

EU GDPR Premium Documentation Toolkit

<https://advisera.com/eugdpracademy/eu-gdpr-premium-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	01.1	EU GDPR Readiness Assessment		
2	01.2	Project Plan for Complying with the EU GDPR		
	2	Personal Data Policy Framework		
3	02.1	Personal Data Protection Policy	Article 24(2)	✓
4	02.2	Employee Personal Data Protection Policy	Article 24(2)	
5	02.3	Data Retention Policy	Articles 5(1)(e), 13(1), 17, 30	✓
6	02.4	Appendix – Data Retention Schedule	Article 30	✓
	3	Privacy Notices		
7	03.1	Privacy Notice	Articles 12, 13, 14	✓
8	03.2	Employee Privacy Notice	Articles 12, 13, 14	✓
9	03.3	Supplier Employee Privacy Notice	Articles 12, 13, 14	✓
10	03.4	Register of Privacy Notices	Articles 12, 13, 14	
	4	Data Protection Officer		
11	04.1	Data Protection Officer Job Description	Articles 37, 38, 39	✓ *
12	04.2	Data Protection Officer Appointment Letter	Articles 37, 38, 39	
13	04.3	Data Protection Officer Terms of Appointment	Articles 37, 38, 39	
	5	Website Documents		
14	05.1	Website Privacy Policy	Articles 12, 13	✓
15	05.2	Website Terms & Conditions		
16	05.3	Cookie Policy	Articles 12, 13	✓
	6	Mapping of Processing Activities		
17	06.1	Guidelines for Data Inventory and Processing Activities Mapping	Article 30	

No.	Document code	Document name	Relevant articles in EU GDPR	Mandatory according to EU GDPR
18	06.2	Appendix – Inventory of Processing Activities	Article 30	✓ **
	7	Managing Data Subject Rights		
19	07.1	Data Subject Consent Form	Articles 6(1)(a), 7(1), 9(2)	✓
20	07.2	Data Subject Consent Withdrawal Form	Article 7(3)	
21	07.3	Parental Consent Form	Article 8	✓
22	07.4	Parental Consent Withdrawal Form	Article 8	✓
23	07.5	Data Subject Access Request Procedure	Articles 7(3), 15, 16, 17, 18, 20, 21, 22	
24	07.6	Data Subject Access Request Form	Article 15	
25	07.7	Data Subject Disclosure Form	Article 15	
26	07.8	Request for Confirmation of Authority		✓ ***
27	07.9	Confirmation of Data Subject Access Request	Article 15	✓
28	07.10	Confirmation of Data Subject Rights Request	Article 15	✓
29	07.11	Rejection of Unfounded/Excessive Request	Article 12(5)	✓
30	07.12	Confirmation for Closed DSAR	Article 15	✓
31	07.13	Response to Data Subject Access Request	Article 15	✓
32	07.14	Cover Letter to Portability Response	Article 20	✓
33	07.15	Response to Rectification of Data Request	Article 16	✓
34	07.16	Response on Consent Withdrawal/Restriction Request (Rejected)	Article 7(3)	✓
35	07.17	Response on Consent Withdrawal/Restriction Request (Accepted)	Article 7(3)	✓
36	07.18	Response on Processing Restriction Request/Complaint (Rejected)	Article 18	✓
37	07.19	Response on Processing Restriction Request/Complaint (Accepted)	Article 18	✓
38	07.20	Response on Auto Decision Making/Restriction on Processing (Rejected)	Article 22	✓
39	07.21	Response on Auto Decision Making/Restriction on Processing (Accepted)	Article 22	✓
40	07.22	Request Closing Letter		
41	07.23	Confirmation for Erasure of Data	Article 17	✓

42	07.24	Data Subject Requests Communication Register		
	8	Data Protection Impact Assessment		
43	08.1	Data Protection Impact Assessment Methodology	Article 35	
44	08.2	DPIA Register	Article 35	✓
	9	Personal Data Transfers		
45	09.1	Cross Border Personal Data Transfer Procedure	Articles 1(3), 44, 45, 46, 47, 49	
46	09.2	Annex 1 – Standard Contractual Clauses for the Transfer of Personal Data to Controllers	Article 46(5)	✓ ****
47	09.3	Annex 2 – Standard Contractual Clauses for the Transfer of Personal Data to Processors	Article 46(5)	✓ *****
48	09.4	Agreement for the Appointment of an EU Representative	Article 27	✓ *****
	10	Third Party Compliance		
49	10.1	Processor GDPR Compliance Questionnaire	Articles 28, 32	
50	10.2	Supplier Data Processing Agreement version A	Articles 28, 32, 82	✓
51	10.3	Supplier Data Processing Agreement version B	Articles 28, 32, 82	✓
52	10.4	Controller to Controller Data Processing Agreement		
	11	Security of Personal Data		
53	11.1	IT Security Policy	Article 32	
54	11.2	Access Control Policy	Article 32	
55	11.3	Security Procedures for IT Department	Article 32	
56	11.4	Bring Your Own Device (BYOD) Policy	Article 32	
57	11.5	Mobile Device and Teleworking Policy	Article 32	
58	11.6	Clear Desk and Clear Screen Policy	Article 32	
59	11.7	Information Classification Policy	Article 32	
60	11.8	Anonymization and Pseudonymization Policy	Article 32	
61	11.9	Policy on the Use of Encryption	Article 32	
62	11.10	Disaster Recovery Plan	Article 32	
63	11.11	Internal Audit Procedure	Article 32	
64	11.12	Appendix – ISO 27001 Internal Audit Checklist	Article 32	
	12	Personal Data Breaches		
65	12.1	Data Breach Response and Notification Procedure	Articles 4(12), 33, 34	✓
66	12.2	Data Breach Register	Article 33(5)	✓
67	12.3	Data Breach Notification Form to the Supervisory Authority	Article 33	✓
68	12.4	Data Breach Notification Form to Data Subjects	Article 34	✓

* This document is mandatory 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 of processing on a large scale of 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.

*** This document is mandatory only if the requestor is not the data subject.

**** 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.