[Your company logo here]

COMPANYNAME FRANCE

**PROJECT PLAN**  
**for Complying with the European General Data Protection Regulation**

|  |  |  |
| --- | --- | --- |
| Document ID  […] | Created by  […] | Date prepared  […] |
| Document version  [,,,] | Reviewed by  […] | Date reviewed  […] |
| Effective date  […] | Approved by  […] | Date approved  […] |

**Document Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reviewed by** | **Revision Description** |
| 0.1 | YYY/MM/DD | [*the name of the person in charge*] | Added a new section |
| 0.2 | YYY/MM/DD | [*the name of the person in charge*] | Changed the user category of the document |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, Scope and Users 3](#_Toc496534071)

[2. Reference Documents 3](#_Toc496534072)

[3. EU GDPR Implementation Project 3](#_Toc496534073)

[3.1. Project Objective 3](#_Toc496534074)

[3.2. Project Results 3](#_Toc496534075)

[3.3. Deadlines 6](#_Toc496534076)

[3.4. Project Organization 6](#_Toc496534077)

[3.4.1. Project Sponsor 7](#_Toc496534078)

[3.4.2. Project Manager 7](#_Toc496534079)

[3.4.3. Project Team 7](#_Toc496534080)

[3.5. Main Project Risks 7](#_Toc496534081)

[3.6. Tools for Project Implementation, Reporting 8](#_Toc496534082)

[4. Managing Records Kept on the Basis of this Document 8](#_Toc496534083)

[5. Validity and document management 8](#_Toc496534084)

# Purpose, Scope and Users

The purpose of this document is to clearly define the objective of the European General Data Protection Regulation (EU GDPR) implementation project, documents to be written, measures to be taken, deadlines, roles and responsibilities in the project.

The Project Plan is applied to all activities performed in the EU GDPR implementation project, as shown in the *EU GDPR Scope* document.

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

# Reference Documents

* 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)
* *Loi Informatique et Libertés du 6 janvier 1978*,as amended by the law n° 2018-493 of 20th June 2018 in order to implement under French Law some specifications of the GDPR
* The security guide of the CNIL (version of July 2018)
* French labor regulations relating to the surveillance of employees and employees right to privacy and article 1121-1 of French Labor Code
* GDPR Assessment Report
* GDPR Scope document

# EU GDPR Implementation Project

## Project Objective

Project objective is to implement a data privacy and protection framework, within the boundaries set in the *EU GDPR SCOPE* document, ensuring that all the applicable requirements set by the EU GDPR 2016/679 and relevant National Laws are met by the 1st of April 2019 at the latest.

## Project Results

In order to solve the non-conformities identified during the assessment performed against the EU GDPR 2016/679 requirements and ensure an efficient project planning and implementation, the Company will use the corrective actions recommended in the *EU GDPR Assessment Report* document. Consequently, there will be taken necessary technical and organization measures to eliminate the identified non-conformities affecting the areas of: employment, recruiting new personnel, third party compliance, regulatory and contractual obligations towards the clients, relation with the Mother Company (COMPANYNAME HQ), incident management and breach notification, security of personal data, accountability.

To ensure the implementation of EU GDPR 2016/679 requirements the Company shall take measures as per recommendations given in the EU GDPR Assessment Report document.

To ensure the implementation of EU GDPR 2016/679 requirements and **to be able to demonstrate compliance**, the Company must create a set of documents related to both data privacy and data security. Some of them have been already created during the assessment phase and the other shall be documented during the implementation phase, as shown below.

During the assessment phase the following documents have been produced:

**PERSONAL DATA IDENTIFICATION AND ANALYSIS**

* **The GDPR Project Scope –** an internal document setting the boundaries of the GDPR project.
* **Personal Data Analysis Form –** a document meant to list the categories of personal data, and the processes managed by the Company with all relevant details.
* **Personal Data Asset Inventory –** a document identifying the main assets such as personal data and the supporting assets such information systems, hardware and software relevant for processing of personal data.
* **Documents related to personal data identification and flow –** Personal Data Flow and Personal Data Mapping, accompanied by their graphical representations as separate documents.
* **The list of Third-Party Processing Providers –** a document identifying the third parties and other recipient to whom the Company is transferring the personal data.

