SHARED IT PROFESSIONAL

münchow commandeur + partner

Rechtsanwälte | Fachanwälte

Partnerschaftsgesellschaft mbB

Einführung zur Europäischen Datenschutzgrundverordnung (EU-DSGVO)

Agenda

- Die zu erfüllenden Grundprinzipien der DSGVO
- Erstellung Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO
- IT-Sicherheit Pflichten nach der DSGVO Art. 30, 32 (EDV, Webseite u.a.)
- Gemeinsame Verantwortung der Verarbeiter von personenbez. Daten Art 26 DSGVO
- Weitergabe und Dienst-Hardware, private Nutzung und BYOD
- Sichere Übermittlungen von Personenbezogenen Daten in Drittländer nach DSGVO
- Vertragswesen, Einwilligungen und Notwendigkeiten der Anpassung von Verträgen

Die Grundregeln aus Art. 5 DSGVO

- Rechtmäßigkeit, Treu und Glauben
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Vertraulichkeit und Integrität
- Rechenschaftspflicht

Art. 30 DSGVO, Verzeichnis der Verarbeitungstätigkeiten für Verantwortliche und Auftragsverarbeiter (DL)

Dokumentation aller wesentlichen Verarbeitungstätigkeiten pbD -> entscheidende Neuerung der DSGVO, der Nachweis des Art.5

Dient der Rechtmäßigkeitskontrolle durch Aufsichtsbehörden

Unterlassung ist sanktionsfähiger Rechtsverstoß, Art. 58, 83 DSGVO

Unter anderem Verarbeitungszweck definieren, um den zulässigen Umfang der Verarbeitung darzustellen

Beweislastumkehr: Rechenschaftspflicht aus Art. 5 Abs.2 DSGVO

Insofern zentrales Werkzeug zur Umsetzung der Datenschutzpflichten

Definition

Das Verarbeitungsverzeichnis dient der Transparenz über die Verarbeitung personenbezogener Daten und der rechtlichen Absicherung des Unternehmens. Es dient dem betrieblichen Datenschutzbeauftragten, sowie der Aufsichtsbehörde zur Erfüllung ihrer Aufgaben. Der Verantwortliche oder der Auftragsverarbeiter stellen nach Art. 30 Abs. 4 DS-GVO das Verarbeitungsverzeichnis der Aufsichtsbehörde auf Anfrage zur Verfügung. Das Verarbeitungsverzeichnis dient gegenüber der Aufsichtsbehörde zum Nachweis, dass die Vorschriften der DS-GVO vom Verantwortlichen eingehalten wurden. Dies gehört zu der generellen Pflicht des Verantwortlichen, mit der Aufsichtbehörde bei der Erfüllung ihrer Aufgabe auf Anfrage zusammenzuarbeiten (Art. 31 DS-GVO).

Das Verarbeitungsverzeichnis ist somit gleichermaßen Grundlage zur Erfüllung unternehmerischer Pflichten eines Verantwortlichen oder eines **Auftragsverarbeiters** und Hilfsmittel der Tätigkeit von deren Datenschutzbeauftragten.

