EU GDPR & ISO 27001 Integrated Documentation Toolkit

https://advisera.com/eugdpracademy/eu-gdpr-iso-27001-integrated-documentation-toolkit

Note: The documentation should preferably be implemented in the order in which it is listed here. The order of implementation of documentation related to folder 11 (Security Controls) is defined in the Risk Treatment Plan.

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		
	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.18.1.1		
5	02.1	Appendix – List of Legal, Regulatory, Contractual and Other Requirements	ISO/IEC 27001 4.2, A.18.1.1		✓*
	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		✓
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**			
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	✓**	
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	✓***	
	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)		
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		✓****	
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	✓	
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)		✓
	13	**Implementation Plan**			
55	13	Risk Treatment Plan	ISO/IEC 27001 6.1.3, 6.2, 8.3		✓
	14	**Security Controls**			
	14.A.6	Organization of Information Security			
56	14.A.6.1	Bring Your Own Device (BYOD) Policy	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1 GDPR Article 32		
57	14.A.6.2	Mobile Device and Teleworking Policy	ISO/IEC 27001 A.6.2, A.11.2.6 GDPR Article 32		
	14.A.7	Human Resource Security			
58	14.A.7.1	Confidentiality Statement	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2		✓*
59	14.A.7.2	Statement of Acceptance of ISMS Documents	ISO/IEC 27001 A.7.1.2		✓*
	14.A.8	Asset Management			
60	14.A.8.1	Inventory of Assets	ISO/IEC 27001 A.8.1.1, A.8.1.2		✓*
61	14.A.8.2	IT Security Policy	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2,		✓*

			A.13.2.3, A.18.1.2 GDPR Article 32		
62	14.A.8.3	Information Classification Policy	ISO/IEC 27001 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3 GDPR Article 32		
	14.A.9	Access Control			
63	14.A.9.1	Access Control Policy	ISO/IEC 27001 A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3 GDPR Article 32		✓*
64	14.A.9.2	Password Policy (note: it can be implemented as part of the Access Control Policy)	ISO/IEC 27001 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3 GDPR Article 32		
	14.A.10	Cryptography			
65	14.A.10.1	Policy on the Use of Encryption Controls	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.3, A.18.1.5 GDPR Article 32		
66	14.A.10.2	Anonymization and Pseudonymization Policy	ISO/IEC 27001 A.10.1.1, A.18.1.3, A.18.1.5 GDPR Article 32		
	14.A.11	Physical and Environmental Security			
67	14.A.11.1	Clear Desk and Clear Screen Policy (note: it can be implemented as part of IT Security Policy)	ISO/IEC 27001 A.11.2.8, A.11.2.9 GDPR Article 32		
68	14.A.11.2	Disposal and Destruction Policy (note: it can be implemented as part of Security Procedures for IT Department)	ISO/IEC 27001 A.8.3.2, A.11.2.7 GDPR Article 32		
69	14.A.11.3	Procedures for Working in Secure Areas	ISO/IEC 27001 A.11.1.5 GDPR Article 32		

	14.A.12	Operations Security			
70	14.A.12.1	Security Procedures for IT Department	ISO/IEC 27001 A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.14.2.4 GDPR Article 32		✓*
71	14.A.12.2	Change Management Policy (note: it can be implemented as part of Security Procedures for IT Department)	ISO/IEC 27001 A.12.1.2, A.14.2.4 GDPR Article 32		
72	14.A.12.3	Backup Policy (note: it can be implemented as part of Security Procedures for IT Department)	ISO/IEC 27001 A.12.3.1		
	14.A.13	Communications Security and Personal Data Transfers			
73	14.A.13	Cross Border Personal Data Transfer Procedure	ISO/IEC 27001 A.13.2.1, A.13.2.2 GDPR Articles 1(3), 44, 45, 46, 47, 49		
74	14.A.13.1	Annex 1 – Standard Contractual Clauses for the Transfer of Personal Data to Controllers	ISO/IEC 27001 13.2.2 GDPR Article 46(5)	✓*****	✓*
75	14.A.13.2	Annex 2 – Standard Contractual Clauses for the Transfer of Personal Data to Processors	ISO/IEC 27001 13.2.2 GDPR Article 46(5)	✓******	✓*
76	14.A.13.3	Agreement for the Appointment of an EU Representative	GDPR Article 27	✓*******	
	14.A.14	System Acquisition Development and Maintenance			
77	14.A.14	Secure Development Policy	ISO/IEC A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1 GDPR Article 32		✓*

78	14.A.14.1	Appendix – Specification of Information System Requirements	ISO/IEC 27001 A.14.1.1 GDPR Article 32		✓*
	14.A.15	Supplier Relationships			
79	14.A.15	Supplier Security Policy	ISO/IEC 27001 A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 GDPR Article 28, 32		
80	14.A.15.1	Processor GDPR Compliance Questionnaire	ISO/IEC 27001 A.7.1.1 GDPR Articles 28, 32		
81	14.A.15.2	Supplier Data Processing Agreement version A	ISO/IEC 27001 A.7.1.2, A.15.1.2, A.15.1.3 GDPR Articles 28, 32, 82	✓	✓*
82	14.A.15.3	Supplier Data Processing Agreement version B	ISO/IEC 27001 A.7.1.2, A.15.1.2, A.15.1.3 GDPR Articles 28, 32, 82	✓	✓*
83	14.A.15.4	Controller to Controller Data Processing Agreement			
84	14.A.15.5	Security Clauses for Suppliers and Partners	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3		✓*
	14.A.16	Incident Management and Data Breaches			
85	14.A.16	Data Breach Response and Notification Procedure	ISO/IEC 27001 A.7.2.3, A.16.1.1, A.6.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7 GDPR Articles 4(12), 33, 34	✓	✓*
86	14.A.16.1	Data Breach Register	ISO/IEC 27001 A.16.1.6 GDPR Article 33(5)	✓	
87	14.A.16.2	Data Breach Notification Form to the Supervisory Authority	ISO/IEC 27001 7.4, A.16.1.5 GDPR Article 33	✓	

88	14.A.16.3	Data Breach Notification Form to Data Subjects	ISO/IEC 27001 7.4, A.16.1.5 GDPR Article 34	✓	
	14.A.17	Business Continuity			
89	14.A.17	Disaster Recovery Plan	ISO/IEC 27001 A.17.1.2 GDPR Article 32		✓*
	15	**Training & Awareness**			
90	15	Training and Awareness Plan	ISO/IEC 27001 7.2, 7.3 GDPR Article 39(1)		✓
	16	**Internal Audit**			
91	16	Internal Audit Procedure	ISO/IEC 27001 9.2 GDPR Article 32		
92	16.1	Appendix 1 – Annual Internal Audit Program	ISO/IEC 27001 9.2 GDPR Article 32		✓
93	16.2	Appendix 2 – Internal Audit Report	ISO/IEC 27001 9.2 GDPR Article 32		✓
94	16.3	Appendix 3 – Internal Audit Checklist	ISO/IEC 27001 9.2 GDPR Article 32		
	17	**Management Review**			
95	17.1	Measurement Report	ISO/IEC 27001 6.2, 9.1		✓
96	17.2	Management Review Minutes	ISO/IEC 27001 9.3		✓
	18	**Corrective Actions**			
97	18	Procedure for Corrective Action	ISO/IEC 27001 10.1		
98	18.1	Appendix – Corrective Action Form	ISO/IEC 27001 10.1		✓

* The listed documents are only mandatory if the corresponding controls are identified as applicable in the Statement of Applicability.

** 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.