL DECLARATION

X Limited is a company incorporated in England and is a member of the X Retail Group ("the Group"). The Group ("we/us") also includes Y Limited and Z Limited and their associated companies from time to time. The personal identifiable information you provide will be processed in accordance with the Data Protection Acts 1984 and 1998 and other applicable laws. We will use your information so that we can process your order. This includes administering any accounts, processing your bank/credit card details in order to obtain payment, arranging delivery of any goods purchased, and the prevention and detection of fraud. We can hand over your information to anyone to whom we transfer our rights and duties under our agreement with you or if we have a duty to do so and the law allows us to do it. We will use your information for market research and the marketing of our products and services. This may include contacting you by post, telephone, email or SMS unless you indicate you do not want to be contacted in any of these ways by calling us on 0870 23 45 67. We will use your information to search the files of credit reference agencies who will record that search. This information may be used by other lenders in making credit decisions about you, members of your household and those with whom you may be financially linked. Information held about you by the credit reference agencies may already be linked to records relating to people with whom you are financially linked. For the purposes of credit searching, you may be treated as financially linked and you will be assessed with reference to any associated records. We will share our information with other companies, for the purposes of market research and the marketing of their products and services, unless you indicate that you wish to be excluded from such uses by contacting us on 08701 23 45 67. By signing this form you consent to the information you provide being processed for the above purposes.

Customer Signature

Date

Confusing and legalistic language. Closely spaced text, small italic font in light grey.

Unnecessary – means little to the public.

Specific opt-in consent is required for some e-marketing and is good practice for all direct marketing.

Confusing language.

No details of what type of companies.

Bad practice to seek one consent for several types of processing.

Source: ICO



DPbD - Good and bad example on obtaining consent for data collection



Please provide telephone numbers in case we need to contact you about your claim.

You do not have to tell us your phone number but it will help us to contact you quickly if we have a question about your claim.

Home:

Mobile:

Clear explanation of why it would be helpful to provide this information.



You must provide the following telephone numbers. It will delay your claim if you don't provide your telephone numbers.

Home:

Mobile:

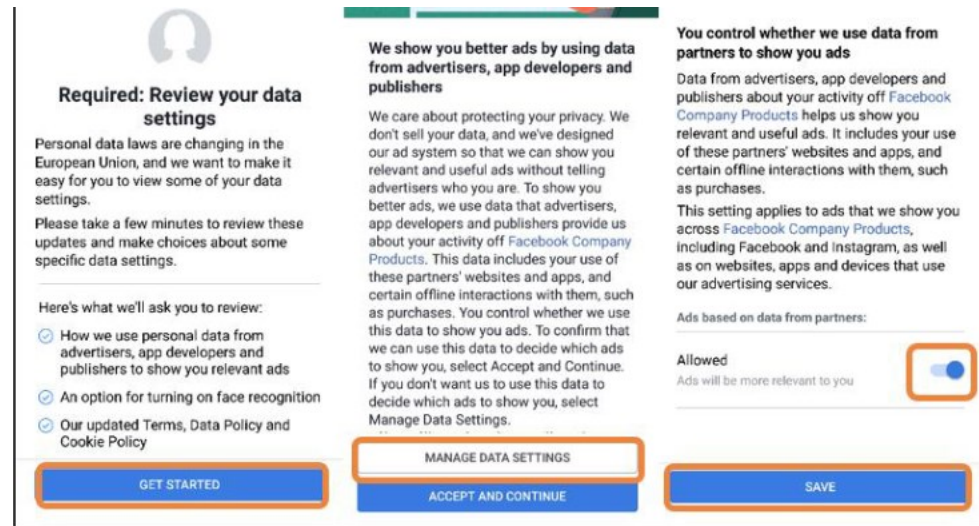
Implies it is mandatory to give this information when in this case it is voluntary.

Source: ICO



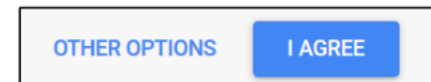
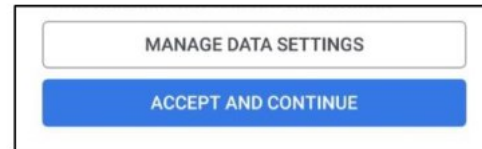
DPdD – Bad practices on obtaining consent (“dark patterns”)

Source: “Deceived by Design” report, Norwegian Consumer Council, 2018.



Typically, opt-out consent is not correct

The user is somehow “motivated” to accept, due to the bad design





DPbD – Trasparency (An example)

- The necessary information should be provided in the right context, at the appropriate time.
 - A general privacy policy may not be always sufficient
 - Design of information flows may be the proper way



Source: A. Rossi, G. Lenzini, "Transparency by design in data-informed research: A collection of information design patterns", Computer Law and Security Review, Elsevier, 2020

An example for describing the process of revoking consent for a processing regarding research purposes

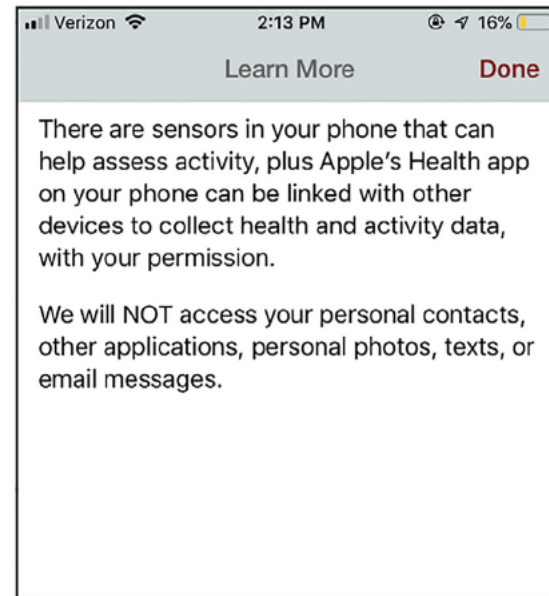
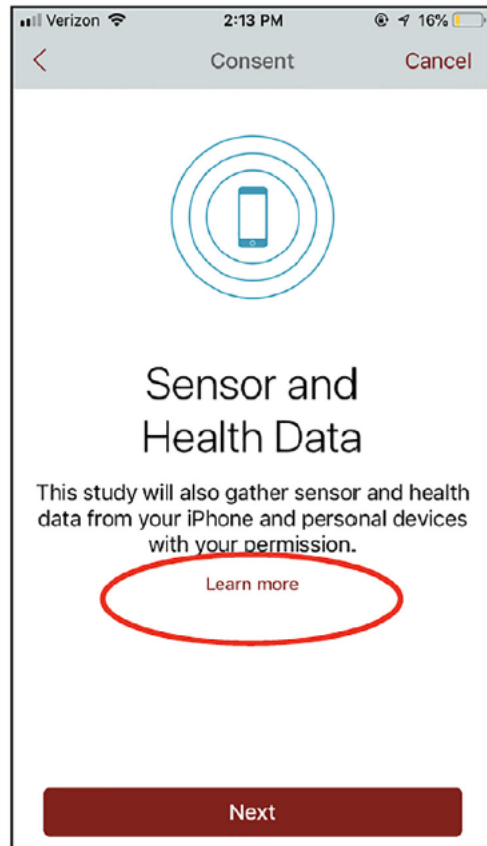


