

DSGVO-Compliance-Checkliste

Die vollständige DSGVO-Readiness-Checkliste für KMU · DE

Geprüft von einem zertifizierten Datenschutzbeauftragten (CIPP/E) · Bereitgestellt von ETHYX · Version 1.0 · Juni 2026 · Keine Rechtsberatung

ANLEITUNG Arbeiten Sie jeden Abschnitt durch und haken Sie das Kästchen ab, wenn die Anforderung erfüllt ist. Nutzen Sie die Spalte Status / Notizen für Lücken, Verantwortliche und Zieldaten. Eine abgehakte Checkliste ist eine Momentaufnahme, kein Compliance-Nachweis – bewahren Sie die zugrunde liegenden Unterlagen auf (VVT, AVV, Richtlinien). Beginnen Sie mit den Abschnitten 1–4; sie gelten für fast jedes Unternehmen.

Unternehmen: _____ **Ausgefüllt von:** _____
Nächste Prüfung: _____ **Datum:** _____

1 Governance & Rechenschaftspflicht

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Wir können die Einhaltung der DSGVO-Grundsätze nachweisen (Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität & Vertraulichkeit). [Art. 5]	
☐	Eine benannte Person oder Rolle ist für den Datenschutz in unserer Organisation verantwortlich. [Art. 24]	
☐	Wir haben geprüft, ob wir einen Datenschutzbeauftragten (DSB) benennen müssen. [Art. 37, §38 BDSG]	
☐	Datenschutzverantwortlichkeiten sind dokumentiert und den Mitarbeitenden bekannt. [Art. 24]	
☐	Wir haben interne Datenschutzrichtlinien (oder eine kombinierte Richtlinie) eingeführt. [Art. 24(2)]	

2 Verzeichnis von Verarbeitungstätigkeiten (VVT)

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Wir führen ein Verzeichnis von Verarbeitungstätigkeiten (VVT), das alle Verarbeitungen abdeckt. [Art. 30]	
☐	Jeder Eintrag nennt Zweck, Rechtsgrundlage, Datenkategorien, Empfänger, Aufbewahrung und TOM. [Art. 30(1)]	
☐	Das VVT wird mindestens jährlich und nach jeder neuen Verarbeitung überprüft und aktualisiert. [Art. 30]	
☐	Wir haben alle besonderen Datenkategorien identifiziert, die wir verarbeiten (Gesundheit, Biometrie usw.). [Art. 9]	

3

Rechtsgrundlage & Einwilligung

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Jede Verarbeitungstätigkeit hat eine dokumentierte Rechtsgrundlage (Art. 6). [Art. 6]	
☐	Wo wir uns auf Einwilligung stützen, ist sie freiwillig, spezifisch, informiert, unmissverständlich – und dokumentiert. [Art. 7]	
☐	Personen können die Einwilligung so einfach widerrufen, wie sie sie erteilt haben. [Art. 7(3)]	
☐	Wo wir uns auf berechnete Interessen stützen, haben wir eine Abwägung (LIA) durchgeführt. [Art. 6(1)(f)]	
☐	Verarbeitung besonderer Kategorien hat eine zusätzliche Bedingung nach Art. 9. [Art. 9(2)]	

4

Transparenz & Datenschutzhinweise

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Wir stellen betroffenen Personen einen klaren, zugänglichen Datenschutzhinweis bereit. [Art. 12-14]	
☐	Der Hinweis umfasst Identität, Zwecke, Rechtsgrundlagen, Empfänger, Übermittlungen, Aufbewahrung und Rechte. [Art. 13-14]	
☐	Hinweise werden bei der Datenerhebung gegeben (oder binnen eines Monats bei indirekter Erhebung). [Art. 14(3)]	
☐	Unser Website-Datenschutzhinweis ist aktuell und entspricht unserer tatsächlichen Verarbeitung. [Art. 12]	

5

Betroffenenrechte

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Wir haben einen dokumentierten Prozess für Auskunft, Berichtigung, Löschung, Einschränkung, Übertragbarkeit und Widerspruch. [Art. 15-22]	
☐	Wir können eine Anfrage binnen eines Monats beantworten (um zwei verlängerbar). [Art. 12(3)]	
☐	Wir überprüfen die Identität des Antragstellers vor der Datenoffenlegung. [Art. 12(6)]	
☐	Mitarbeitende wissen, wie sie eine Betroffenenanfrage erkennen und eskalieren. [Art. 12]	
☐	Wir können Lösch- und Übertragbarkeitsanfragen technisch erfüllen. [Art. 17, 20]	

