EUGDPR Academy

Checklist of Mandatory Documentation Required by EU GDPR

Advisera
Making certification simple.

Table of Contents

1. Introduction 3
2. Required documents and records 3
3. Commonly used non-mandatory documents 4
4. Description of the required documents and records 5
5. Sample documents 8

1. Introduction

The purpose of this document is to get an overview of the documents required by the EU GDPR, as well as the reasoning behind the documents marked as mandatory. Once you go through this document, you should be able to get a good idea of the documents and records that are needed to be able to achieve compliance with the EU GDPR.

2. Required documents and records

The table below shows the minimum set of documents and records required by the EU GDPR:

Documents	Relevant EU GDPR article
Personal Data Protection Policy	Article 24(2)
Privacy Notice	Articles 12, 13 and 14
Employee Privacy Notice	Articles 12, 13 and 14
Website Privacy Policy	Articles 12 and 13
Data Retention Policy	Articles 5(1)(e), 13(1), 17, 30
Data Retention Schedule	Article 30
Data Protection Officer Job Description*	Articles 37, 38, 39
Cookie Policy	Articles 12 and 13
Inventory of Processing Activities**	Article 30
Data Subject Consent Form	Articles 6(1)(a), 7(1), 9(2)
Data Subject Consent Withdrawal Form	Article 7(3)
Parental Consent Form	Article 8
Parental Consent Withdrawal Form	Article 8
DPIA Register	Article 35
Standard Contractual Clauses for the Transfer of Personal Data to Controllers	Article 46(5)
Standard Contractual Clauses for the Transfer of Personal Data to Processors	Article 46(5)
Supplier Data Processing Agreement	Articles 28, 32, 82
Data Breach Response and Notification Procedure	Articles 4(12), 33, 34
Data Breach Register	Article 33(5)
Data Breach Notification Form to the Supervisory Authority	Article 33
Data Breach Notification Form to Data Subjects	Article 34

*It is compulsory to appoint a Data Protection Officer 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 of the legal entity consist of processing operations which, by their nature, their scope, and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the legal entity consist of processing, on a large scale, special categories of data pursuant to Article 9 of the EU GDPR and personal data relating to criminal convictions and offences referred to in Article 10 of the EU GDPR.

**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 (personal 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); or (e) the processing includes personal data relating to criminal convictions and offences.

3. Commonly used non-mandatory documents

Other documents may be used by an organisation to help with their EU GDPR compliance; you can find the list below:

Documents	Relevant EU GDPR article
EU GDPR Readiness Assessment	N/A
Project Plan for Complying with the EU GDPR	N/A
Employee Personal Data Protection Policy	Article 24(2)
Register of Privacy Notices	Articles 12, 13 and 14
Website Terms & Conditions	
Guidelines for Data Inventory and Processing Activities Mapping	Article 30
Data Subject Access Request Procedure	Articles 7(3), 15, 16, 17, 18, 20, 21, 22
Data Subject Access Request Form	Article 15
Data Subject Disclosure Form	Article 15
Data Protection Impact Assessment Methodology	Article 35
Cross Border Personal Data Transfer Procedure	Articles 1(3), 44, 45, 46, 47, 49
Processor GDPR Compliance Questionnaire	Article 46(5)
IT Security Policy	Article 32
Access Control Policy	Article 32
Security Procedures for IT Department	Article 32

Documents	Relevant EU GDPR article
Bring Your Own Device (BYOD) Policy	Article 32
Mobile Device and Teleworking Policy	Article 32
Clear Desk and Clear Screen Policy	Article 32
Information Classification Policy	Article 32
Anonymization and Pseudonymization Policy	Article 32
Policy on the Use of Encryption	Article 32
Disaster Recovery Plan	Article 32
Internal Audit Procedure	Article 32
ISO 27001 Internal Audit Checklist	Article 32

4. Description of the required documents and records

Personal Data Protection Policy

Your company management, customers, and employees do not need to know the details of your EU GDPR compliance program, but they need to know what to expect from it – this is the purpose of the Personal Data Protection Policy.

This is usually a high-level policy document that is meant to prove accountability and commitment from the company with regards to the EU GDPR provisions**.**

Read more here: Contents of the Data Protection Policy according to GDPR.

Privacy Notice

This is your main tool for providing the necessary information to the data subjects. In most cases, a Privacy Notice must be supplied to the individual at the time they provide you with their personal data**.**

This document is meant to be a general template to be considered whenever you need to draft a Privacy Notice.

Learn more here: Privacy Notices under the EU GDPR [free webinar on demand].

Employee Privacy Notice

This document serves a similar purpose to that of the Personal Data Protection Policy, but is directed towards the employees. Therefore, you need to make it available to your employees. You can either publish it on your intranet or send it via email to all your employees.

This document should be quite broad to address all the processing activities related to employment.

Learn more here: Privacy Notices under the EU GDPR [free webinar on demand].

Website Privacy Policy

This policy serves the same purpose as the Privacy Notice, but it is directed towards the data usually processed by website owners. This should be accurate and describe the processing activities undertaken when your website is visited, or when your website is used as a platform to provide goods or services.

Data Retention Policy

This is usually a high-level policy document meant to set the basic rules when it comes to the retention of personal data. Only some high-level criteria need to be mentioned in this document. Because it is meant to be used exclusively within the company, it only needs to be published internally.