DPbD – Fairness (An example)

- Streaming service where users may choose between a regular subscription of standard quality and a premium subscription with higher quality.
 - As part of the premium subscription, subscribers get prioritized customer service.
- With regard to the fairness principle, the prioritized customer service granted to premium subscribers cannot discriminate the regular subscribers' access to exercise their rights
 - Although the premium subscribers get prioritized service, such prioritization cannot result in a lack of appropriate measures to respond to request from regular subscribers without undue delay and in any event within one month of receipt of the requests.



DPbD – Layered approach for transparency



Images from My Heart Counts (Stanford University)

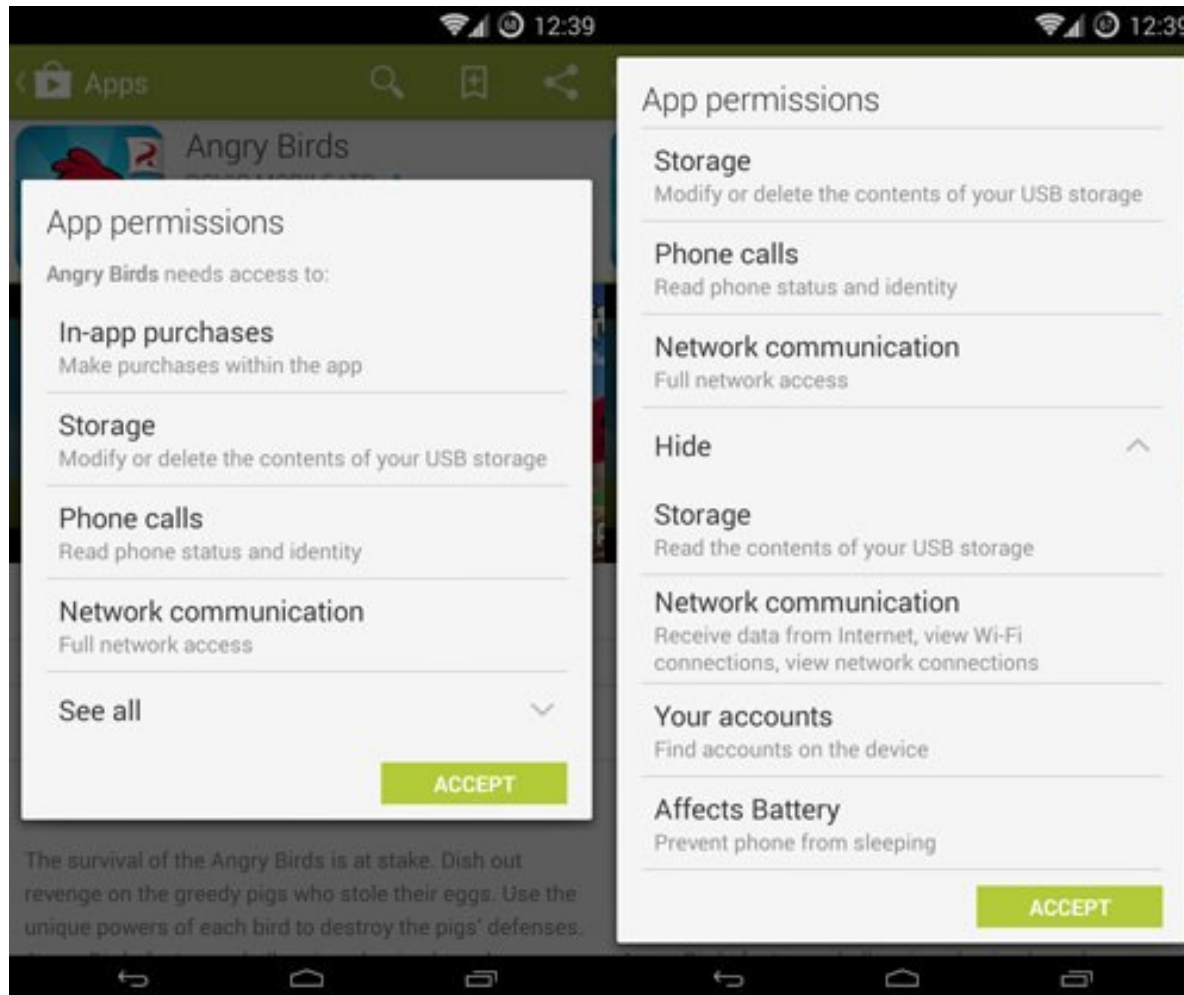
An example of a layered approach in a smart app being used for research purposes

- Consent is (indeed) the legal basis

- **Source:** A. Rossi, G. Lenzini, “Transparency by design in data-informed research: A collection of information design patterns”, Computer Law and Security Review, Elsevier, 2020