Umsetzung und Gestaltung

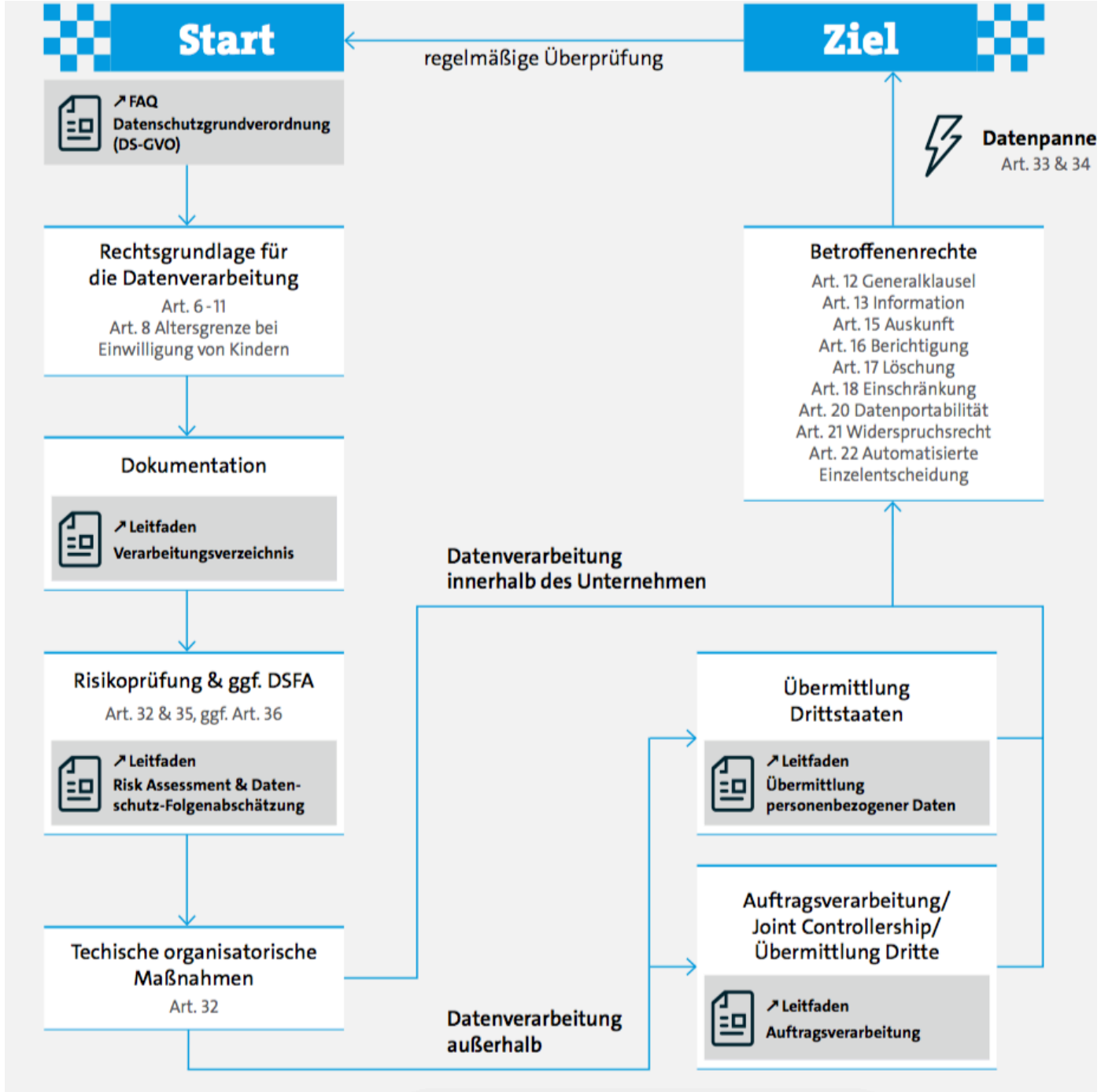
Verfahrensverzeichnis nach Bestandsaufnahme aller Verfahren (GAP) erstellen, dazu zunächst:

Dienstleisterverzeichnis erstellen, Dienstleister nach Beziehung (ADV, NDA..) bewerten, Dienstleister entsprechend verpflichten.

Softwareverzeichnis erstellen, Software nach privacy by design / p.b. default bewerten, Dokumentation nach Art. 32 DSGVO

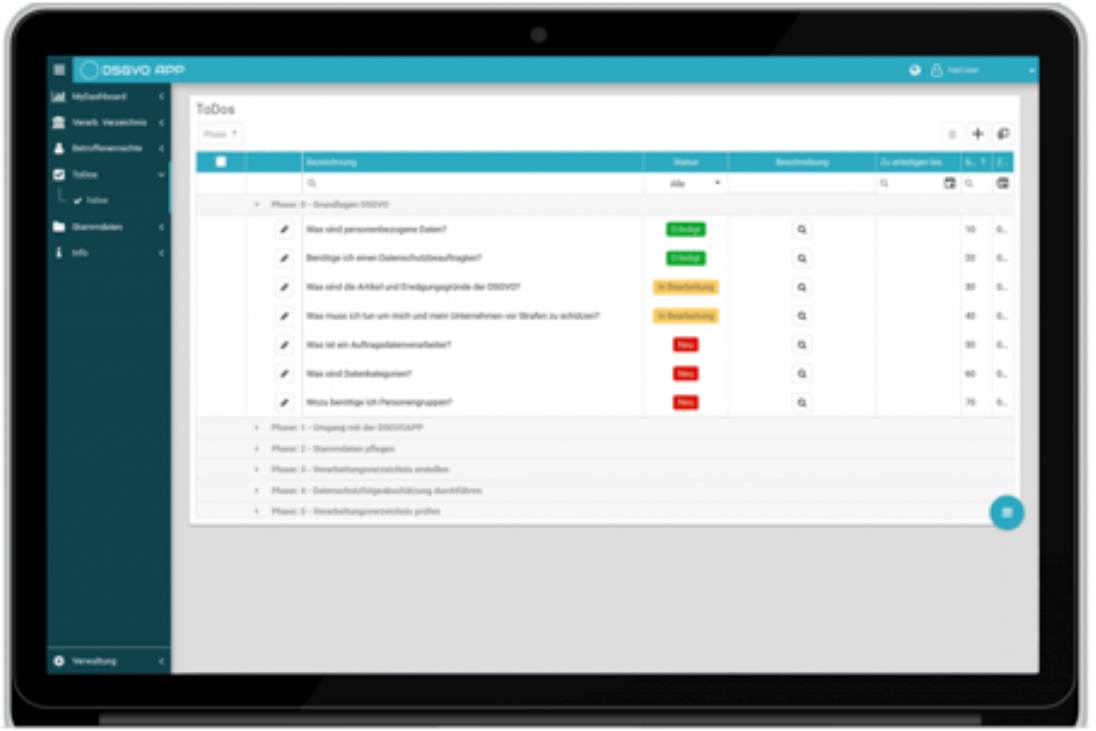
Verweis auf TOM (technische- organisatorische Maßnahmen) in Art. 30. DSGVO -> Inhalt orientiert sich nach Art. 32. DSGVO, TOM – Dokumentation erstellen.