Data Retention Schedule

This is usually not a stand-alone document, but one that is meant to be an annex to the Data Retention Policy. This document needs to be quite detailed and accurate, as it sets up the retention periods for all the personal data held by the company.

Data Protection Officer Job Description

If you are required to have a DPO, or if you wish to appoint one, you will need to have some specific tasks assigned. The Task Description or Job Description is the document establishing the duties of the DPO.

Read more here: The role of the DPO in light of the General Data Protection Regulation.

Cookie Policy

Like a Website Policy, the Cookie Policy is meant to provide website visitors with information about the cookies that are placed on their browsers. This is required under the transparency obligation set out in the EU GDPR, as well as according to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive).

This should be quite specific, considering the cookies used and the purpose for which the cookies are used.

Inventory of Processing Activities

If you are among the entities that need to keep such records, you must know that they need to be quite accurate and always up to date. Most likely, this would be among the first documents required of you if you were to find yourself facing a Supervisory Authority.

This document should be able to provide an overview of your company's processing activities.

Data Subject Consent Form

If you rely on consent as a lawful basis for processing, you must know that consent needs to be a freely given, specific, informed, and unambiguous indication of the individual's wishes. The controller must keep records so that it can demonstrate that consent has been given by the relevant individual; this is why the forms need to be kept.

Read more here: Is consent needed? Six legal bases to process data according to GDPR.

Learn more here: How to handle consents under GDPR [free webinar on demand].

Data Subject Consent Withdrawal Form

The data subjects need to be able to withdraw their consent at any time and must be notified of that right prior to giving consent via a privacy notice. It should be as easy to withdraw consent as it is to give it. Therefore, the consent withdrawal form should be simple and accessible.

Learn more here: Four main questions for obtaining and managing data subjects' consent under GDPR.

Parental Consent Form & Parental Consent Withdrawal Form

These two documents serve the same purposes as the Data Subject Consent Form and Data Subject Consent Withdrawal Form, but they are aimed at underaged data subjects who cannot consent for themselves and need to be represented by either their parents or legal guardians.

DPIA Register

Performing Data Protection Impact Assessment is a new requirement of the EU GDPR that only needs to be considered for some specific processing activities, namely those activities that might have a significant impact on the rights and freedoms of data subjects.

DPIAs should be carried out for the processing activities where you are the controller.

Learn more here: Seven steps of Data Protection Impact Assessment (DPIA) according to EU GDPR [free webinar on demand].

Read more here: 5 phases of the EU GDPR Data Protection Impact Assessment.

Standard Contractual Clauses for the Transfer of Personal Data to Controllers & Standard Contractual Clauses for the Transfer of Personal Data to Processors

The EU GDPR bans transfers outside the EEA unless specific safeguards are in place. One such safeguard – and the most popular among companies – is the use of Standard Contractual Clauses. These documents are issued by the EU Commission, and the only thing that must be done is to fill them in. Be aware that the content of the document must not be altered (except, of course, for filling it in).

Learn more here: How to make personal data transfers to other countries compliant with GDPR [free webinar on demand].

Supplier Data Processing Agreement

The EU GDPR requires that controllers only use processors that are providing sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the EU GDPR.

The Supplier Data Processing Agreement is meant to ensure that the controllers and processors have binding rules in place (consistent with EU GDPR Article 28 – Processor) to regulate the way data is being processed by the processor on behalf of the controller.

Data Breach Response and Notification Procedure

Controllers and processors alike would need a centralised way to deal with personal data breaches, and this is achieved by having a documented process for how to handle data breaches to ensure that they meet the new notification requirements of the EU GDPR.

This document would also be used as proof when audited by a Supervisory Authority.

Learn more here: A How-to Guide for GDPR Data Breach Notifications [free webinar on demand].

Data Breach Register

All personal data breaches need to be recoded, even those that do not fall under the notification requirements set up by the EU GDPR. Therefore, it is essential to keep the Data Breach Register updated and to present it to the Supervisory Authorities when requested to do so.

Data Breach Notification Form to the Supervisory Authority & Data Breach Notification Form to Data Subjects

One of the new requirements of the EU GDPR is to notify the Supervisory Authority of any data breaches and, sometimes, to notify the affected data subjects. Controllers must report data breaches to their Supervisory Authority (unless the breach is unlikely to be a risk for the affected data subjects). The data subjects need to be notified if there is a high risk with regard to their rights and freedoms.

Both notifications need to include some specific information mandated by the EU GDPR.

Learn more here: A How-to Guide for GDPR Data Breach Notifications [free webinar on demand].

Read more here: Assessing the severity of personal data breaches according to GDPR.

5. Sample documents

Here you can download a free preview of the EU GDPR Documentation Toolkit – in this free preview, you will be able to see the Table of Contents of each of the mentioned policies and procedures, as well as a few sections from each document.

EUGDPR Academy
EU GDPR Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com

EXPLORE **ADVISERA**

9001 Academy · 9100 Academy · 13485 Academy · 14001 Academy · 16949 Academy · 45001 Academy

20000 Academy · 27001 Academy · EUGDPR Academy · Conformio · eTraining · AdviseraBooks

Advisera
Making certification simple.