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

**DATA SUBJECT RIGHTS**

**(employees, candidates, clients)**

* **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 Data Protection Policy –** a policyto set out the conditions under which the company processes personal data of its employees;
* **Privacy Notice (also Employee Privacy Notice and Job Applicant Privacy Notice**) **–** a notice to set out the conditions under which the company processes personal data of its clients or any other data subject that might be affected by the processing of personal by the Company;
* **Privacy Policy –** a Policy which is made available to everyone who might be affected by the Company processing the personal data. It describes how the Company is processing the personal data;
* **Register of Privacy Notices** – a document where you need to list and keep track of all the published notices;
* **Legitimate interest assessment form** – a document used to demonstrate and justify the choice of the Company to use legitimate interest as a lawful basis for processing personal data;
* **Data Subject Access Request Procedure** – a document to set up the process by which the Company answers to data subjects requests;
* **Data Subject Access Request Form -** a document enabling the data subject to request access to the its personal data being processed by the Company;

**RELATION WITH COMPANYNAME HQ**

* **Joint Controller Agreement –** this is an agreement that should be signed between the Mother Company and CompanyName France. Its purpose is to share the risks, set the responsibilities and obligations in terms of GDPR compliance.

**THIRD PARTY COMPLIANCE**

* **Processor GDPR Compliance Questionnaire –** a questionnaire meant to assess supplier’s compliance with EU GDPR;
* **Processor Security Controls -** This document describes the information security controls that are in place by an organisation acting as a processor in the context of the 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 SECURITY**

* **IT Security Policy** – describes basic security rules for all employees;
* **Access Control Policy** – defines how the management approves the access rights given to particular users to gain access to information systems;
* **Security Procedures for IT Department** – describes security rules that need to be used for the IT infrastructure;
* **Bring Your Own Device (BYOD) Policy** – describes the rules for using mobile and other non-company devices for business purposes;
* **Teleworking Policy** – describes security rules for using laptops, outside of the company premises;
* **Clear Desk and Clear Screen Policy** – defines how to protect the information that is located in the workplace and on computer screens;
* **Information Classification Policy** – defines how to classify data according to confidentiality, and how to protect the data accordingly;
* **Policy on the Use of Encryption** – defines how to use cryptographic controls and keys to protect the confidentiality and integrity of the data;
* **Data Retention Policy –** a policy to set out the period for which personal data may be kept by the company;
* **Data Destruction Procedure –** this is a document determining which is the practice to destroy the data in a safe way.
* **Data Transfer procedure -** this is a document to ensure the security of information and software when they are exchanged within or outside the organization.
* **Internal Audit Procedure** – defines how to test, assess and evaluate the organizational and technical safeguards in a company;

**INCIDENT MANAGEMENT**

* **Disaster Recovery Plan** – defines how to recover the infrastructure and the data after a disrupting incident;
* **Incident Management Procedure –** this document ensures a quick detection of security events and weaknesses, and quick reaction and response to security incidents;
* **Data Breach Response and Notification Procedure –** a procedure that establishes the Company’s obligations in case of a personal data breach;
* **Data Breach Notification to the Supervisory Authority** – the document to be used in case of a data breach;
* **Data Breach Notification to the Data Subjects**– the document to be used in case of a data breach;
* **Data Breach Register/Incident Log –** a register that keeps track of each security incident

**ACCOUNTABILITY**

* **Checklist to demonstrate GDPR compliance –** this is a list containing all the documents that needs to be produce so that the Company is capable of demonstrating compliance to EU GDPR requirements and by means of this, to respect the principle of accountability required by the said regulation.
* **GDPR Readiness Statement** – a document which is meant to inform that the Company has implemented technical and organizational controls to ensure the EU GDPR compliance. It assures the third parties that the organisation meets the GDPR requirements.

***Note:*** *the list can be adjusted, and some other documents might be generated during the implementation phase.*

## Deadlines

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Action/document** | **Who** | **Deadline** | **Comments** | **Status** |
| Encrypt HDD of laptops and upgrade File server (HW and SW) | IT Manager | dd/mm/yyyy |  | Open |
| Define a retention policy (in written form) for all personal data types | Consulting company | dd/mm/yyyy |  | Open |
|  | TBD | dd/mm/yyyy |  | Open |
|  | TBD | dd/mm/yyyy |  | Open |

The final presentation of the 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 of the progress, and to carry out administrative work related to the project. The project manager's authority should 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* |
|  |  | IT manager |  |  |
|  |  | Financial Manager |  |  |
|  |  | Consultant |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Main Project Risks

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

1. Extension of deadlines
2. Performing activities that incur unnecessary costs and waste time
3. Shortage or lack of competent employees

Measures to reduce the above-mentioned risks are the following:

* The project manager ensures 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
* Contracting a data protection expert to propose the most appropriate activities

## 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 keep updated the project implementation plan 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 […] years |

# Validity and document management

This document is valid as of [date].

Owner of this document is [job title].

[job title]

[name]

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

[signature]