EU GDPR & ISO 27001

Opomba: Dokumentacija se gradi po vrstnem redu. Vrstni red izvajanja dokumentacije v zvezi z mapo 11 (varnost in nadzor) je opredeljen v načrtu za obvladovanje tveganja. Upoštevajte, da nekateri dokumenti niso obvezni - odvisno od velikosti in kompleksnosti vašega podjetja lahko izberete, ali jih želite izvajati ali ne. Obvezne dokumente po GDPR smo označili z rdečo barvo.

Št.	*Oznaka*	*Naslov dokumenta*	*Relevantni členi po GDPR / klavzule v ISO 27001*	*Obvezno po GDPR*	*Obvezno po ISO 27001*
	0	**Upravljanje dokumentov**			
	1	**Priprave za projekt**			
	2	**Identifikacija zahtev**			
	3	**ISMS področje uporabe**			
	4	**Generalne politike**			
7	04.1	Politika varovanja informacij	ISO/IEC 27001 5.2 in 5.3		✓
8	04.2	Politika zaščite osebnih podatkov	GDPR člen 24(2)	✓	
9	04.3	Politika zaščite osebnih podatkov zaposlenih	GDPR člen 24(2)		
10	04.4	Obvestilo o zasebnosti	GDPR člen 12, 13 in 14	✓	
11	04.5	Obvestilo o zasebnosti zaposlenih	GDPR člen 12, 13 in 14	✓	
12	04.6	Register obvestil zasebnosti	GDPR člen 12, 13 in 14		
13	04.7	Pravilnik o hranjenju podatkov	GDPR člen 5(1)(e), 13(1), 17, 30	✓	
14	04.8	Priloga – Urnik hranjenja podatkov	GDPR člen 30	✓	
15	04.9	Opis dela pooblaščene osebe za varovanje podatkov (Data Protection Officer)	GDPR člen 37, 38, 39	✓**	
	5	**Mapiranje aktivnosti obdelave**			
17	05.2	Priloga – Seznam aktivnosti obdelav	GDPR člen 30	***	
	6	**Upravljanje pravic subjektov podatkov**			
18	06.1	Obrazec za soglasje subjekta podatkov	GDPR člen 6(1)(a), 7(1), 9(2)	✓	
19	06.2	Obrazec za umik soglasja subjekta podatkov	GDPR člen 7(3)		
20	06.3	Obrazec za soglasje staršev	GDPR člen 8	✓	

21	06.4	Obrazec za umik soglasja staršev	GDPR člen 8	✓	
22	06.5	Procedura zahtev za dostop subjekta podatkov	GDPR člen 7(3), 15, 16, 17, 18, 20, 21, 22		
23	06.6	Obrazec za zahtevo dostopa subjekta podatkov	GDPR člen 15		
24	06.7	Obrazec za razkritje subjekta podatkov	GDPR člen 15		
	7	**Ocena tveganja in obvladovanje**			
	8	**Ocena vpliva na varovanje podatkov**			
30	08.2	DPIA Register	GDPR člen 35	✓	
	9	**Uporabnost kontrol**			
	10	**Izvedbeni načrt**			
	11	**Varnostni ukrepi**			

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 – Standardne pogodbene klavzule za prenos osebnih podatkov do upravljalcev	ISO/IEC 27001 13.2.2 GDPR člen 46(5)	****	✓*
52	A.13.2	Annex 2 – Standardne pogodbene klavzule za prenos osebnih podatkov do obdelovalcev	ISO/IEC 27001 13.2.2 GDPR člen 46(5)	✓*****	✓*
57	A.15.2	Sporazum s ponudnikom obdelave osebnih podatkov	ISO/IEC 27001 A.7.1.2, A.15.1.2, A.15.1.3 GDPR člen 28, 32, 82	✓	✓*
58	A.15.3	Varnostne klavzule za dobavitelje in partnerje	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3		✓*
59	A.16	Procedura odziva in prijave kršitve varovanja podatkov (Data Breach 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 člen 4(12), 33, 34	✓	✓*
60	A.16.1	Register kršitev	ISO/IEC 27001 A.16.1.6 GDPR člen 33(5)	✓	

61	A.16.2	Obrazec za obvestilo o kršitvi za nadzorni organ	ISO/IEC 27001 7.4, A.16.1.5 GDPR člen 33	✓	
62	A.16.3	Obrazec za obvestilo o kršitvi za subjekte podatkov	ISO/IEC 27001 7.4, A.16.1.5 GDPR člen 34	✓	
63	A.17	Načrt za obnovitev po nesreči (Disaster Recovery Plan)	ISO/IEC 27001 A.17.1.2 GDPR člen 32		✓*
	12	**Usposabljanja in ozaveščanje**			
	13	**Notranja revizija**			
	14	**Vodstveni pregled**			
	15	**Korektivni ukrepi**			

* Navedeni dokumenti so obvezni, če so kontrole identificirane v Izjavi o uporabnosti.

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

** Obvezen dokument za del javne uprave:

** 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.

** Obvezen dokument za podjetja, ki imajo več kot 250 zaposlenih:

*** 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.

**** Obvezen dokument, če se prenašajo podatki upravljalcu izven EEA:

****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.

***** Obvezen dokument, če se prenašajo podatki obdelovalcu izven EEA:

***** 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.