

## EU DSGVO & ISO 27001 Integriertes Dokumentations-Toolkit

<https://advisera.com/eugdpracademy/de/eu-dsgvo-iso-27001-integriertes-dokumentations-toolkit/>

Bemerkung: Die Dokumentation sollte vorzugsweise in der Reihenfolge umgesetzt werden, in der sie hier aufgeführt ist. Die Reihenfolge der Umsetzung der Dokumentation zu Ordner 11 (Sicherheits-kontrollen) ist im Risikobehandlungsplan definiert.

Bitte beachten Sie, dass einige Dokumente in diesem Toolkit nicht vorgeschrieben sind. Je nach Größe und Komplexität Ihres Unternehmens können Sie wählen, ob Sie diese umsetzen möchten oder nicht.

Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
	<b>0</b>	<b>Dokumentenmanagement</b>			
1	00	Verfahren zur Lenkung von Dokumenten und Aufzeichnungen	ISO/IEC 27001 7.5		
	<b>1</b>	<b>Vorbereitungen für das Projekt</b>			
2	01.1	EU DSGVO Bereitschaftsbewertung			
3	01.2	Projektplan für die Umsetzung des ISMS und für die Einhaltung der EU DSGVO			
	<b>2</b>	<b>Identifikation von Anforderungen</b>			
4	02	Verfahren zur Identifikation der Anforderungen	ISO/IEC 27001 4.2, A.18.1.1		
5	02.1	Anhang – Liste gesetzlicher, amtlicher, vertraglicher und anderer Anforderungen	ISO/IEC 27001 4.2, A.18.1.1		✓ *
	<b>3</b>	<b>ISMS Anwendungsbereich</b>			
6	03	Dokument zum ISMS Anwendungsbereich	ISO/IEC 27001 4.3		✓
	<b>4</b>	<b>Allgemeine Politiken</b>			
7	04.1	Informationssicherheitspolitik	ISO/IEC 27001 5.2, 5.3		✓
8	04.2	Politik des Schutzes personenbezogener Daten	DSGVO Artikel 24(2)	✓	
9	04.3	Politik des Schutzes personenbezogener Daten von Arbeitnehmern	DSGVO Artikel 24(2)		

Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
10	04.4	Politik der Datenspeicherung	DSGVO Artikel 5(1)(e), 13(1), 17, 30	✓	
11	04.5	Anhang – Datenspeicherungszeitplan	DSGVO Artikel 30	✓	
	<b>5</b>	<b>Datenschutzerklärungen</b>			
12	05.1	Datenschutzerklärung	DSGVO Artikel 12, 13, 14	✓	
13	05.2	Datenschutzerklärung für Arbeitnehmer	DSGVO Artikel 12, 13, 14	✓	
14	05.3	Datenschutzerklärung für Lieferantenmitarbeiter	DSGVO Artikel 12, 13, 14	✓	
15	05.4	Verzeichnis der Datenschutzerklärungen	DSGVO Artikel 12, 13, 14		
	<b>6</b>	<b>Datenschutzbeauftragter</b>			
16	06.1	Arbeitsbeschreibung des Datenschutzbeauftragten	DSGVO Artikel 37, 38, 39	✓ **	
17	06.2	Datenschutzbeauftragter-Erennungsschreiben	DSGVO Artikel 37, 38, 39		
18	06.3	Schreiben der Ernennungsbedingungen des Datenschutzbeauftragten	DSGVO Artikel 37, 38, 39		
	<b>7</b>	<b>Webseite_Dokumente</b>			
19	07.1	Webseiten - Datenschutzpolitik	DSGVO Artikel 12, 13	✓	
20	07.2	Webseite-Geschäftsbedingungen			
21	07.3	Cookie-Politik	DSGVO Artikel 12, 13	✓	
	<b>8</b>	<b>Mapping der Verarbeitungstätigkeiten</b>			
22	08.1	Richtlinien für das Datenverzeichnis und die Zuordnung der Verarbeitungstätigkeiten	DSGVO Artikel 30		
23	08.2	Anhang – Verzeichnis der Verarbeitungstätigkeiten	DSGVO Artikel 30	✓ ***	
	<b>9</b>	<b>Rechte betroffener Personen managen</b>			

Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
24	09.1	Formular der Einverständniserklärung betroffener Personen	DSGVO Artikel 6(1)(a), 7(1), 9(2)	✓	
25	09.2	Formular für die Widerrufung der Einverständniserklärung betroffener Personen	DSGVO Artikel 7(3)		
26	09.3	Formular der elterlichen Einverständniserklärung	DSGVO Artikel 8	✓	
27	09.4	Formular für die Widerrufung der elterlichen Einverständniserklärung	DSGVO Artikel 8	✓	
28	09.5	Verfahren des Zugangersuchens betroffener Personen	DSGVO Artikel 7(3), 15, 16, 17, 18, 20, 21, 22		
29	09.6	Formular des Zugangersuchens betroffener Personen	DSGVO Artikel 15		
30	09.7	Formular der Offenlegung für betroffene Personen	DSGVO Artikel 15		
31	09.8	Aufforderung zur Bestätigung der Befugnis		✓ ****	
32	09.9	Bestätigung des Zugangersuchens betroffener Personen	DSGVO Artikel 15	✓	
33	09.10	Bestätigung des Ersuchens bezüglich der Rechte betroffener Personen	DSGVO Artikel 15	✓	
34	09.11	Ablehnung eines unbegründeten/übermäßigen Ersuchens	DSGVO Artikel 12(5)	✓	
35	09.12	Bestätigung über den Abschluss des Zugangersuchens einer betroffenen Person	DSGVO Artikel 15	✓	
36	09.13	Antwort auf das Zugriffsersuchen betroffener Personen	DSGVO Artikel 15	✓	

Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
37	09.14	Begleitschreiben zur Beantwortung der Übertragbarkeit	DSGVO Artikel 20	✓	
38	09.15	Antwort auf das Ersuchen Daten zu berichtigen	DSGVO Artikel 16	✓	
39	09.16	Antwort auf die Widerrufung der Einwilligung/Ersuchen um Einschränkung (Ablehnung)	DSGVO Artikel 7(3)	✓	
40	09.17	Antwort auf die Widerrufung der Einwilligung/Ersuchen um Einschränkung (Annahme)	DSGVO Artikel 7(3)	✓	
41	09.18	Antwort auf das Ersuchen zur Verarbeitungseinschränkung/Beschwerde (Ablehnung)	DSGVO Artikel 18	✓	
42	09.19	Antwort auf das Ersuchen zur Verarbeitungseinschränkung/Beschwerde (Annahme)	DSGVO Artikel 18	✓	
43	09.20	Antwort auf die automatische Entscheidungsfindung/Einschränkung der Verarbeitung (Ablehnung)	DSGVO Artikel 22	✓	
44	09.21	Antwort auf die automatische Entscheidungsfindung/Einschränkung der Verarbeitung (Annahme)	DSGVO Artikel 22	✓	
45	09.22	Schreiben zum Abschluss des Ersuchens			
46	09.23	Bestätigung zur Datenlöschung	DSGVO Artikel 17	✓	
47	09.24	Verzeichnis der Kommunikation über Ersuchen von betroffenen Personen			
	<b>10</b>	<b>Risikoeinschätzung und Risikobehandlung</b>			
48	10	Methodik zur Risikoeinschätzung und Risikobehandlung	ISO/IEC 27001 6.1.2, 6.1.3, 8.2, 8.3		✓
49	10.1	Anhang 1 – Verzeichnis der Risikoeinschätzung	ISO/IEC 27001 6.1.2, 8.2		✓

Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
50	10.2	Anhang 2 – Verzeichnis der Risikobehandlung	ISO/IEC 27001 6.1.3, 8.3		✓
51	10.3	Anhang 3 – Bericht zur Risikoeinschätzung und Risikobehandlung	ISO/IEC 27001 8.2, 8.3		✓
	<b>11</b>	<b>Datenschutz-Folgenabschätzung</b>			
52	11.1	Methodik der Datenschutz-Folgenabschätzung	DSGVO Artikel 35		
53	11.2	Verzeichnis der DSFA	DSGVO Artikel 35	✓	
	<b>12</b>	<b>Anwendbarkeit der Maßnahmen</b>			
54	12	Erklärung zur Anwendbarkeit	ISO/IEC 27001 6.1.3 d)		✓
	<b>13</b>	<b>Plan der Umsetzung</b>			
55	13	Plan zur Risikobehandlung	ISO/IEC 27001 6.1.3, 6.2, 8.3		✓
	<b>14</b>	<b>Sicherheitskontrollen</b>			
	14.A.6	Organisierung der Informationssicherheit			
56	14.A.6.1	Bring Your Own Device (BYOD) Richtlinie	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1 DSGVO Artikel 32		
57	14.A.6.2	Richtlinie zu Mobilgeräten und Telearbeit	ISO/IEC 27001 A.6.2 A.11.2.6 DSGVO Artikel 32		
	14.A.7	Personelle Sicherheit			
58	14.A.7.1	Vertraulichkeitserklärung	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2		✓ *
59	14.A.7.2	Erklärung zur Akzeptanz von ISMS-Dokumenten	ISO/IEC 27001 A.7.1.2		✓ *
	14.A.8	Management von Werten			

Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
60	14.A.8.1	Inventar der Werte	ISO/IEC 27001 A.8.1.1, A.8.1.2		✓ *
61	14.A.8.2	IT-Sicherheitspolitik	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 DSGVO Artikel 32		✓ *
62	14.A.8.3	Richtlinie zur Klassifizierung von Informationen	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 DSGVO Artikel 32		
	14.A.9	Zugangssteuerung			
63	14.A.9.1	Zugangssteuerungsrichtlinie	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 DSGVO Artikel 32		✓ *
64	14.A.9.2	Kennwort-Richtlinie (Anmerkung: Sie kann auch als Teil der Zugangssteuerungsrichtlinie umgesetzt werden)	ISO/IEC 27001 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3		

Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
			DSGVO Artikel 32		
	14.A.10	Kryptografie			
65	14.A.10.1	Richtlinie des Einsatzes von Verschlüsselung	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.3, A.18.1.5 DSGVO Artikel 32		
66	14.A.10.2	Richtlinie der Anonymisierung und Pseudonymisierung	ISO/IEC 27001 A.10.1.1, A.18.1.3, A.18.1.5 DSGVO Artikel 32		
	14.A.11	Physische und Umgebungs Sicherheit			
67	14.A.11.1	Richtlinie zum aufgeräumten Arbeitsplatz und leeren Bildschirm (Anmerkung: Sie kann auch als Teil der Richtlinie zum zulässigen Gebrauch umgesetzt werden)	ISO/IEC 27001 A.11.2.8, A.11.2.9 DSGVO Artikel 32		
68	14.A.11.2	Richtlinie zur Entsorgung und Vernichtung (Anmerkung: Sie kann auch als Teil des Sicherheitsverfahren für die IT-Abteilung umgesetzt werden)	ISO/IEC 27001 A.8.3.2, A.11.2.7 DSGVO Artikel 32		
69	14.A.11.3	Verfahren zur Arbeit in sicheren Bereichen	ISO/IEC 27001 A.11.1.5 DSGVO Artikel 32		
	14.A.12	Betriebssicherheit			
70	14.A.12.1	Sicherheitsverfahren für die IT-Abteilung	ISO/IEC 27001 A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2,		✓ *

Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
			A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.14.2.4 DSGVO Artikel 32		
71	14.A.12.2	Richtlinie zum Änderungsmanagement (Anmerkung: Sie kann auch als Teil des Sicherheitsverfahrens für die IT-Abteilung umgesetzt werden)	ISO/IEC 27001 A.12.1.2, A.14.2.4 DSGVO Artikel 32		
72	14.A.12.3	Backup-Richtlinie (Anmerkung: Sie kann auch als Teil des Sicherheitsverfahrens für die IT-Abteilung umgesetzt werden)	ISO/IEC 27001 A.12.3.1		
	14.A.13	Kommunikationssicherheit und Übertragung personenbezogener Daten			
73	14.A.13	Verfahren der grenzüberschreitenden personenbezogenen Datenübertragung	ISO/IEC 27001 A.13.2.1, A.13.2.2 DSGVO Artikel 1(3), 44, 45, 46, 47, 49		
74	14.A.13.1	Anhang 1 – Standardvertragsklauseln für die Übertragung personenbezogener Daten an Verantwortliche	ISO/IEC 27001 13.2.2 DSGVO Artikel 46(5)	✓ *****	✓ *
75	14.A.13.2	Anhang 2 – Standardvertragsklauseln für die Übertragung personenbezogener Daten an Auftragsverarbeiter	ISO/IEC 27001 13.2.2 DSGVO Artikel 46(5)	✓ *****	✓ *



Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
76	14.A.13.3	Vereinbarung über die Ernennung eines EU-Vertreterers	DSGVO Artikel 27	✓ *****	
	14.A.14	Systembeschaffung Entwicklung und Wartung			
77	14.A.14	Richtlinie zur Entwicklungssicherheit	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 DSGVO Artikel 32		✓ *
78	14.A.14.1	Anhang – Spezifikation der Sicherheitsanforderungen	ISO/IEC 27001 A.14.1.1 DSGVO Artikel 32		✓ *
	14.A.15	Beziehungen zu Lieferanten			
79	14.A.15	Sicherheitspolitik für Lieferanten	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 DSGVO Artikel 28, 32		✓ *
80	14.A.15.1	DSGVO Einhaltungsfagebogen für den Auftragsverarbeiter	ISO/IEC 27001 A.7.1.1 DSGVO Artikel 28, 32		

Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
81	11.A.15.2	Vereinbarung über die Datenverarbeitung mit Lieferanten Version A	ISO/IEC 27001 A.7.1.2, A.15.1.2, A.15.1.3 DSGVO Artikel 28, 32, 82	✓	✓ *
82	11.A.15.3	Vereinbarung über die Datenverarbeitung mit Lieferanten Version B	ISO/IEC 27001 A.7.1.2, A.15.1.2, A.15.1.3 DSGVO Artikel 28, 32, 82	✓	✓ *
83	11.A.15.4	Datenverarbeitungsvereinbarung zwischen Verantwortlichen und Verantwortlichen			
84	14.A.15.5	Sicherheitsabschnitte für Lieferanten und Partner	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3		✓ *
	14.A.16	Vorfallsmanagement und Schutzverletzung personenbezogener Daten			
85	14.A.16	Reaktion auf eine Datenschutzverletzung und Meldeverfahren	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 DSGVO Artikel 4(12), 33, 34	✓	✓ *
86	14.A.16.1	Verzeichnis der Datenschutzverletzung	ISO/IEC 27001 A.16.1.6 DSGVO Artikel 33(5)	✓	

Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
87	14.A.16.2	Meldungsformular der Datenschutzverletzung an die Aufsichtsbehörde	ISO/IEC 27001 7.4, A.16.1.5 DSGVO Artikel 33	✓	
88	14.A.16.3	Meldungsformular der Datenschutzverletzung an betroffene Personen	ISO/IEC 27001 7.4, A.16.1.5 DSGVO Artikel 34	✓	
	14.A.17	Kontinuitätsmanagement			
89	14.A.17	Notfallwiederherstellungsplan	ISO/IEC 27001 A.17.1.2 DSGVO Artikel 32		✓ *
	15	<b>Training und Awareness</b>			
90	15	Plan für Training und Awareness	ISO/IEC 27001 7.2, 7.3 DSGVO Artikel 39(1)		✓
	16	<b>Internes Audit</b>			
91	16	Verfahren für interne Audits	ISO/IEC 27001 9.2 DSGVO Artikel 32		
92	16.1	Anhang 1 – Internes Audit-Programm	ISO/IEC 27001 9.2 DSGVO Artikel 32		✓
93	16.2	Anhang 2 – Interner Audit-Bericht	ISO/IEC 27001 9.2 DSGVO Artikel 32		✓
94	16.3	Anhang 3 – Interne Audit-Checkliste	ISO/IEC 27001 9.2 DSGVO Artikel 32		
	17	<b>Managementbewertung</b>			
95	17.1	Messbericht	ISO/IEC 27001 6.2, 9.1		✓

