

VVT-Checkliste DSGVO

Systematische Anleitung zur Erstellung und Pflege eines DSGVO-konformen Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DSGVO mit allen Pflichtangaben und praktischen Prüfpunkten für Unternehmen.

Diese Checkliste führt Sie Schritt für Schritt durch die Erstellung eines vollständigen Verzeichnisses von Verarbeitungstätigkeiten (VVT). Haken Sie alle erledigten Schritte ab und vermeiden Sie typische Fehler.

Phase 1: Vorbereitung & Strukturierung

- Unternehmen in Bereiche strukturiert (z. B. Personalwesen, Marketing, IT, Buchhaltung)
- Verantwortliche für jeden Bereich benannt (Ansprechpartner identifiziert)
- Alle Anwendungen, Software-Tools und Systeme aufgelistet
- Excel-Vorlage oder Datenschutz-Software ausgewählt

Phase 2: Datenerfassung

- Fachabteilungen systematisch befragt
- Alle Verarbeitungstätigkeiten dokumentiert (inkl. Website-Tracking, Cloud-Speicher)
- Externe Dienstleister erfasst (Hosting, Newsletter, CRM, Lohnbüro)
- Automatisierte Verarbeitungen identifiziert

Phase 3: Pflichtangaben nach Art. 30 DSGVO

- Name & Kontaktdaten des Verantwortlichen eingetragen
- Kontaktdaten des Datenschutzbeauftragten hinterlegt
- Zweck der Verarbeitung für jeden Prozess beschrieben
- Rechtsgrundlagen korrekt zugeordnet (Art. 6 Abs. 1 lit. a-f DSGVO)
- Kategorien betroffener Personen spezifisch genannt (Kunden, Mitarbeiter, Bewerber)
- Kategorien personenbezogener Daten detailliert aufgelistet
- Kategorien von Empfängern dokumentiert (intern und extern)
- Drittlandtransfers erfasst (inkl. Garantien wie SCC)
- Löschfristen für alle Prozesse definiert

Phase 4: TOM-Beschreibung

- Zutrittskontrolle beschrieben (physischer Zugang zu Räumen)
- Zugangskontrolle dokumentiert (Passwortschutz, Firewall)
- Zugriffskontrolle definiert (Berechtigungskonzept)
- Weitergabekontrolle geregelt (Verschlüsselung, VPN)
- Eingabekontrolle festgelegt (Protokollierung)
- Verfügbarkeitskontrolle gesichert (Backups, USV)
- Trennungskontrolle umgesetzt (Mandantentrennung)

Phase 5: Verweise & Struktur

- Verweise auf Datenschutzkonzept gesetzt
- DSFA (Datenschutz-Folgenabschätzung) bei Hochrisikoverarbeitungen durchgeführt
- Auftragsverarbeitungsverträge (AVV) mit allen Dienstleistern geschlossen
- VVT als Loseblattwerk strukturiert (ein Formblatt pro Prozess)

Phase 6: Qualitätssicherung

Typische Fehler vermeiden:

- Alle Verarbeitungsprozesse vollständig erfasst (auch Tracking, Cloud, Social Media)
- Rechtsgrundlagen konkret benannt (nicht pauschal 'berechtigtes Interesse')
- Beschreibungen spezifisch formuliert (nicht 'Kundendaten', sondern 'Name, E-Mail, ...')
- TOM konkret beschrieben (nicht nur 'Datensicherheit wird gewährleistet')
- Alle Drittlandtransfers mit Garantien dokumentiert
- Löschfristen realistisch und rechtlich zulässig

Phase 7: Pflege & Aktualisierung

- Verantwortlicher für VVT-Pflege benannt
- Jährliche Erinnerung zur Überprüfung gesetzt
- Prozess für sofortige Aktualisierung bei Änderungen etabliert
- Vorversionen des VVT archiviert (mindestens 1 Jahr zurück)
- VVT zentral gespeichert und innerhalb 72 Stunden abrufbar

Phase 8: Behörden-Prüfungsmappe

Diese Dokumente müssen bei Anforderung vorgelegt werden:

- Vollständiges VVT
- TOM-Dokumentation (Art. 32 DSGVO)
- DSFA bei Hochrisikoverarbeitungen (Art. 35 DSGVO)
- Löschkonzept
- Alle Auftragsverarbeitungsverträge (AVV)
- Datenschutzkonzept
- Nachweise über Einwilligungen (Art. 7 DSGVO)

Wichtig: Bei fehlendem oder unvollständigem VVT drohen Bußgelder bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes nach Art. 83 Abs. 4 lit. a DSGVO. Diese Checkliste ersetzt keine individuelle Datenschutzberatung.