EU GDPR & ISO 27001

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	**Preparations for the Project**			
	2	**Identification of Requirements**			
	3	**ISMS Scope**			
	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	Employee Privacy Notice	GDPR Articles 12, 13 and 14	✓	
12	04.6	Register of Privacy Notices	GDPR Articles 12, 13 and 14		

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	Data Retention Policy	GDPR Articles 5(1)(e), 13(1), 17, 30	✓	
14	04.8	Appendix – Data Retention Schedule	GDPR Article 30	✓	
15	04.9	Data Protection Officer Job Description	GDPR Articles 37, 38, 39	✓**	
	5	**Mapping of Processing Activities**			
17	05.2	Appendix – Inventory of Processing Activities	GDPR Article 30	***	
	6	**Managing Data Subject Rights**			
18	06.1	Data Subject Consent Form	GDPR Articles 6(1)(a), 7(1), 9(2)	✓	

19	06.2	Data Subject Consent Withdrawal Form	GDPR Article 7(3)		
20	06.3	Parental Consent Form	GDPR Article 8	✓	
21	06.4	Parental Consent Withdrawal Form	GDPR Article 8	✓	
22	06.5	Data Subject Access Request Procedure	GDPR Articles 7(3), 15, 16, 17, 18, 20, 21, 22		
23	06.6	Data Subject Access Request Form	GDPR Article 15		
24	06.7	Data Subject Disclosure Form	GDPR Article 15		
	7	**Risk Assessment and Risk Treatment**			
	8	**Data Protection Impact Assessment**			
30	08.2	DPIA Register	GDPR Article 35	✓	
	9	**Applicability of Controls**			
	10	**Implementation Plan**			
	11	**Security Controls**			
No.	***Document code***	***Document name***	***Relevant articles in GDPR / clauses in ISO 27001***	***Mandatory according to GDPR***	***Mandatory according to ISO 27001***
51	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)	****	✓*
52	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)	✓*****	✓*
57	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	✓	✓*
58	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		✓*
59	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	✓	✓*
60	A.16.1	Data Breach Register	ISO/IEC 27001 A.16.1.6 GDPR Article 33(5)	✓	

61	A.16.2	Data Breach Notification Form to the Supervisory Authority	ISO/IEC 27001 7.4, A.16.1.5 GDPR Article 33	✓	
62	A.16.3	Data Breach Notification Form to Data Subjects	ISO/IEC 27001 7.4, A.16.1.5 GDPR Article 34	✓	
63	A.17	Disaster Recovery Plan	ISO/IEC 27001 A.17.1.2 GDPR Article 32		✓*
	12	**Training & Awareness**			
	13	**Internal Audit**			
	14	**Management Review**			

* 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 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.