6

Auftragsverarbeiter & Verträge

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Wir haben mit jedem Auftragsverarbeiter einen Auftragsverarbeitungsvertrag (AVV). [Art. 28]	
☐	Jeder AVV enthält die verpflichtenden Klauseln nach Art. 28(3). [Art. 28(3)]	
☐	Wir prüfen die Sicherheit von Auftragsverarbeitern vor Beauftragung (Due Diligence). [Art. 28(1)]	
☐	Unterauftragsverarbeiter sind genehmigt und gelistet. [Art. 28(2), (4)]	

7

Internationale Übermittlungen

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Wir haben alle Übermittlungen personenbezogener Daten außerhalb der EU/des EWR identifiziert. [Art. 44]	
☐	Jede Übermittlung hat eine gültige Garantie (Angemessenheit, SCC, BCR oder Ausnahme). [Art. 45-49]	
☐	Wo wir SCC nutzen, haben wir ein Transfer Impact Assessment (TIA) durchgeführt. [Art. 46]	
☐	Unser Datenschutzhinweis nennt die Drittländer, in die Daten übermittelt werden. [Art. 13(1)(f)]	

8

Sicherheit (TOM)

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Wir haben angemessene technische und organisatorische Maßnahmen umgesetzt. [Art. 32]	
☐	Der Zugriff auf personenbezogene Daten ist nach dem Need-to-know-Prinzip beschränkt. [Art. 32(1)(b)]	
☐	Personenbezogene Daten werden bei Übertragung und ggf. im Ruhezustand verschlüsselt. [Art. 32(1)(a)]	
☐	Wir haben unsere TOM dokumentiert (z. B. über die TOM-Checkliste). [Art. 32]	
☐	Wir testen, bewerten und überprüfen regelmäßig die Wirksamkeit unserer Maßnahmen. [Art. 32(1)(d)]	

9

Datenpannen

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Wir haben ein dokumentiertes Verfahren zur Reaktion auf Datenpannen. [Art. 33-34]	
☐	Mitarbeitende wissen, wie sie eine vermutete Panne intern und schnell melden. [Art. 33]	

9

Datenpannen

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Wir können die Aufsichtsbehörde bei Bedarf binnen 72 Stunden benachrichtigen. [Art. 33(1)]	
☐	Wir führen ein internes Pannenregister, auch für nicht gemeldete Pannen. [Art. 33(5)]	

10

DSFA & Datenschutz durch Technikgestaltung

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Wir prüfen, ob neue Verarbeitungen eine Datenschutz-Folgenabschätzung (DSFA) erfordern. [Art. 35]	
☐	Wir wenden Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen an. [Art. 25]	
☐	Hochrisiko-Verarbeitung ohne ausreichende Minderung löst eine vorherige Konsultation aus. [Art. 36]	

11

Aufbewahrung & Löschung

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Wir haben Aufbewahrungsfristen für jede Kategorie personenbezogener Daten definiert. [Art. 5(1)(e)]	
☐	Daten werden gelöscht oder anonymisiert, wenn die Aufbewahrungsfrist endet. [Art. 17]	
☐	Gesetzliche Aufbewahrungspflichten (z. B. Steuer-, Handelsrecht) sind dokumentiert. [Art. 17(3)(b)]	

12

Schulung & Sensibilisierung

ERL.	ANFORDERUNG	STATUS / NOTIZEN
☐	Mitarbeitende, die personenbezogene Daten verarbeiten, erhalten Datenschutzschulungen. [Art. 39(1)(b)]	
☐	Schulungen werden regelmäßig und beim Onboarding aufgefrischt. [Art. 24]	
☐	Wir dokumentieren, wer wann geschult wurde. [Art. 5(2)]	

Diese Checkliste dient nur als Orientierung und stellt keine Rechtsberatung dar. Sie basiert auf der Verordnung (EU) 2016/679 (DSGVO) und dem deutschen BDSG. Geprüft von einem zertifizierten Datenschutzbeauftragten (CIPP/E). Bereitgestellt von ETHYX – ethyx.eu. DSGVO-Höchststrafe: 20 Mio. € / 4 % des weltweiten Jahresumsatzes. Lassen Sie Ihre Compliance-Lage von einem qualifizierten Datenschutzbeauftragten oder Anwalt prüfen. Version 1.0 · Juni 2026.