



**Erasmus+ Programme – Strategic Partnership**

**Project Title:** Governance, Risk management and Compliance Essentials

**Project Agreement No.:** 2019-1-CY01-KA202-058375

**Personal Data Protection Implementation Process**

Personal Data Protection Implementation Process



**Permission to Copy:** No part of this document may be copied, reproduced, or modified in whole or in part for any purpose without written permission from the GRCEssentials consortium. In addition to this written permission to copy, reproduce, or modify in whole or part of this document, an acknowledgement of the authors of the document and all applicable sections of the copyright notice must be clearly referenced. All rights reserved.

**Reservation concerning changes:** All information, content, links or other messages may be changed by the authors, at any time without prior notice or explanation. However, all consortium members should be informed.

**Copyright**

© Copyright 2020 GRCEssentials

Project consortium:

Applicant - LP PCX COMPUTERS & INFORMATION SYSTEMS LTD

Partner - P1 L.T. Synergy Ltd

Partner - P2 TOURNIS SYMVOULEFTIKI EE

Partner - P3 EUROPEAN CENTER FOR QUALITY OOD - ECQ

Partner - P4 emcra GmbH

Partner - P5 Budapesti Kereskedelmi és Iprakamara

Partner - P6 EUROCERT S.A.

Contents

[Introduction 5](#_Toc89085491)

[Definitions 6](#_Toc89085492)

[Principles 6](#_Toc89085493)

[Personal Data Protection Implementation Process 7](#_Toc89085494)

[Step 1 – Implementation Process Preparation and Initiation 7](#_Toc89085495)

[Step 2 – Roles and Awareness 8](#_Toc89085496)

[Step 3 – Personal Data Identification and Analysis 8](#_Toc89085497)

[Step 4 – Data Protection Policy and Notices 9](#_Toc89085498)

[Step 5 – Rights of the Data Subject 10](#_Toc89085499)

[Step 6 – Controllers and Processors 10](#_Toc89085500)

[Step 7 – Privacy by Design and Data Protection Impact Assessment 11](#_Toc89085501)

[Step 8 – International Transfers 12](#_Toc89085502)

[Step 9 – Data Breach Management 13](#_Toc89085503)

[Step 10 – Information Security Measures and Policies 14](#_Toc89085504)

[Step 11 – Monitoring and Evaluation and a Life-Cycle approach 15](#_Toc89085505)

[Annex A – Templates 16](#_Toc89085506)

[Personal Data Inventory 16](#_Toc89085507)

[DPO Job Description 16](#_Toc89085508)

[GDPR Training Material 16](#_Toc89085509)

[Data Breach Management 16](#_Toc89085510)

[Personal Data Protection Policy 16](#_Toc89085511)

# Introduction

The purpose of this document is to help “GRCEssentials” target group prepare their organization how to manage compliance with EU Regulation for General Data Protection (GDPR – 679/2016) as well as any other relevant national law or regulation for personal data protection. All organizations must consult with their legal advisors for legal documents such as Privacy Notices, Data Processing Agreements, Disclaimers etc. The current is a guidance that will mainly assist organizations to manage the processing of personal data adopting organizational and technical measures.

In 2016, the European Commission replaced its long-existing Data Protection Directive with a modernized version, the [General Data Protection Regulation (GDPR)](https://securiti.ai/what-is-gdpr/). The GDPR is based on the EU Charter of Fundamental Rights that considers the protection of personal data an individual’s fundamental human right.

The objective of the GDPR is to ensure the protection of personal information through a human rights centric approach and allow secure transfer of personal information within and across jurisdictions. At present, the GDPR is one of the best global practices in relation to data protection and privacy legal landscape.

For organizations to stay in compliance with this regulation and ensure that all personal data is safe, organizations need to have a solid grip on all their customers’ data and be able to map it back to the owners. Traditional methods may make this task virtually impossible and with data collection and processing growing and changing rapidly, organizations will need to incorporate a tool that will help them map their data assets. Doing so can help organizations map back their data to the customer and in turn improve processes.