DPbD – The permission model in smart apps

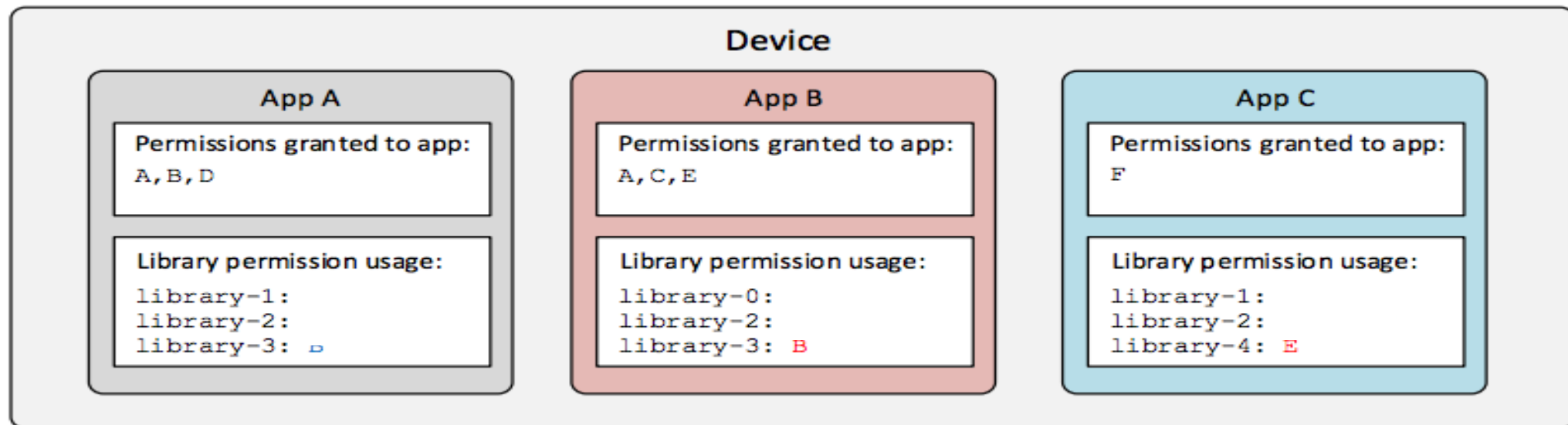


- Are all the permissions necessary?
- Are they justified?
 - Is the consent informed?
- What if the user does not grant a permission?
 - Is the consent free?
- Do other third-parties get access due to the permission granted?
 - Is the user informed on this?
 - See the intra-library collusion issue



DPbD – The intra-library collusion issue

Source: Vincent F. Taylor, Alastair R. Beresford, Ivan Martinovic, «Intra-Library Collusion: A Potential Privacy Nightmare on Smartphones», arXiv:1808.03520, 2017.



- Library 2 is being used by apps A, B and C
- So, the library 2 provider obtains all the permissions A, B, C, D, E, F!!
 - Even if the user thoroughly examines all the permissions granted to her apps independently, she may believe that none gets all the permissions...



Actual risks of intra-library collusion

- Libraries may abuse the privileges granted to the host applications.
 - Libraries may track the users.
 - Libraries may aggregate multiple signals for detailed user profiling.
 - => The user is not aware of these!
-
- The developer should be very cautious on the use of third-party libraries
 - The designer should be very cautious on identifying the absolutely necessary permissions



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

DPbD – Purpose limitation



Key design elements for purpose limitation



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

- **Predetermination** – The legitimate purposes shall be determined before the design of the processing.
- **Specificity** – The purposes shall be specified and explicit.
- **Purpose orientation** – The purpose of processing should guide the design of the processing and set processing boundaries.
- **Necessity** – The purpose determines what personal data is necessary for the processing.
- **Compatibility** – Any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design.
- **Limit further processing** – No connecting datasets or perform any further processing for new incompatible purposes.
- **Limitations of reuse** – Using technical measures, including hashing and encryption, as well as organisational measure, such as policies, to limit the possibility of repurposing personal data.
- **Review** – Regularly test the design against purpose limitation.



DPbD - Bad practices in purpose limitation

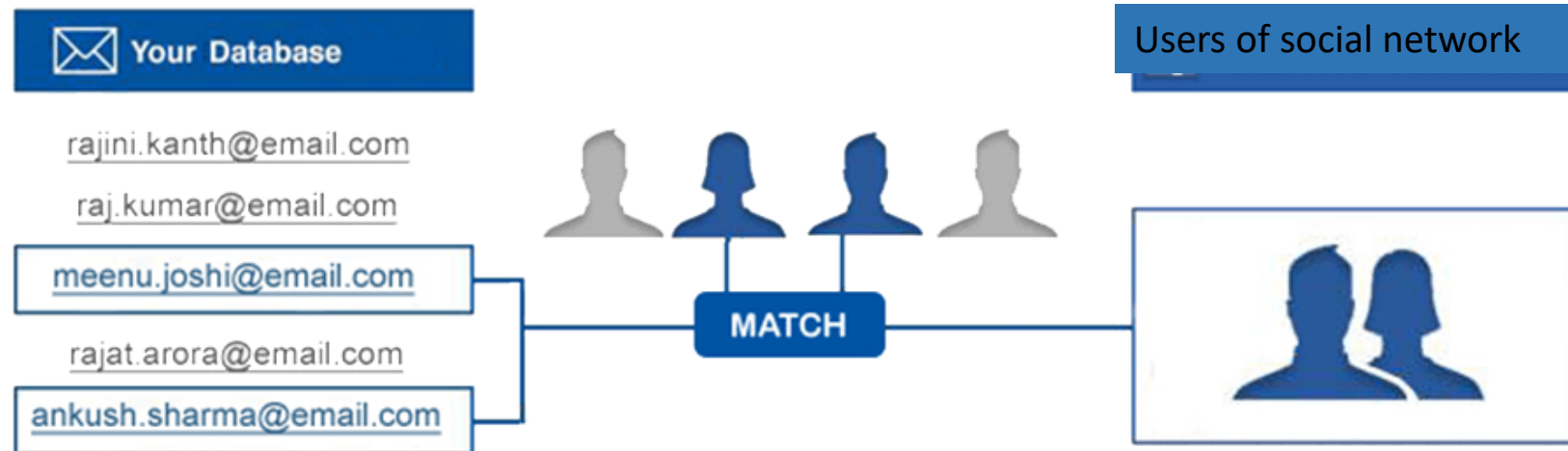


Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

- Common bad practices:
 - The process does not “stick” to what it has been said in the privacy notice
 - Consent is being “translated” as permission to do anything with the data collected
 - Personal data are being transmitted to other parties – e.g. for behavioral advertising, or, more generally, for creating profiling
 - Personal data are being connecting with other available datasets, where some users are common



DPbD – A bad example on purpose limitation



- Sending users e-mail addresses to the social network, for advertisements through the network, is a different purpose
- Matching of common addresses (for the same purpose as above) is also a different purpose
 - Even if a proper legal basis exists for this new process (e.g. consent), emphasis should be put on data minimization (discussed further subsequently)



