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 clause 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 and A.18.1.1		
5	02.1	Appendix – List of Legal, Regulatory, Contractual and Other Requirements	ISO/IEC 27001 4.2 and 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 and 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	Privacy Notice	GDPR Articles 12, 13 and 14	✓	
11	04.5	Register of Privacy Notices	GDPR Articles 12, 13 and 14		
12	04.6	Data Retention Policy	GDPR Articles 5(1)(e), 13(1), 17, 30	✓	

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
13	04.7	Appendix – Data Retention Schedule	GDPR Article 30	✓	
14	04.8	Data Protection Officer Job Description	GDPR Articles 37, 38, 39	✓**	
	5	**Mapping of Processing Activities**			
15	05.1	Guidelines for Data Inventory and Processing Activities Mapping	GDPR Article 30		
16	05.2	Appendix – Inventory of Processing Activities	GDPR Article 30	✓	
	6	**Managing Data Subject Rights**			
17	06.1	Data Subject Consent Form	GDPR Articles 6(1)(a), 7(1), 9(2)	✓	
18	06.2	Data Subject Consent Withdrawal Form	GDPR Article 7(3)		
19	06.3	Parental Consent Form	GDPR Article 8	✓	
20	06.4	Parental Consent Withdrawal Form	GDPR Article 8	✓	
21	06.5	Data Subject Access Request Procedure	GDPR Articles 7(3), 15, 16, 17, 18, 20, 21, 22		
22	06.6	Data Subject Access Request Form	GDPR Article 15		
23	06.7	Data Subject Disclosure Form	GDPR Article 15		
	7	**Risk Assessment and Risk Treatment**			
24	07	Risk Assessment and Risk Treatment Methodology	ISO/IEC 27001 6.1.2, 6.1.3, 8.2, and 8.3		✓
25	07.1	Appendix 1 – Risk Assessment Table	ISO/IEC 27001 6.1.2 and 8.2		✓
26	07.2	Appendix 2 – Risk Treatment Table	ISO/IEC 27001 6.1.3 and 8.3		✓
27	07.3	Appendix 3 – Risk Assessment and Treatment Report	ISO/IEC 27001 8.2 and 8.3		✓
	8	**Data Protection Impact Assessment**			
28	08.1	Data Protection Impact Assessment Methodology	GDPR Article 35		
29	08.2	DPIA Register	GDPR Article 35	✓	
	9	**Applicability of Controls**			

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
30	09	Statement of Applicability	ISO/IEC 27001 6.1.3 d)		✓
	10	**Implementation Plan**			
31	10	Risk Treatment Plan	ISO/IEC 27001 6.1.3, 6.2 and 8.3		✓
	11	**Security Controls**			
32	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		
33	A.6.2	Mobile Device and Teleworking Policy	ISO/IEC 27001 A.6.2 A.11.2.6 GDPR Article 32		
34	A.7.1	Confidentiality Statement	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2		✓*
35	A.7.2	Statement of Acceptance of ISMS Documents	ISO/IEC 27001 A.7.1.2		✓*
36	A.8.1	Inventory of Assets	ISO/IEC 27001 A.8.1.1, A.8.1.2		✓*
37	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		✓*
38	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		
39	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,		✓*

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
			A.9.3.1, A.9.4.1, A.9.4.3 GDPR Article 32		
40	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		
41	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		
42	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		
43	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		
44	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		
45	A.11.3	Procedures for Working in Secure Areas	ISO/IEC 27001 A.11.1.5 GDPR Article 32		
46	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		✓*
47	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		
48	A.12.3	Backup Policy (note: it can be implemented as part of	ISO/IEC 27001 A.12.3.1		

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
		Security Procedures for IT Department)			
49	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		
50	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)	✓	✓*
51	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)	✓	✓*
52	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		✓*
53	A.14.1	Appendix – Specification of Information System Requirements	ISO/IEC 27001 A.14.1.1 GDPR Article 32		✓*
54	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		
55	A.15.1	Processor GDPR Compliance Questionnaire	ISO/IEC 27001 A.7.1.1 GDPR Articles 28, 32		
56	A.15.2	Supplier Data Processing Agreement	ISO/IEC 27001 A.7.1.2, A.15.1.2, A.15.1.3 GDPR Articles 28, 32, 82	✓	✓*

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
57	A.15.3	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		✓*
58	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	✓	✓*
59	A.16.1	Data Breach Register	ISO/IEC 27001 A.16.1.6 GDPR Article 33(5)	✓	
60	A.16.2	Data Breach Notification Form to the Supervisory Authority	ISO/IEC 27001 7.4, A.16.1.5 GDPR Article 33	✓	
61	A.16.3	Data Breach Notification Form to Data Subjects	ISO/IEC 27001 7.4, A.16.1.5 GDPR Article 34	✓	
62	A.17	Disaster Recovery Plan	ISO/IEC 27001 A.17.1.2 GDPR Article 32		✓*
	12	**Training & Awareness**			
63	12	Training and Awareness Plan	ISO/IEC 27001 clauses 7.2, 7.3 GDPR Article 39(1)		✓
	13	**Internal Audit**			
64	13	Internal Audit Procedure	ISO/IEC 27001 clause 9.2 GDPR Article 32		
65	13.1	Appendix 1 – Annual Internal Audit Program	ISO/IEC 27001 clause 9.2 GDPR Article 32		✓
66	13.2	Appendix 2 – Internal Audit Report	ISO/IEC 27001 clause 9.2 GDPR Article 32		✓
67	13.3	Appendix 3 – Internal Audit Checklist	ISO/IEC 27001 clause 9.2 GDPR Article 32		
	14	**Management Review**			
68	14.1	Measurement Report	ISO/IEC 27001 clauses 6.2, 9.1		✓

No.	Document code	Document name	Relevant articles in GDPR / clauses in ISO 27001	Mandatory according to GDPR	Mandatory according to ISO 27001
69	14.2	Management Review Minutes	ISO/IEC 27001 clause 9.3		✓
	15	**Corrective Actions**			
70	15	Procedure for Corrective Action	ISO/IEC 27001 clause 10.1		
71	15.1	Appendix – Corrective Action Form	ISO/IEC 27001 clause 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.