

## EU DSGVO Dokumentations-Toolkit

<https://advisera.com/de/toolkits/eu-dsgvo-dokumentations-toolkit/>

Bemerkung: Die Dokumentation sollte im Idealfall in der Reihenfolge umgesetzt werden, in der sie hier angeführt ist.

Nr.	Dokument code	Bezeichnung des Dokumentes	Relevante Artikel in der EU DSGVO	Vorgeschrieben gemäß EU DSGVO
	<b>1</b>	<b>Projektvorbereitung</b>		
1	1.1	EU DSGVO Bereitschaftsbewertung		
2	1.2	Projektplan für die Einhaltung der EU DSGVO		
	<b>2</b>	<b>Politikrahmen personenbezogener Daten</b>		
3	2.1	Politik des Schutzes personenbezogener Daten	Artikel 24(2)	✓
4	2.2	Politik der Datenspeicherung	Artikel 5(1)(e), 13(1), 17, 30	✓
5	2.3	Anhang – Datenspeicherungszeitplan	Artikel 30	✓
	<b>3</b>	<b>Datenschutzerklärungen</b>		
6	3.1	Datenschutzerklärung	Artikel 12, 13, 14	✓
7	3.2	Verzeichnis der Datenschutzerklärungen	Artikel 12, 13, 14	
	<b>4</b>	<b>Mapping der Verarbeitungstätigkeiten</b>		
8	4.1	Richtlinien für das Datenverzeichnis und die Zuordnung der Verarbeitungstätigkeiten	Artikel 30	
9	4.2	Anhang – Verzeichnis der Verarbeitungstätigkeiten	Artikel 30	✓*
	<b>5</b>	<b>Rechte betroffener Personen managen</b>		
10	5.1	Formular der Einverständniserklärung betroffener Personen	Artikel 6(1)(a), 7(1), 9(2)	✓
11	5.2	Formular für die Widerrufung der Einverständniserklärung betroffener Personen	Artikel 7(3)	
12	5.3	Formular der elterlichen Einverständniserklärung	Artikel 8	✓
13	5.4	Formular für die Widerrufung der elterlichen Einverständniserklärung	Artikel 8	✓
	<b>6</b>	<b>Datenschutz-Folgenabschätzung</b>		

Nr.	Dokument code	Bezeichnung des Dokumentes	Relevante Artikel in der EU DSGVO	Vorgeschrieben gemäß EU DSGVO
14	6.1	Methodik der Datenschutz-Folgenabschätzung	Artikel 35	
15	6.2	Verzeichnis der DSFA	Artikel 35	✓
	<b>7</b>	<b>Übertragung personenbezogener Daten</b>		
16	7.1	Verfahren der grenzüberschreitenden personenbezogenen Datenübertragung	Artikel 1(3), 44, 45, 46, 47, 49	
17	7.2	Anhang 1 – Standardvertragsklauseln für die Übermittlung personenbezogener Daten von Verantwortlichen an Verantwortliche	Artikel 46(5)	✓ **
18	7.3	Anhang 2 – Standardvertragsklauseln für die Übermittlung personenbezogener Daten von Verantwortlichen an Auftragsverarbeiter	Artikel 46(5)	✓ ***
19	7.4	Anhang 3 – Standardvertragsklauseln für die Übermittlung personenbezogener Daten von Auftragsverarbeitern an Auftragsverarbeitern	Artikel 46(5)	✓ ****
20	7.5	Anhang 4 – Standardvertragsklauseln für die Übermittlung personenbezogener Daten von Auftragsverarbeitern an Verantwortliche	Artikel 46(5)	✓ *****
21	7.6	Vereinbarung über die Ernennung eines EU-Vertreters	Artikel 27	✓ *****
	<b>8</b>	<b>Einhaltung Dritter</b>		
22	8.1	Vereinbarung über die Datenverarbeitung mit Lieferanten Version A	Artikel 28, 32, 82	✓
23	8.2	Vereinbarung über die Datenverarbeitung mit Lieferanten Version B	Artikel 28, 32, 82	✓
	<b>9</b>	<b>Sicherheit personenbezogener Daten</b>		
24	9.1	IT Sicherheitspolitik	Artikel 32	
25	9.2	Zugangssteuerungsrichtlinie	Artikel 32	
26	9.3	Sicherheitsverfahren für die IT-Abteilung	Artikel 32	

Nr.	Dokument code	Bezeichnung des Dokumentes	Relevante Artikel in der EU DSGVO	Vorgeschrieben gemäß EU DSGVO
27	9.4	Bring Your Own Device (BYOD) Richtlinie	Artikel 32	
28	9.5	Richtlinie zu Mobilgeräten und Telearbeit	Artikel 32	
29	9.6	Richtlinie zum aufgeräumten Arbeitsplatz und leeren Bildschirm	Artikel 32	
30	9.7	Richtlinie zur Klassifizierung von Informationen	Artikel 32	
31	9.8	Richtlinie der Anonymisierung und Pseudonymisierung	Artikel 32	
32	9.9	Richtlinie des Einsatzes von Verschlüsselung	Artikel 32	
33	9.10	Notfallwiederstellungsplan	Artikel 32	
34	9.11	Verfahren für interne Audits	Artikel 32	
35	9.12	Anhang – ISO 27001 Interne Audit Checkliste	Artikel 32	
	<b>10</b>	<b>Schutzverletzung personenbezogener Daten</b>		
36	10.1	Reaktion auf eine Datenschutzverletzung und Meldeverfahren	Artikel 4(12), 33, 34	✓
37	10.2	Verzeichnis der Datenschutzverletzung	Artikel 33(5)	✓
38	10.3	Meldungsformular der Datenschutzverletzung an die Aufsichtsbehörde	Artikel 33	✓
39	10.4	Meldungsformular der Datenschutzverletzung an betroffene Personen	Artikel 34	✓

\* 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 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 Dokument ist obligatorisch, wenn Sie als Auftragsverarbeiter handeln und personenbezogene Daten an einen Auftragsverarbeiter außerhalb des Europäischen Wirtschaftsraums (EWR) übermitteln und sich auf die Modellklauseln als rechtmäßige Grundlage für grenzüberschreitende Datenübermittlungen berufen.

\*\*\*\*\* Dieses Dokument ist obligatorisch, wenn Sie als Auftragsverarbeiter tätig sind und personenbezogene Daten an einen Verantwortlichen außerhalb des Europäischen Wirtschaftsraums (EWR) übermitteln und sich auf die Modellklauseln als rechtmäßige Grundlage für grenzüberschreitende Datenübermittlungen berufen.

\*\*\*\*\* Dieses Dokument ist für Verantwortliche, die nicht in der Europäischen Union ansässig sind, obligatorisch.