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

DPbD – Data minimization



Key design elements for data minimization



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

- **Data avoidance** – Avoid processing personal data altogether when this is possible for the relevant purpose.
- **Limitation** – Limit the amount of personal data collected to what is necessary for the purpose
- **Access limitation** – Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly.
- **Relevance** – Personal data should be relevant to the processing in question
- **Necessity** – Each personal data category shall be absolutely necessary for the specified purposes
- **Aggregation** – Use aggregated data when possible.
- **Pseudonymization** – Pseudonymize personal data as soon as it is no longer necessary to have directly identifiable personal data
- **Anonymization and deletion** – Where personal data is not, or no longer necessary for the purpose, personal data shall be anonymized or deleted.
- **Data flow** – The data flow should be made efficient enough to not create more copies than necessary.
- **“State of the art”** – Application of up to date appropriate technologies



DPbD - Bad practices in data minimisation



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

- Common bad practices:
 - Process of more personal data that are needed – e.g. collecting data that are not actually needed
 - E.g. Applications request high-precision location when they only need to know the city or the country.
 - Collecting data for several different purposes which, if combined, allow processing for a new purpose (not transparent to the users)
 - During the data flow, extensive personal data may be available to people/systems that should not have access to such data (violation of the “need-to-know” principle)
 - Bad pseudonymisation – it is believed that identities are protected, but this is not the case
 - I.e. bad pseudonymisation design/technique, insufficient protection of data allowing pseudonymisation reversal etc.
 - Data are being considered as anonymous but this is not the case
 - Anonymisation is a non-trivial task that needs much attention...



An example

- **Web form of a bookstore:**
 - Asking information including the customer's date of birth, phone number and home address
 - Are all these necessary?
 - If the user pays for the product up front, the user's date of birth and phone number are not necessary for the purchase of the product
 - The home address may be also unnecessary – e.g. in case of an e-book or in cases that the user chooses to go to the physical store
- **Possible best practice:**
 - Two web forms: one for ordering books, with a field for the customer's address and one web form for ordering eBooks without a field for the customer's address.
 - In any case, the mandatory information is explicitly described and justified



An example

- A public transportation company wishes to gather statistical information based on travellers' routes
- The passengers have to pass their ticket through a reader every time they enter a transport (e-ticket system)
- The information collected by the company may allow identification of the passengers in some circumstances, based on single route identification thanks to the ticket identifier.
 - E.g. if they live or work in scarcely populated areas
- **Solution:** the ticket identifier is not stored
- Challenge: What if the ticket identifier is needed for another legal purpose?
- => the overall process should be carefully designed (e.g. proper pseudonymisation, logical and physical separation of databases for different purposes so as to be unlinkable etc.)



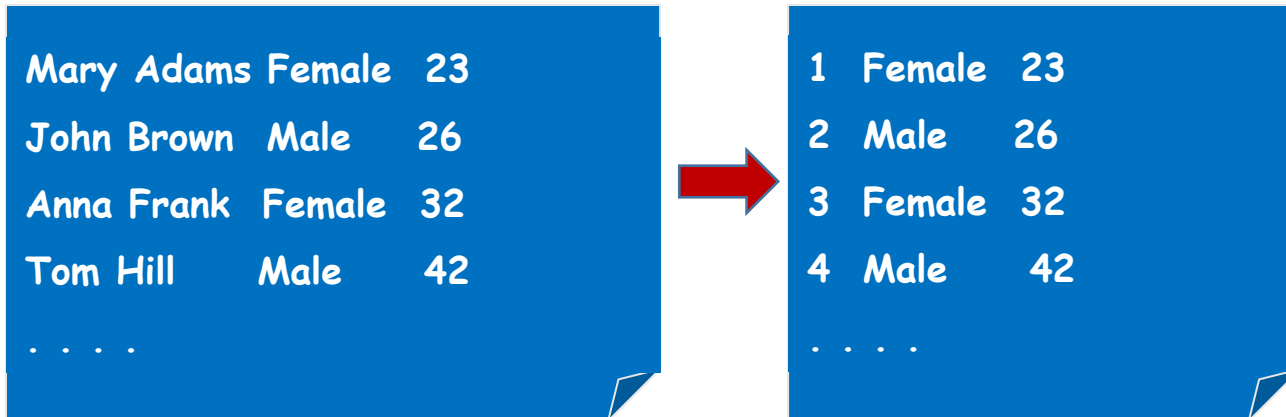
An example

- A hospital utilizes an electronic health record
- By default, access is granted to only those members of the medical staff who are assigned to the treatment of the respective patient in the specific department she/he is assigned to
- The group of people with access to a patient's file is enlarged if other departments or diagnostic units are involved in the treatment.
- After the patient is discharged, and billing is completed, access is reduced to a small group of employees per speciality department who answer requests for medical information or a consultation made or asked for by other medical service providers upon authorization by the respective patient.
- If access is needed for research purposes, the researcher should not know the exact identity of the patients
 - This may be achieved by, e.g, proper pseudonymisation (for example, through a deterministic pseudonymisation scheme on the Social Security Number)



Why pseudonymisation?

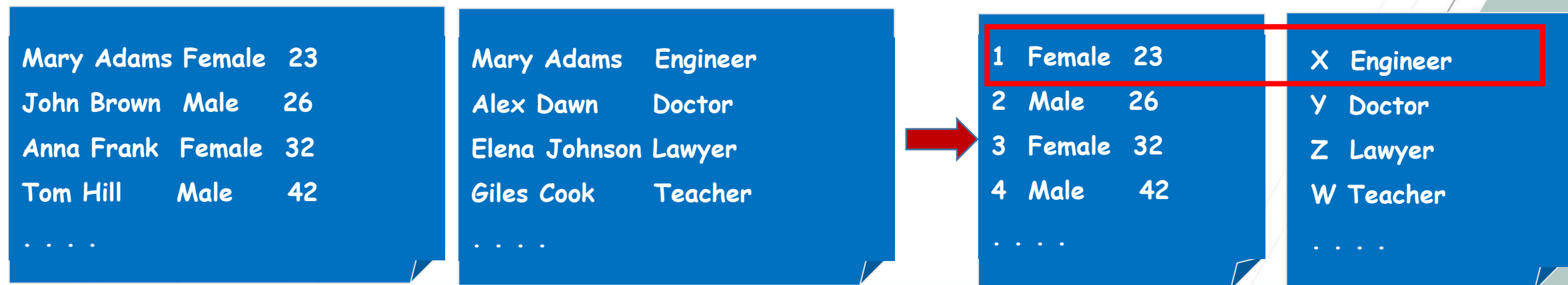
1. Hiding identities (related to confidentiality)



- Pseudonymisation is explicitly mentioned in the GDPR as a possible safeguard towards achieving data protection by design (see subsequent seminar)
- Special attention:
 - State-of-the-art
 - Is re-identification possible through the remaining information?

