[Organization logo]

[Organization name]

**PROJECT PLAN**  
**for Implementation of the Information Security Management System and for Complying with the European General Data Protection Regulation**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| dd.mm.yyyy | 0.1 | EUGDPRAcademy | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc114478316)

[2. Reference documents 3](#_Toc114478317)

[3. ISMS implementation project 3](#_Toc114478318)

[3.1. Project objective 3](#_Toc114478319)

[3.2. Project results 3](#_Toc114478320)

[3.3. Deadlines 5](#_Toc114478321)

[3.4. Project organization 6](#_Toc114478322)

[3.4.1. Project sponsor 6](#_Toc114478323)

[3.4.2. Project manager 6](#_Toc114478324)

[3.4.3. Project team 6](#_Toc114478325)

[3.5. Main project risks 7](#_Toc114478326)

[3.6. Tools for project implementation, reporting 7](#_Toc114478327)

[4. Managing records kept on the basis of this document 7](#_Toc114478328)

[5. Validity and document management 7](#_Toc114478329)

# Purpose, scope and users

The purpose of the Project Plan is to clearly define the objective of the Information Security Management System (ISMS) and European General Data Protection Regulation (EU GDPR) implementation project, documents to be written, deadlines, and roles and responsibilities in the project.

The Project Plan is applied to all activities performed in the ISMS/EU GDPR implementation project.

Users of this document are members of [top management] and members of the project team.

# Reference documents

* ISO/IEC 27001 standard
* EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
* [decision or any similar document prescribing project launching]
* [methodology for project management]

# ISMS implementation project

## Project objective

To implement the Information Security Management System in accordance with the ISO 27001 standard and comply with the EU GDPR by [date] at the latest.

## Project results

In order to ensure the most efficient project planning, the Company should use the GDPR Readiness Questionnaire to determine which areas of GDPR compliance need the most work.

During the ISMS/EU GDPR implementation project, the following documents will be written (this is not an exhaustive list of all the documents):

* **Procedure for Document and Record Control** – procedure prescribing basic rules for writing, approving, distributing and updating documents and records;
* **Procedure for Identification of Requirements** – procedure for identification of statutory, regulatory, contractual and other obligations;
* **ISMS Scope Document** – a document precisely defining assets, locations, technology, etc. which are part of the scope;
* **Information Security Policy** – this is a key document used by management to control information security management;
* **Personal Data Protection Policy** – a policy meant to establish the general data protection principles as well as to prove the commitment of the company to those principles;
* **Employee Personal Data Protection Policy** – a policyto set out the conditions under which the company processes personal data of its employees;
* **Privacy Notice** – a notice to set out the conditions under which the company processes personal data of its clients/website visitors;
* **Register of Privacy Notices** – a document where you need to list all the published notices;
* **Data Retention Policy** – a policy to set out the period for which personal data may be kept by the company;
* **Data Protection Officer Job Description** – a document that describes the responsibilities of the data protection officer;
* **Guidelines for Data Inventory and Processing Activities Mapping** – a document which explains how to list all the data processing activities;
* **Inventory of Processing Activities** – a document meant to be used by the Company to prove compliance with the requirements of Article 30 of the EU GDPR;
* **Data Subject Consent Form** – a document used by the Company to obtain consent from the data subjects for processing personal data for a specific purpose;
* **Data Subject Consent Withdrawal Form** – a document used by the data subjects to withdraw their consent;
* **Parental Consent Form** – a document used by the Company to obtain consent from the parent/legal guardian/representative of a minor to process personal data for a specific purpose;
* **Parental Consent Withdrawal Form** – a document used by the parent/legal guardian/representative of a minor to withdraw the consent from processing personal data for a specific purpose;
* **Data Subject Access Request Procedure** – a document to set up the process by which the Company answers to data subjects requests;
* **Risk Assessment and Risk Treatment Methodology** – describes the methodology for managing information risks;
* **Risk Assessment Table** – the table is the result of assessment of asset values, threats and vulnerabilities;
* **Risk Treatment Table** – a table in which appropriate security controls are selected for each unacceptable risk;
* **Risk Assessment and Risk Treatment Report** – a document containing all key documents made in the process of risk assessment and risk treatment;
* **Data Protection Impact Assessment Methodology** – a document that describes how to assess the necessity and proportionality of a certain processing activity and provide measures to mitigate potential risks to the rights and freedoms of data subjects;
* **DPIA Register** – a document used by the Company to document the DPIA process. It includes the Threshold questionnaire and the DPIA questionnaire;
* **Statement of Applicability** – a document which determines the objectives and applicability of each control according to Annex A of the ISO 27001 standard;
* **Risk Treatment Plan** – an implementation document specifying controls to be implemented, who is responsible for implementation, deadlines and resources;
* **Bring Your Own Device (BYOD) Policy** – describes the rules for using mobile and other non-company devices for business purposes;
* **Mobile Device, Teleworking and Work from Home Policy** – describes security rules for using laptops, mobile phones and other devices outside of the company premises;
* **IT Security Policy** – describes basic security rules for all employees;
* **Information Classification Policy** – defines how to classify data according to confidentiality, and how to protect the data accordingly;
* **Access Control Policy** – defines how the management approves the access rights to particular users of information systems;
* **Policy on the Use of Encryption** – defines how to use cryptographic controls and keys to protect the confidentiality and integrity of the data;
* **Anonymization and Pseudonymization Policy** – defines how to use these techniques in order to protect the personal data processing;
* **Clear Desk and Clear Screen Policy** – defines how to protect the information that is located in the workplace and on computer screens;
* **Security Procedures for IT Department** – describes security rules that need to be used for the IT infrastructure;
* **Cross Border Data Transfer Procedure** – a document for establishing the conditions under which a cross border data transfer may be carried out;
* **Standard Contractual Clauses** – model clauses issued by the EU Commission to provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights;
* **Processor GDPR Compliance Questionnaire** – a questionnaire meant to assess supplier’s compliance with EU GDPR;
* **Supplier Data Processing Agreement** – a contractual document meant to establish the limits and conditions under which a supplier (processor) can process personal data on behalf of the Company (controller);
* **Data Breach Response and Notification Procedure** – a procedure that establishes the Company’s obligations in case of a personal data breach;
* **Data Breach Register** – Company’s internal register of data breaches;
* **Data Breach Notification Form to the Supervisory Authority** – the document to be used in case of a data breach;
* **Data Breach Notification Form to the Data Subjects** – the document to be used in case of a data breach;
* **Disaster Recovery Plan** – defines how to recover the infrastructure and the data after a disrupting incident;
* **Procedure for Internal Audit** – defines how auditors are selected, how audit programs are written, how audits are conducted and how audit results are reported;
* **Procedure for Corrective Action** – describes the process of implementation for corrective and preventive actions;
* **Form for Management Review Minutes** – a form used to create minutes from the management meeting held to review ISMS adequacy.