## Definitions

**Personal Data** – any information related to a natural person or ‘Data Subject’, that can be used to identify the person directly or indirectly

**Sensitive Personal Data**- any 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 shall be prohibited.

**Data Subject** – a natural person whose personal data is processed by a controller or processor

**Processing** – any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

**Data Controller** – the entity that determines the purposes, conditions and means of the processing of personal data

**Data Processor** – the entity that processes data on behalf of the Data Controller

**Consent** – freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data

**Third Country** – any country other than the EU and EEA Member States.

**Personal Data Breach** – a breach of security leading to the accidental or unlawful access to, destruction, misuse, etc. of personal data

## Principles

* **Lawfulness, fairness and transparency**

It requires that personal data are processed in a lawful, fair and transparent manner in relation to data subjects. Essentially, it means that data cannot be processed unless it is needed to process them in order achieve the above-mentioned purposes.

* **Purpose limitation**

Organisations should only collect personal data for a specific purpose, clearly state what that purpose is, and only collect data for as long as necessary to complete that purpose.

Processing that’s done for archiving purposes in the public interest or for scientific, historical or statistical purposes is given more freedom.

* **Data minimisation**

Organisations must only process the personal data that they need to achieve its processing purposes.

* **Accuracy**

The accuracy of personal data is integral to data protection. The GDPR states that “every reasonable step must be taken” to erase or rectify data that is inaccurate or incomplete.

Individuals have the right to request that inaccurate or incomplete data be erased or rectified within 30 days.

* **Storage limitation**

Storage limitation is a form of data standardization, similar to data minimization and accuracy principles. Organizations should perform periodic reviews to identify, and address, data stored beyond intended use. Similarly, organisations need to delete personal data when it’s no longer necessary.

* **Integrity and confidentiality**

This is the only principle that deals explicitly with security. The GDPR states that personal data must be

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. The GDPR is deliberately vague about what measures organisations should take, because technological and organisational best practices are constantly changing. Currently, organisations should encrypt and/or pseudonymise personal data wherever possible, but they should also consider whatever other options are suitable.

# Personal Data Protection Implementation Process

## Step 1 – Implementation Process Preparation and Initiation

Key Tasks:

* Define, plan and initiate a project kick-off meeting
* Plan the implementation project, involve the right persons, allocate the required resources, set the minimum specifications and requirements for the GDPR Project
* Perform a gap analysis assessment to identify key findings and non-conformities

Before starting the GDPR Implementation project, you have to get the support from top management and to be demonstratable by an official support letter. Once you secure management commitment, you have to plan how to achieve GDPR compliance.

At this stage you have to plan the project in defining, planning and tracking the implementation effort. More specifically, roles that will be actively involved, timescales, budget, activities, reporting shall be defined and agreed by the top management.

Following the above, a gap analysis against GDPR (EU 679/2016) and any other local National Law for Data Protection must be performed.

## Step 2 – Roles and Awareness

Key Tasks:

* Raise awareness and inform the stakeholders about GDPR
* Identify the needs for training, provide awareness material and run training sessions
* Identify and define roles and responsibilities

It is important to establish form the beginning who is going to be responsible for the personal data issues. The only role that is explicitly mandated in the GPDR is the role of the Data Protection Officer (DPO). Your company may or may not need to appoint this role. If your organization is a public body, then you will need to have a DPO. To decide if your company needs to appoint a DPO, whether it's a controller or a processor, you should consider if its core activities involve processing of sensitive data on a large scale or involve large scale, regular and systematic monitoring of individuals. In that respect, monitoring the behavior of individuals includes all forms of tracking and profiling on the internet, including for the purposes of behavioral advertising.

The Data Protection Officer (DPO) reports directly to the CEO (most senior level of management), in matters relating to data protection assurance and compliance. Data Protection Officer responsibilities include advising on company’s compliance with GDPR and local data protection laws, monitoring adherence to GDPR standards and acting as a point of contact with supervisory authorities and data subjects. The DPO will also create policies that enforce compliance with legislation and deliver GDPR trainings to company’s staff to increase awareness of data protection measures. To be successful in this role, the DPO should have in-depth knowledge of GDPR and local data protection laws and be familiar with company’s industry and the nature of its data processing activities. The DPO should also know how to perform audits to current procedures.