A risk-based approach

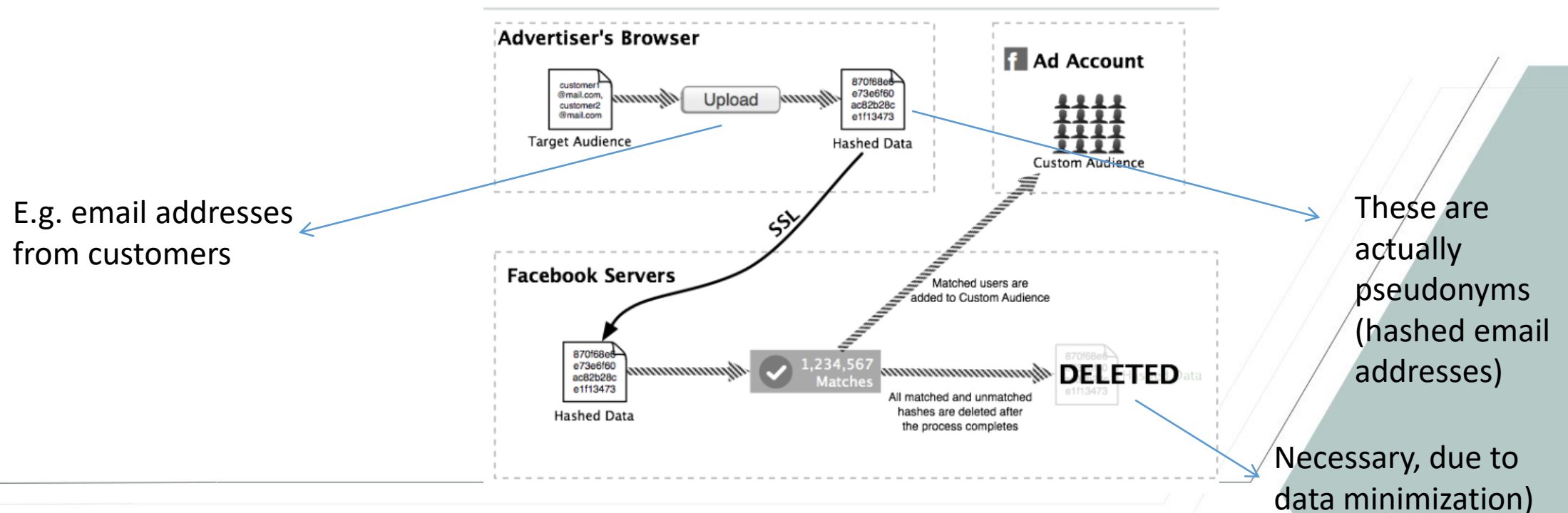
2. Unlinkability





An example of (bad?) pseudonymisation

- Custom audience match process in Facebook (Under the assumption that valid users consents exist)
- (source: https://3qdigital.com/wp-content/uploads/2016/06/facebook_audiences_data_security_overview.pdf)





An example of (bad?) pseudonymisation (Cont.)

- Hashed data are mathematically irreversible, but..
 - If a controller knows hashed email addresses, recovering some of them is possible...



Source: ENISA Report, Pseudonymisation techniques and best practices, 2019.

- Not a state-of-the-art solution => data minimization is put at risk
- More advanced state-of-the-art techniques should be considered in the design process – e.g. private set intersection techniques (see ENISA Report, Data Pseudonymisation: Advanced Techniques and Use Cases, 2021)



Example of bad anonymisation – The famous AOL example



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

August 2006: research.aol.com

AOL is embarking on a new direction for its business making its content and products freely available to all consumers. To support those goals, AOL is also embracing the vision of an open research community. To get started, we invite you to visit us at <http://research.aol.com>, where you will find:

- ...
- **Query streams for 500,000 users over 3 months (20 million queries)**
-
- A random ID was associated to each user
 - The same (meaningless) ID, for the same user
 - This is actually a pseudonymisation procedure..
- However, a combination of the published information with other available data could allow identification!



Re-identification from “anonymous” data



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

HOME PAGE | MY TIMES | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

The New York Times

Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

CAMCORDERS | CAMERAS | CELLPHONES | COMPUTERS | HANDHELDS | HOME VIDEO | MUSIC | PERIPHERALS

A Face Is Exposed for AOL Searcher No. 4417749

By MICHAEL BARBARO and TOM ZELLER Jr.
Published: August 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.



No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from “numb fingers” to “60 single men” to “dog that urinates on everything.”

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for “landscapers in Lilburn, Ga.,” several people with the last name Arnold and “homes sold in shadow lake subdivision gwinnett county georgia.”

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. “Those are my searches,” she said, after a reporter read part of the list to her.

AOL removed the search data from its site over the weekend and apologized for its release, saying it was an unauthorized move by a team that had hoped it would benefit academic researchers.

But the detailed records of searches conducted by Ms. Arnold and 657,000 other Americans, copies of which continue to circulate online, underscore how much people unintentionally reveal about themselves when they use search engines — and how risky it

Multimedia
Graphic: What Revealing Search Data Reveals

ARTICLE TOOLS
SPONSORED BY
HISTORY BOYS

SIGN IN TO E-MAIL THIS
PRINT
SINGLE PAGE
REPRINTS
SAVE

- The characterization of anonymous data is not an easy task
- Simply removing “obvious identifiers” is not adequate
- In other words, the notions of identifiers or “identifying data” is wide
 - Identifier in which context?
- A proper design on the anonymisation/pseudonymisation procedure is needed to be performed from the beginning



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

DPbD – Accuracy



Key design elements for accuracy

- Data source – Sources of personal data should be reliable in terms of data accuracy.
- Degree of accuracy – Each personal data element should be as accurate as necessary for the purposes.
- Measurably accurate - Reduce the number of false positives/negatives, for example biases in automated decisions and artificial intelligence.
- Verification – Verify the correctness of personal data with the data subject before and at different stages of the processing
- Erasure/rectification – Without delay.
- Error propagation avoidance – Mitigating the effect of an accumulated error in the processing chain.
- Access – Users should be allowed having effective access to personal data
- Continued accuracy – Tests of accuracy should be carried out at several stages
- Up to date – Personal data shall be updated if necessary for the purpose.
- Data design - Use of appropriate design features to decrease inaccuracy – e.g. present concise predetermined choices instead of free text fields.