Nutzung von Datenschutzmanagement Software zur Dokumentation


Start
regelmäßige Überprüfung
Ziel
↗ FAQ
Datenschutzgrundverordnung (DS-GVO)
Datenpanne
Art. 33 & 34
Rechtsgrundlage für die Datenverarbeitung
Art. 6 - 11
Art. 8 Altersgrenze bei Einwilligung von Kindern
Betroffenenrechte
Art. 12 Generalklausel
Art. 13 Information
Art. 15 Auskunft
Art. 16 Berichtigung
Art. 17 Löschung
Art. 18 Einschränkung
Art. 20 Datenportabilität
Art. 21 Widerspruchsrecht
Art. 22 Automatisierte Einzelentscheidung
Dokumentation
↗ Leitfaden
Verarbeitungsverzeichnis
Datenverarbeitung innerhalb des Unternehmen
Risikoprüfung & ggf. DSFA
Art. 32 & 35, ggf. Art. 36
↗ Leitfaden
Risk Assessment & Daten-schutz-Folgenabschätzung
Übermittlung Drittstaaten
↗ Leitfaden
Übermittlung personenbezogener Daten
Auftragsverarbeitung/ Joint Controllership/ Übermittlung Dritte
↗ Leitfaden
Auftragsverarbeitung
Techische organisatorische Maßnahmen
Art. 32
Datenverarbeitung außerhalb

Verzeichnis der Verarbeitungstätigkeiten Art. 30 DSGVO

- Titel
- Zweck
- Rechtsgrundlage
- Inhalt der Verarbeitung (Datenkategorien)
- Betroffene Personen
- Empfänger (in/ex/Drittland)
- Löschfristen
- Technische Besonderheiten
- DSFA (Datenschutzfolgeabschätzung)



Datenschutzmanagementsoftware

Umsetzung und Gestaltung

- Aufbau eines Datenschutzmanagement-Teams
- Datenschutzkommunikation, einschließlich Geschäftsleitung (Haftung)
- Einbeziehung des Datenschutzbeauftragten, ggf. Bestellung
- Unabhängiges IT-Security Audit -> Maßnahmenkatalog
- Vertragswesen: Prüfung aller rechtlichen Regelungen zum Datenschutz, einschl. Einwilligungen, bestehende Verträge, Vorlagen, AGB, Webseite, Datenschutzrichtlinie, Nutzungsbedingungen und Nutzungsvereinbarungen
- Ggf. ISO (27001) nutzen

Umsetzung und Gestaltung: Verzeichnis der Verarbeitungstätigkeiten Art. 30 DSGVO

- Eindeutige Bezeichnung der dokumentierten Verarbeitung/der Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden.
- Zwecke: *Verarbeitungstätigkeit*: „Allgemeine Kundenverwaltung“; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“ *Verarbeitungstätigkeit*: „Customer-Relationship-Management“; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Kundenbeziehungen, Marketing, Neukundenakquise, Kundenbindungsmaßnahmen, Kundenberatung, Beschwerdemanagement, Kündigungsprozess“

Umsetzung und Gestaltung: Verzeichnis der Verarbeitungstätigkeiten Art. 30 DSGVO

- Die Nennung der einschlägigen Rechtsgrundlage ist für Accountability-Pflichten und die Gewährleistung von Transparenzpflichten ggü. betroffenen Personen notwendig.
- Nennung der betroffenen Personen und die jeweils auf sie bezogenen verwendeten Daten oder Datenkategorien.
- Empfänger der Daten nennen, weitere Fachabteilungen, Vertragspartner, Kunden, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleis- tungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.
- Übermittlungen in Drittländer angeben
- Aufbewahungsfristen, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich. Soweit diese in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.

Umsetzung und Gestaltung: Verzeichnis der Verarbeitungstätigkeiten Art. 30 DSGVO

- Im Hinblick auf die vielfältigen Nachweispflichten, denen das Unternehmen im Datenschutz unterliegt, kann es sinnvoll sein, weitere Aspekte zur Verarbeitungstätigkeit zu dokumentieren. Diese sind nur intern zu verwenden. Zu diesen zusätzlichen Dokumentationen, die sinnvollerweise hier erfolgen, gehören z. B.
- Angaben zur Zusammenstellung der Informationspflichten (insbes. Art. 13,14 DS-GVO)
- Verträge mit Dienstleistern (Art. 28 DS-GVO)
- Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DS-GVO)
- **>>** Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen
- **>>** durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DS-GVO)

Art. 26 DSGVO gemeinsame Verantwortung

- Definition, Zweck und Mittel durch mehr als einen festgelegt
- Vereinbarungen aus dem Innenverhältnis („wesentliche der Vereinbarung“) werden dem betroffenen (im Sinne der Art.12-15 DSGVO) zur Wahrnehmung seiner Rechte nach jeweiligen Zuständigkeiten der Verantwortlichen, dargestellt.

Übermittlung von Daten in Drittländer

- Drittland nach DSGVO: außerhalb EU - > Geltungsbereich DSGVO
- Definition Übermittlung: Weitergabe an Dritte (Art.4. Nr. 10 DSGVO)
- Definition Auftragsverarbeiter und Verantwortlicher
- Übermittlung in technischer Hinsicht (Verschlüsselungspflicht Art 32 DSGVO), Übermittlung an Schiffe aus Sicht der Aufsichtsbehörde
- Zweistufige Prüfung: Zulässigkeit der Verarbeitung und Übermittlung der Daten in Drittstaaten nach geeigneten Garantien.
    - Standardvertragsklauseln der EU (STANDARD CONTRACTUAL CLAUSES (PROCESSORS))
- Auftragsvergabe an Auftragsverarbeiter außerhalb EU
  „Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.“

IT Sicherheit, Art. 30,32 DSGVO

- Verpflichtung aus der DSGVO auf Integrität und Vertraulichkeit Art.5.1.f) im Zusammenhang mit der Rechenschaftspflicht.
- Bußgeldrisiken (2%) , Meldepflichten, Notfallplanung
- Verpflichtung der Auftragsverarbeiter / Dienstleister Art. 28 DSGVO

  -> „Erfolgt eine **Verarbeitung im Auftrag eines Verantwortlichen**, so arbeitet dieser **nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten**, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“
  -> Sub-Auftragnehmer Pflichten und Rechte
  -> Haftung: nach Art. 82 Abs. 1, 1 DSGVO der Auftragsverarbeiter gemeinsam mit dem Verantwortlichen gegenüber der betroffenen Person bei einem Datenschutzverstoß während der Verarbeitung ihrer Daten.

Weitergabe Diensthardware und BYOD

Rechts-Folgen der Nutzung von dienstlicher Hardware zu privaten Zwecken

Sicherheitsrisiken bei der Nutzung zu privaten Zwecken

„Surfen“ auf dem Smartphone oder am Rechner in der Mittagspause oder z.B. Wartezeit am Flughafen -> Möglichkeiten der Gestaltung von Richtlinien

BYOD: Risiken bei Nutzung privater Hardware und Grenzen

Homeoffice: Anordnung birgt Pflichten (Datenschutz und Arbeitsrecht)

Verträge – Prüfung von Anpassungsnotwendigkeiten

Einwilligung: Voraussetzungen der Wirksamkeit nach DSGVO „informiert, freiwillig, konkret“ – Einwilligung in der Praxis

Weitere vertragliche Regelungen im Lichte der DSGVO
- Grundregeln der DSGVO Art.5 Abs.1 und Informationspflichten Art. 12-15, sowie Art. 26 bis 28 DSGVO

Regelungen der DSGVO

Behörden können Bußgelder von bis zu 20 Millionen Euro oder vier Prozent des globalen Umsatzes verhängen (bzw. 2% / 10 Mio)

Schadensersatzansprüche geltend machen (Kunden, Arbeitnehmer oder andere Verbraucher)

Verbraucher und Verbände haben nach DSGVO Verbandsklagerechte