Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

Bitte füllen Sie diese Checkliste so vollständig wie möglich aus. Sie dient als Grundlage für die erste Datenschutzbestandsaufnahme. Alle Angaben werden vertraulich behandelt.

Mandant (Organisation):

Ansprechpartner Datenschutz:

Branche:

Datum der Ausfüllung:

Anzahl Mitarbeitende:

A – Auftragsverarbeitungsverträge (AVV)

A1 Setzen Sie externe Dienstleister ein, die in Ihrem Auftrag personenbezogene Daten verarbeiten (z. B. Cloud, IT-Dienstleister, Steuerberater, Lohnbüro)?

☐ Ja ☐ Nein

A2 Bestehen mit diesen Dienstleistern bereits schriftliche AVV-Verträge?

☐ Ja ☐ Nein ☐ Teilweise

A3 Wie viele externe Auftragsverarbeiter sind aktuell im Einsatz (ca.)?

Antwort / Bemerkung:

A4 Können Sie eine Liste dieser Dienstleister bereitstellen?

☐ Ja ☐ Nein ☐ In Vorbereitung

A5 Werden AVV-Verträge regelmäßig überprüft oder aktualisiert?

☐ Ja ☐ Nein ☐ Unbekannt

B – Betroffenenrechte & Betroffenenanfragen

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

B1 Existiert ein definierter Prozess für den Umgang mit Betroffenenanfragen (Auskunft, Löschung, Berichtigung etc.)?

☐ Ja ☐ Nein

B2 Wurde bisher eine Betroffenenanfrage gestellt?

☐ Ja ☐ Nein

B3 Wenn ja: Wie wurde damit umgegangen?

Antwort / Bemerkung:

B4 Ist eine verantwortliche Person für die Bearbeitung von Anfragen benannt?

☐ Ja ☐ Nein

B5 Sind Mitarbeitende über Betroffenenrechte informiert?

☐ Ja ☐ Nein ☐ Unklar

C – Cookie-Management & Website-Tracking

C1 Betreiben Sie eine eigene Website?

☐ Ja ☐ Nein

C2 URL(s) der Website(s):

Antwort / Bemerkung:

C3 Ist ein Cookie-Consent-Banner/Tool vorhanden?

☐ Ja ☐ Nein

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

C4 Welche Tracking-Tools werden eingesetzt (z. B. Google Analytics, Meta Pixel, Matomo)?

Antwort / Bemerkung:

C5 Werden auf der Website Kontaktformulare, Newsletter-Anmeldungen oder Shops betrieben?

☐ Ja ☐ Nein

C6 Wer ist technisch für die Website verantwortlich (intern/extern)?

Antwort / Bemerkung:

D – Datenschutzerklärung

D1 Ist eine Datenschutzerklärung auf der Website vorhanden?

☐ Ja ☐ Nein

D2 Wann wurde die Datenschutzerklärung zuletzt aktualisiert?

Antwort / Bemerkung:

D3 Deckt die Datenschutzerklärung alle aktuellen Verarbeitungstätigkeiten ab?

☐ Ja ☐ Nein ☐ Unbekannt

D4 Existiert eine Datenschutzerklärung auch für Bewerber, Mitarbeitende oder Kunden?

☐ Ja ☐ Nein ☐ Teilweise

E – Einwilligungen

E1 Werden personenbezogene Daten auf Basis von Einwilligungen verarbeitet (z. B. Newsletter, Fotos, Werbung)?

☐ Ja ☐ Nein

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

E2 Werden Einwilligungen schriftlich oder nachweisbar dokumentiert?

☐ Ja ☐ Nein

E3 Gibt es eine Möglichkeit für Betroffene, eine Einwilligung zu widerrufen?

☐ Ja ☐ Nein

E4 Werden Einwilligungen von Minderjährigen eingeholt? Falls ja: Wie?

☐ Ja ☐ Nein

Antwort / Bemerkung:

E5 Werden veraltete Einwilligungen regelmäßig überprüft?

