[organization logo]

[organization name]

**PROJECT PROPOSAL FOR EU GDPR IMPLEMENTATION**

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

**Distribution list**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Copy No. | Distributed to | Date | Signature | Returned | |
| Date | Signature |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| xx/xx/2018 | 0.1 | EUGDPRAcademy | Basic document template |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose 2](#_Toc384142166)

[2. Reasoning 2](#_Toc384142167)

[3. Project objectives 3](#_Toc384142168)

[4. Project duration and structure 3](#_Toc384142169)

[5. Responsibilities 3](#_Toc384142170)

[6. Resources 3](#_Toc384142171)

[7. Deliverables 4](#_Toc384142172)

# 

# Purpose

The purpose of this document is to propose the project of EU GDPR implementation to the top management.

This document is not a project plan ‑ the Project Plan will be developed once the project is formally approved.

# Reasoning for the implementation

Primary reasons for EU GDPR implementation are:

* to avoid penalties applied by the EU GDPR
* to make a register of data processing activities
* to demonstrate transparency
* to secure the personal data

# Project objectives

The objectives for the project are:

* implementation of the GDPR on or before [date]
* implementation of the GDPR should not interrupt normal operating activities
* members of the project team may spend up to [xyz%] of their time on this project

# Project duration and structure

The implementation project is divided into different phases:

1. Initiation, planning, and assessment – the project is set, and assessment is carried out of existing processes, as well as of the types of personal data that are collected. Gap analysis is performed.
2. The key roles and responsibilities are defined.
3. Implementation of the policies, documents, and controls in accordance with the EU GDPR.

Main milestones of the implementation project are:

|  |  |
| --- | --- |
| **Milestone** | **Due date** |
| Initiation |  |
| Planning |  |
| Assessment |  |
| Defining roles and responsibilities |  |
| Implementation |  |

Detailed content of the milestones and respective responsibilities will be described in the Project Plan document.

# Resources

Resources required to implement the project include financial, human, and technical resources.

Financial resources include:

* Amount: [define amount of money needed to finish the project]
  + Cost types: [split costs according to the cost type and include all resources listed here, e.g., human resources ‑ internal and external, technical and other]

Human resources include:

* Internal resources ‑ [list internal resources, e.g., group name, project name, etc.]
* External resources ‑ [list all external resources, e.g., consulting company, etc.]

Technical resources include:

* Tool ‑ tool name: [enter tool name]
* Equipment ‑ [list equipment needed]

Other resources include:

* Documentation ‑ [list all documentation that is required, e.g., EU GDPR Documentation Toolkit, full text of the EU GDPR]
* Resources to leverage the employees’ knowledge about the GDPR - [books, training, etc.]

# Deliverables

During the EU GDPR implementation project, the following documents will be written:

* **Personal Data Protection Policy** ‑ this is a top-level document for managing privacy in your company, which defines what you want to achieve and how.
* **Privacy Notice** ‑ this document (which can also be published on your website) explains in simple words how you will process the personal data of your customers, website visitors, and others.
* **Employee Privacy Notice** ‑ a document that explains how your company is going to process the personal data of your employees (which could include health records, criminal records, etc.).
* **Data Retention Policy** ‑ this document describes the process of deciding how long a particular type of personal data will be kept, and how it will be securely destroyed.
* **Data Retention Schedule** ‑ lists all of your personal data and describes how long each type of data will be kept.
* **Data Subject Consent Form** ‑ this is the most common way to obtain consent from a data subject to process his/her personal data.
* **Parental Consent Form** ‑ if the data subject is below the age of 16 years, then a parent needs to provide the consent for processing personal data.
* **DPIA Register** ‑ this is where you’ll record all the results from your Data Protection Impact Assessment.
* **Supplier Data Processing Agreement** ‑ you need this document to regulate data protection with a processor or any other supplier.
* **Data Breach Response and Notification Procedure** ‑ it describes what to do before, during, and after a data breach.
* **Data Breach Register** ‑ this is a document where you’ll record all of your data breaches.
* **Data Breach Notification Form to the Supervisory Authority** ‑ in case you do have a data breach, you’ll need to notify the Supervisory Authority in a formal way.
* **Data Breach Notification Form to Data Subjects** ‑ in case of a data breach, you need to inform the affected data subjects in a formal way.

In some cases, a company may need additional documents in order to comply with the EU GDPR, like:

* **Data Protection Officer Job Description** ‑ you’ll need to have a Data Protection Officer (DPO) if (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; or (b) the core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities process, on a large scale, special categories of data and personal data relating to criminal convictions and offences.
* **Inventory of Processing Activities** ‑ this document is mandatory if (a) the company has more than 250 employees; or (b) the processing the company carries out is likely to result in a risk to the rights and freedoms of data subjects; or (c) the processing is not occasional; or (d) the processing includes special categories of data; or (e) the processing includes personal data relating to criminal convictions and offences.
* **Standard Contractual Clauses for the Transfer of Personal Data to Controllers** ‑ mandatory if you are transferring personal data to a controller outside the European Economic Area (EEA) and you are relying on model clauses as your lawful grounds for cross-border data transfers.
* **Standard Contractual Clauses for the Transfer of Personal Data to Processors** ‑ mandatory if you are transferring personal data to a processor outside the EEA and you are relying on model clauses as your lawful grounds for cross-border data transfers.