

EU GDPR Toolkit	
Level 1 – Objectives and Policies	
Objectives	
1.	GDPR Roles and Responsibilities
Policies	
1.	Records Retention and Protection Policy
2.	Data Protection Policy
3.	Website Privacy Policy
4.	CCTV Policy
5.	GDPR Controller - Processor Agreement Policy
6.	Information Security Policy
7.	Mobile Device Policy
8.	Access Control Policy
9.	Cryptographic Policy
10.	Physical Security Policy
11.	Anti-Malware Policy
12.	Network Security Policy
13.	Electronic Messaging Policy
14.	Cloud Computing Policy
15.	Acceptable Use Policy
16.	HR Security Policy
17.	Social Media Policy
Level 2 - Procedures	
1.	GDPR Competence Development Procedure
2.	Personal Data Analysis Procedure
3.	Legitimate Interest Assessment Procedure
4.	Privacy Notice Procedure
5.	Data Subject Request Procedure
6.	Processor GDPR Assessment Procedure
7.	International Transfers of Personal Data Procedure
8.	Information Security Incident Response Procedure
9.	Personal Data Breach Notification Procedure
Level 3 – SOPs	
1.	Group Internal and E-mail Usage

2.	Software Configuration Management
3.	Handling of Virus Attacks
4.	Personal Security
5.	Warehouse Security
Level 4 – Formats, Templates & Presentations	
Formats	
1.	Compliance Evidence
2.	Meeting Minutes Template
3.	GDPR Competence Development Questionnaire
4.	Records of Processing Activities
5.	Personal Data Analysis Form
6.	Personal Data - Initial Questionnaire
7.	Legitimate Interest Assessment Form
8.	Privacy Notice Planning Form - Data Subjects
9.	Consent Request Form
10.	Privacy Notice Planning Form - Other Source
11.	Data Subject Request Form
12.	Data Subject Request Rejection
13.	Data Subject Request Charge
14.	Data Subject Request Time Extension
15.	GDPR Contract Review Tool
16.	Processor GDPR Assessment
17.	Processor Employee Confidentiality Agreement
18.	Data Processing Agreement
19.	Sub-Processor Agreement
20.	Data Protection Impact Assessment Tool
21.	Data Protection Impact Assessment Questionnaire
22.	Personal Data Breach Notification Form
23.	Breach Notification Letter to Data Subjects
24.	Information Security Incident Report
Templates	
1.	GDPR Documentation Log
2.	GDPR Communication Programme
3.	Data Subject Request Register

4.	Processor Security Controls
5.	GDPR Letter to Processors
6.	Data Protection Impact Assessment Process
7.	Data Protection Impact Assessment Report
8.	Personal Data Breach Register
9.	Incident Response Plan Data Breach
Presentations	
1.	Introduction to GDPR Presentation
2.	GDPR Awareness Training Presentation
3.	Information Security Awareness Training Presentation
Guidelines for Implementation Methodology	
1.	Guidelines for GDPR Implementation
2.	GDPR All-In-One Toolkit User Guide
3.	GDPR Toolkit Index
4.	GDPR Project Initiation Document
5.	GDPR Implementation Project Plan
6.	GDPR Readiness Statement
7.	GDPR Gap Assessment Tool
8.	GDPR Readiness Checklist
Guidelines for European Data Protection Board	
1.	EDPB Guidelines on Data Portability 5 Apr 2017
2.	EDPB Guidelines on Data Protection Officers 5 Apr 2017
3.	EDPB Guidelines on Lead Supervisory Authority 5 Apr 2017
4.	EDPB Guidelines on DPIA 4 Oct 2017
5.	EDPB Guidelines on Breach Notification 6 Feb 2018
6.	EDPB Guidelines on Profiling 6 Feb 2018
7.	EDPB Guidelines on Transparency 11 Apr 2018
8.	EDPB Guidelines on Online Services 8 Oct 2019
9.	EDPB Guidelines on Contractual Lawful Basis 8 Oct 2019
10.	EDPB Guidelines on Territorial Scope 12 Nov 2019
11.	EDPB Guidelines on Use of Video Devices 29 Jan 2020
12.	EDPB Guidelines on Contact Tracing for COVID-19 21 Apr 2020
13.	EDPB Guidelines on Consent 4 May 2020
14.	EDPB FAQs on the Schrems II Judgement 23 Jul 2020

15.