Nr.	Dokument-code	Bezeichnung des Dokumentes	Relevante Artikel der DSGVO / Abschnitte in ISO 27001	Vorgeschrieben gemäß DSGVO	Vorgeschrieben gemäß ISO 27001
96	17.2	Protokoll zur Managementbewertung	ISO/IEC 27001 9.3		✓
	<b>18</b>	<b>Korrekturmaßnahmen</b>			
97	18	Verfahren zu Korrekturmaßnahmen	ISO/IEC 27001 10.1		
98	18.1	Anhang – Formblatt der Korrekturmaßnahmen	ISO/IEC 27001 10.1		✓

\* Die aufgeführten Dokumente sind nur dann verpflichtend, wenn die entsprechenden Kontrollen in der Anwendbarkeitserklärung als anwendbar eingestuft wurden.

\*\* Dieses Dokument ist vorgeschrieben, falls (a) die Verarbeitung ausgeführt wird von einer öffentlichen Behörde oder öffentlichen Stelle, außer für Gerichte, die im Rahmen ihrer Recht sprechenden Befugnisse handeln; oder (b) die Kerntätigkeit des Rechtsträgers aus Verarbeitungsprozessen besteht, die aufgrund ihrer Natur, ihrem Anwendungsbereichs und/oder ihres Zwecks in großem Umfang regelmäßige und systematische Überwachung betroffener Personen verlangt; oder (c) die Kerntätigkeit der Rechtsträger auf der Verarbeitung besonderer Kategorien von Daten in großem Umfang entsprechend Artikel 9 der EU DSGVO und personenbezogener Daten bezüglich strafrechtlicher Verurteilung und strafbarer Handlung, auf die sich Artikel 10 des EU DSGVO bezieht, beruhen.

\*\*\* Dieses Dokument ist vorgeschrieben, wenn (a) das Unternehmen mehr als 250 Mitarbeiter beschäftigt; oder (b) die Verarbeitung, die das Unternehmen ausführt wahrscheinlich zu einer Gefährdung der Rechte und Freiheiten der betroffenen Personen führt; oder (c) die Verarbeitung ist nicht gelegentlich; oder (d) die Verarbeitung umfasst besondere Datenkategorien (personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Mitgliedschaft in Gewerkschaften hervorgehen, sowie die Verarbeitung genetischer Daten, biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten über Gesundheit oder Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person) oder (e) die Verarbeitung umfasst personenbezogene Daten in Bezug auf strafrechtliche Verurteilungen und Straftaten.

\*\*\*\* Dieses Dokument ist vorgeschrieben, wenn der Antragsteller nicht die betroffene Person ist.

\*\*\*\*\* Dieses Dokument ist vorgeschrieben, wenn Sie personenbezogene Daten an einen Verantwortlichen außerhalb des Europäischen Wirtschaftsraums (EWR) übermitteln und Sie sich auf die Modellklauseln als rechtmäßigen Grund für grenzüberschreitende Datenübertragungen berufen.

\*\*\*\*\* Dieses Dokument ist vorgeschrieben, wenn Sie personenbezogene Daten an einen Auftragsverarbeiter außerhalb des Europäischen Wirtschaftsraums (EWR) übermitteln und Sie sich auf die Modellklauseln als rechtmäßigen Grund für grenzüberschreitende Datenübertragungen berufen.

\*\*\*\*\* Dieses ist ein Pflichtdokument für Datenverantwortliche, die ihren Sitz nicht in der Europäischen Union haben.