☐ Ja ☐ Nein

F – Fotos, Film & Videoüberwachung

F1 Werden Fotos oder Videos von Mitarbeitenden, Kunden oder Veranstaltungen erstellt und verwendet?

☐ Ja ☐ Nein

F2 Liegt dafür eine dokumentierte Einwilligung vor?

☐ Ja ☐ Nein ☐ Teilweise

F3 Betreiben Sie Videoüberwachung (z. B. Kameras in Gebäuden oder auf dem Gelände)?

☐ Ja ☐ Nein

F4 Falls ja: Sind Hinweisschilder vorhanden und Speicherfristen definiert?

☐ Ja ☐ Nein

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

F5 Wer hat Zugriff auf Videoaufzeichnungen?

Antwort / Bemerkung:

G – Gemeinsame Verantwortlichkeit (Joint Controllership)

G1 Verarbeiten Sie personenbezogene Daten gemeinsam mit anderen Unternehmen oder Organisationen?

☐ Ja ☐ Nein

G2 Beispiele: gemeinsame Social-Media-Seiten, konzernweite Systeme, Kooperationspartner?

Antwort / Bemerkung:

G3 Existieren dafür Vereinbarungen nach Art. 26 DSGVO?

☐ Ja ☐ Nein ☐ Unbekannt

H – HR / Beschäftigtendatenschutz

H1 Wie viele Mitarbeitende (inkl. Minijobber, Praktikanten) sind beschäftigt?

Antwort / Bemerkung:

H2 Werden Personalakten digital oder in Papierform geführt?

☐ Digital ☐ Papier ☐ Beides

H3 Welche Software wird für Lohn-/Gehaltsabrechnung genutzt?

Antwort / Bemerkung:

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

H4 Werden Zeiterfassungssysteme eingesetzt?

☐ Ja ☐ Nein

Antwort / Bemerkung:

H5 Werden Bewerberdaten datenschutzkonform verwaltet und fristgerecht gelöscht?

☐ Ja ☐ Nein ☐ Unklar

H6 Sind Mitarbeitende auf Vertraulichkeit/Datenschutz verpflichtet worden?

☐ Ja ☐ Nein

I – IT-Sicherheit & Informationssicherheit

I1 Existiert ein Virenschutz auf allen genutzten Endgeräten?

☐ Ja ☐ Nein ☐ Teilweise

I2 Wird eine Firewall eingesetzt?

☐ Ja ☐ Nein ☐ Unbekannt

I3 Werden regelmäßige Datensicherungen (Backups) durchgeführt?

☐ Ja ☐ Nein

I4 Werden Backups regelmäßig auf Wiederherstellbarkeit getestet?

☐ Ja ☐ Nein

I5 Gibt es ein Patch-/Update-Management für Software und Betriebssysteme?

☐ Ja ☐ Nein

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

I6 Ist der Zugang zu IT-Systemen durch starke Passwörter und/oder Multi-Faktor-Authentifizierung geschützt?

☐ Ja ☐ Nein ☐ Teilweise

I7 Wird ein zentrales Passwort-Management-Tool genutzt?

☐ Ja ☐ Nein

Antwort / Bemerkung:

J – Juristische Rechtsgrundlagen der Verarbeitung

J1 Sind die Rechtsgrundlagen für Ihre wesentlichen Datenverarbeitungen bekannt (Art. 6 DSGVO)?

☐ Ja ☐ Nein ☐ Teilweise

J2 Werden besondere Kategorien personenbezogener Daten verarbeitet (z. B. Gesundheit, Religion, Gewerkschaft, biometrische Daten)?

☐ Ja ☐ Nein

J3 Falls ja: Auf welcher Grundlage (Art. 9 DSGVO)?

Antwort / Bemerkung:

J4 Sind Ihnen branchenspezifische Datenschutzvorschriften bekannt (z. B. SGB, KDG, ärztliche Schweigepflicht)?

