



DATENSCHUTZ-SCHNELLCHECK

Für Unternehmen

Erste Standortbestimmung in ca. 15–20 Minuten

Was ist bereits gut aufgestellt?
Wo bestehen Lücken oder Unsicherheiten?
Welche Themen sollten Sie zuerst prüfen?

Kostenlose allgemeine Arbeitshilfe

Stand: 07. August 2026

So nutzen Sie den Schnellcheck

Gehen Sie die Prüffragen zügig durch und markieren Sie pro Frage genau eine Antwort. Der Schnellcheck ist bewusst als erste Standortbestimmung aufgebaut. Er ersetzt weder ein Datenschutz-Audit noch die Prüfung des konkreten Einzelfalls.

JA	TEILWEISE / UNKLAR	NEIN	N. R.
Anforderung erkennbar erfüllt	nicht vollständig oder Nachweis unklar	Handlungsbedarf	für Ihr Unternehmen nicht relevant

★ **Kernfrage:** Ein „Nein“ bei einer Kernfrage sollte unabhängig vom Gesamteindruck zeitnah geprüft werden.

Wichtig: Die Ampel am Ende ist nur eine Orientierung. Sie ist keine Rechtsbewertung, kein Auditurteil und keine Aussage über Bußgeld- oder Haftungsrisiken.

Ihre Angaben

Unternehmen	
Ansprechperson	
Datum	

1. Datenschutzorganisation und Verantwortung

u. a. Art. 5 Abs. 2, Art. 24, Art. 37–39 DSGVO; § 38 BDSG

Nr.	Prüffrage	Bewertung
1	★ Ist intern klar, wer Datenschutzthemen koordiniert und Entscheidungen dazu vorbereitet bzw. trifft?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
2	★ Ist geprüft und dokumentiert, ob eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter benannt werden muss, und ist die Benennung bei bestehender Pflicht ordnungsgemäß erfolgt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
3	Werden neue Prozesse, Software, Dienstleister und wesentliche Änderungen vor dem Start datenschutzrechtlich betrachtet?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
4	Gibt es einen regelmäßigen Termin oder Prüfzyklus, in dem Datenschutzmaßnahmen, offene Punkte und Änderungen überprüft werden?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

2. Verarbeitungsverzeichnis, Zwecke und Rechtsgrundlagen

u. a. Art. 5, Art. 6, Art. 9 und Art. 30 DSGVO

Nr.	Prüffrage	Bewertung
5	★ Ist ein aktuelles Verzeichnis der Verarbeitungstätigkeiten vorhanden, soweit erforderlich?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
6	Sind Zwecke, Datenkategorien, betroffene Personen, Empfänger, Löschfristen und wesentliche Schutzmaßnahmen nachvollziehbar dokumentiert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
7	★ Ist für jede wesentliche Verarbeitung eine tragfähige Rechtsgrundlage festgelegt und dokumentiert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
8	★ Werden besondere Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) gesondert geprüft und nur auf einer zulässigen Grundlage verarbeitet?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
9	Wird vor einer wesentlichen Zweckänderung geprüft, ob die weitere Verarbeitung zulässig ist?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

3. Transparenz und Betroffenenrechte

u. a. Art. 12–22 DSGVO

Nr.	Prüffrage	Bewertung
10	★ Erhalten betroffene Personen die erforderlichen Datenschutzinformationen, z. B. Kunden, Beschäftigte, Bewerber und Website-Nutzer?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

Nr.	Prüffrage	Bewertung
11	★ Gibt es einen festgelegten Ablauf für Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und Datenübertragbarkeit?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
12	Werden Identität, Eingang, Frist, Entscheidung und Antwort bei Betroffenenanfragen nachvollziehbar dokumentiert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
13	Ist bekannt, ob Profiling oder automatisierte Entscheidungen mit erheblicher Wirkung eingesetzt werden, und werden die zusätzlichen Anforderungen berücksichtigt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

