byDesign

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)*

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ

ΚΕΝΤΡΟ ΕΡΕΥΝΩΝ
ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ

ICT abovo
Information & Communication Technologies

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

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

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 in order to meet the relulatory 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?

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

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 by introducing adequate control features
- Privacy requirements are generally in compliance with legislation or data privacy rules existing in a country

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

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

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

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

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

Privacy Requirements Elicitation Methodologies

- 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

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

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

Privacy Requirements Elicitation Methodologies: LINDDUN

- 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

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

Privacy Requirements Elicitation Methodologies: LINDDUN

- 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

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

Privacy Requirements Elicitation Methodologies: LINDDUN

- 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

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

Privacy Requirements Elicitation Methodologies: LINDDUN

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

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

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

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

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.

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

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

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

Privacy Requirements Elicitation Methodologies: PriS

- 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

- 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

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

Privacy Requirements Elicitation Methodologies: PriS

- 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 goas
  - Modeling of privacy processes based on the relevant privacy process patterns
  - Definition of a system architecture that supports the privacy processes: Process pattern are used to identify the proper implementation technique(s) that best implement the corresponding processes

Privacy Requirements Elicitation Methodologies: PriS

- 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

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

Privacy Requirements Elicitation Methodologies: RBAC

- 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

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

Privacy Requirements Elicitation Methodologies: RBAC

- 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

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

Privacy Requirements Elicitation Methodologies: STRAP

- 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

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

Privacy Requirements Elicitation Methodologies: STRAP

- 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

- 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

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

Privacy Requirements Elicitation Methodologies: The i* method

- 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

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

Privacy Requirements Elicitation Methodologies: The i* method

- 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

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

Privacy Requirements Elicitation Methodologies: PRET

- 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

- 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

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

Privacy Requirements Elicitation Methodologies: MAPaS

- 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

- 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)