☐ Ja ☐ Nein

K – Kommunikation, E-Mail & Messenger

K1 Welche E-Mail-Dienste werden genutzt (z. B. Microsoft 365, Google Workspace, eigener Server)?

Antwort / Bemerkung:

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

K2 Werden geschäftliche Messenger-Dienste genutzt (z. B. WhatsApp, Signal, Teams, Slack)?

☐ Ja ☐ Nein

Antwort / Bemerkung:

K3 Ist der E-Mail-Verkehr verschlüsselt (TLS, Ende-zu-Ende)?

☐ Ja ☐ Nein ☐ Unbekannt

K4 Werden personenbezogene Daten per E-Mail an Externe übermittelt?

☐ Ja ☐ Nein

K5 Gibt es Regelungen zur privaten Nutzung von Firmengeräten und -kommunikation?

☐ Ja ☐ Nein

L – Löschkonzept & Aufbewahrungsfristen

L1 Existiert ein Löschkonzept oder eine Übersicht über Aufbewahrungsfristen?

☐ Ja ☐ Nein

L2 Werden Daten nach Ablauf der Fristen tatsächlich gelöscht oder gesperrt?

☐ Ja ☐ Nein ☐ Manuell ☐ Automatisch

L3 Wie werden Papierdokumente mit personenbezogenen Daten vernichtet (z. B. Aktenvernichter, Dienstleister)?

Antwort / Bemerkung:

L4 Werden auch digitale Altdaten regelmäßig bereinigt?

☐ Ja ☐ Nein

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

M – Meldepflichten bei Datenpannen

M1 Gab es in der Vergangenheit Datenpannen oder Sicherheitsvorfälle?

☐ Ja ☐ Nein

M2 Falls ja: Wurden diese der zuständigen Aufsichtsbehörde gemeldet?

☐ Ja ☐ Nein ☐ Nicht notwendig

M3 Existiert ein internes Verfahren/Prozess für die Erkennung und Meldung von Datenpannen?

☐ Ja ☐ Nein

M4 Wissen die Mitarbeitenden, was im Fall einer Datenpanne zu tun ist?

☐ Ja ☐ Nein

M5 Welche Aufsichtsbehörde ist für Ihre Organisation zuständig?

Antwort / Bemerkung:

N – Newsletter & Marketing

N1 Werden Newsletter oder E-Mail-Marketing-Kampagnen durchgeführt?

☐ Ja ☐ Nein

N2 Welches Tool wird genutzt (z. B. Mailchimp, CleverReach, HubSpot)?

Antwort / Bemerkung:

N3 Erfolgt die Anmeldung per Double-Opt-in?

☐ Ja ☐ Nein

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

N4 Ist ein AVV mit dem Newsletter-Dienstleister abgeschlossen?

☐ Ja ☐ Nein

N5 Können Empfänger sich einfach abmelden (Opt-out)?

☐ Ja ☐ Nein

O – Organigramm & interne Zuständigkeiten

O1 Existiert ein aktuelles Organigramm der Organisation?

☐ Ja ☐ Nein

O2 Gibt es eine klare interne Zuständigkeit für Datenschutzfragen?

☐ Ja ☐ Nein

Antwort / Bemerkung:

O3 Ist ein interner oder externer Datenschutzbeauftragter bestellt?

☐ Intern ☐ Extern ☐ Nein

O4 Sind datenschutzrelevante Rollen (z. B. Systemadministrator, HR-Leitung) definiert?

☐ Ja ☐ Nein

P – Prozesse & Verarbeitungstätigkeiten

P1 Welche Hauptprozesse Ihrer Organisation beinhalten die Verarbeitung personenbezogener Daten?

Antwort / Bemerkung:

P2 Verarbeiten Sie Daten von Kunden, Interessenten, Lieferanten, Mitarbeitenden oder anderen Personen?