EDPB Guidelines on Data Protection by Design and by Default 20 Oct 2020

Contents

1	Introduction.....	4
2	Privacy Notice Procedure	4
2.1	Has the Data Subject Already Been Provided with the Information?.....	5
2.2	When Personal Data is Obtained from the Data Subject	5
2.3	When Personal Data is Not Obtained from Data Subject.....	6
2.4	Informing the Data Subject.....	7
2.5	Further Processing.....	8

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

Introduction

The purpose of this procedure is to be applied whenever a new or modified business process is implemented, necessitating the collection of personal data from data subjects falling under the scope of the European Union General Data Protection Regulation (GDPR).

The GDPR, particularly in articles 13 and 14, mandates the provision of specific information to data subjects at the point of data collection or receipt. This information should cover the purpose of data usage and the rights the data subjects have over their data. As these requirements may vary based on specific circumstances, this procedure is designed to ensure that accurate information is provided in the appropriate format, thereby maintaining Organization Name's GDPR compliance at all times.

Privacy Notice Procedure

This procedure aims to develop a suitable privacy notice that offers data subjects the necessary information they are entitled to receive in a fair and transparent manner.

Under the scope of the GDPR, there are two primary methods of obtaining personal data:

1. When personal data is collected directly from the data subject (GDPR Article 13).
2. When personal data is acquired without direct involvement from the data subject (GDPR Article 14).

Has the Data Subject Already Been Provided with the Information?

As per the GDPR, the listed information must be provided to the data subject unless they already possess it. Hence, it is crucial to ascertain whether it is reasonable to assume that the data subject is already aware of all the information that would typically be required to be provided.

When Personal Data is Obtained from the Data Subject

In case the data subject lacks the necessary information, the following details must be furnished at the time of collecting personal data:

1. Identity and contact information of the controller, and if applicable, the controller's representative.
2. The individuals or groups who receive the data, or the categories of recipients, if applicable.

Contents

1	Introduction.....	4
2	Processor GDPR Assessment Procedure	4
2.1	Prerequisites	4
2.2	Timing and Scheduling.....	4
2.3	Procedure.....	4

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Introduction

Organization Name understands the vital importance of utilizing suitable, secure, and efficient processors to ensure compliance with the General Data Protection Regulation (GDPR). These processors not only facilitate the smooth functioning of the company but also directly deliver services to customers, as seen in web hosting and similar cases. Moreover, the contributions of other suppliers significantly impact Organization Name's success in achieving its objectives, particularly in terms of attracting an ample number of visitors to its website.

However, processors are not only expected to provide high-quality products and services but also to do so securely, safeguarding both Organization Name and its customers' personal data from any potential risks. This procedure aims to ensure that necessary measures are taken and thorough research is conducted to make a fair assessment of whether a processor is fulfilling its GDPR obligations satisfactorily.

2 Processor GDPR Assessment Procedure

2.1 Prerequisites

Prior to commencing the procedure, the following prerequisites must be fulfilled:

- Clearly defined requirements for the product or service.
- Confirmation that the processor is currently or will be handling the storage and processing of personal data belonging to our customers, employees, or other stakeholders.

2.2 Timing and Scheduling

This procedure is flexible and can be initiated at any time, though it holds particular relevance during personal data mapping exercises.

2.3 Procedure

Ensure that the Processor GDPR Assessment is documented using the provided form and kept as evidence of the assessment.

Regular monitoring of assessment progress is essential and should occur at least on a weekly basis during the ongoing process, although many assessments may be completed within a shorter timeframe.

