EU GDPR Documentation Toolkit

https://advisera.com/eugdpracademy/eu-gdpr-documentation-toolkit/

Note: The documentation should ideally be implemented in the order in which it is listed here.

No.	Document code	Document name	Relevant articles in EU GDPR	Mandatory according to EU GDPR
	1	**Preparations for the Project**		
1	1.1	EU GDPR Readiness Assessment		
2	1.2	Project Plan for Complying with the EU GDPR		
	2	**Personal Data Policy Framework**		
3	2.1	Personal Data Protection Policy	Article 24(2)	✓
4	2.2	Data Retention Policy	Articles 5(1)(e), 13(1), 17, 30	✓
5	2.3	Appendix – Data Retention Schedule	Article 30	✓
	3	**Privacy Notices**		
6	3.1	Privacy Notice	Articles 12, 13, 14	✓
7	3.2	Register of Privacy Notices	Articles 12, 13, 14	
	4	**Mapping of Processing Activities**		
8	4.1	Guidelines for Data Inventory and Processing Activities Mapping	Article 30	
9	4.2	Appendix – Inventory of Processing Activities	Article 30	✓*
	5	**Managing Data Subject Rights**		
10	5.1	Data Subject Consent Form	Articles 6(1)(a), 7(1), 9(2)	✓
11	5.2	Data Subject Consent Withdrawal Form	Article 7(3)	
12	5.3	Parental Consent Form	Article 8	✓
13	5.4	Parental Consent Withdrawal Form	Article 8	✓
	6	**Data Protection Impact Assessment**		
14	6.1	Data Protection Impact Assessment Methodology	Article 35	
15	6.2	DPIA Register	Article 35	✓
	7	**Personal Data Transfers**		
16	7.1	Cross Border Personal Data Transfer Procedure	Articles 1(3), 44, 45, 46, 47, 49	

No.	Document code	Document name	Relevant articles in EU GDPR	Mandatory according to EU GDPR
17	7.2	Annex 1 – Standard Contractual Clauses for the Transfer of Personal Data to Controllers	Article 46(5)	✓**
18	7.3	Annex 2 – Standard Contractual Clauses for the Transfer of Personal Data to Processors	Article 46(5)	✓***
19	7.4	Agreement for the Appointment of an EU Representative	Article 27	✓****
	8	**Third Party Compliance**		
20	8.1	Supplier Data Processing Agreement ver A	Articles 28, 32, 82	✓
21	8.2	Supplier Data Processing Agreement ver B	Articles 28, 32, 82	✓
	9	**Security of Personal Data**		
22	9.1	IT Security Policy	Article 32	
23	9.2	Access Control Policy	Article 32	
24	9.3	Security Procedures for IT Department	Article 32	
25	9.4	Bring Your Own Device (BYOD) Policy	Article 32	
26	9.5	Mobile Device and Teleworking Policy	Article 32	
27	9.6	Clear Desk and Clear Screen Policy	Article 32	
28	9.7	Information Classification Policy	Article 32	
29	9.8	Anonymization and Pseudonymization Policy	Article 32	
30	9.9	Policy on the Use of Encryption	Article 32	
31	9.10	Disaster Recovery Plan	Article 32	
32	9.11	Internal Audit Procedure	Article 32	
33	9.12	Appendix – ISO 27001 Internal Audit Checklist	Article 32	
	10	**Personal Data Breaches**		
34	10.1	Data Breach Response and Notification Procedure	Articles 4(12), 33, 34	✓
35	10.2	Data Breach Register	Article 33(5)	✓
36	10.3	Data Breach Notification Form to the Supervisory Authority	Article 33	✓
37	10.4	Data Breach Notification Form to Data Subjects	Article 34	✓

* 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.

** This document is 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.

*** This document is mandatory if you are transferring personal data to a *Processor* outside the European Economic Area (EEA) and you are relying on Model Clauses as your lawful grounds for cross border data transfers.

**** This document is mandatory for controllers that are not established in the European Union.