4. Auftragsverarbeitung und externe Empfänger

u. a. Art. 26 und Art. 28 DSGVO

Nr.	Prüffrage	Bewertung
14	★ Sind alle wesentlichen Dienstleister identifiziert, die personenbezogene Daten im Auftrag verarbeiten?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
15	★ Bestehen mit Auftragsverarbeitern geeignete Verträge nach Art. 28 DSGVO und sind diese aktuell?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
16	Werden technische und organisatorische Maßnahmen, Unterauftragnehmer und wesentliche Vertragsänderungen der Auftragsverarbeiter geprüft?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
17	Ist bei gemeinsamen Projekten geklärt, ob eine gemeinsame Verantwortlichkeit vorliegt und ob eine Vereinbarung nach Art. 26 DSGVO erforderlich ist?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

5. Drittlandübermittlungen

u. a. Art. 44–49 DSGVO

Nr.	Prüffrage	Bewertung
18	★ Ist bekannt, ob personenbezogene Daten außerhalb des EWR verarbeitet werden, z. B. durch Cloud-, Support- oder Analyse-Dienste?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
19	★ Ist für relevante Drittlandübermittlungen eine zulässige Übermittlungsgrundlage dokumentiert, z. B. Angemessenheitsbeschluss oder Standardvertragsklauseln?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
20	Wird bei Bedarf geprüft, ob zusätzliche Schutzmaßnahmen oder eine Transfer-Risikobewertung erforderlich sind?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
21	Werden Änderungen bei Datenstandorten, Unterauftragnehmern und Supportzugriffen regelmäßig überprüft?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

6. Technische und organisatorische Maßnahmen (TOM)

u. a. Art. 25 und Art. 32 DSGVO

Nr.	Prüffrage	Bewertung
22	★ Sind Zugriffs- und Berechtigungskonzepte vorhanden und auf das erforderliche Maß beschränkt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
23	Werden angemessene Maßnahmen wie Mehr-Faktor-Authentisierung, sichere Passwortrichtlinien oder gleichwertige Schutzmechanismen eingesetzt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
24	Werden personenbezogene Daten bei Übertragung und Speicherung angemessen geschützt, z. B. durch Verschlüsselung, wenn dies erforderlich ist?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
25	★ Gibt es Datensicherungen und wurde die Wiederherstellung kritischer Daten und Systeme praktisch getestet?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
26	Werden Sicherheitsereignisse, Zugriffe und relevante Systemaktivitäten angemessen protokolliert bzw. überwacht?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
27	Gibt es geregelte Prozesse für Updates, Schwachstellen, Endgeräte, mobile Geräte und die sichere Vernichtung bzw. Rückgabe von Datenträgern?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

7. Aufbewahrung und Löschung

u. a. Art. 5 Abs. 1 lit. e und Art. 17 DSGVO; gesetzliche Aufbewahrungspflichten beachten

Nr.	Prüffrage	Bewertung
28	★ Sind für wesentliche Datenarten Aufbewahrungs- und Löschfristen festgelegt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
29	Werden gesetzliche Aufbewahrungspflichten und datenschutzrechtliche Löschpflichten aufeinander abgestimmt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
30	★ Werden Löschungen technisch umgesetzt und regelmäßig durchgeführt, einschließlich relevanter Fachsysteme und Ablagen?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
31	Ist dokumentiert, wie mit Daten in Backups, Archiven und bei Beendigung von Dienstleistungsverträgen umgegangen wird?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

8. Datenschutzverletzungen und Vorfälle

u. a. Art. 33 und Art. 34 DSGVO

Nr.	Prüffrage	Bewertung
32	★ Gibt es einen bekannten internen Meldeweg, damit Datenschutzverletzungen unverzüglich an die zuständige Stelle gemeldet werden?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
33	★ Kann innerhalb der gesetzlichen Fristen bewertet werden, ob eine Meldung an die Aufsichtsbehörde erforderlich ist?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
34	Ist geregelt, wann betroffene Personen informiert werden müssen?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
35	★ Werden Datenschutzverletzungen einschließlich Bewertung, Auswirkungen und Maßnahmen dokumentiert, auch wenn keine Behördenmeldung erfolgt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