## Step 3 – Personal Data Identification and Analysis

Key Tasks:

* Discover the personal data that your company process and/or transfer
* Identify the type of personal data, the procedure that your company process it for, and the storage method
* Identify the lawful basis of processing each group of personal data
* Development of a Data Mapping Record

For privacy law compliance, it’s vital to have a clear view of the personal data under your control. This involves understanding what data you hold, what it’s for, where it’s located, where it goes, how long you keep it for and what you do with it once you no longer need it. Done in the right way, data mapping gives you precisely the information you need to create such an understanding. Data mapping has always been good practice for data compliance. However, as we’ll see, the arrival of The General Data Protection Regulation (GDPR) makes it even more of a priority to take data mapping seriously.

Data mapping tracks the flow of data to, through and from your organisation. More specifically, a data map (also known as a data flow) should give you the following information regarding the personal data under your control:

* Where it comes from (e.g. customers, staff and third parties)
* It’s purpose (e.g. order fulfilment or payroll)
* The entry point; i.e. how it enters your company (e.g. a telephone call, email or online form)
* Its format, such as Excel spreadsheet, simple Word doc or CRM customer account page
* Where it’s stored; such as a filing cabinet, in-house server or Cloud database
* The country it’s stored in
* Where it’s accessible from and who has access to it

## Step 4 – Data Protection Policy and Notices

Key Tasks:

* Define your Data Privacy Policy, Data Protection Policy and Data Retention Policy
* Create or update Privacy notice
* Identify the necessity of the consent

The company has to define the overall policy on Data Protection and also on how long you retain personal data for, to ensure compliance with the GDPR. You should also create a procedure to communicate your policies to the data subjects, ensure that they get the information that are required by the Regulation. In this respect all personal data shall be:

* processed lawfully, fairly and in a transparent manner in relation to individuals;
* collected for specified, explicit and legitimate purposes;
* adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
* accurate and, where necessary, kept up to date;
* 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;
* 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.
* only transferred outside the EEA in circumstances where it can be adequately protected;

## Step 5 – Rights of the Data Subject

Key Tasks:

* Define how data subjects request will be handled
* Create new procedures to be able to process them
* Prepare a Data Subjects’ Requests Record

Under the GPDR Regulation, there are eight (8) rights that belong to data subjects, namely: the right to be informed; the right to access; the right to object; the right to erasure and blocking; the right to rectify; the right to file a complaint; the right to damages; and the right to data portability.

The steps of the procedure of handling a data subject request are:

1. Data Subject Request Received: The data subject submits a request via one of several methods, including electronically, by letter or on the telephone. A Data Subject Request Form is available for this purpose
2. Log Data Subject Request: The fact that the request has been received is logged and the date of the request recorded.
3. Confirm identity of data subject: The identity of the data subject is confirmed via an approved method. More information may be requested to confirm identity if required. If the identity of the data subject cannot be confirmed, the request is rejected and the reason for this communicated to the data subject.
4. Compile requested information: The relevant information is compiled according to the type of request. This may involve planning how the requested action, e.g. erasure or restriction of processing, will be achieved. A maximum of one month is permitted; if the request will take longer than that then a maximum of two further months are allowed and the data subject must be informed of the delay and the reasons for it within one month of the request being submitted.
5. Provide Response/ Requested Information: Confirmation of action taken / the information requested is provided to the data subject electronically, if that is the preferred method, or via other means.
6. Close data subject request: The fact that the request has been responded to is logged in the Data Subjects’ Requests Record, together with the date of closure.

## Step 6 – Controllers and Processors

Key Tasks:

* Update your contracts to be GDPR compliant
* Identify your processors and find out how they process and protect personal data
* In case you are a processor, inform the data controller about your GDPR Policy
* Ensure the confidentiality from your employees
* Perform regular audits to ensure that your processors are in line with GDPR

In GDPR the data controller has the most responsibility when it comes to protecting the privacy and rights of the data's subject, such as the user of a website. Simply put, the data controller controls the procedures and purpose of data usage. In short, the data controller will be the one to dictate how and why data is going to be used by the organization. A data controller can process collected data using its own processes. In some instances, however, a data controller needs to work with a third-party or an external service in order to work with the data that has been gathered. Even in this situation, the data controller will not relinquish control of the data to the third-party service. The data controller will remain in control by specifying how the data is going to be used and processed by that external service.

A data processor simply [processes any data](https://www.dataprotection.ie/docs/Are-you-a-Data-Controller/y/43.htm) that the data controller gives them. Following the example above, the data processor is the third-party company that the data controller chose to use and process the data.

The third-party data processor does not own the data that they process nor do they control it. This means that the data processor will not be able to change the purpose and the means in which the data is used. Furthermore, data processors are bound by the instructions given by the data controller.

The GDPR is very specific about the fact that there must be a contract in place between a controller and a processor, and about the terms and conditions that must be included in such a contract. Where your organization acts as a processor for other controllers, you will need to provide information about how your company protects their personal data. You will also need to be able to show that your employees who have access to personal data are bound by a confidentiality agreement.

## Step 7 – Privacy by Design and Data Protection Impact Assessment

Key Tasks:

* Identify the necessity of a DPIA when needed
* Preparation of conducting a Data Protection Impact Assessment (DPIA)
* Implement a DPIA

DPIA is mandatory for any high-risk processing activities related to private data and information. The DPIA process will allow the company to make informed decisions about the acceptability of data protection risks and communicate effectively with the individuals affected.

Not all risks can be eliminated, but a DPIA can allow us to identify and mitigate against data protection risks, plan for the implementation of any solutions to those risks and assess the viability of a personal data processing project at an early stage.

The first step of DPIA conduction is the collection of several information related to the specific process (existing or new) that are required and should be available in order DPIA necessity to be determined as well as the DPIA to be carried out. For each personal data, the organization should identify the supporting assets (on which the personal information relies) that will be used or that are being used. Then, the company shall seek consultation from any of the (internal or external) stakeholders identified or 3rd parties that play an important role in the specific processing activity.

The company as a next step should conduct a risk assessment with the following phases:

1. Phase 1: Risk/ threats identification
2. Phase 2; Evaluation
3. Phase 3: Risk Treatment and Management

The final report is submitted to Top Management for approval. The approved report is used to inform on the outcome of the DPIA to the stakeholders, on a need-to-know basis. An updated version of a registry of DPIA reports is maintained, as well as all versions of the DPIAs conducted.

## Step 8 – International Transfers

Key Tasks:

* Discover if you transfer data internationally
* Identify in which country you transfer your data
* Implementation of safeguard measures

Besides protecting personal data within your own company, you also need to think where else you send it to, and how well it is protected in an international environment. In fact, the EU GDPR allows personal data transfers to a third country only if a set of conditions are fulfilled. These include also the conditions for onward transfer (transferring personal data from a processor outside of EU/EEA to another sub-processor based outside of EU/EEA). The first step to ensure compliance with the above statement is to know what data you send, where and why. There are 4 mechanisms used to lawfully transfer personal data of EU individuals outside of the EU/EEA:

The EU GDPR allows personal data transfers to a third country only if a set of conditions are fulfilled. These include also the conditions for onward transfer (transferring personal data from a processor outside of EU/EEA to another sub-processor based outside of EU/EEA).

There are 4 mechanisms used to lawfully transfer personal data of EU individuals outside of the EU/EEA:

1. Adequacy Decision - The EU GDPR allows for personal data transfers to countries whose legal regime is deemed by the European Commission to provide for an “adequate” level of personal data protection. The European Commission has so far recognized Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, United States of America[[1]](#footnote-2) (limited to the Privacy Shield framework) as providing adequate protection.
2. Binding Corporate Rules (BCRs) - an intracompany code of conduct applies to a group of companies and should be submitted to Greek Supervisory Authority for approval. These Rules can cover those cases where a company established in the EU/EEA transfers data to another company within the Group based in a 3rd Country.
3. Model Contractual Clauses (Model Clauses) - In the absence of a decision pursuant to Adequacy Decision, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards. The appropriate safeguards referred may be provided for, without requiring any specific authorisation from a supervisory authority, by standard data protection clauses adopted by the Commission in accordance with the examination procedure (Annex1, Annex2).
4. In the absence of an adequacy decision or of appropriate safeguards, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