☐ Kunden ☐ Mitarbeitende ☐ Lieferanten ☐ Sonstige

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

P3 Werden personenbezogene Daten in die EU/EWR oder in Drittländer übermittelt?

☐ Nur EU/EWR ☐ Auch Drittländer

Antwort / Bemerkung:

P4 Werden automatisierte Entscheidungen (z. B. Scoring, Profiling) getroffen?

☐ Ja ☐ Nein

Q – Qualitätssicherung im Datenschutzmanagement

Q1 Existiert ein Datenschutzkonzept oder eine Datenschutzrichtlinie?

☐ Ja ☐ Nein

Q2 Werden Datenschutzmaßnahmen intern regelmäßig überprüft oder auditiert?

☐ Ja ☐ Nein

Q3 Sind Datenschutzthemen in interne Prozesse und Projekte eingebettet (Privacy by Design)?

☐ Ja ☐ Nein ☐ Teilweise

Q4 Gibt es ein internes Datenschutzhandbuch oder vergleichbare Dokumentation?

☐ Ja ☐ Nein

R – Risikoanalyse & Datenschutz-Folgenabschätzung (DSFA)

R1 Wurden für Verarbeitungstätigkeiten Risikoanalysen durchgeführt?

☐ Ja ☐ Nein

R2 Wurden Verarbeitungen identifiziert, die voraussichtlich ein hohes Risiko für Betroffene darstellen?

☐ Ja ☐ Nein ☐ Unbekannt

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

R3 Wurde in solchen Fällen eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt?

☐ Ja ☐ Nein ☐ Nicht notwendig

R4 Sind Ergebnisse der DSFA dokumentiert?

☐ Ja ☐ Nein

S – Schulungen & Sensibilisierung der Mitarbeitenden

S1 Werden Mitarbeitende regelmäßig zum Thema Datenschutz geschult?

☐ Ja ☐ Nein

S2 Wie erfolgen die Schulungen (Präsenz, Online, intern, extern)?

Antwort / Bemerkung:

S3 Wann fand die letzte Datenschutzschulung statt?

Antwort / Bemerkung:

S4 Werden neue Mitarbeitende beim Onboarding zum Datenschutz unterwiesen?

☐ Ja ☐ Nein

S5 Werden Schulungsnachweise dokumentiert?

☐ Ja ☐ Nein

T – Technisch-organisatorische Maßnahmen (TOM)

T1 Existiert eine Dokumentation der technisch-organisatorischen Maßnahmen (TOM)?

☐ Ja ☐ Nein

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

T2 Ist der Zugang zu Gebäuden und Serverräumen gesichert (Zutrittskontrolle)?

☐ Ja ☐ Nein

T3 Gibt es Regelungen zum Sperren von Bildschirmen bei Abwesenheit?

☐ Ja ☐ Nein

T4 Werden mobile Geräte (Laptops, Smartphones) verschlüsselt?

☐ Ja ☐ Nein ☐ Teilweise

T5 Gibt es ein Berechtigungskonzept – wer hat Zugriff auf welche Daten?

☐ Ja ☐ Nein

T6 Werden Aktivitäten in IT-Systemen protokolliert (Logging)?

☐ Ja ☐ Nein

U – Unterauftragnehmer & Drittlandtransfers

U1 Setzen Ihre Auftragsverarbeiter ihrerseits Unterauftragnehmer ein?

☐ Ja ☐ Nein ☐ Unbekannt

U2 Werden personenbezogene Daten in Länder außerhalb der EU/EWR übermittelt (z. B. USA, Indien)?

☐ Ja ☐ Nein

U3 Falls ja: Auf welcher Grundlage (z. B. Standardvertragsklauseln, Angemessenheitsbeschluss)?

Antwort / Bemerkung:

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

U4 Sind die Drittlandtransfers in der Datenschutzdokumentation erfasst?

☐ Ja ☐ Nein

V – Verarbeitungsverzeichnis (VVT)

V1 Existiert ein Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO?