9. Datenschutz-Folgenabschätzung und Risikoprüfung

u. a. Art. 35 und Art. 36 DSGVO

Nr.	Prüffrage	Bewertung
36	★ Wird vor neuen oder wesentlich geänderten risikoreichen Verarbeitungen geprüft, ob eine Datenschutz-Folgenabschätzung erforderlich ist?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
37	Gibt es für erforderliche Datenschutz-Folgenabschätzungen einen nachvollziehbaren Ablauf mit Beschreibung, Notwendigkeit, Risiken und Maßnahmen?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
38	Werden hohe verbleibende Risiken erkannt und wird gegebenenfalls eine vorherige Konsultation der Aufsichtsbehörde geprüft?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

10. Beschäftigtendatenschutz

u. a. Art. 5, 6, 9 und 88 DSGVO; § 26 BDSG; ggf. BetrVG

Nr.	Prüffrage	Bewertung
39	★ Sind Zugriffe auf Personal-, Bewerber- und Abwesenheitsdaten auf die erforderlichen Personen begrenzt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
40	Gibt es nachvollziehbare Lösch- und Aufbewahrungsregeln für Bewerber- und Beschäftigtendaten?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
41	Werden neue Systeme zur Leistungs-, Verhaltens- oder Personalauswertung vor Einführung datenschutzrechtlich geprüft und ggf. Mitbestimmungsrechte berücksichtigt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

Nr.	Prüffrage	Bewertung
42	Sind Veröffentlichungen von Beschäftigtenfotos, Videos oder Profilinformationen rechtlich geprüft und dokumentiert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

11. Website, Cookies, Marketing und Kommunikation

u. a. DSGVO; § 25 TDDDG; zusätzlich ggf. UWG

Nr.	Prüffrage	Bewertung
43	★ Ist die Datenschutzerklärung aktuell und bildet sie die tatsächlich eingesetzten Dienste, Formulare, Analyse-, Marketing- und Einbettungsfunktionen ab?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
44	★ Werden nicht unbedingt erforderliche Cookies bzw. Zugriffe auf Endgeräte erst nach wirksamer Einwilligung gesetzt, soweit § 25 TDDDG dies verlangt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
45	Ist ein vorhandenes Consent-Management so konfiguriert, dass Auswahl, Widerruf und Nachweis der Einwilligung nachvollziehbar sind?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
46	Werden Newsletter, Werbe-E-Mails, Tracking und ähnliche Marketingmaßnahmen nur auf einer zulässigen Grundlage durchgeführt und Abmeldungen zuverlässig umgesetzt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
47	Sind Kontaktformulare und eingebundene Drittanbieter technisch und datenschutzrechtlich angemessen abgesichert?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

12. Neue Systeme, KI und Änderungsmanagement

u. a. Art. 25, Art. 28, Art. 32 und Art. 35 DSGVO

Nr.	Prüffrage	Bewertung
48	★ Werden neue Software, Cloud-Dienste und KI-Anwendungen vor Nutzung auf Datenarten, Anbieterrolle, Speicherorte und Vertragsgrundlagen geprüft?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
49	★ Ist geregelt, ob personenbezogene oder vertrauliche Daten in KI-Systeme eingegeben werden dürfen und ob Anbieter diese Eingaben für eigene Zwecke bzw. Training verwenden?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
50	Werden datenschutzfreundliche Voreinstellungen und Datenminimierung bereits bei Auswahl und Konfiguration neuer Lösungen berücksichtigt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
51	Lösen wesentliche Änderungen bei Zweck, Anbieter, Datenkategorien oder Systemfunktion eine erneute Datenschutzprüfung aus?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

13. Schulung, Vertraulichkeit und regelmäßige Kontrolle

u. a. Art. 5 Abs. 2, Art. 24, Art. 32 und Art. 39 DSGVO

Nr.	Prüffrage	Bewertung
52	★ Werden Mitarbeitende regelmäßig und passend zu ihren Aufgaben zu Datenschutz und sicherem Umgang mit personenbezogenen Daten geschult?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
53	Sind Beschäftigte und externe Personen, soweit erforderlich, auf Vertraulichkeit verpflichtet bzw. entsprechend gebunden?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
54	Werden Datenschutzmaßnahmen regelmäßig überprüft und festgestellte Abweichungen nachvollziehbar nachverfolgt?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.
55	Sind wichtige Nachweise, Freigaben, Verträge, Prüfungen und Schulungsnachweise zentral auffindbar und aktuell?	☐ Ja ☐ Teilweise ☐ Nein ☐ N. r.