DPbD - Bad practices in accuracy

- Common bad practices:
 - Non-verification of accuracy during the collection of data
 - E.g. The validity of the email address is not being checked
 - No appropriate ways to discriminate individuals with “similar” identifiers
 - E.g. Two records for two different individuals with the same name, such as “Mary Adams”
 - Collection of data from untrusted sources
 - E.g. from social networks or public web sites (note that such a collection may not even have a legal basis!)
 - No easy means for the users to update their information that they have provided

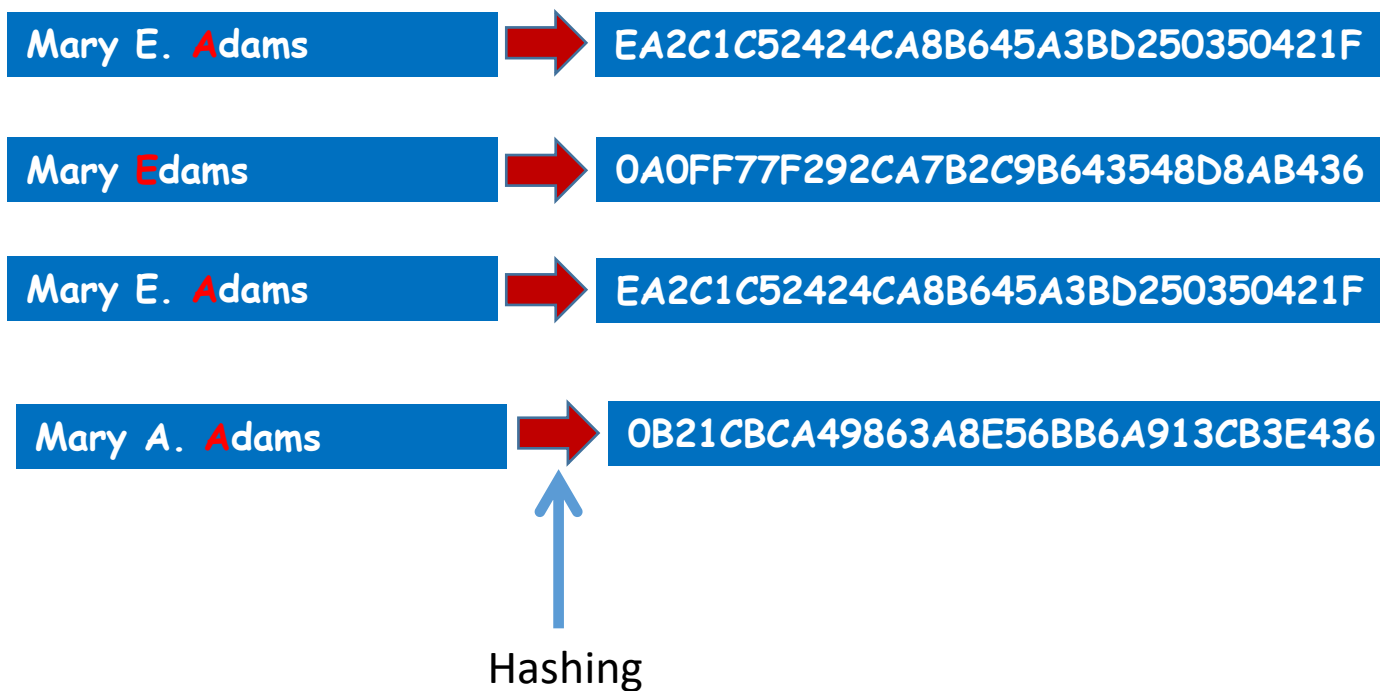


An example

- A health institution is looking to find methods to ensure the accuracy of personal data in their client registers.
- Where two persons arrive at the institution at the same time and receive the same treatment, there is a risk of mistaking them if the only parameter to distinguish them is by name.
- Need for a unique indistinguishable identifier for each person.
- Possible solution: Unique identifier per user (pseudonymisation)
 - Via, e.g., cryptographic solutions such as hashing



An example (Cont.)





An example

- An insurance company wishes to use artificial intelligence (AI) to profile customers buying insurance as a basis for their decision making when calculating the insurance risk
 - Assuming that a valid legal basis is in place
- The model is being trained based on large pool of existing customers
 - Proper pseudonymisation of data to feed the training module
- The accuracy of input data is essential (only trusted sources of data)
- The company should check whether the AI is reliable and provides non-discriminatory results both during its development and finally before the product is released



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

DPbD – Storage limitation



Key design elements for storage limitation



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

- Deletion and anonymization – Clear internal procedures and functionalities for deletion and/or anonymization.
- Effectiveness of anonymization/deletion – Ensure that it is not possible to re-identify anonymized data or recover deleted data
- Automation – Deletion of certain personal data should be automated
- Storage criteria – Determine what data and length of storage is necessary for the purpose.
- Enforcement of retention policies – Determination of such policies and tests of whether the policies are implemented
- Justification – Justify why the period of storage is necessary for the purpose and the personal data in question (be able to disclose the rationale behind).
- Backups/logs – Determination of what personal data and length of storage is necessary for back-ups and logs.
- Data flow – Beware of the flow of personal data, and the storage of any copies thereof, and seek to limit their “temporary” storage.



DPbD - Bad practices in storage limitation



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

- Common bad practices:
 - The necessary retention period is not determined
 - The information that is given is of the type “We keep your personal data as long as necessary”
 - No automated methods for deletion – manual deletions
 - Not prohibitive, but vulnerable to human errors....
 - Anonymisation instead of deletion, but anonymisation is not effective
 - E.g. simply deleting identifiers does not yield anonymous data
 - De-activation instead of deletion
 - Data are “flagged” as deleted, but they are still there!

