Contents

Chapter 1

DSGVO Datenschutz-Handbuch - Metadaten

Dokument-ID: 0000
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: {{ meta.status }}
Klassifizierung: {{ meta.classification }}
Letzte Aktualisierung: {{ meta.date }}

1.1 Handbuch-Informationen

Handbuch-Titel: DSGVO Datenschutz-Handbuch
Organisation: {{ meta.organization }}
Autor: Andreas Huemmer [andreas.huemmer@adminsend.de]
Geltungsbereich: {{ meta.scope }}
Gültig ab: {{ meta.valid_from }}
Nächste Überprüfung: {{ meta.next_review }}

1.2 Dokumentenzweck

Dieses Handbuch dokumentiert die Datenschutzmaßnahmen und -prozesse der Organisation gemäß der Datenschutz-Grundverordnung (DSGVO/GDPR - EU 2016/679). Es beschreibt die Struktur, Prozesse, Verantwortlichkeiten und Verfahren zur Sicherstellung des Schutzes personenbezogener Daten.

1.3 Geltungsbereich

Das Datenschutz-Managementsystem gilt für: - {{ meta.gdpr_scope }}

1.4 Normative Verweise

- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung - DSGVO)
- Bundesdatenschutzgesetz (BDSG) - nationale Anpassungen
- Relevante sektorspezifische Datenschutzvorschriften

1.5 Änderungshistorie

Version	Datum	Autor	Änderung
{{ meta.version }}	{{ meta.date }}	Andreas Huemmer [andreas.huemmer@adminsend.de]	Initiale Version

ewpage

Chapter 2

Geltungsbereich und Anwendungsbereich

Dokument-ID: 0010
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

2.1 Zweck

Dieses Dokument definiert den Geltungsbereich und Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) für {{ meta.organization }}. Es legt fest, welche Verarbeitungstätigkeiten personenbezogener Daten unter die DSGVO fallen und welche Ausnahmen gelten.

2.2 Sachlicher Anwendungsbereich (Art. 2 DSGVO)

2.2.1 Anwendbare Verarbeitungen

Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

In unserer Organisation umfasst dies:

Verarbeitungsbereich	Beschreibung	Automatisiert	Dateisystem
[TODO: z.B. Kundenverwaltung]	[TODO: Beschreibung]	Ja/Nein	Ja/Nein
[TODO: z.B. Personalverwaltung]	[TODO: Beschreibung]	Ja/Nein	Ja/Nein

Verarbeitungsbereich	Beschreibung	Automatisiert	Dateisystem
[TODO: z.B. Marketing]	[TODO: Beschreibung]	Ja/Nein	Ja/Nein
[TODO: z.B. Lieferantenverwaltung]	[TODO: Beschreibung]	Ja/Nein	Ja/Nein

2.2.2 Ausnahmen vom Anwendungsbereich

Gemäß Art. 2 Abs. 2 DSGVO gilt die Verordnung nicht für die Verarbeitung personenbezogener Daten:

1. **Im Rahmen einer Tätigkeit außerhalb des Unionsrechts** (Art. 2 Abs. 2 lit. a)
   - [TODO: Relevanz für Organisation prüfen]
2. **Durch die Mitgliedstaaten im Rahmen von Tätigkeiten des GASP** (Art. 2 Abs. 2 lit. b)
   - [TODO: Relevanz für Organisation prüfen]
3. **Durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten** (Art. 2 Abs. 2 lit. c)
   - [TODO: Relevanz für Organisation prüfen]
4. **Durch zuständige Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten** (Art. 2 Abs. 2 lit. d)
   - [TODO: Relevanz für Organisation prüfen]

2.3 Räumlicher Anwendungsbereich (Art. 3 DSGVO)

2.3.1 Niederlassungsprinzip (Art. 3 Abs. 1)

Die DSGVO findet Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der Union, unabhängig davon, ob die Verarbeitung in der Union stattfindet.

Niederlassungen unserer Organisation:

Standort	Land	EU/EWR	Verarbeitungstätigkeiten
[TODO: Hauptsitz]	[TODO: Land]	Ja/Nein	[TODO: Tätigkeiten]
[TODO: Zweigstelle]	[TODO: Land]	Ja/Nein	[TODO: Tätigkeiten]

2.3.2 Marktortprinzip (Art. 3 Abs. 2)

Die DSGVO findet auch Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Verarbeitungstätigkeiten im Zusammenhang damit stehen:

1. **Angebot von Waren oder Dienstleistungen an betroffene Personen in der Union** (Art. 3 Abs. 2 lit. a)
   - [TODO: Beschreibe Angebote an EU-Bürger]
   - [TODO: Zielgerichtete Aktivitäten dokumentieren]

2. **Beobachtung des Verhaltens betroffener Personen in der Union** (Art. 3 Abs. 2 lit. b)
   - [TODO: Beschreibe Tracking/Profiling von EU-Bürgern]
   - [TODO: Online-Verhaltensbeobachtung dokumentieren]

2.3.3 Vertreterpflicht (Art. 27)

Wenn Art. 3 Abs. 2 Anwendung findet und der Verantwortliche oder Auftragsverarbeiter nicht in der Union niedergelassen ist, muss ein Vertreter in der Union benannt werden.

Status: [TODO: Vertreter erforderlich? Ja/Nein]
Vertreter: [TODO: Name und Kontaktdaten, falls zutreffend]

2.4 Personenbezogene Daten

2.4.1 Definition (Art. 4 Nr. 1)

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

In unserer Organisation verarbeiten wir:

Datenkategorie	Beispiele	Besondere Kategorie (Art. 9)
[TODO: z.B. Kontaktdaten]	[TODO: Name, E-Mail, Telefon]	Nein
[TODO: z.B. Vertragsdaten]	[TODO: Kundennummer, Bestellungen]	Nein
[TODO: z.B. Gesundheitsdaten]	[TODO: Beschreibung]	Ja
[TODO: z.B. Finanzdaten]	[TODO: Bankverbindung, Gehalt]	Nein

2.4.2 Besondere Kategorien (Art. 9)

Besondere Kategorien personenbezogener Daten unterliegen erhöhten Schutzanforderungen: - Rassische und ethnische Herkunft - Politische Meinungen - Religiöse oder weltanschauliche Überzeugungen - Gewerkschaftszugehörigkeit - Genetische Daten - Biometrische Daten zur eindeutigen Identifizierung - Gesundheitsdaten - Daten zum Sexualleben oder der sexuellen Orientierung

Verarbeitung besonderer Kategorien: [TODO: Ja/Nein]
Rechtsgrundlage: [TODO: Art. 9 Abs. 2 lit. a-j]

2.5 Grenzüberschreitende Verarbeitung

2.5.1 Datenübermittlung in Drittländer

Status: [TODO: Werden Daten in Drittländer übermittelt? Ja/Nein]

Drittland	Zweck	Rechtsgrundlage	Garantien
[TODO: Land]	[TODO: Zweck]	[TODO: Art. 45/46/49]	[TODO: Garantien]

2.5.2 Konzerninterner Datenaustausch

Status: [TODO: Konzerninterner Datenaustausch? Ja/Nein]
Binding Corporate Rules (BCR): [TODO: Vorhanden? Ja/Nein]

2.6 Nationale Öffnungsklauseln

Die DSGVO enthält Öffnungsklauseln, die es den Mitgliedstaaten ermöglichen, spezifischere Bestimmungen zu erlassen.

Relevante nationale Regelungen: - [TODO: z.B. BDSG (Deutschland)] - [TODO: Sektorspezifische Regelungen] - [TODO: Weitere nationale Anpassungen]

2.7 Überprüfung und Aktualisierung

2.7.1 Überprüfungsfrequenz

Der Geltungsbereich wird überprüft: - **Regelmäßig:** [TODO: z.B. jährlich] - **Bei Bedarf:** Bei wesentlichen Änderungen der Verarbeitungstätigkeiten - **Bei neuen Produkten/Dienstleistungen:** Vor Einführung

2.7.2 Verantwortlichkeiten

- **Verantwortlich für Überprüfung:** [TODO: Datenschutzbeauftragter/Rolle]
- **Genehmigung:** [TODO: Geschäftsführung/Rolle]
- **Dokumentation:** [TODO: Datenschutzteam/Rolle]

2.8 Verknüpfung zu anderen Dokumenten

- **Verzeichnis von Verarbeitungstätigkeiten (Art. 30):** Detaillierte Auflistung aller Verarbeitungen
- **Datenschutzgrundsätze (Art. 5):** Grundsätze für alle Verarbeitungen
- **Rechtsgrundlagen (Art. 6):** Rechtmäßigkeit der Verarbeitung
- **Datenübermittlung (Art. 44-50):** Regelungen für Drittlandübermittlung

---

Nächste Schritte: 1. Identifizieren Sie alle Verarbeitungstätigkeiten in Ihrer Organisation 2. Prüfen Sie den räumlichen Anwendungsbereich (Niederlassungen, Marktortprinzip) 3. Dokumentieren Sie Ausnahmen und Sonderfälle 4. Erstellen Sie das Verzeichnis von Verarbeitungstätigkeiten (Art. 30) 5. Überprüfen Sie regelmäßig bei Änderungen

ewpage

Chapter 3

Rollen und Verantwortlichkeiten

Dokument-ID: 0020
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

3.1 Zweck

Dieses Dokument definiert die Rollen und Verantwortlichkeiten im Datenschutz-Management der {{ meta.organization }} gemäß DSGVO. Es legt fest, wer für welche Datenschutzaufgaben verantwortlich ist und wie die Zusammenarbeit organisiert ist.

3.2 Zentrale Rollen gemäß DSGVO

3.2.1 Verantwortlicher (Art. 4 Nr. 7)

Definition: Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

In unserer Organisation:

Verantwortlicher	Bereich	Verarbeitungstätigkeiten	Kontakt
[TODO: Name/Rolle]	[TODO: Bereich]	[TODO: Tätigkeiten]	[TODO: Kontakt]

3.2.2 Auftragsverarbeiter (Art. 4 Nr. 8)

Definition: Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Unsere Auftragsverarbeiter:

Auftragsverarbeiter	Dienstleistung	Verarbeitete Daten	AVV vorhanden
[TODO: Name]	[TODO: Service]	[TODO: Datenkategorien]	Ja/Nein

3.2.3 Betroffene Person (Art. 4 Nr. 1)

Definition: Identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten verarbeitet werden.

Kategorien betroffener Personen: - [TODO: z.B. Kunden] - [TODO: z.B. Mitarbeiter] - [TODO: z.B. Bewerber] - [TODO: z.B. Lieferanten-Kontakte] - [TODO: z.B. Website-Besucher]

3.2.4 Datenschutzbeauftragter (Art. 37-39)

Benennungspflicht: [TODO: Ja/Nein - Begründung gemäß Art. 37]

Datenschutzbeauftragter: - **Name:** [TODO: Name] - **Kontakt:** [TODO: E-Mail, Telefon] - **Stellung:** Intern/Extern - **Qualifikation:** [TODO: Fachkunde]

Aufgaben des Datenschutzbeauftragten (Art. 39): - Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten - Überwachung der Einhaltung der DSGVO - Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung - Zusammenarbeit mit der Aufsichtsbehörde - Anlaufstelle für die Aufsichtsbehörde

3.3 Organisatorische Rollen

3.3.1 Geschäftsführung/Management

Verantwortlichkeiten: - Gesamtverantwortung für Datenschutz-Compliance - Bereitstellung von Ressourcen - Genehmigung von Datenschutzrichtlinien - Rechenschaftspflicht (Art. 5 Abs. 2)

Ansprechpartner: [TODO: Name, Kontakt]

3.3.2 Datenschutz-Koordinatoren

Rolle: Dezentrale Datenschutzverantwortliche in Fachabteilungen

Abteilung	Koordinator	Verantwortlichkeiten	Kontakt
[TODO: IT]	[TODO: Name]	[TODO: Aufgaben]	[TODO: Kontakt]
[TODO: HR]	[TODO: Name]	[TODO: Aufgaben]	[TODO: Kontakt]
[TODO: Marketing]	[TODO: Name]	[TODO: Aufgaben]	[TODO: Kontakt]

3.3.3 IT-Sicherheitsbeauftragter

Verantwortlichkeiten: - Technische und organisatorische Maßnahmen (Art. 32) - IT-Sicherheitskonzept - Incident Response - Zusammenarbeit mit Datenschutzbeauftragtem

Ansprechpartner: [TODO: Name, Kontakt]

3.3.4 Datenschutz-Team

Zusammensetzung: - Datenschutzbeauftragter (Leitung) - Datenschutz-Koordinatoren - IT-Sicherheitsbeauftragter - Rechtsabteilung (bei Bedarf)

Aufgaben: - Entwicklung und Pflege von Datenschutzrichtlinien - Durchführung von Datenschutz-Folgenabschätzungen - Schulung und Sensibilisierung - Bearbeitung von Betroffenenanfragen - Meldung von Datenschutzverletzungen

3.4 RACI-Matrix Datenschutzprozesse

Prozess	Verantwortlich (R)	Rechenschaftspflichtig (A)	Konsultiert (C)	Informiert (I)
Datenschutzrichtlinien	[TODO]	[TODO]	[TODO]	[TODO]
DSFA-Durchführung	[TODO]	[TODO]	[TODO]	[TODO]
Betroffenenanfragen	[TODO]	[TODO]	[TODO]	[TODO]
Breach-Meldung	[TODO]	[TODO]	[TODO]	[TODO]
Schulungen	[TODO]	[TODO]	[TODO]	[TODO]
AVV-Verwaltung	[TODO]	[TODO]	[TODO]	[TODO]

3.5 Gemeinsam Verantwortliche (Art. 26)

Status: [TODO: Gibt es gemeinsame Verantwortlichkeiten? Ja/Nein]

Partner	Verarbeitungszweck	Vereinbarung	Ansprechpartner
[TODO: Name]	[TODO: Zweck]	[TODO: Datum]	[TODO: Kontakt]

3.6 Vertretung (Art. 27)

Erforderlich: [TODO: Ja/Nein - bei Nicht-EU-Niederlassung mit EU-Verarbeitung]

Vertreter in der EU: - **Name:** [TODO: Name] - **Adresse:** [TODO: Adresse] - **Kontakt:** [TODO: E-Mail, Telefon]

3.7 Schulung und Sensibilisierung

3.7.1 Schulungsprogramm

Zielgruppe	Schulungsinhalt	Frequenz	Verantwortlich
Alle Mitarbeiter	Datenschutz-Grundlagen	Jährlich	[TODO]
Führungskräfte	Datenschutz-Management	Jährlich	[TODO]
IT-Personal	Technische Maßnahmen	Halbjährlich	[TODO]
HR	Beschäftigtendatenschutz	Jährlich	[TODO]

3.7.2 Verpflichtung auf Vertraulichkeit

Alle Personen, die Zugang zu personenbezogenen Daten haben, werden auf Vertraulichkeit verpflichtet.

Prozess: [TODO: Beschreibe Verpflichtungsprozess]

3.8 Kommunikation und Berichtswesen

3.8.1 Interne Kommunikation

- **Datenschutz-Newsletter:** [TODO: Frequenz]
- **Intranet-Seite:** [TODO: URL]
- **Datenschutz-Hotline:** [TODO: Kontakt]

3.8.2 Berichtswesen

Bericht	Empfänger	Frequenz	Verantwortlich
Datenschutz-Status	Geschäftsführung	Quartalsweise	DSB
Incident-Report	Geschäftsführung	Bei Bedarf	DSB
Audit-Ergebnisse	Management	Jährlich	DSB

3.9 Kontakt zur Aufsichtsbehörde

Zuständige Aufsichtsbehörde: [TODO: Name der Behörde]
Adresse: [TODO: Adresse]
Kontakt: [TODO: E-Mail, Telefon, Website]
Ansprechpartner Organisation: [TODO: Datenschutzbeauftragter]

3.10 Überprüfung und Aktualisierung

- **Überprüfungsfrequenz:** [TODO: z.B. jährlich]
- **Verantwortlich:** [TODO: Datenschutzbeauftragter]
- **Genehmigung:** [TODO: Geschäftsführung]

Nächste Schritte: 1. Benennen Sie alle relevanten Rollen und Verantwortliche 2. Erstellen Sie eine vollständige RACI-Matrix 3. Prüfen Sie die Benennungspflicht für einen Datenschutzbeauftragten 4. Dokumentieren Sie alle Auftragsverarbeiter-Beziehungen 5. Implementieren Sie ein Schulungsprogramm

ewpage

Chapter 4

Datenschutzgrundsätze

Dokument-ID: 0030
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

4.1 Zweck

Dieses Dokument beschreibt die Datenschutzgrundsätze gemäß Art. 5 DSGVO und deren Umsetzung in der {{ meta.organization }}. Diese Grundsätze sind bei jeder Verarbeitung personenbezogener Daten zu beachten.

4.2 Grundsätze gemäß Art. 5 Abs. 1 DSGVO

4.2.1 1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a)

Grundsatz:
Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Umsetzung in unserer Organisation: - [TODO: Prüfung der Rechtsgrundlage vor jeder Verarbeitung] - [TODO: Transparente Datenschutzerklärungen] - [TODO: Klare Informationen bei Datenerhebung] - [TODO: Faire Verarbeitungspraktiken]

Maßnahmen: - Rechtsgrundlagen-Check bei neuen Verarbeitungen - Datenschutzerklärungen in verständlicher Sprache - Informationspflichten gemäß Art. 13-14 - Dokumentation aller Verarbeitungen

4.2.2 2. Zweckbindung (Art. 5 Abs. 1 lit. b)

Grundsatz:
Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Umsetzung in unserer Organisation: - [TODO: Klare Zweckdefinition bei Datenerhebung] - [TODO: Prüfung der Zweckvereinbarkeit bei Weiterverarbeitung] - [TODO: Dokumentation im Verzeichnis von Verarbeitungstätigkeiten]

Maßnahmen: - Zweckdefinition im Verzeichnis von Verarbeitungstätigkeiten (Art. 30) - Prüfung bei Zweckänderung gemäß Art. 6 Abs. 4 - Neue Rechtsgrundlage oder Einwilligung bei inkompatiblen Zwecken

4.2.3 3. Datenminimierung (Art. 5 Abs. 1 lit. c)

Grundsatz:
Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Umsetzung in unserer Organisation: - [TODO: Prüfung der Erforderlichkeit bei Datenerhebung] - [TODO: Regelmäßige Überprüfung gespeicherter Daten] - [TODO: Vermeidung von "nice-to-have" Daten]

Maßnahmen: - Datenerhebung nur bei nachgewiesener Erforderlichkeit - Regelmäßige Datenbereinigung - Privacy by Design bei neuen Systemen - Anonymisierung/Pseudonymisierung wo möglich

4.2.4 4. Richtigkeit (Art. 5 Abs. 1 lit. d)

Grundsatz:
Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige Daten unverzüglich gelöscht oder berichtigt werden.

Umsetzung in unserer Organisation: - [TODO: Prozesse zur Datenaktualisierung] - [TODO: Berichtigungsmöglichkeiten für betroffene Personen] - [TODO: Regelmäßige Datenqualitätsprüfungen]

Maßnahmen: - Berichtigungsrecht gemäß Art. 16 umsetzen - Regelmäßige Datenqualitätschecks - Aktualisierungsprozesse bei Stammdaten - Fehlerkorrekturverfahren

4.2.5 5. Speicherbegrenzung (Art. 5 Abs. 1 lit. e)

Grundsatz:
Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke erforderlich ist.

Umsetzung in unserer Organisation: - [TODO: Löschkonzept mit definierten Fristen] - [TODO: Automatisierte Löschroutinen] - [TODO: Archivierung mit Zugriffsbeschränkungen]

Maßnahmen: - Löschfristen im Verzeichnis von Verarbeitungstätigkeiten - Automatisierte Löschprozesse - Regelmäßige Löschläufe - Anonymisierung für statistische Zwecke - Berücksichtigung gesetzlicher Aufbewahrungsfristen

4.2.6 6. Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f)

Grundsatz:
Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Umsetzung in unserer Organisation: - [TODO: Technische und organisatorische Maßnahmen (TOM)] - [TODO: Zugriffskontrollsysteme] - [TODO: Verschlüsselung] - [TODO: Backup-Strategien]

Maßnahmen: - Technische und organisatorische Maßnahmen gemäß Art. 32 - Zugriffskontrolle und Berechtigungskonzept - Verschlüsselung sensibler Daten - Regelmäßige Sicherheitsaudits - Incident Response Plan

4.3 Rechenschaftspflicht (Art. 5 Abs. 2)

Grundsatz:
Der Verantwortliche ist für die Einhaltung der Grundsätze verantwortlich und muss deren Einhaltung nachweisen können ("Accountability").

Umsetzung in unserer Organisation:

Nachweis	Dokument/Maßnahme	Verantwortlich
Verarbeitungsverzeichnis	Art. 30 Verzeichnis	[TODO: DSB]
Rechtsgrundlagen	Dokumentation je Verarbeitung	[TODO: Fachabteilung]
TOM	Sicherheitskonzept	[TODO: IT-Sicherheit]
DSFA	DSFA-Berichte	[TODO: DSB]
AVV	Verträge mit Auftragsverarbeitern	[TODO: Einkauf/Legal]
Schulungen	Schulungsnachweise	[TODO: HR]
Datenschutzverletzungen	Incident-Log	[TODO: DSB]

4.4 Umsetzung in Verarbeitungsprozessen

4.4.1 Checkliste für neue Verarbeitungen

- ☐ Zweck klar definiert und dokumentiert
- ☐ Rechtsgrundlage identifiziert (Art. 6 oder Art. 9)
- ☐ Datenminimierung geprüft
- ☐ Speicherfrist festgelegt
- ☐ TOM definiert und implementiert
- ☐ Informationspflichten erfüllt (Art. 13-14)
- ☐ Verzeichnis von Verarbeitungstätigkeiten aktualisiert
- ☐ DSFA durchgeführt (falls erforderlich)
- ☐ AVV abgeschlossen (bei Auftragsverarbeitung)

4.5 Kontrollen und Überwachung

4.5.1 Regelmäßige Überprüfungen

Kontrolle	Frequenz	Verantwortlich	Dokumentation
Verarbeitungsverzeichnis	Quartalsweise	DSB	Prüfprotokoll
Löschfristen	Monatlich	IT	Löschprotokoll
Zugriffsprotokolle	Monatlich	IT-Sicherheit	Audit-Log
TOM-Wirksamkeit	Jährlich	DSB	Audit-Bericht
Schulungsstand	Quartalsweise	HR	Schulungsmatrix

4.6 Verknüpfung zu anderen Dokumenten

- **Rechtsgrundlagen (Art. 6):** Rechtmäßigkeit der Verarbeitung
- **TOM (Art. 32):** Sicherheit der Verarbeitung
- **Verzeichnis (Art. 30):** Dokumentation aller Verarbeitungen
- **DSFA (Art. 35):** Risikobewertung
- **Betroffenenrechte (Art. 12-23):** Transparenz und Kontrolle

---

Nächste Schritte: 1. Überprüfen Sie alle Verarbeitungen auf Einhaltung der Grundsätze 2. Implementieren Sie Kontrollen für jeden Grundsatz 3. Dokumentieren Sie Nachweise für Rechenschaftspflicht 4. Schulen Sie Mitarbeiter zu den Grundsätzen 5. Etablieren Sie regelmäßige Überprüfungsprozesse

ewpage

Chapter 5

Rechtmäßigkeit der Verarbeitung

Dokument-ID: 0040
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

5.1 Zweck

Dieses Dokument beschreibt die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten in der {{ meta.organization }} gemäß Art. 6 DSGVO. Jede Verarbeitung muss auf mindestens einer dieser Rechtsgrundlagen basieren.

5.2 Rechtsgrundlagen gemäß Art. 6 Abs. 1 DSGVO

5.2.1 Art. 6 Abs. 1 lit. a - Einwilligung

Rechtsgrundlage:
Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben.

Anforderungen an Einwilligung: - Freiwillig - Für bestimmte Zwecke - Informiert - Unmissverständlich - Widerrufbar

Anwendungsfälle in unserer Organisation:

Verarbeitungszweck	Datenarten	Einwilligungsform	Widerrufsmöglichkeit
[TODO: z.B. Newsletter]	[TODO: E-Mail, Name]	[TODO: Double-Opt-In]	[TODO: Abmeldelink]
[TODO: z.B. Marketing-Cookies]	[TODO: Tracking-Daten]	[TODO: Cookie-Banner]	[TODO: Cookie-Einstellungen]

Verwaltung von Einwilligungen: - Dokumentation: [TODO: System/Prozess] - Nachweisführung: [TODO: Methode] - Widerrufsprozess: [TODO: Beschreibung]

5.2.2 Art. 6 Abs. 1 lit. b - Vertragserfüllung

Rechtsgrundlage:
Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich.

Anwendungsfälle in unserer Organisation:

Vertragsart	Verarbeitungszweck	Erforderliche Daten	Speicherdauer
[TODO: Kaufvertrag]	[TODO: Bestellabwicklung]	[TODO: Name, Adresse, Zahlung]	[TODO: Frist]
[TODO: Arbeitsvertrag]	[TODO: Personalverwaltung]	[TODO: Personaldaten]	[TODO: Frist]
[TODO: Dienstleistungsvertrag]	[TODO: Leistungserbringung]	[TODO: Kontaktdaten]	[TODO: Frist]

Erforderlichkeitsprüfung: - Ist die Verarbeitung objektiv erforderlich für die Vertragserfüllung? - Gibt es mildere Mittel? - Ist der Zweck klar mit dem Vertrag verbunden?

5.2.3 Art. 6 Abs. 1 lit. c - Rechtliche Verpflichtung

Rechtsgrundlage:
Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.

Anwendungsfälle in unserer Organisation:

Rechtliche Verpflichtung	Rechtsgrundlage	Verarbeitungszweck	Datenarten	Speicherdauer
[TODO: Steuerrecht]	[TODO: AO, UStG]	[TODO: Buchhaltung]	[TODO: Rechnungsdaten]	[TODO: 10 Jahre]
[TODO: Sozialversicherung]	[TODO: SGB]	[TODO: Meldungen]	[TODO: Sozialdaten]	[TODO: Gesetzlich]
[TODO: Handelsrecht]	[TODO: HGB]	[TODO: Archivierung]	[TODO: Geschäftsdaten]	[TODO: 6-10 Jahre]

5.2.4 Art. 6 Abs. 1 lit. d - Schutz lebenswichtiger Interessen

Rechtsgrundlage:
Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

Anwendungsfälle in unserer Organisation: - [TODO: z.B. Notfallkontakte] - [TODO: z.B. Gesundheitsnotfälle] - [TODO: Nur in Ausnahmefällen anwendbar]

5.2.5 Art. 6 Abs. 1 lit. e - Öffentliches Interesse/Ausübung öffentlicher Gewalt

Rechtsgrundlage:
Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt.

Anwendbarkeit: [TODO: Relevant für öffentliche Stellen - für private Unternehmen meist nicht anwendbar]

5.2.6 Art. 6 Abs. 1 lit. f - Berechtigtes Interesse

Rechtsgrundlage:
Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Dreistufiger Test: 1. Berechtigtes Interesse des Verantwortlichen 2. Erforderlichkeit der Verarbeitung 3. Interessenabwägung

Anwendungsfälle in unserer Organisation:

Verarbeitungszweck	Berechtigtes Interesse	Erforderlichkeit	Interessenabwägung	Ergebnis
[TODO: Direktwerbung]	[TODO: Marketing]	[TODO: Begründung]	[TODO: Abwägung]	Zulässig/Unzulässig
[TODO: IT-Sicherheit]	[TODO: Schutz der Systeme]	[TODO: Begründung]	[TODO: Abwägung]	Zulässig/Unzulässig
[TODO: Videoüberwachung]	[TODO: Sicherheit]	[TODO: Begründung]	[TODO: Abwägung]	Zulässig/Unzulässig

Dokumentation der Interessenabwägung: - Beschreibung des berechtigten Interesses - Nachweis der Erforderlichkeit - Bewertung der Interessen der betroffenen Person - Ergebnis der Abwägung - Maßnahmen zur Minimierung von Eingriffen

5.3 Besonderheiten bei Kindern (Art. 8)

Einwilligung bei Kindern: - Unter 16 Jahren (oder niedriger nach nationalem Recht): Einwilligung der Eltern erforderlich - In Deutschland: Ab 16 Jahren eigenständige Einwilligung möglich

Anwendungsfälle: - [TODO: Beschreibe Verarbeitungen mit Daten von Kindern] - [TODO: Altersverifikationsprozess] - [TODO: Elterneinwilligung]

5.4 Dokumentation der Rechtsgrundlagen

5.4.1 Verzeichnis von Verarbeitungstätigkeiten (Art. 30)

Für jede Verarbeitungstätigkeit muss die Rechtsgrundlage dokumentiert werden:

Verarbeitungstätigkeit	Zweck	Rechtsgrundlage	Datenarten	Speicherdauer
[TODO: Kundenverwaltung]	[TODO: Vertragserfüllung]	Art. 6 Abs. 1 lit. b	[TODO: Stammdaten]	[TODO: Frist]
[TODO: Newsletter]	[TODO: Marketing]	Art. 6 Abs. 1 lit. a	[TODO: E-Mail]	[TODO: Bis Widerruf]
[TODO: Buchhaltung]	[TODO: Steuerrecht]	Art. 6 Abs. 1 lit. c	[TODO: Rechnungsdaten]	[TODO: 10 Jahre]

5.5 Prüfprozess für neue Verarbeitungen

5.5.1 Checkliste Rechtsgrundlage

1. **Zweck der Verarbeitung klar definiert?** Ja/Nein
2. **Rechtsgrundlage identifiziert?** Ja/Nein
3. **Bei Einwilligung:**
   - Freiwillig? Ja/Nein
   - Informiert? Ja/Nein
   - Widerrufbar? Ja/Nein
4. **Bei Vertragserfüllung:**
   - Objektiv erforderlich? Ja/Nein
   - Keine milderen Mittel? Ja/Nein
5. **Bei berechtigtem Interesse:**
   - Interesse dokumentiert? Ja/Nein
   - Erforderlichkeit geprüft? Ja/Nein
   - Interessenabwägung durchgeführt? Ja/Nein
6. **Dokumentation im Verzeichnis?** Ja/Nein

5.6 Änderung der Rechtsgrundlage

Prozess bei Änderung: 1. Prüfung der Zweckvereinbarkeit (Art. 6 Abs. 4) 2. Neue Rechtsgrundlage oder Einwilligung erforderlich 3. Information der betroffenen Personen 4. Aktualisierung der Dokumentation

5.7 Verknüpfung zu anderen Dokumenten

- **Datenschutzgrundsätze (Art. 5):** Rechtmäßigkeit als Grundprinzip
- **Verzeichnis (Art. 30):** Dokumentation der Rechtsgrundlagen
- **Informationspflichten (Art. 13-14):** Mitteilung der Rechtsgrundlage
- **Berechtigtes Interesse:** Interessenabwägungstest

Nächste Schritte: 1. Identifizieren Sie die Rechtsgrundlage für jede Verarbeitungstätigkeit 2. Dokumentieren Sie Einwilligungen und deren Verwaltung 3. Führen Sie Interessenabwägungen für berechtigte Interessen durch 4. Aktualisieren Sie das Verzeichnis von Verarbeitungstätigkeiten 5. Schulen Sie Mitarbeiter zur Identifikation von Rechtsgrundlagen

ewpage

Chapter 6

Besondere Kategorien personenbezogener Daten

Dokument-ID: 0050
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

6.1 Zweck

Dieses Dokument beschreibt den Umgang mit besonderen Kategorien personenbezogener Daten in der {{ meta.organization }} gemäß Art. 9 DSGVO. Diese sensiblen Daten unterliegen erhöhten Schutzanforderungen.

6.2 Besondere Kategorien (Art. 9 Abs. 1)

6.2.1 Verarbeitungsverbot

Die Verarbeitung folgender Datenkategorien ist grundsätzlich untersagt: - Rassische und ethnische Herkunft - Politische Meinungen - Religiöse oder weltanschauliche Überzeugungen - Gewerkschaftszugehörigkeit - Genetische Daten - Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person - Gesundheitsdaten - Daten zum Sexualleben oder der sexuellen Orientierung

6.2.2 Verarbeitung in unserer Organisation

Status: [TODO: Werden besondere Kategorien verarbeitet? Ja/Nein]

Datenkategorie	Verarbeitungszweck	Rechtsgrundlage (Art. 9 Abs. 2)	Betroffene Personen
[TODO: z.B. Gesundheitsdaten]	[TODO: Zweck]	[TODO: lit. a-j]	[TODO: Mitarbeiter]
[TODO: z.B. Biometrische Daten]	[TODO: Zweck]	[TODO: lit. a-j]	[TODO: Gruppe]

6.3 Ausnahmen vom Verarbeitungsverbot (Art. 9 Abs. 2)

6.3.1 Art. 9 Abs. 2 lit. a - Ausdrückliche Einwilligung

Voraussetzungen: - Ausdrückliche (nicht nur stillschweigende) Einwilligung - Freiwillig, informiert, unmissverständlich - Für bestimmte Zwecke - Widerrufbar

Anwendungsfälle: - [TODO: Beschreibe Fälle mit ausdrücklicher Einwilligung] - [TODO: Einwilligungsformular] - [TODO: Widerrufsprozess]

6.3.2 Art. 9 Abs. 2 lit. b - Arbeitsrecht und Sozialrecht

Voraussetzungen: - Erforderlich für Arbeitsrecht oder Sozialrecht - Auf Grundlage von Unionsrecht, Mitgliedstaatenrecht oder Kollektivvereinbarung - Angemessene Garantien für Grundrechte

Anwendungsfälle: - [TODO: z.B. Krankheitsdaten für Lohnfortzahlung] - [TODO: z.B. Schwerbehinderung] - [TODO: Nationale Rechtsgrundlage angeben]

6.3.3 Art. 9 Abs. 2 lit. c - Schutz lebenswichtiger Interessen

Voraussetzungen: - Schutz lebenswichtiger Interessen - Betroffene Person ist außerstande, Einwilligung zu geben

Anwendungsfälle: - [TODO: z.B. Medizinische Notfälle] - [TODO: Nur in Ausnahmesituationen]

6.3.4 Art. 9 Abs. 2 lit. d - Verarbeitung durch Stiftungen, Vereinigungen

Voraussetzungen: - Verarbeitung durch Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht - Im Rahmen ihrer berechtigten Tätigkeiten - Mit angemessenen Garantien

Anwendbarkeit: [TODO: Relevant? Ja/Nein]

6.3.5 Art. 9 Abs. 2 lit. e - Offensichtlich öffentlich gemachte Daten

Voraussetzungen: - Daten wurden von der betroffenen Person offensichtlich öffentlich gemacht

Anwendungsfälle: - [TODO: z.B. Öffentliche Social-Media-Profile] - [TODO: Vorsicht bei Interpretation “offensichtlich öffentlich”]

6.3.6 Art. 9 Abs. 2 lit. f - Rechtliche Ansprüche

Voraussetzungen: - Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche - Inanspruchnahme der Gerichte

Anwendungsfälle: - [TODO: z.B. Arbeitsgerichtsverfahren] - [TODO: z.B. Schadensersatzansprüche]

6.3.7 Art. 9 Abs. 2 lit. g - Erhebliches öffentliches Interesse

Voraussetzungen: - Erhebliches öffentliches Interesse - Auf Grundlage von Unionsrecht oder Mitgliedstaatenrecht - Verhältnismäßig zum verfolgten Ziel - Angemessene Garantien

Anwendbarkeit: [TODO: Relevant? Ja/Nein]

6.3.8 Art. 9 Abs. 2 lit. h - Gesundheitsvorsorge und Arbeitsmedizin

Voraussetzungen: - Gesundheitsvorsorge, Arbeitsmedizin, medizinische Diagnostik - Auf Grundlage von Unionsrecht oder Mitgliedstaatenrecht - Berufsgeheimnis oder gesetzliche Geheimhaltungspflicht

Anwendungsfälle: - [TODO: z.B. Betriebsarzt] - [TODO: z.B. Arbeitsschutz]

6.3.9 Art. 9 Abs. 2 lit. i - Öffentliches Interesse im Bereich Gesundheit

Voraussetzungen: - Öffentliches Interesse im Bereich der öffentlichen Gesundheit - Schutz vor schwerwiegenden Gesundheitsgefahren - Auf Grundlage von Unionsrecht oder Mitgliedstaatenrecht

Anwendbarkeit: [TODO: Relevant? Ja/Nein]

6.3.10 Art. 9 Abs. 2 lit. j - Archivzwecke, Forschung, Statistik

Voraussetzungen: - Archivzwecke im öffentlichen Interesse - Wissenschaftliche oder historische Forschungszwecke - Statistische Zwecke - Auf Grundlage von Unionsrecht oder Mitgliedstaatenrecht - Angemessene Garantien

Anwendungsfälle: - [TODO: z.B. Wissenschaftliche Studien] - [TODO: z.B. Statistische Auswertungen]

6.4 Erhöhte Schutzmaßnahmen

6.4.1 Technische Maßnahmen

Maßnahme	Beschreibung	Implementiert
Verschlüsselung	[TODO: Verschlüsselung sensibler Daten]	Ja/Nein
Zugriffskontrolle	[TODO: Strenge Zugriffsbeschränkungen]	Ja/Nein
Pseudonymisierung	[TODO: Wo möglich]	Ja/Nein
Logging	[TODO: Protokollierung aller Zugriffe]	Ja/Nein
Separate Speicherung	[TODO: Getrennt von anderen Daten]	Ja/Nein

6.4.2 Organisatorische Maßnahmen

Maßnahme	Beschreibung	Implementiert
Need-to-know-Prinzip	[TODO: Zugriff nur bei Erforderlichkeit]	Ja/Nein
Vertraulichkeitsverpflichtung	[TODO: Besondere Verpflichtung]	Ja/Nein
Schulungen	[TODO: Spezielle Schulungen]	Ja/Nein
DSFA	[TODO: Datenschutz-Folgenabschätzung]	Ja/Nein
Incident Response	[TODO: Besondere Breach-Prozesse]	Ja/Nein

6.5 Datenschutz-Folgenabschätzung (DSFA)

Erforderlichkeit:
Bei Verarbeitung besonderer Kategorien ist eine DSFA gemäß Art. 35 in der Regel erforderlich.

Status: [TODO: DSFA durchgeführt? Ja/Nein]
Ergebnis: [TODO: Zusammenfassung]
Maßnahmen: [TODO: Risikominderungsmaßnahmen]

6.6 Nationale Regelungen

6.6.1 Deutschland - BDSG

Relevante Vorschriften: - § 22 BDSG: Verarbeitung besonderer Kategorien für Beschäftigte - § 23 BDSG: Verarbeitung zu wissenschaftlichen Zwecken - [TODO: Weitere relevante nationale Regelungen]

6.7 Dokumentation

6.7.1 Verzeichnis von Verarbeitungstätigkeiten

Für jede Verarbeitung besonderer Kategorien muss dokumentiert werden: - Datenkategorie (Art. 9 Abs. 1) - Verarbeitungszweck - Rechtsgrundlage (Art. 9 Abs. 2 lit. a-j) - Betroffene Personen - Empfänger - Speicherdauer - TOM (erhöhte Schutzmaßnahmen) - DSFA-Referenz

6.7.2 Nachweisführung

- Dokumentation der Ausnahmetatbestände
- DSFA-Berichte
- Einwilligungserklärungen (bei lit. a)
- Nationale Rechtsgrundlagen (bei lit. b, g, h, i, j)
- TOM-Dokumentation

6.8 Betroffenenrechte

Besonderheiten: - Erhöhte Informationspflichten - Auskunftsrecht umfasst auch Rechtsgrundlage - Widerspruchsrecht bei berechtigtem Interesse - Widerruf der Einwilligung jederzeit möglich

6.9 Schulung und Sensibilisierung

Schulungsinhalte: - Identifikation besonderer Kategorien - Verarbeitungsverbot und Ausnahmen - Erhöhte Schutzmaßnahmen - Incident Response bei Datenschutzverletzungen - Sanktionen bei Verstößen

Zielgruppe: Alle Mitarbeiter mit Zugriff auf besondere Kategorien

6.10 Verknüpfung zu anderen Dokumenten

- **Rechtsgrundlagen (Art. 6):** Zusätzlich zu Art. 9 erforderlich
- **TOM (Art. 32):** Erhöhte Sicherheitsmaßnahmen
- **DSFA (Art. 35):** In der Regel erforderlich
- **Verzeichnis (Art. 30):** Dokumentation aller Verarbeitungen

---

Nächste Schritte: 1. Identifizieren Sie alle Verarbeitungen besonderer Kategorien 2. Prüfen Sie die Rechtsgrundlage gemäß Art. 9 Abs. 2 3. Implementieren Sie erhöhte Schutzmaßnahmen 4. Führen Sie DSFA durch 5. Schulen Sie betroffene Mitarbeiter

ewpage

Chapter 7

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Dokument-ID: 0100
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

7.1 Zweck

Dieses Dokument beschreibt die Umsetzung des Grundsatzes der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz in der {{ meta.organization }}. Dieser Grundsatz bildet die Basis für alle Datenverarbeitungen.

7.2 Grundsatz gemäß Art. 5 Abs. 1 lit. a DSGVO

Rechtliche Anforderung:
Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

7.2.1 Drei Komponenten

1. **Rechtmäßigkeit:** Verarbeitung muss auf einer Rechtsgrundlage gemäß Art. 6 oder Art. 9 DSGVO basieren
2. **Verarbeitung nach Treu und Glauben:** Faire und angemessene Verarbeitung ohne Täuschung
3. **Transparenz:** Nachvollziehbare und verständliche Information für betroffene Personen

7.3 Umsetzung der Rechtmäßigkeit

7.3.1 Rechtsgrundlagen-Prüfung

Prozess vor jeder neuen Verarbeitung:

1. **Identifikation der Rechtsgrundlage**
   - Art. 6 Abs. 1 lit. a: Einwilligung
   - Art. 6 Abs. 1 lit. b: Vertragserfüllung
   - Art. 6 Abs. 1 lit. c: Rechtliche Verpflichtung
   - Art. 6 Abs. 1 lit. d: Schutz lebenswichtiger Interessen
   - Art. 6 Abs. 1 lit. e: Öffentliches Interesse
   - Art. 6 Abs. 1 lit. f: Berechtigtes Interesse
2. **Dokumentation der Rechtsgrundlage**
   - Im Verzeichnis von Verarbeitungstätigkeiten (Art. 30)
   - In Datenschutzerklärungen
   - In internen Verarbeitungsrichtlinien
3. **Regelmäßige Überprüfung**
   - Quartalsweise Prüfung bestehender Verarbeitungen
   - Bei Änderung von Zwecken oder Umfang

7.3.2 Maßnahmen in unserer Organisation

Maßnahme	Beschreibung	Verantwortlich	Status
[TODO: Rechtsgrundlagen-Check]	[TODO: Prüfprozess vor neuen Verarbeitungen]	[TODO: DSB]	[TODO]
[TODO: Dokumentation]	[TODO: Pflege des Verzeichnisses Art. 30]	[TODO: Fachabteilung]	[TODO]
[TODO: Schulung]	[TODO: Mitarbeiterschulung zu Rechtsgrundlagen]	[TODO: HR]	[TODO]

7.4 Umsetzung von Treu und Glauben

7.4.1 Faire Verarbeitungspraktiken

Grundsätze: - Keine Täuschung oder Irreführung betroffener Personen - Keine versteckten oder unerwarteten Verarbeitungen - Angemessene und verhältnismäßige Datenverarbeitung - Berücksichtigung berechtigter Erwartungen

7.4.2 Konkrete Maßnahmen

Vermeidung unfairer Praktiken: - [TODO: Keine versteckten Einwilligungen in AGB] - [TODO: Klare Trennung von Pflichtangaben und freiwilligen Angaben] - [TODO: Keine Kopplung von Diensten an unnötige Einwilligungen] - [TODO: Angemessene Verarbeitungsumfänge]

Beispiele fairer Verarbeitung:

Verarbeitungszweck	Faire Praxis	Unfaire Praxis (zu vermeiden)
[TODO: Newsletter]	[TODO: Separate Einwilligung, einfacher Widerruf]	[TODO: Versteckt in AGB, komplizierter Widerruf]
[TODO: Kundenkonto]	[TODO: Nur erforderliche Daten]	[TODO: Übermäßige Datenerhebung]
[TODO: Cookies]	[TODO: Echte Wahlmöglichkeit]	[TODO: Cookie-Wall ohne Alternative]

7.5 Umsetzung von Transparenz

7.5.1 Informationspflichten

Gemäß Art. 13-14 DSGVO müssen betroffene Personen informiert werden über:

- Identität und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Zwecke und Rechtsgrundlage der Verarbeitung
- Berechtigte Interessen (bei Art. 6 Abs. 1 lit. f)
- Empfänger oder Kategorien von Empfängern
- Absicht der Übermittlung an Drittländer
- Speicherdauer
- Betroffenenrechte
- Widerrufsrecht bei Einwilligung
- Beschwerderecht bei Aufsichtsbehörde
- Pflicht oder Freiwilligkeit der Bereitstellung
- Automatisierte Entscheidungsfindung

7.5.2 Transparenzmechanismen in unserer Organisation

Datenschutzerklärungen: - [TODO: Website-Datenschutzerklärung] - [TODO: App-Datenschutzerklärung] - [TODO: Datenschutzhinweise bei Datenerhebung] - [TODO: Informationsblätter für spezifische Verarbeitungen]

Anforderungen an Datenschutzerklärungen: - Verständliche Sprache (keine übermäßige Juristensprache) - Strukturierte und übersichtliche Darstellung - Leicht zugänglich und auffindbar - Vollständige Information gemäß Art. 13-14 - Mehrsprachigkeit bei internationalen Nutzern

7.5.3 Kommunikationskanäle

Kanal	Zweck	Zielgruppe	Aktualisierung
[TODO: Website]	[TODO: Datenschutzerklärung]	[TODO: Websitebesucher]	[TODO: Bei Änderungen]
[TODO: E-Mail]	[TODO: Direktinformation bei Erhebung]	[TODO: Kunden]	[TODO: Bei Erstkontakt]

Kanal	Zweck	Zielgruppe	Aktualisierung
[TODO: Formular]	[TODO: Einwilligungserklärung]	[TODO: Betroffene]	[TODO: Vor Verarbeitung]
[TODO: Aushang]	[TODO: Videoüberwachung]	[TODO: Besucher]	[TODO: Permanent]

7.6 Verständlichkeit und Zugänglichkeit

7.6.1 Anforderungen an Informationen

Verständlichkeit: - Klare und einfache Sprache - Vermeidung von Fachbegriffen oder deren Erklärung - Strukturierte Darstellung mit Überschriften - Kurze Sätze und Absätze

Zugänglichkeit: - Leicht auffindbar (z.B. Link im Footer) - Barrierefrei (WCAG-Konformität) - Mehrere Formate (Web, PDF, Papier) - Mehrsprachigkeit bei Bedarf

7.6.2 Checkliste für transparente Information

- ☐ Information erfolgt vor Beginn der Verarbeitung
- ☐ Alle Pflichtinformationen gemäß Art. 13-14 enthalten
- ☐ Verständliche und klare Sprache
- ☐ Strukturiert und übersichtlich
- ☐ Leicht zugänglich
- ☐ Barrierefrei
- ☐ Aktuell und vollständig
- ☐ Kontaktmöglichkeiten angegeben

7.7 Nachweis der Einhaltung (Accountability)

7.7.1 Dokumentation

Nachweisdokumente: - Verzeichnis von Verarbeitungstätigkeiten mit Rechtsgrundlagen - Datenschutzerklärungen und Informationsblätter - Einwilligungserklärungen und deren Verwaltung - Schulungsnachweise für Mitarbeiter - Prüfprotokolle für Rechtsgrundlagen

7.7.2 Kontrollen

Kontrolle	Frequenz	Verantwortlich	Dokumentation
[TODO: Rechtsgrundlagen-Prüfung]	Quartalsweise	DSB	Prüfprotokoll
[TODO: Datenschutzerklärungen]	Bei Änderungen	Legal/DSB	Versionshistorie
[TODO: Transparenz-Audit]	Jährlich	DSB	Audit-Bericht

Kontrolle	Frequenz	Verantwortlich	Dokumentation
[TODO: Schulungsstand]	Quartalsweise	HR	Schulungsmatrix

7.8 Verknüpfung zu anderen Dokumenten

- **Rechtsgrundlagen (Art. 6):** Basis für Rechtmäßigkeit
- **Informationspflichten (Art. 13-14):** Umsetzung der Transparenz
- **Verzeichnis (Art. 30):** Dokumentation der Rechtsgrundlagen
- **Betroffenenrechte (Art. 12-23):** Transparenz über Rechte

7.9 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Fehlende Rechtsgrundlage	Verarbeitung ohne Prüfung	Rechtsgrundlagen-Check vor Verarbeitung
Intransparente Information	Versteckte Datenschutzerklärung	Prominente Platzierung und klare Sprache
Unfaire Praktiken	Cookie-Wall ohne Alternative	Echte Wahlmöglichkeiten bieten
Unverständliche Sprache	Juristische Fachsprache	Verständliche Formulierungen

---

Nächste Schritte: 1. Implementieren Sie Rechtsgrundlagen-Prüfung für alle Verarbeitungen 2. Überarbeiten Sie Datenschutzerklärungen auf Verständlichkeit 3. Etablieren Sie faire Verarbeitungspraktiken 4. Schulen Sie Mitarbeiter zu Transparenzanforderungen 5. Dokumentieren Sie alle Maßnahmen für Accountability

ewpage

Chapter 8

Zweckbindung

Dokument-ID: 0110
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

8.1 Zweck

Dieses Dokument beschreibt die Umsetzung des Grundsatzes der Zweckbindung in der {{ meta.organization }}. Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben und verarbeitet werden.

8.2 Grundsatz gemäß Art. 5 Abs. 1 lit. b DSGVO

Rechtliche Anforderung:
Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

8.2.1 Kernelemente

1. **Festgelegte Zwecke:** Zwecke müssen vor der Erhebung definiert sein
2. **Eindeutige Zwecke:** Zwecke müssen klar und präzise formuliert sein
3. **Legitime Zwecke:** Zwecke müssen rechtmäßig und nachvollziehbar sein
4. **Keine inkompatible Weiterverarbeitung:** Neue Zwecke müssen vereinbar sein oder neue Rechtsgrundlage haben

8.3 Zweckdefinition

8.3.1 Anforderungen an Zweckbeschreibungen

Zwecke müssen sein: - Konkret und spezifisch (nicht “geschäftliche Zwecke”) - Verständlich für betroffene Personen - Vor der Datenerhebung festgelegt - Dokumentiert im Verzeichnis von Verarbeitungstätigkeiten - Kommuniziert in Datenschutzerklärungen

8.3.2 Beispiele für Zweckdefinitionen

Gut definiert	Schlecht definiert
“Abwicklung von Kundenbestellungen”	“Geschäftliche Zwecke”
“Versand des monatlichen Newsletters”	“Marketing”
“Erfüllung steuerrechtlicher Pflichten”	“Rechtliche Anforderungen”
“Bearbeitung von Bewerbungen”	“Personalverwaltung”

8.4 Zweckbindung in unserer Organisation

8.4.1 Verarbeitungszwecke

Verarbeitungstätigkeit	Definierter Zweck	Rechtsgrundlage	Datenarten
[TODO: Kundenverwaltung]	[TODO: Vertragserfüllung, Kundenbetreuung]	Art. 6 Abs. 1 lit. b	[TODO: Stammdaten]
[TODO: Newsletter]	[TODO: Versand von Produktinformationen]	Art. 6 Abs. 1 lit. a	[TODO: E-Mail, Name]
[TODO: Buchhaltung]	[TODO: Erfüllung steuerrechtlicher Pflichten]	Art. 6 Abs. 1 lit. c	[TODO: Rechnungsdaten]
[TODO: Bewerbermanagement]	[TODO: Bearbeitung von Bewerbungen]	Art. 6 Abs. 1 lit. b	[TODO: Bewerberdaten]

8.4.2 Prozess zur Zweckdefinition

Bei neuen Verarbeitungen:

1. **Zweck klar definieren**
   - Was soll erreicht werden?
   - Warum werden die Daten benötigt?
   - Wie trägt die Verarbeitung zum Zweck bei?
2. **Zweck dokumentieren**
   - Im Verzeichnis von Verarbeitungstätigkeiten (Art. 30)
   - In Datenschutzerklärungen (Art. 13-14)
   - In internen Verarbeitungsrichtlinien
3. **Zweck kommunizieren**
   - Betroffene Personen informieren
   - Mitarbeiter schulen

- Auftragsverarbeiter instruieren

8.5 Weiterverarbeitung für andere Zwecke

8.5.1 Prüfung der Zweckvereinbarkeit (Art. 6 Abs. 4)

Wenn Daten für einen neuen Zweck verarbeitet werden sollen, muss geprüft werden:

1. **Ist der neue Zweck mit dem ursprünglichen Zweck vereinbar?**

Kriterien für Vereinbarkeit (Art. 6 Abs. 4): - Verbindung zwischen ursprünglichem und neuem Zweck - Kontext der Datenerhebung - Art der personenbezogenen Daten - Mögliche Folgen für betroffene Personen - Vorhandene Garantien (z.B. Verschlüsselung, Pseudonymisierung)

2. **Wenn vereinbar:** Weiterverarbeitung ist zulässig
3. **Wenn nicht vereinbar:** Neue Rechtsgrundlage oder Einwilligung erforderlich

8.5.2 Vereinbarkeitstest

Kriterium	Prüffrage	Bewertung
Verbindung	Besteht ein sachlicher Zusammenhang?	[TODO]
Kontext	Entspricht es den Erwartungen der betroffenen Person?	[TODO]
Datenart	Sind die Daten für den neuen Zweck geeignet?	[TODO]
Folgen	Welche Auswirkungen hat die Weiterverarbeitung?	[TODO]
Garantien	Welche Schutzmaßnahmen sind vorhanden?	[TODO]

Ergebnis: Vereinbar / Nicht vereinbar

8.5.3 Beispiele für Zweckvereinbarkeit

Vereinbare Weiterverarbeitung: - Kundendaten für Vertragserfüllung → Weiterverarbeitung für Gewährleistungsansprüche - Mitarbeiterdaten für Gehaltsabrechnung → Weiterverarbeitung für Sozialversicherungsmeldungen - Bestelldaten → Weiterverarbeitung für Buchhaltung und Steuern

Nicht vereinbare Weiterverarbeitung (neue Rechtsgrundlage erforderlich): - Kundendaten für Vertragserfüllung → Weiterverarbeitung für Werbung (Einwilligung erforderlich) - Bewerberdaten → Weiterverarbeitung für andere Stellenangebote (neue Einwilligung erforderlich) - Gesundheitsdaten für Behandlung → Weiterverarbeitung für Forschung (neue Rechtsgrundlage erforderlich)

8.6 Ausnahmen von der Zweckbindung

8.6.1 Weiterverarbeitung für bestimmte Zwecke (Art. 5 Abs. 1 lit. b)

Immer zulässig (keine Vereinbarkeitsprüfung erforderlich): - Archivzwecke im öffentlichen Interesse - Wissenschaftliche oder historische Forschungszwecke - Statistische Zwecke

Voraussetzung: Geeignete Garantien (z.B. Pseudonymisierung, Zugriffsbeschränkungen)

8.7 Maßnahmen zur Sicherstellung der Zweckbindung

8.7.1 Organisatorische Maßnahmen

Maßnahme	Beschreibung	Verantwortlich	Status
[TODO: Zweckdefinition]	Klare Zweckdefinition vor Datenerhebung	Fachabteilung	[TODO]
[TODO: Dokumentation]	Pflege des Verzeichnisses Art. 30	DSB	[TODO]
[TODO: Vereinbarkeitsprüfung]	Prozess für neue Zwecke	DSB	[TODO]
[TODO: Schulung]	Mitarbeiterschulung zur Zweckbindung	HR	[TODO]

8.7.2 Technische Maßnahmen

- [TODO: Zugriffskontrolle nach Zwecken]
- [TODO: Zweckbasierte Datenbanksegmentierung]
- [TODO: Automatisierte Zweckprüfung bei Datenzugriff]
- [TODO: Logging von Zweckänderungen]

8.8 Kontrollen und Überwachung

8.8.1 Regelmäßige Überprüfungen

Kontrolle	Frequenz	Verantwortlich	Dokumentation
Zweckdefinitionen	Quartalsweise	DSB	Prüfprotokoll
Vereinbarkeitsprüfungen	Bei Bedarf	DSB	Vereinbarkeitstest
Verarbeitungsverzeichnis	Quartalsweise	DSB	Aktualisierungsprotokoll
Mitarbeiterschulungen	Jährlich	HR	Schulungsnachweise

8.9 Dokumentation

8.9.1 Nachweispflichten

Für jede Verarbeitung dokumentieren: - Definierter Zweck - Rechtsgrundlage für den Zweck - Datenarten, die für den Zweck erforderlich sind - Speicherdauer in Bezug auf den Zweck - Bei Weiterverarbeitung: Vereinbarkeitstest oder neue Rechtsgrundlage

8.9.2 Checkliste für neue Verarbeitungen

- ☐ Zweck klar und eindeutig definiert
- ☐ Zweck ist legitim und rechtmäßig
- ☐ Zweck vor Datenerhebung festgelegt
- ☐ Zweck im Verzeichnis Art. 30 dokumentiert
- ☐ Zweck in Datenschutzerklärung kommuniziert
- ☐ Nur für den Zweck erforderliche Daten erhoben
- ☐ Speicherdauer am Zweck orientiert
- ☐ Mitarbeiter über Zweck informiert

8.10 Verknüpfung zu anderen Dokumenten

- **Datenschutzgrundsätze (Art. 5):** Zweckbindung als Grundprinzip
- **Rechtsgrundlagen (Art. 6):** Legitimität der Zwecke
- **Verzeichnis (Art. 30):** Dokumentation der Zwecke
- **Informationspflichten (Art. 13-14):** Kommunikation der Zwecke
- **Datenminimierung (Art. 5 Abs. 1 lit. c):** Zweckbezogene Datenerhebung

8.11 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Unklare Zwecke	"Geschäftliche Zwecke"	Konkrete Zweckdefinition
Zweckentfremdung	Kundendaten für Werbung ohne Einwilligung	Vereinbarkeitsprüfung durchführen
Fehlende Dokumentation	Zweck nicht im Verzeichnis	Verzeichnis Art. 30 pflegen
Nachträgliche Zweckänderung	Zweck nach Erhebung geändert	Zweck vor Erhebung festlegen

---

Nächste Schritte: 1. Definieren Sie klare Zwecke für alle Verarbeitungstätigkeiten 2. Dokumentieren Sie Zwecke im Verzeichnis von Verarbeitungstätigkeiten 3. Implementieren Sie Vereinbarkeitsprüfung für neue Zwecke 4. Schulen Sie Mitarbeiter zur Zweckbindung 5. Überprüfen Sie regelmäßig die Einhaltung der Zweckbindung

ewpage

Chapter 9

Datenminimierung

Dokument-ID: 0120
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

9.1 Zweck

Dieses Dokument beschreibt die Umsetzung des Grundsatzes der Datenminimierung in der {{ meta.organization }}. Es dürfen nur die personenbezogenen Daten erhoben werden, die für den jeweiligen Zweck tatsächlich erforderlich sind.

9.2 Grundsatz gemäß Art. 5 Abs. 1 lit. c DSGVO

Rechtliche Anforderung:
Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

9.2.1 Drei Kriterien

1. **Angemessen:** Daten müssen in einem vernünftigen Verhältnis zum Zweck stehen
2. **Erheblich:** Daten müssen für den Zweck relevant sein
3. **Auf das Notwendige beschränkt:** Nur die minimal erforderlichen Daten erheben

9.3 Erforderlichkeitsprüfung

9.3.1 Prüfprozess für Datenerhebung

Vor jeder Datenerhebung prüfen:

1. **Ist die Datenerhebung für den Zweck erforderlich?**

- Kann der Zweck ohne diese Daten erreicht werden?
- Gibt es mildere Mittel?
- Ist die Datenerhebung verhältnismäßig?

2. **Welche Daten sind minimal erforderlich?**
   - Welche Daten sind zwingend notwendig?
   - Welche Daten sind "nice-to-have" (zu vermeiden)?
   - Können Daten anonymisiert oder pseudonymisiert werden?
3. **Dokumentation der Erforderlichkeit**
   - Begründung im Verzeichnis von Verarbeitungstätigkeiten
   - Nachweis der Erforderlichkeitsprüfung
   - Regelmäßige Überprüfung

9.3.2 Erforderlichkeitsmatrix

Datenart	Zweck	Erforderlich?	Begründung	Alternative
[TODO: Name]	[TODO: Vertragserfüllung]	Ja	[TODO: Identifikation]	Keine
[TODO: Geburtsdatum]	[TODO: Newsletter]	Nein	[TODO: Nicht erforderlich]	Weglassen
[TODO: Adresse]	[TODO: Lieferung]	Ja	[TODO: Zustellung]	Packstation
[TODO: Telefon]	[TODO: Kontakt]	Teilweise	[TODO: Alternative E-Mail]	E-Mail

9.4 Umsetzung in unserer Organisation

9.4.1 Datenerhebung nach Kategorien

Pflichtangaben vs. freiwillige Angaben:

Verarbeitungszweck	Pflichtangaben	Freiwillige Angaben	Nicht erforderlich
[TODO: Bestellung]	[TODO: Name, Adresse, Zahlung]	[TODO: Telefon]	[TODO: Geburtsdatum]
[TODO: Newsletter]	[TODO: E-Mail]	[TODO: Name]	[TODO: Adresse]
[TODO: Kundenkonto]	[TODO: E-Mail, Passwort]	[TODO: Profilbild]	[TODO: Soziale Medien]

Kennzeichnung in Formularen: - Pflichtfelder mit * markieren - Freiwillige Felder klar kennzeichnen - Erklärung, warum Daten benötigt werden

9.4.2 Maßnahmen zur Datenminimierung

Maßnahme	Beschreibung	Verantwortlich	Status
[TODO: Erforderlichkeitsprüfung]	Prüfung vor neuen Verarbeitungen	DSB	[TODO]
[TODO: Formularoptimierung]	Reduzierung von Eingabefeldern	IT	[TODO]
[TODO: Anonymisierung]	Wo möglich anonyme Daten nutzen	IT	[TODO]
[TODO: Pseudonymisierung]	Pseudonyme statt Klardaten	IT	[TODO]

9.5 Technische Umsetzung

9.5.1 Privacy by Design (Art. 25)

Datenminimierung durch Technikgestaltung:

- [TODO: Formulare nur mit erforderlichen Feldern]
- [TODO: Optionale Felder klar gekennzeichnet]
- [TODO: Automatische Anonymisierung nach Zweckerfüllung]
- [TODO: Pseudonymisierung sensibler Daten]
- [TODO: Aggregation statt Einzeldaten für Statistiken]

9.5.2 Anonymisierung und Pseudonymisierung

Anonymisierung: - Vollständige Entfernung des Personenbezugs - Keine Rückführbarkeit auf Personen - Keine DSGVO-Anwendung mehr

Pseudonymisierung: - Trennung von Identifikationsdaten und Inhaltsdaten - Rückführbarkeit nur mit Zusatzinformation - Weiterhin DSGVO-Anwendung, aber geringeres Risiko

Anwendungsfälle:

Zweck	Methode	Beispiel
[TODO: Statistik]	Anonymisierung	Aggregierte Nutzungsdaten
[TODO: Analyse]	Pseudonymisierung	Nutzer-ID statt Name
[TODO: Forschung]	Anonymisierung	Entfernung aller Identifikatoren
[TODO: Backup]	Pseudonymisierung	Verschlüsselte Personendaten

9.6 Vermeidung übermäßiger Datenerhebung

9.6.1 Häufige Fehler

Fehler	Beispiel	Korrektur
“Nice-to-have” Daten	Geburtsdatum für Newsletter	Nur E-Mail erheben
Übermäßige Profilbildung	Tracking aller Aktivitäten	Nur notwendiges Tracking
Vorratsdatenspeicherung	“Könnte mal nützlich sein”	Nur bei konkretem Zweck

Fehler	Beispiel	Korrektur
Fehlende Differenzierung	Alle Daten als Pflicht	Pflicht vs. freiwillig trennen

9.6.2 Checkliste gegen übermäßige Datenerhebung

- ☐ Jedes Datenfeld hat einen dokumentierten Zweck
- ☐ Keine "nice-to-have" Datenfelder
- ☐ Pflicht- und freiwillige Felder getrennt
- ☐ Anonymisierung/Pseudonymisierung geprüft
- ☐ Keine Vorratsdatenspeicherung
- ☐ Regelmäßige Überprüfung der Erforderlichkeit
- ☐ Mitarbeiter geschult zu Datenminimierung

9.7 Regelmäßige Überprüfung

9.7.1 Datenbestandsprüfung

Quartalsweise prüfen:

1. **Welche Daten werden erhoben?**
   - Inventarisierung aller Datenfelder
   - Zuordnung zu Verarbeitungszwecken
2. **Sind alle Daten noch erforderlich?**
   - Erforderlichkeitsprüfung für bestehende Daten
   - Identifikation überflüssiger Daten
3. **Können Daten reduziert werden?**
   - Möglichkeiten zur Anonymisierung
   - Möglichkeiten zur Pseudonymisierung
   - Löschung nicht mehr erforderlicher Daten

9.7.2 Kontrollen

Kontrolle	Frequenz	Verantwortlich	Dokumentation
Erforderlichkeitsprüfung	Bei neuen Verarbeitungen	DSB	Prüfprotokoll
Datenbestandsprüfung	Quartalsweise	DSB	Inventarliste
Formularprüfung	Jährlich	IT/DSB	Prüfbericht
Anonymisierungspotenzial	Jährlich	IT	Analysebericht

9.8 Dokumentation

9.8.1 Nachweispflichten

Für jede Verarbeitung dokumentieren: - Welche Daten werden erhoben? - Warum ist jede Datenart erforderlich? - Wurden Alternativen geprüft (Anonymisierung, Pseudonymisierung)? - Wie wird die Erforderlichkeit regelmäßig überprüft?

9.8.2 Verzeichnis von Verarbeitungstätigkeiten (Art. 30)

Dokumentation der Datenminimierung: - Kategorien personenbezogener Daten - Begründung der Erforderlichkeit - Maßnahmen zur Minimierung - Anonymisierung/Pseudonymisierung

9.9 Verknüpfung zu anderen Dokumenten

- **Datenschutzgrundsätze (Art. 5):** Datenminimierung als Grundprinzip
- **Zweckbindung (Art. 5 Abs. 1 lit. b):** Zweckbezogene Erforderlichkeit
- **Privacy by Design (Art. 25):** Technische Umsetzung
- **Verzeichnis (Art. 30):** Dokumentation der Datenarten
- **Informationspflichten (Art. 13-14):** Information über erhobene Daten

9.10 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Übermäßige Datenerhebung	Alle Daten "für alle Fälle"	Erforderlichkeitsprüfung
Fehlende Differenzierung	Alle Felder als Pflicht	Pflicht vs. freiwillig
Vorratsdatenspeicherung	Daten ohne konkreten Zweck	Zweckbindung beachten
Keine Anonymisierung	Klardaten wo nicht nötig	Anonymisierung prüfen

---

Nächste Schritte: 1. Führen Sie Erforderlichkeitsprüfung für alle Datenerhebungen durch 2. Optimieren Sie Formulare und reduzieren Sie Datenfelder 3. Implementieren Sie Anonymisierung und Pseudonymisierung 4. Schulen Sie Mitarbeiter zu Datenminimierung 5. Etablieren Sie regelmäßige Datenbestandsprüfungen

ewpage

Chapter 10

Richtigkeit

Dokument-ID: 0130
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

10.1 Zweck

Dieses Dokument beschreibt die Umsetzung des Grundsatzes der Richtigkeit in der {{ meta.organization }}. Personenbezogene Daten müssen sachlich richtig und aktuell sein.

10.2 Grundsatz gemäß Art. 5 Abs. 1 lit. d DSGVO

Rechtliche Anforderung:
Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

10.2.1 Zwei Komponenten

1. **Sachliche Richtigkeit:** Daten müssen den Tatsachen entsprechen
2. **Aktualität:** Daten müssen auf dem neuesten Stand gehalten werden

10.3 Maßnahmen zur Sicherstellung der Richtigkeit

10.3.1 Datenqualitätsmanagement

Prozesse zur Qualitätssicherung:

Maßnahme	Beschreibung	Verantwortlich	Frequenz
[TODO: Eingabevalidierung]	Prüfung bei Dateneingabe	IT	Kontinuierlich
[TODO: Plausibilitätsprüfung]	Automatische Konsistenzprüfung	IT	Kontinuierlich
[TODO: Datenabgleich]	Abgleich mit externen Quellen	Fachabteilung	[TODO: Monatlich]
[TODO: Aktualisierungsaufforderung]	Erinnerung an Datenaktualisierung	IT	[TODO: Jährlich]

10.3.2 Eingabevalidierung

Technische Maßnahmen bei Dateneingabe: - [TODO: Formatprüfung (E-Mail, Telefon, PLZ)] - [TODO: Pflichtfeldprüfung] - [TODO: Wertebereichsprüfung] - [TODO: Duplikatsprüfung] - [TODO: Konsistenzprüfung zwischen Feldern]

10.3.3 Datenaktualisierung

Prozesse zur Aktualitätssicherung:

Datenart	Aktualisierungsprozess	Frequenz	Verantwortlich
[TODO: Kundenstammdaten]	[TODO: Aktualisierung bei Kontakt]	Bei Bedarf	Vertrieb
[TODO: Mitarbeiterdaten]	[TODO: Jährliche Überprüfung]	Jährlich	HR
[TODO: Kontaktdaten]	[TODO: Validierung bei Nutzung]	Bei Nutzung	IT
[TODO: Vertragsdaten]	[TODO: Update bei Vertragsänderung]	Bei Änderung	Legal

10.4 Berichtigungsrecht (Art. 16 DSGVO)

10.4.1 Umsetzung des Berichtigungsrechts

Betroffene Personen haben das Recht auf: - Unverzügliche Berichtigung unrichtiger Daten - Vervollständigung unvollständiger Daten - Ergänzende Erklärung

Prozess für Berichtigungsanträge:

1. **Eingang des Antrags**
   - Identifikation der betroffenen Person
   - Dokumentation des Antrags
   - Bestätigung des Eingangs
2. **Prüfung der Unrichtigkeit**

- Überprüfung der beanstandeten Daten
- Abgleich mit Nachweisen
- Entscheidung über Berichtigung

3. **Durchführung der Berichtigung**
   - Korrektur in allen Systemen
   - Information an Empfänger (Art. 19)
   - Dokumentation der Berichtigung
4. **Rückmeldung an betroffene Person**
   - Information über durchgeführte Berichtigung
   - Frist: Unverzüglich, spätestens 1 Monat

10.4.2 Berichtigungskanäle

Kanal	Beschreibung	Bearbeitungszeit	Verantwortlich
[TODO: Online-Portal]	Selbstberichtigung durch Nutzer	Sofort	IT
[TODO: E-Mail]	Antrag per E-Mail	1 Monat	DSB
[TODO: Schriftlich]	Antrag per Post	1 Monat	DSB
[TODO: Telefon]	Telefonische Berichtigung	Sofort	Kundenservice

10.5 Fehlerkorrekturverfahren

10.5.1 Identifikation von Fehlern

Fehlerquellen: - Eingabefehler bei Datenerfassung - Veraltete Daten durch Zeitablauf - Fehlerhafte Datenübermittlung - Systemfehler bei Datenverarbeitung - Unvollständige Datenerhebung

Fehlererkennung: - [TODO: Automatische Plausibilitätsprüfung] - [TODO: Meldung durch betroffene Personen] - [TODO: Regelmäßige Datenqualitätsprüfung] - [TODO: Rückmeldungen von Empfängern]

10.5.2 Korrekturprozess

Schritte bei Fehlererkennung:

1. **Fehleranalyse**
   - Art des Fehlers
   - Umfang der Betroffenheit
   - Ursache des Fehlers
2. **Fehlerkorrektur**
   - Berichtigung der fehlerhaften Daten
   - Korrektur in allen betroffenen Systemen
   - Dokumentation der Korrektur
3. **Benachrichtigung**

- Information der betroffenen Person
- Mitteilung an Empfänger (Art. 19)
- Dokumentation der Benachrichtigungen

4. **Ursachenbeseitigung**
   - Analyse der Fehlerursache
   - Maßnahmen zur Fehlervermeidung
   - Prozessverbesserung

10.6 Mitteilungspflicht (Art. 19 DSGVO)

10.6.1 Benachrichtigung von Empfängern

Bei Berichtigung oder Löschung müssen Empfänger informiert werden:

Empfängertyp	Benachrichtigungspflicht	Ausnahme	Dokumentation
Auftragsverarbeiter	Ja	Unmöglich/unverhältnismäßig	Benachrichtigungsprotokoll
Dritte Empfänger	Ja	Unmöglich/unverhältnismäßig	Benachrichtigungsprotokoll
Öffentliche Stellen	Ja	Unmöglich/unverhältnismäßig	Benachrichtigungsprotokoll

Prozess: 1. Identifikation aller Empfänger 2. Benachrichtigung über Berichtigung/Löschung 3. Dokumentation der Benachrichtigungen 4. Information der betroffenen Person über Empfänger (auf Verlangen)

10.7 Datenqualitätskontrollen

10.7.1 Regelmäßige Überprüfungen

Kontrolle	Frequenz	Verantwortlich	Dokumentation
Datenqualitätsaudit	Jährlich	DSB	Audit-Bericht
Stichprobenprüfung	Quartalsweise	Fachabteilung	Prüfprotokoll
Systemvalidierung	Bei Änderungen	IT	Testprotokoll
Berichtigungsstatistik	Monatlich	DSB	Statistikbericht

10.7.2 Qualitätskennzahlen

KPIs für Datenqualität: - Fehlerquote bei Dateneingabe - Anzahl Berichtigungsanträge - Durchschnittliche Bearbeitungszeit - Anteil veralteter Datensätze - Vollständigkeitsgrad der Daten