* the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
* the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
* the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
* the transfer is necessary for important reasons of public interest
* the transfer is necessary for the establishment, exercise or defence of legal claims
* the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent

## Step 9 – Data Breach Management

Key Tasks:

* Verify if a personal data breach has occurred
* Conduct a personal data breach risk assessment
* Notify affected individuals (if required) and provision of suggested measures to protect themselves
* Documentation of all data breaches and maintenance of a Data Breach Record

After first being informed of a potential breach by an individual, a media organization, or another source, the company shall undertake a short period of investigation to establish whether or not a personal data breach has in fact occurred. Once the breach report is completed, the company performs a Risk Assessment. When the personal data breach is likely to result in a risk (**Medium-Low risks & Medium-High risks)** to the rights and freedoms of natural persons as assessed in the step above the Company when acts as a Controller shall not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.

The responsible team of the company shall at minimum collect the information below in order to notify the Supervisory Authority:

1. description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
3. description of the likely consequences of the personal data breach;
4. description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

When the personal data breach is likely to result in high risk (**High Risks**) the Company shall inform all individuals whose personal data have been compromised.

The information provided to individuals shall at least include the following:

1. a description of the nature of the breach;
2. the name and contact details of the data protection officer or other contact point;
3. a description of the likely consequences of the breach;
4. a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

The communication channel that will be selected is dependent on the nature of the relation between the Company and the Individuals. Indicatively the Company may use Email notification, Telephone calls and SMS.

The Company needs to ensure that the communication is accessible in appropriate alternative formats and relevant languages to ensure individuals are able to understand the information being provided to them. For example, communication in the native language of the recipient will help to ensure their understanding of the nature of the breach and steps they can take to protect themselves.

## Step 10 – Information Security Measures and Policies

Key Tasks:

* Identify the areas in which you need to create Information Security Policies and Procedures
* Preparation and Approval of the policies
* Communication of the roles and responsibilities to staff
* Company’s Compliance with the policies and procedures

In this step, it is important to start strengthening the controls that your company have in place to protect the personal data. By implementing Information security policies and procedures, you may need to ensure that all required controls are based on risk, objectives are clearly defined, and all the documents will be improved as a lifecycle process. By implementing the principles of ISO 27001 Standard, you will ensure that you process personal data in a safe way.

## Step 11 – Monitoring and Evaluation and a Life-Cycle approach

Key Tasks:

* Monitoring and Evaluation of the Data Protection Management System
* Internal Audit
* Management Review
* Improvement

When you complete all the above steps (Step 1 – Step 10) you have to determine what need to be monitored and evaluated as well as the method that you will adopt to do so. Your company should be able to understand and analyze the results from the monitoring and evaluation.

To this extent, the company should conduct internal audits on the management system the company has in place on a regular predefined basis for assessing:

1. If the company complies with GDPR and other national laws
2. If management system performs according to planned goals

The company’s management should review the performance of the data protection management system at planned intervals to ensure its effectiveness. Top Management should check at least the following:

* nonconformities and corrective actions from gap analysis report
* monitoring and evaluation results
* audit results
* risks that have been identified (Step 3 and 7)
* review of policies, procedures and records
* security breaches and/or incidents
* complaints handling

Your company should focus its effort on continually improving the effectiveness shall continually improve the suitability, adequacy and effectiveness of the PIMS.

through the audit results, preventive and corrective actions and management review.

Complaints, security breaches, subject access requests, technological advances and other issues shall

be used as an aid to improve the effectiveness of the PIMS.

# Annex A – Templates

## Personal Data Inventory



## DPO Job Description



## GDPR Training Material



## Data Breach Management



## Personal Data Protection Policy



1. The Adequacy Decision may not be anymore in force. Contractual Clauses might be required. [↑](#footnote-ref-2)