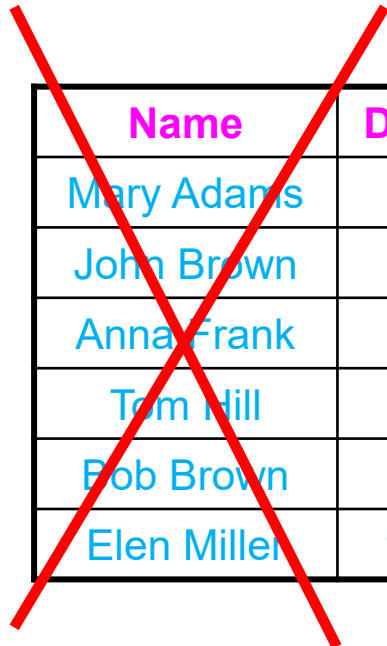


An example

- A company collects personal data where the purpose of the processing is to administer a membership of the data subject.
- The personal data shall be deleted when the membership is terminated (no legal basis for further storage of the data).
- => Internal procedure for manual deletion
 - from any devices, from backups, logs, e-mails and other relevant storage media
- To make deletion more effective, and less error-prone, the company then implements an automatic system instead, in order to delete data automatically, reliably and more regularly.



An example on bad anonymisation



| Name | Date of birth | Sex | Zip code | Disease |
|-------------|---------------|--------|----------|------------|
| Mary Adams | 5/3/1995 | Female | 12635 | Flu |
| John Brown | 4/8/1992 | Male | 53715 | Hepatitis |
| Anna Frank | 10/1/1986 | Female | 53703 | Brochitis |
| Tom Hill | 1/2/1976 | Male | 12635 | Broken Arm |
| Bob Brown | 4/3/1990 | Male | 53706 | Flu |
| Elen Miller | 12/10/1959 | Male | 53700 | Broken leg |

Simply deleting the identifiers does not mean that the remaining data are anonymous

- Be careful on the quasi-identifiers and the relevant risks (see next seminars)



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

DPbD – Confidentiality and integrity



Key design elements for confidentiality and integrity

- Information security management system (ISMS) – Have an operative means of managing policies and procedures for information security.
- Risk analysis – Assess the risks against the security of personal data (several standard methodologies exist).
- Security by design – Consider security requirements as early as possible in the design
- Maintenance – Regular review and test software, hardware, systems and services, etc. to uncover vulnerabilities
- Secure transfers and storage – against unauthorized and accidental access and changes.
- Access control management – Only authorised access to strictly necessary personal data
- Pseudonymization – As a security measure to minimise risks of potential data breaches
- Backups/logs – Keep back-ups and logs that are necessary for information security, use audit trails and event monitoring as a routine security control.
- Disaster recovery/ business continuity
- Security incident response management



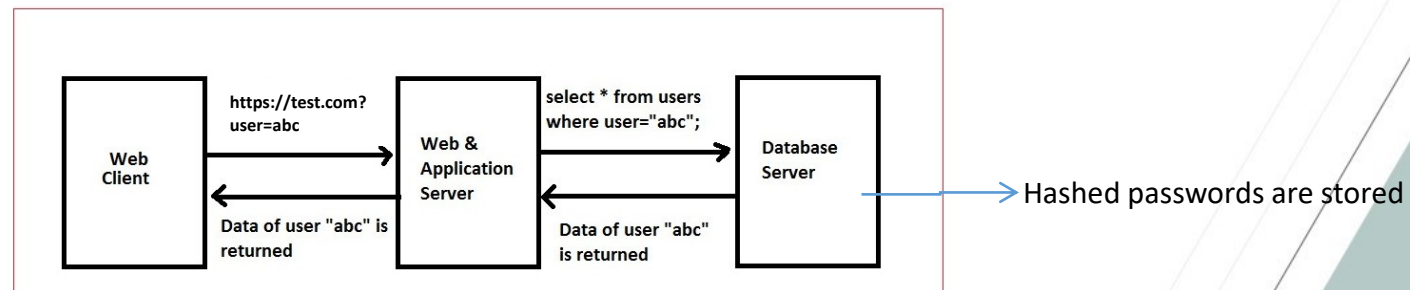
DPbD - Bad practices in confidentiality and integrity

- Common bad practices:
 - Security measures have been adopted empirically, without a systematic risk analysis
 - No proper identification of risks, which in turn means no proper choice of security measures (and not fulfillment of the accountability principle)
 - No proper access control
 - E.g. not strong authentication mechanisms or not cautious permission model for users
 - Not usage of state-of-the-art technologies (e.g. obsolete encryption)
 - E.g. Usage of the RC4 cryptographic algorithm
 - Not proper configuration of network security protocols
 - E.g. even the TLS or IPSec protocols may have vulnerabilities if they are not properly configured from the beginning
 - No regular updates/patches to critical software supporting the data processing
 - E.g. to e-commerce platforms, operating systems, other supporting software etc.



A bad example

- Web form of a bookstore:
 - Use of the TLS protocol (i.e. https), version 1.2 – to protect communications with clients
 - However, protocol downgrade is possible, for allowing old browsers to connect
 - An SQL database operates “behind” the application server
 - No input sanitization; any character that the user enters in the form, passes to the SQL database
 - Passwords of the registered users are being stored in hashed form
 - Hash is mathematically irreversible, so it is being considered as a secure means to protect passwords





A bad example (Cont.)

- TLS is not panacea
 - TLS 1.2 supports some weak ciphers and modes of operation, that should be avoided
 - Allowing a client to downgrade the protocol yields security issues, even for previous communications that took place with the 1.2 version! (DROWN attack)

This server supports SSL 2, which is obsolete and insecure, and can be used against TLS (DROWN attack). Grade set to F. [MORE INFO »](#)

This server uses SSL 3, which is obsolete and insecure. Grade capped to B. [MORE INFO »](#)

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. [MORE INFO »](#)

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. [MORE INFO »](#)

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. [MORE INFO »](#)

This server supports TLS 1.0. Grade capped to B. [MORE INFO »](#)

Configuration

| Protocols | |
|-----------|---------------------|
| TLS 1.3 | No |
| TLS 1.2 | Yes |
| TLS 1.1 | No |
| TLS 1.0 | Yes |
| SSL 3 | INSECURE Yes |
| SSL 2 | INSECURE Yes |