Contents

1	Introduction.....	4
2	Business Requirements of Access Control	5
3	User Access Management.....	6
3.1	User Registration and Deregistration.....	6
3.2	User Access Provisioning	7
3.3	Removal or Adjustment of Access Rights.....	7
3.4	Management of Privileged Access Rights	7
3.5	User Authentication for External Connections	8
3.6	Supplier Remote Access to the Organization Network.....	8
3.7	Review of User Access Rights.....	9
3.8	User Authentication and Password Policy.....	9
4	User Responsibilities	10
5	System and Application Access Control	11

DOCUMENT NO:	
REVISION NO:	
DATE OF REVISION:	
PREPARED BY:	
REVIEWED BY:	
APPROVED BY:	
SIGNATURE:	

1 Introduction

Safeguarding access to our information assets is a fundamental component of our defense in- depth approach to information security. Ensuring the protection of classified data's confidentiality, integrity, and availability requires the implementation of a comprehensive array of both physical and logical controls.

These requirements can vary based on several factors, including:

- Applicable legislation, such as the GDPR or Sarbanes Oxley.
- The potential threats, vulnerabilities, and associated risks.

2 Business Requirements of Access Control

As part of the requirements-gathering stage for new or substantially changed systems and services, it is essential to establish business requirements for access control. These requirements should be thoroughly incorporated into the resulting design.

Besides the specific requirements, several general principles will guide the design of access controls for Organization Name's systems and services. These principles are as follows:

- **Defense in Depth:** Security measures should not rely solely on a single control but rather integrate a combination of complementary controls for enhanced protection.
- **Least Privilege:** The default approach should be based on the assumption that access is not necessary unless proven otherwise, ensuring minimal access rights to maintain security.
- **Need to Know:** Access will be granted solely to the information required for performing a specific role, avoiding unnecessary disclosure of sensitive data.
- **Need to Use:** Users will have access only to the physical and logical facilities essential for their designated roles, preventing unauthorized entry.

3 User Access Management

Comprehensive user access control procedures must be documented, implemented, and regularly updated for each application and information system. These procedures aim to ensure authorized user access while preventing unauthorized access. They should encompass all stages of the user access lifecycle, starting from the initial registration of new users to the final de- registration of users who no longer require access.

INFORMATION SECURITY INCIDENT REPORT	
Incident Identification Information	
Incident Detector's Information:	
Name:	Date/Time Detected:
Title:	Location:
Phone/Contact No:	System/Application:

Incident Summary			
Type of Incident Detected:			
☐	Denial of Service	☐	Malware/Ransom Ware
☐	Loss / Theft	☐	Unauthorized Access
☐	Inadvertent Site Security	☐	Phishing
☐		☐	Unauthorized Use/Disclosure
☐		☐	Unplanned Downtime
☐		☐	Other

Description of Incident:

Names of Others Involved:	
1.	2.
3.	4.

Incident Notification	
☐	IS Leadership
☐	System / Application Owner
☐	Public Affairs
☐	Administration
☐	Security Incident Response Team
☐	System / Application Vendor
☐	Legal Counsel
☐	Human Resources

Actions (Include Start & Stop Times)
(Phase I) Identification Measures (Incident Verified, Assessed, Options Evaluated):
(Phase II) Containment Measures:
Evidence Collected (Systems Logs, etc.):
(Phase III) Eradication Measures:
(Phase IV) Recovery Measures

Evaluation
How Well Did the Workforce Members Respond?
Were the Documented Procedures Followed? Were They Adequate?
What Information Was Needed Sooner?

Were Any Steps or Actions Taken That Might Have Inhibited the Recovery?
What Could the Workforce Members Do Differently the Next Time an Incident Occurs?
What Corrective Actions Can Prevent Similar Incidents in the Future?
What Additional Resources Are Needed to Detect, Analyze, and Mitigate Future Incidents?
Other Conclusions/Recommendations:

Follow-Up			
Review By (Organization to Determine):			
☐	Security Official	☐	IS Department / Team
☐			Other
Recommended Actions Carried Out:			
Initial Report Completed By:		Follow-Up Completed By:	