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

Privacy Requirements Elicitation Methodologies: GBRAM

- 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

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

Privacy Requirements Elicitation Methodologies: GBRAM

- 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

Personal Data Retention

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

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

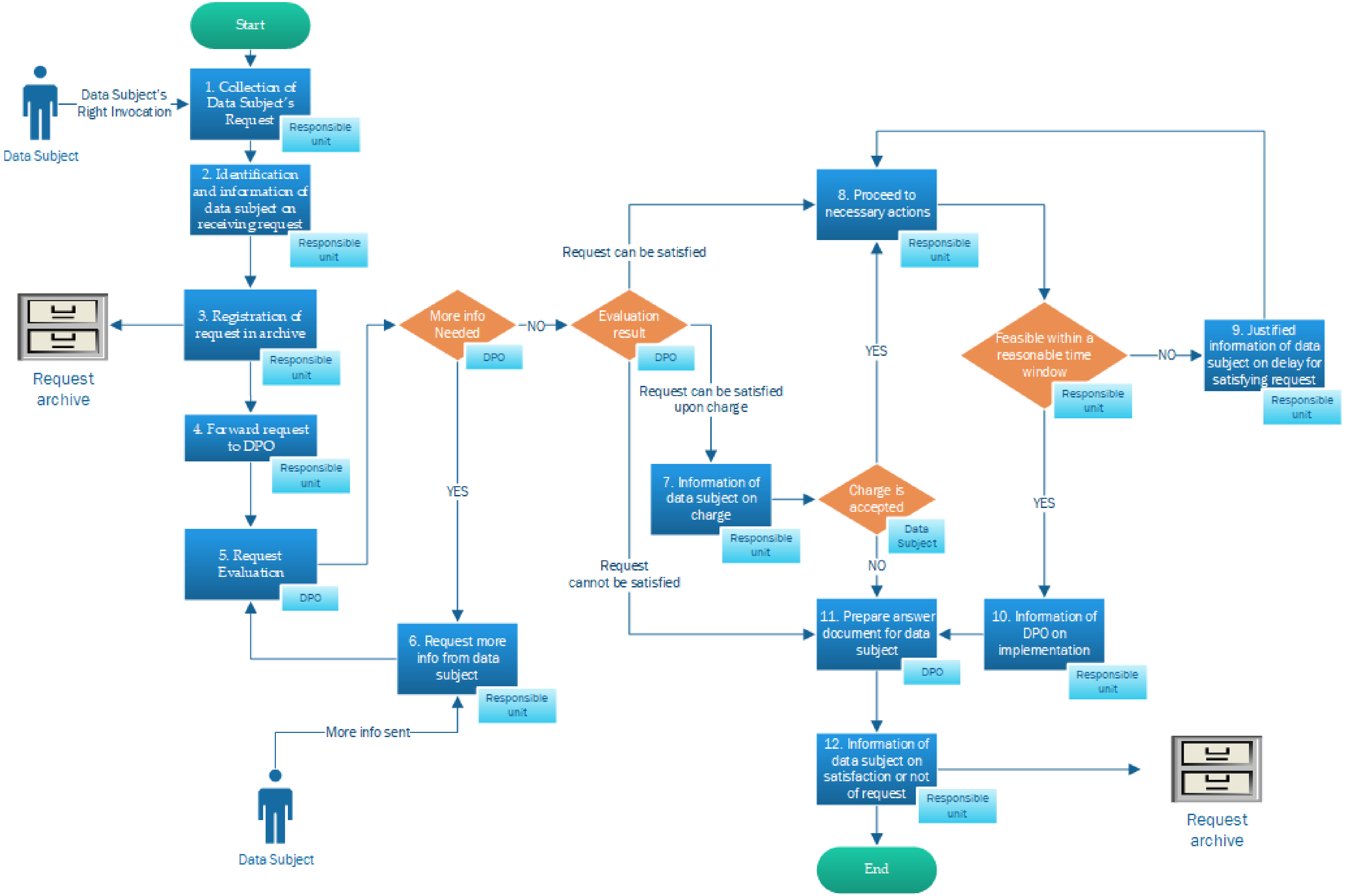
Data Subjects' Rights Management

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


Start
Data Subject's Right Invocation
Data Subject
1. Collection of Data Subject's Request
Responsible unit
2. Identification and information of data subject on receiving request
Responsible unit
3. Registration of request in archive
Responsible unit
Request archive
4. Forward request to DPO
Responsible unit
5. Request Evaluation
DPO
More info Needed
DPO
NO
YES
6. Request more info from data subject
Responsible unit
More info sent
Data Subject
Evaluation result
DPO
Request can be satisfied
Request can be satisfied upon charge
Request cannot be satisfied
7. Information of data subject on charge
Responsible unit
Charge is accepted
Data Subject
YES
NO
8. Proceed to necessary actions
Responsible unit
Feasible within a reasonable time window
Responsible unit
NO
9. Justified information of data subject on delay for satisfying request
Responsible unit
YES
10. Information of DPO on implementation
Responsible unit
11. Prepare answer document for data subject
DPO
12. Information of data subject on satisfaction or not of request
Responsible unit
Request archive
End

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

Data Subjects’ Rights Management:

Step 1: Collection of Data Subject’s Request

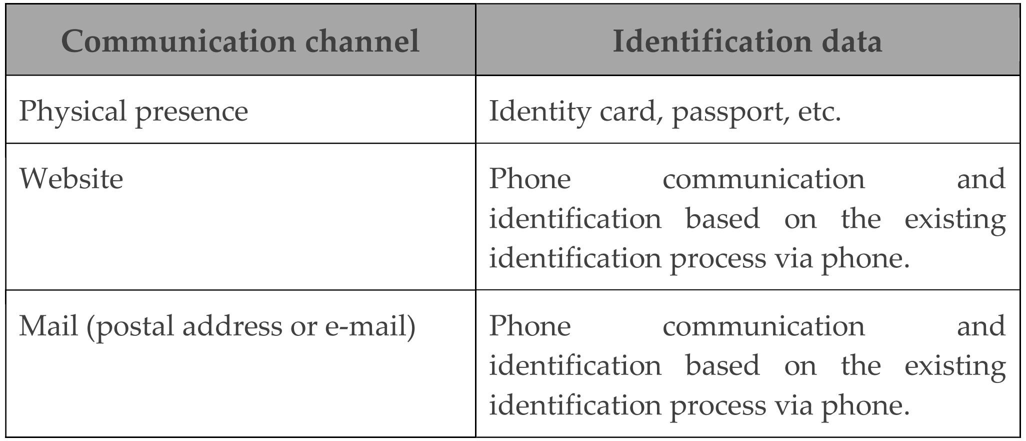
- The Data Subject submits, via the available channels, his/her request regarding his/her personal data, in order to exercise his/her corresponding right(s). The communication channels that the Data Subjects can use are (indicatively):
  - Physical Presence: The Data Subject completes a standardised 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.

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

Data Subjects’ Rights Management:

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.

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

Data Subjects’ Rights Management:

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.

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

Data Subjects' Rights Management:

Step 4: Forwarding the request to the Data Protection Officer

- 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.

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

Data Subjects’ Rights Management:

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.

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

Data Subjects’ Rights Management:

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).	• 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).	• 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).	• 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

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

Data Subjects’ Rights Management:

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	√	√	√	√	√	×	√ (withdrawal of consent)
Performance of a contract	√	√	√	√	√	×	√
Legal obligation	√	√	×	√	×	×	√
Legitimate interest	√	√	√	√	×	√	√
Vital interest	√	√	×	√	×	×	√
Public interest	√	√	√	√	×	√	√

- 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.

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

Data Subjects’ Rights Management:

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.

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

Data Subjects’ Rights Management:

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.

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

Data Subjects’ Rights Management:

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.

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

Data Subjects’ Rights Management:

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.

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

Data Subjects’ Rights Management:

Step 11: Prepare the response document for the Data Subject

- 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.

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

Data Subjects’ Rights Management:

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

- 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!