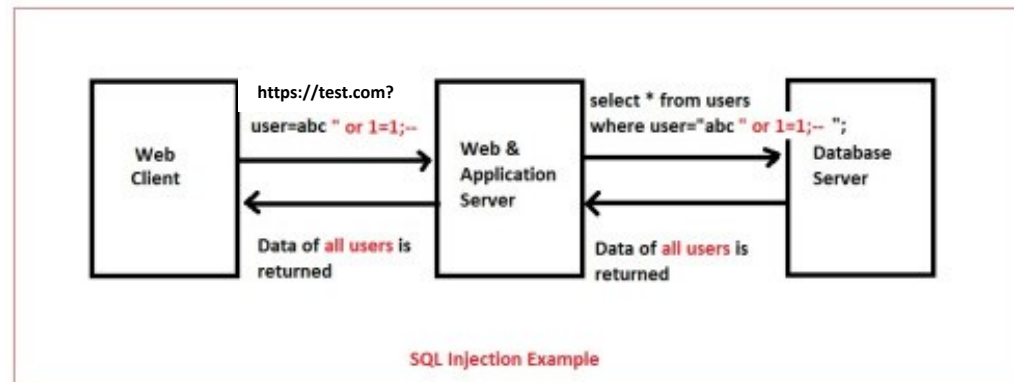
| Cipher Suites | |
|--|---------------------|
| # TLS 1.2 (suites in server-preferred order) | |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) | WEAK 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) | WEAK 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) | WEAK 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | WEAK 256 |
| TLS_RSA_WITH_RC4_128_SHA (0x5) | INSECURE 128 |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) | WEAK 112 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS | WEAK 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS | WEAK 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS | WEAK 256 |
| TLS_RSA_WITH_RC4_128_MD5 (0x4) | INSECURE 128 |

Output of a TLS scanner tool



A bad example (*Cont.*)

- Take care of SQL injection attacks!



- They can be avoided only if a proper design has been implemented
- A security scanner tool may detect such a vulnerability:

Vulnerabilities

42424 - CGI Generic SQL Injection (blind)





A bad example (*Cont.*)

- Hashed passwords, without salt, may be recovered
- E.g. through rainbow attacks (easily available rainbow tables, with huge number of entries)

| Password | SHA-2 Hash value |
|---------------|--|
| 123456 | 8D969EEF6ECAD3C29A3A629280E686CF0C3F5D5A86AFF3CA 12020C923ADC6C92 |
| abc123 | 6CA13D52CA70C883E0F0BB101E425A89E8624DE51DB2D239 2593AF6A84118090 |
| 123456789 | 15E2B0D3C33891EBB0F1EF609EC419420C20E320CE94C65FB C8C3312448EB225 |
| qwerty | 65E84BE33532FB784C48129675F9EFF3A682B27168C0EA744 B2CF58EE02337C5 |
| iloveyou | E4AD93CA07ACB8D908A3AA41E920EA4F4EF4F26E7F86CF829 1C5DB289780A5AE |
| Antetokounmpo | 3AB6EAC678B05C7CFBC67E1F996D19B0F8F06C19EFDB65070 B60C0BA3F6905DD |
| | |

A solution would be salted hashes, where the salts are being stored in a separate place



An example

- A company wants to extract large quantities of personal data from a medical database containing electronic (patient) health records to a dedicated database server in the company in order to process the extracted data for quality assurance purposes.
- Since there is only one department in the company who needs to process the patient data extracts, the controller decides to restrict access to the dedicated server to employees in that department.
- Moreover, to further reduce risk, the data will be pseudonymized before they are transferred.



An example (*Cont.*)

- The company decides to segregate the network, and establish access controls to the server (to regulate access, protect from malware etc).
- In addition, they put up security monitoring and an intrusion detection and prevention system and isolates it from routine use
- An automated auditing system is put in place to monitor access and changes. Reporting and automated alerts are generated from this when certain events related to usage are configured.
- The company will ensure that users only have access on a “need to know” basis and with the appropriate access level.
 - Inappropriate use can be quickly and easily detected



An example (*Cont.*)

- Some of the extracts have to be compared with new extracts, and therefore are required to be stored for three months.
- The company decides to put them into separate databases on the same server, and use both transparent and column-level encryption to store them.
- Keys for column data decryption are stored in dedicated security modules that can only be used by authorized personnel, but not extracted.



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

Data protection by default – Guiding questions for defining the defaults



Guiding questions

- What are the specific purposes of the data processing? Are the data subjects informed about the purposes and the data processing?
- For any built-in functionality:
 - Are there situations conceivable where users would prefer or need a different functionality? In which way?
 - Does the built-in functionality implement the data protection principles of the GDPR? Which data-protection principles are supported by this functionality, which are not?

Source: ENISA Report, Exploring the notion of data protection by default, 2018



Guiding questions (*Cont.*)

- For any configuration option:
 - Which are the possible settings/options?
 - Which are the settings/options that minimise the amount of personal data, the extent of processing, the storage period and the accessibility taking into account each specific purpose? Is this the default pre-setting?
 - If more than one setting may come into question, are there specific criteria for preferring one setting? (This could be the case for different target groups, e.g. different pre-settings for children.)
 - How are the alternative choices presented so that the user can make a privacy-aware decision?
- For any configuration option without a default pre-setting: What is the reason for not using a pre-setting?

Source: ENISA Report, Exploring the notion of data protection by default, 2018



Guiding questions (*Cont.*)

- For any configuration option with a default pre-setting:
 - Does the default setting realise that only personal data which are necessary for each specific purpose of the processing are processed? With respect to:
 - the amount of personal data collected (can there be less personal data, e.g. fewer attributes, aggregated information, less sensitive data, no (temporary) copies?),
 - the extent of their processing (can the processing be reduced, e.g. less analysis, less transfer, less linkage with other data?),
 - the period of their storage (can the storage period be shortened?) and
 - their accessibility (can the amount of people or parties or machines that will or may have access to the personal data can be decreased, e.g. by local storage, limited access rights, encryption, secure erasure without any traces?)

Source: ENISA Report, Exploring the notion of data protection by default, 2018



Guiding questions (*Cont.*)

- For any configuration option with a default pre-setting:
 - Does the default setting work for achieving the purpose (at least with basic functionality)?
 - Does the change of the pre-setting increase or decrease the user's privacy? To what extent? Are gradual changes possible?
 - How are users supported in changing the settings, e.g. explanation of the effects, offering typical combined settings profiles (e.g. appropriate for a chosen risk level), allowing for specific individual customisation?
 - Can the user conveniently reset the configured setting and go back to the pre-setting?
 - How is the handling of pre-settings and settings changed by the users when the system is updated? Are the previous settings maintained? How are users informed about new settings, new options, new functionality or privacy risks?

Source: ENISA Report, Exploring the notion of data protection by default, 2018



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

Thank you for your participation!