Schnellauswertung

Betrachten Sie nicht nur die Anzahl der Markierungen, sondern vor allem die Kernfragen (★) und die Themenbereiche, in denen mehrere Punkte „Teilweise / unklar“ oder „Nein“ markiert wurden.

GRÜN	Gute Grundlage Überwiegend „Ja“ und keine wesentliche Kernfrage mit „Nein“. Einzelne gelbe Punkte gezielt prüfen und den Stand regelmäßig aktualisieren.
GELB	Verbesserungsbedarf Mehrere Punkte sind nur teilweise geklärt oder einzelne Anforderungen fehlen. Prioritäten festlegen und Nachweise bzw. Prozesse nachziehen.
ORANGE	Deutlicher Handlungsbedarf Mindestens eine wichtige Kernfrage ist mit „Nein“ beantwortet oder mehrere Themenbereiche weisen Lücken auf. Strukturierte Prüfung und Maßnahmenplan sind sinnvoll.
ROT	Zeitnah prüfen Mehrere Kernfragen sind offen, grundlegende Dokumentationen fehlen oder wesentliche Risiken sind nicht bewertet. Datenschutz sollte zeitnah systematisch überprüft werden.

Ihre wichtigsten nächsten Schritte

1. _____
2. _____
3. _____
4. _____
5. _____

Kernfragen mit „Nein“ oder „unklar“

- _____
- _____
- _____

Wo steht Ihr Datenschutz heute?

Wenn der Schnellcheck offene Punkte zeigt, können Sie die Ergebnisse im ANDLIS-Orientierungsgespräch einordnen lassen. Sie erhalten eine verständliche erste Einschätzung, bevor Sie über weitere Schritte entscheiden.

Kein Verkaufsgespräch. Sondern Klarheit für Ihre nächsten Entscheidungen.

Hinweise zur Verwendung

Diese Checkliste ist eine allgemeine Arbeitshilfe zur ersten Orientierung. Sie erhebt keinen Anspruch auf Vollständigkeit für jede Branche, Rechtsform oder Verarbeitungssituation und ersetzt keine Prüfung des konkreten Einzelfalls. Aus einer Ampelfarbe lässt sich weder Datenschutzkonformität noch ein konkretes Haftungs- oder Bußgeldrisiko ableiten.

Je nach Tätigkeit können zusätzliche Vorschriften gelten, zum Beispiel Landesdatenschutzrecht, Beschäftigten- und Mitbestimmungsrecht, Sozial- oder Gesundheitsdatenschutz, kirchliches Datenschutzrecht, Berufsgeheimnisse sowie branchenspezifische Regelungen.

Bei neuen Technologien und KI-Anwendungen können neben der DSGVO weitere Anforderungen hinzukommen. Dieser Schnellcheck bewertet keine AI-Act-Risikoklasse und ersetzt kein AI-Compliance-Assessment.

Rechtsgrundlagen – Auswahl

- [Datenschutz-Grundverordnung \(EU\) 2016/679](#)
- [Bundesdatenschutzgesetz \(BDSG\)](#)
- [§ 38 BDSG – Datenschutzbeauftragte nichtöffentlicher Stellen](#)
- [Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz \(TDDDG\)](#)
- [§ 25 TDDDG – Schutz der Privatsphäre bei Endeinrichtungen](#)

Wichtige DSGVO-Themen in diesem Schnellcheck

Art. 5 und 24 Rechenschaftspflicht und Verantwortung · Art. 6 und 9 Rechtsgrundlagen · Art. 12–22 Betroffenenrechte · Art. 25 Datenschutz durch Technikgestaltung · Art. 26/28 gemeinsame Verantwortlichkeit und Auftragsverarbeitung · Art. 30 Verzeichnis der Verarbeitungstätigkeiten · Art. 32 Sicherheit der Verarbeitung · Art. 33/34 Datenschutzverletzungen · Art. 35/36 Datenschutz-Folgenabschätzung · Art. 37–39 Datenschutzbeauftragte · Art. 44–49 Drittlandübermittlungen.