Other documents which must be written during ISMS/EU GDPR implementation will be specified in the Risk Treatment Plan.

## Deadlines

Deadlines for acceptance of individual documents in the course of ISMS/EU GDPR implementation are as follows:

|  |  |
| --- | --- |
| ***Document*** | ***Deadlines for document acceptance*** |
| \* |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Final presentation of project results is planned for [date].

## Project organization

### Project sponsor

Each project has an assigned "sponsor" who does not actively participate in the project. The project sponsor must be regularly briefed by the project manager about the project status, and intervene if the project is halted.

[Name, job title] has been appointed project sponsor.

### Project manager

The role of the project manager is to ensure resources necessary for project implementation, to coordinate the project, to inform the sponsor about the progress, and to carry out administrative work related to the project. Project manager's authority should be such as to ensure uninterrupted project implementation within set deadlines.

[Name, job title] has been appointed project manager.

### Project team

The role of the project team is to assist in various aspects of project implementation, to perform tasks as specified in the project, and to make decisions about various issues that require a multidisciplinary approach. The project team meets each time before the final version of a document from section 2 of this Project Plan is completed, and in all other cases when the project manager deems it necessary.

*Table of participants in the project*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Name* | *Organizational unit* | *Job title* | *Phone* | *E-mail* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Main project risks

The main risks in the implementation of the project are the following:

1. Extension of deadlines in the risk assessment phase
2. Extension of deadlines during the development of business continuity plans
3. Performing activities that incur unnecessary costs and waste time
4. Selection of too many and/or too expensive controls

Measures to reduce the abovementioned risks are the following:

* The project manager monitors that all activities in the project are performed within defined deadlines, and seeks intervention by the project sponsor in a timely manner
* Hiring a consultant to ensure that time or resources are not spent on activities that are not important for the project, and that individual activities are not headed in the wrong direction
* Hiring a consultant to propose the most cost-effective controls

## Tools for project implementation, reporting

A shared folder including all documents produced during the project will be created on the local network. All members of the project team will have access to these documents. Only the project manager [and members of the project team] will be authorized to make changes and delete files.

The project manager will prepare a project implementation report on a monthly basis and forward it to the project sponsor.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Control for record protection | Retention time |
| Project implementation report (in electronic form) | Shared folder for project-related activities | Project manager | Only the project manager is authorized to edit data | The report is stored for a period of 3 years |

# Validity and document management

This document is valid as of [date].

Owner of this document is [job title].

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

* whether all employees engaged in the project perform their activities in line with this document
* whether all project deadlines are met

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]