☐ Ja ☐ Nein

V2 Wird das Verzeichnis aktuell gehalten?

☐ Ja ☐ Nein ☐ Unbekannt

V3 In welchem Format liegt das Verzeichnis vor (Excel, Word, Software)?

Antwort / Bemerkung:

V4 Ist das Verzeichnis für alle wesentlichen Verarbeitungen vollständig?

☐ Ja ☐ Nein ☐ Teilweise

W – Website, Social Media & Online-Auftritte

W1 Auf welchen Plattformen sind Sie mit Unternehmensprofilen aktiv (z. B. LinkedIn, Instagram, Facebook, Xing)?

Antwort / Bemerkung:

W2 Werden auf Social Media personenbezogene Daten von Followern oder Kunden verarbeitet?

☐ Ja ☐ Nein

W3 Sind Social-Media-Profile in der Datenschutzerklärung berücksichtigt?

☐ Ja ☐ Nein

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

W4 Werden auf der Website Daten in die USA übermittelt (z. B. durch Google Fonts, YouTube, reCAPTCHA)?

☐ Ja ☐ Nein ☐ Unbekannt

W5 Ist ein Impressum vorhanden und aktuell?

☐ Ja ☐ Nein

X – eXterne Dienstleister & Cloud-Dienste

X1 Welche Cloud-Dienste werden eingesetzt (z. B. Microsoft 365, Google Workspace, Dropbox)?

Antwort / Bemerkung:

X2 Sind mit allen Cloud-Anbietern AVV-Verträge abgeschlossen?

☐ Ja ☐ Nein ☐ Teilweise

X3 Welche externen Dienstleister haben Zugang zu Ihren IT-Systemen oder Daten (z. B. IT-Support, Buchhaltung, Steuerberater)?

Antwort / Bemerkung:

X4 Werden externe Zugriffe protokolliert und kontrolliert?

☐ Ja ☐ Nein

Y – sYsteme & Software-Inventar

Y1 Welche zentralen Softwaresysteme werden eingesetzt (z. B. CRM, ERP, Buchhaltung, Warenwirtschaft)?

Antwort / Bemerkung:

Y2 Welche Betriebssysteme sind im Einsatz?

Antwort / Bemerkung:

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

Y3 Werden veraltete oder nicht mehr unterstützte Systeme genutzt?

☐ Ja ☐ Nein ☐ Unbekannt

Y4 Gibt es ein Inventar aller IT-Assets (Hardware und Software)?

☐ Ja ☐ Nein

Y5 Werden KI-Tools oder KI-basierte Dienste eingesetzt (z. B. ChatGPT, Copilot, KI-Analyse-Tools)?

☐ Ja ☐ Nein

Antwort / Bemerkung:

Z – Zeitmanagement & Fristen im Datenschutz

Z1 Ist bekannt, dass Betroffenenanfragen innerhalb von 1 Monat beantwortet werden müssen?

☐ Ja ☐ Nein

Z2 Ist bekannt, dass Datenpannen innerhalb von 72 Stunden der Aufsichtsbehörde gemeldet werden müssen?

☐ Ja ☐ Nein

Z3 Gibt es eine interne Fristenübersicht oder einen Datenschutz-Kalender?

☐ Ja ☐ Nein

Z4 Werden Datenschutzthemen regelmäßig in Meetings oder im Qualitätsmanagement berücksichtigt?

☐ Ja ☐ Nein

Z5 In welchen Abständen soll der Datenschutzbeauftragte regelmäßig berichten oder prüfen?

☐ Monatlich ☐ Quartalsweise ☐ Jährlich ☐ Nach Bedarf

Abschluss & Unterschrift

Datenschutz-Ersterfassung

Interaktive Checkliste für neue Mandanten

Ergänzende Hinweise / Anmerkungen des Mandanten:

Ort, Datum:

Name und Funktion:

Unterschrift: