

EU GDPR & ISO 27001 Integrated Documentation Toolkit

<https://advisera.com/toolkits/eu-gdpr-iso-27001-integrated-documentation-toolkit/>

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

Please note that some documents in this Toolkit are not mandatory – depending on the size and complexity of your company, you can choose whether to implement them or not.


No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
	0	Document Management			
1	00	Procedure for Document and Record Control	ISO/IEC 27001 7.5; A.5.33		
	1	Preparations for the Project			
2	01.1	EU GDPR Readiness Assessment			
3	01.2	Project Plan for Complying with the EU GDPR and ISO 27001			
	2	Identification of Requirements			
4	02	Procedure for Identification of Requirements	ISO/IEC 27001 4.2; A.5.31		
5	02.1	Appendix – List of Legal, Regulatory, Contractual and Other Requirements	ISO/IEC 27001 4.2; A.5.29; A.5.31		✓ ⁽¹⁾
	3	ISMS Scope			
6	03	ISMS Scope Document	ISO/IEC 27001 4.3		✓
	4	General Policies			
7	04.1	Information Security Policy	ISO/IEC 27001 5.2; 5.3 ⁽²⁾ ; 6.2; 7.4; A.6.3		✓
8	04.2	Personal Data Protection Policy	GDPR Article 24(2)	✓	
9	04.3	Employee Personal Data Protection Policy	GDPR Article 24(2)		
10	04.4	Data Retention Policy	GDPR Articles 5(1)(e); 13(1); 17; 30	✓	
11	04.5	Appendix – Data Retention Schedule	GDPR Article 30	✓	
	5	Privacy Notices			

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
12	05.1	Privacy Notice	GDPR Articles 12; 13; 14	✓	
13	05.2	Employee Privacy Notice	GDPR Articles 12; 13; 14	✓	
14	05.3	Supplier Employee Privacy Notice	GDPR Articles 12; 13; 14		
15	05.4	Register of Privacy Notices	GDPR Articles 12; 13; 14		
	6	Data Protection Officer			
16	06.1	Data Protection Officer Job Description	GDPR Articles 37; 38; 39	✓ ⁽³⁾	
17	06.2	Data Protection Officer Appointment Letter	GDPR Articles 37; 38; 39		
18	06.3	Data Protection Officer Terms of Appointment	GDPR Articles 37; 38; 39		
	7	Website Documents			
19	07.1	Website Privacy Policy	GDPR Articles 12; 13	✓	
20	07.2	Website Terms & Conditions			
21	07.3	Cookie Policy	GDPR Articles 12; 13	✓	
	8	Mapping of Processing Activities			
22	08.1	Guidelines for Data Inventory and Processing Activities Mapping	GDPR Article 30		
23	08.2	Appendix – Inventory of Processing Activities	GDPR Article 30	✓ ⁽⁴⁾	
	9	Managing Data Subject Rights			
24	09.1	Data Subject Consent Form	GDPR Articles 6(1)(a); 7(1); 9(2)	✓	
25	09.2	Data Subject Consent Withdrawal Form	GDPR Article 7(3)		

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
26	09.3	Parental Consent Form	GDPR Article 8	✓	
27	09.4	Parental Consent Withdrawal Form	GDPR Article 8	✓	
28	09.5	Data Subject Access Request Procedure	GDPR Articles 7(3); 15; 16; 17; 18; 20; 21; 22		
29	09.6	Data Subject Access Request Form	GDPR Article 15		
30	09.7	Data Subject Disclosure Form	GDPR Article 15		
31	09.8	Request for Confirmation of Authority		✓ ⁽⁵⁾	
32	09.9	Confirmation of Data Subject Access Request	GDPR Article 15		
33	09.10	Confirmation of Data Subject Rights Request	GDPR Article 15		
34	09.11	Rejection of Unfounded/Excessive Request	GDPR Article 12(5)		
35	09.12	Confirmation for Closed DSAR	GDPR Article 15		
36	09.13	Response to Data Subject Access Request	GDPR Article 15		
37	09.14	Cover Letter to Portability Response	GDPR Article 20		
38	09.15	Response to Rectification of Data Request	GDPR Article 16		
39	09.16	Response on Consent Withdrawal/Restriction Request (Rejected)	GDPR Article 7(3)		
40	09.17	Response on Consent Withdrawal/Restriction Request (Accepted)	GDPR Article 7(3)		
41	09.18	Response on Processing Restriction Request/Complaint (Rejected)	GDPR Article 18		

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
42	09.19	Response on Processing Restriction Request/Complaint (Accepted)	GDPR Article 18		
43	09.20	Response on Auto Decision Making/Restriction on Processing (Rejected)	GDPR Article 22		
44	09.21	Response on Auto Decision Making/Restriction on Processing (Accepted)	GDPR Article 22		
45	09.22	Request Closing Letter			
46	09.23	Confirmation for Erasure of Data	GDPR Article 17		
47	09.24	Data Subject Requests Communication Register			
	10	Risk Assessment and Risk Treatment			
48	10	Risk Assessment and Risk Treatment Methodology	ISO/IEC 27001 6.1.2; 6.1.3; 8.2; 8.3		✓
49	10.1	Appendix 1 – Risk Assessment Table	ISO/IEC 27001 6.1.2; 8.2		✓
50	10.2	Appendix 2 – Risk Treatment Table	ISO/IEC 27001 6.1.3; 8.3		✓
51	10.3	Appendix 3 – Risk Assessment and Treatment Report	ISO/IEC 27001 8.2; 8.3		✓
	11	Data Protection Impact Assessment			
52	11.1	Data Protection Impact Assessment Methodology	GDPR Article 35		
53	11.2	DPIA Register	GDPR Article 35	✓	
	12	Applicability of Controls			
54	12	Statement of Applicability	ISO/IEC 27001 6.1.3 d)		✓

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
	13	Implementation Plan			
55	13	Risk Treatment Plan	ISO/IEC 27001 6.1.3; 6.2; 7.1; 8.3; 9.1		✓
	14	Security Policies and Procedures			
56	14.01	IT Security Policy	ISO/IEC 27001 A.5.9; A.5.10; A.5.11; A.5.14; A.5.17; A.5.32; A.6.7; A.7.7; A.7.9; A.7.10; A.8.1; A.8.7; A.8.10; A.8.12; A.8.13; A.8.19; A.8.23 GDPR Article 32		✓ ⁽¹⁾
57	14.02	Clear Desk and Clear Screen Policy (Note: This can be implemented as part of the IT Security Policy.)	ISO/IEC 27001 A.7.7; A.8.1 GDPR Article 32		
58	14.03	Mobile Device, Teleworking and Work from Home Policy (Note: This can be implemented as part of the IT Security Policy.)	ISO/IEC 27001 A.6.7; A.7.9; A.8.1 GDPR Article 32		
59	14.04	Bring Your Own Device (BYOD) Policy	ISO/IEC 27001 A.5.14; A.6.7; A.8.1 GDPR Article 32		
60	14.05	Procedures for Working in Secure Areas	ISO/IEC 27001 A.7.4; A.7.6 GDPR Article 32		
61	14.06	Information Classification Policy	ISO/IEC 27001 A.5.9; A.5.10; A.5.12; A.5.13; A.5.14; A.7.10; A.8.3; A.8.5; A.8.11; A.8.12 GDPR Article 32		✓ ⁽¹⁾
62	14.07	Inventory of Assets	ISO/IEC 27001 A.5.9		✓ ⁽¹⁾

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
63	14.08	Security Procedures for IT Department	ISO/IEC 27001 A.5.7; A.5.14; A.5.37; A.7.10; A.7.14; A.8.4; A.8.6; A.8.7; A.8.8; A.8.9; A.8.10; A.8.12; A.8.13; A.8.15; A.8.16; A.8.17; A.8.18; A.8.20; A.8.21; A.8.22; A.8.23; A.8.31; A.8.32 GDPR Article 32		 ⁽¹⁾
64	14.09	Change Management Policy (Note: This can be implemented as part of the Security Procedures for IT Department.)	ISO/IEC 27001 A.8.32 GDPR Article 32		
65	14.10	Backup Policy (Note: This can be implemented as part of the Security Procedures for IT Department.)	ISO/IEC 27001 A.8.13 GDPR Article 32		
66	14.11	Disposal and Destruction Policy (Note: This can be implemented as part of the Security Procedures for IT Department.)	ISO/IEC 27001 A.7.10; A.7.14; A.8.10 GDPR Article 32		
67	14.12	Policy on the Use of Encryption	ISO/IEC 27001 A.5.31; A.8.24 GDPR Article 32		
68	14.13	Anonymization and Pseudonymization Policy	ISO/IEC 27001 A.5.31; A.5.33; A.8.24 GDPR Article 32		
69	14.14	Access Control Policy	ISO/IEC 27001 A.5.15; A.5.16; A.5.17; A.5.18; A.8.2; A.8.3; A.8.4; A.8.5; A.8.11 GDPR Article 32		
70	14.15	Password Policy (Note: This can be implemented as part of the Access Control Policy.)	ISO/IEC 27001 A.5.16; A.5.17; A.5.18		

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
			GDPR Article 32		
71	14.16	Secure Development Policy	ISO/IEC 27001 A.5.33; A.8.11; A.8.25; A.8.26; A.8.27; A.8.28; A.8.29; A.8.30; A.8.31; A.8.32; A.8.33 GDPR Article 32		✓ ⁽¹⁾
72	14.17	Appendix – Specification of Information System Requirements	ISO/IEC 27001 A.8.26 GDPR Article 32		
73	14.18	Disaster Recovery Plan	ISO/IEC 27001 7.4; A.5.29; A.5.30; A.8.14		
74	14.19	Statement of Acceptance of ISMS Documents	ISO/IEC 27001 A.6.2		
	15	Relationships with Suppliers, Partners, Processors and Controllers			
75	15.01	Supplier Security Policy	ISO/IEC 27001 A.5.7; A.5.11; A.5.19; A.5.20; A.5.21; A.5.22; A.5.23; A.6.1; A.6.2; A.6.3; A.8.30 GDPR Articles 28; 32		
76	15.02	Processor GDPR Compliance Questionnaire	ISO/IEC 27001 A.6.1 GDPR Articles 28; 32		
77	15.03	Supplier Data Processing Agreement Version A	ISO/IEC 27001 A.5.20; A.5.21; A.6.2 GDPR Articles 28; 32; 82	✓	✓ ⁽¹⁾
78	15.04	Supplier Data Processing Agreement Version B	ISO/IEC 27001 A.5.20; A.5.21; A.6.2	✓	✓ ⁽¹⁾

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
			GDPR Articles 28, 32, 82		
79	15.05	Controller to Controller Data Processing Agreement			
80	15.06	Security Clauses for Suppliers and Partners	ISO/IEC 27001 A.5.20; A.5.21; A.6.2; A.6.6; A.8.30		
81	15.07	Confidentiality Statement	ISO/IEC 27001 A.5.20; A.6.2; A.6.5; A.6.6		✓ ⁽¹⁾
82	15.08	Cross-Border Personal Data Transfer Procedure	ISO/IEC 27001 A.5.14 GDPR Articles 1(3), 44, 45, 46, 47, 49		
83	15.09	Annex 1 – Standard Contractual Clauses for the Transfer of Personal Data Controller to Controller	GDPR Article 46(5)	✓ ⁽⁶⁾	
84	15.10	Annex 2 – Standard Contractual Clauses for the Transfer of Personal Data Controller to Processor	GDPR Article 46(5)	✓ ⁽⁷⁾	
85	15.11	Annex 3 – Standard Contractual Clauses for the Transfer of Personal Data Processor to Processor	GDPR Article 46(5)	✓ ⁽⁸⁾	
86	15.12	Annex 4 – Standard Contractual Clauses for the Transfer of Personal Data Processor to Controller	GDPR Article 46(5)	✓ ⁽⁹⁾	
87	15.13	Agreement for the Appointment of an EU Representative	GDPR Article 27	✓ ⁽¹⁰⁾	
	16	Handling Data Breaches			
88	16.1	Data Breach Response and Notification Procedure	ISO/IEC 27001 A.5.24; A.5.25; A.5.26; A.5.27; A.5.28; A.6.4; A.6.8; GDPR Articles 4(12), 33, 34	✓	✓ ⁽¹⁾

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
89	16.2	Data Breach Register	ISO/IEC 27001 A. GDPR Article 33(5)	✓	
90	16.3	Data Breach Notification Form to the Supervisory Authority	ISO/IEC 27001 7.4, A.5.27 GDPR Article 33	✓	
91	16.4	Data Breach Notification Form to Data Subjects	ISO/IEC 27001 7.4, A.5.26 GDPR Article 34	✓	
	17	Training & Awareness			
92	17	Training and Awareness Plan	ISO/IEC 27001 7.2; 7.3; 7.4; A.6.3 GDPR Article 39(1)		✓
	18	Internal Audit			
93	18	Internal Audit Procedure	ISO/IEC 27001 9.2; A.5.30; A.5.35; A.8.34 GDPR Article 32		
94	18.1.	Appendix 1 – Annual Internal Audit Program	ISO/IEC 27001 9.2 GDPR Article 32		✓
95	18.2	Appendix 2 – Internal Audit Report	ISO/IEC 27001 9.2 GDPR Article 32		✓
96	18.3	Appendix 3 – Internal Audit Checklist	ISO/IEC 27001 9.2 GDPR Article 32		
	19	Management Review			
97	19.1	Measurement Report	ISO/IEC 27001 6.2; 9.1		✓
98	19.2	Management Review Minutes	ISO/IEC 27001 9.3		✓
	20	Corrective Actions			
99	20	Procedure for Corrective Action	ISO/IEC 27001 10.1; A.5.27		
100	20.1	Appendix – Corrective Action Form	ISO/IEC 27001 10.1; 10.2		✓

- ⁽¹⁾ The listed documents are only mandatory if the corresponding ISO 27001 controls are identified as applicable in the Statement of Applicability.
- ⁽²⁾ General roles and responsibilities are described in the Information Security Policy, whereas detailed roles and responsibilities are specified in each document of this Toolkit.
- ⁽³⁾ 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.
- ⁽⁴⁾ 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.
- ⁽⁵⁾ This document is mandatory only if the requestor is not the data subject.
- ⁽⁶⁾ This document is mandatory if you act as a Controller and 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.
- ⁽⁷⁾ This document is mandatory if you act as a Controller and 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.
- ⁽⁸⁾ This document is mandatory if act as a Processor and 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.
- ⁽⁹⁾ This document is mandatory if you act as a Processor and 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.
- ⁽¹⁰⁾ This document is mandatory for controllers that are not established in the European Union.