10.8 Dokumentation

10.8.1 Nachweispflichten

Dokumentation für Accountability: - Prozesse zur Sicherstellung der Richtigkeit - Berichtigungsverfahren und -fristen - Bearbeitete Berichtigungsanträge - Benachrichtigungen an Empfänger - Datenqualitätskontrollen und deren Ergebnisse

10.8.2 Berichtigungsregister

Datum	Betroffene Person	Art der Berichtigung	Empfänger benachrichtigt	Bearbeiter
[TODO]	[TODO]	[TODO]	Ja/Nein	[TODO]

10.9 Verknüpfung zu anderen Dokumenten

- **Datenschutzgrundsätze (Art. 5):** Richtigkeit als Grundprinzip
- **Berichtigungsrecht (Art. 16):** Umsetzung des Betroffenenrechts
- **Mitteilungspflicht (Art. 19):** Benachrichtigung von Empfängern
- **Verzeichnis (Art. 30):** Dokumentation der Datenqualität
- **TOM (Art. 32):** Technische Maßnahmen zur Qualitätssicherung

10.10 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Veraltete Daten	Keine Aktualisierung	Regelmäßige Überprüfung
Fehlerhafte Eingabe	Keine Validierung	Eingabevalidierung
Verzögerte Berichtigung	Lange Bearbeitungszeit	Prozessoptimierung
Fehlende Benachrichtigung	Empfänger nicht informiert	Benachrichtigungsprozess

---

Nächste Schritte: 1. Implementieren Sie Eingabevalidierung und Plausibilitätsprüfung 2. Etablieren Sie Prozesse zur regelmäßigen Datenaktualisierung 3. Richten Sie Berichtigungsverfahren gemäß Art. 16 ein 4. Implementieren Sie Benachrichtigungsprozess für Empfänger 5. Führen Sie regelmäßige Datenqualitätskontrollen durch

ewpage

Chapter 11

Speicherbegrenzung

Dokument-ID: 0140
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

11.1 Zweck

Dieses Dokument beschreibt die Umsetzung des Grundsatzes der Speicherbegrenzung in der {{ meta.organization }}. Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für den Verarbeitungszweck erforderlich ist.

11.2 Grundsatz gemäß Art. 5 Abs. 1 lit. e DSGVO

Rechtliche Anforderung:
Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

11.2.1 Kernprinzip

Speicherdauer = Zweckerfüllung + gesetzliche Aufbewahrungsfristen

Nach Ablauf der Speicherdauer müssen Daten: - Gelöscht werden, oder - Anonymisiert werden, oder - Archiviert werden (mit Zugriffsbeschränkungen)

11.3 Löschkonzept

11.3.1 Festlegung von Löschfristen

Kriterien für Löschfristen: 1. Zweck der Verarbeitung 2. Gesetzliche Aufbewahrungsfristen 3. Vertragliche Verpflichtungen 4. Berechtigte Interessen 5. Verjährungsfristen

11.3.2 Löschfristenmatrix

Verarbeitungszweck	Datenart	Löschfrist	Rechtsgrundlage	Ausnahmen
[TODO: Kundenbestellung]	Bestelldaten	Nach Vertragserfüllung + 2 Jahre	Gewährleistung	Steuerrecht: 10 Jahre
[TODO: Newsletter]	E-Mail, Name	Bis Widerruf	Einwilligung	Keine
[TODO: Bewerbung]	Bewerberdaten	6 Monate nach Absage	Berechtigtes Interesse	Mit Einwilligung länger
[TODO: Buchhaltung]	Rechnungsdaten	10 Jahre	AO, HGB	Keine
[TODO: Mitarbeiterdaten]	Personaldaten	10 Jahre nach Austritt	Sozialversicherung	Keine

11.4 Gesetzliche Aufbewahrungsfristen

11.4.1 Steuerrecht (Deutschland)

Dokumentart	Aufbewahrungsfrist	Rechtsgrundlage
Bücher, Aufzeichnungen, Jahresabschlüsse	10 Jahre	§ 147 AO
Handelsbriefe, Buchungsbelege	10 Jahre	§ 147 AO
Sonstige Unterlagen	6 Jahre	§ 147 AO

11.4.2 Handelsrecht (Deutschland)

Dokumentart	Aufbewahrungsfrist	Rechtsgrundlage
Handelsbücher, Inventare, Bilanzen	10 Jahre	§ 257 HGB
Handelsbriefe	6 Jahre	§ 257 HGB
Buchungsbelege	10 Jahre	§ 257 HGB

11.4.3 Weitere gesetzliche Fristen

- [TODO: Sozialversicherungsrecht]
- [TODO: Arbeitsrecht]
- [TODO: Produkthaftung]
- [TODO: Branchenspezifische Vorschriften]

11.5 Löschprozesse

11.5.1 Routinemäßige Löschung

Automatisierte Löschprozesse:

System/Datenbank	Löschrhythmus	Methode	Verantwortlich
[TODO: CRM-System]	Monatlich	Automatisiert	IT
[TODO: Webserver-Logs]	Täglich	Automatisiert	IT
[TODO: Backup-Systeme]	Bei Löschung	Manuell	IT
[TODO: Archiv]	Jährlich	Manuell	Fachabteilung

11.5.2 Löschverfahren

Schritte bei Löschung:

1. **Identifikation löschbarer Daten**
   - Automatische Prüfung der Löschfristen
   - Berücksichtigung von Ausnahmen
   - Erstellung Löschliste
2. **Prüfung vor Löschung**
   - Keine laufenden Verfahren
   - Keine gesetzlichen Aufbewahrungspflichten
   - Keine vertraglichen Verpflichtungen
3. **Durchführung der Löschung**
   - Löschung in allen Systemen
   - Löschung in Backups (oder Markierung)
   - Sichere Löschung (unwiederbringlich)
4. **Dokumentation**
   - Protokollierung der Löschung
   - Nachweis der Löschung
   - Aufbewahrung des Löschprotokolls

11.5.3 Sichere Löschung

Technische Löschmethoden: - Überschreiben von Datenträgern - Kryptografische Löschung (Schlüsselvernichtung) - Physische Vernichtung von Datenträgern - Sichere Löschung in Cloud-Systemen

11.6 Ausnahmen von der Löschpflicht

11.6.1 Archivierung im öffentlichen Interesse (Art. 89 DSGVO)

Zulässige Archivierung für: - Archivzwecke im öffentlichen Interesse - Wissenschaftliche oder historische Forschungszwecke - Statistische Zwecke

Voraussetzungen: - Geeignete Garantien (Pseudonymisierung, Zugriffsbeschränkungen) - Datenminimierung - Technische und organisatorische Maßnahmen

11.6.2 Aufbewahrung für Rechtsansprüche

Aufbewahrung zulässig bei: - Laufenden Gerichtsverfahren - Drohenden Rechtsstreitigkeiten - Verjährungsfristen noch nicht abgelaufen

Maßnahmen: - Einschränkung der Verarbeitung (Art. 18) - Zugriffsbeschränkungen - Dokumentation der Aufbewahrungsgründe

11.7 Löschrecht (Art. 17 DSGVO)

11.7.1 Umsetzung des Löschrechts

Betroffene Personen haben Recht auf Löschung, wenn: - Daten nicht mehr erforderlich - Einwilligung widerrufen - Widerspruch eingelegt (Art. 21) - Daten unrechtmäßig verarbeitet - Rechtliche Verpflichtung zur Löschung

Ausnahmen vom Löschrecht: - Ausübung des Rechts auf freie Meinungsäußerung - Erfüllung rechtlicher Verpflichtungen - Geltendmachung von Rechtsansprüchen - Archivzwecke im öffentlichen Interesse

11.7.2 Löschantragsprozess

1. **Eingang des Antrags**
   - Identifikation der betroffenen Person
   - Dokumentation des Antrags
   - Bestätigung des Eingangs
2. **Prüfung der Löschpflicht**
   - Sind Daten noch erforderlich?
   - Bestehen Aufbewahrungspflichten?
   - Greifen Ausnahmen?
3. **Durchführung oder Ablehnung**
   - Bei Löschpflicht: Löschung durchführen
   - Bei Ausnahme: Begründete Ablehnung
   - Benachrichtigung von Empfängern (Art. 19)
4. **Rückmeldung**
   - Information über Löschung oder Ablehnung
   - Frist: Unverzüglich, spätestens 1 Monat

11.8 Kontrollen und Überwachung

11.8.1 Regelmäßige Überprüfungen

Kontrolle	Frequenz	Verantwortlich	Dokumentation
Löschfristenprüfung	Monatlich	IT	Löschprotokoll
Löschkonzept-Review	Jährlich	DSB	Review-Bericht
Backup-Löschung	Quartalsweise	IT	Backup-Protokoll
Löschanträge	Bei Eingang	DSB	Antragsregister

11.8.2 Löschprotokollierung

Dokumentation jeder Löschung: - Datum und Uhrzeit - Gelöschte Datenarten - Anzahl gelöschter Datensätze - Löschgrund (Frist, Antrag, etc.) - Durchführende Person - Betroffene Systeme

11.9 Dokumentation

11.9.1 Nachweispflichten

Für Accountability dokumentieren: - Löschkonzept mit Fristen - Löschprozesse und -verfahren - Durchgeführte Löschungen (Protokolle) - Bearbeitete Löschanträge - Ausnahmen und deren Begründung

11.9.2 Verzeichnis von Verarbeitungstätigkeiten (Art. 30)

Dokumentation der Speicherdauer: - Löschfristen für jede Verarbeitungstätigkeit - Begründung der Fristen - Gesetzliche Aufbewahrungspflichten - Löschverfahren

11.10 Verknüpfung zu anderen Dokumenten

- **Datenschutzgrundsätze (Art. 5):** Speicherbegrenzung als Grundprinzip
- **Löschrecht (Art. 17):** Umsetzung des Betroffenenrechts
- **Einschränkung (Art. 18):** Alternative zur Löschung
- **Mitteilungspflicht (Art. 19):** Benachrichtigung von Empfängern
- **Verzeichnis (Art. 30):** Dokumentation der Löschfristen

11.11 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Unbegrenzte Speicherung	“Für alle Fälle aufbewahren”	Löschfristen definieren
Fehlende Löschprozesse	Keine automatisierte Löschung	Löschroutinen implementieren
Ignorieren von Löschanträgen	Verzögerte Bearbeitung	Prozess etablieren
Unvollständige Löschung	Nur in einem System gelöscht	Alle Systeme prüfen

---

Nächste Schritte: 1. Definieren Sie Löschfristen für alle Verarbeitungstätigkeiten 2. Implementieren Sie automatisierte Löschprozesse 3. Etablieren Sie Verfahren für Löschanträge 4. Dokumentieren Sie Löschkonzept und -protokolle 5. Schulen Sie Mitarbeiter zu Löschpflichten

ewpage

Chapter 12

Integrität und Vertraulichkeit

Dokument-ID: 0150
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

12.1 Zweck

Dieses Dokument beschreibt die Umsetzung des Grundsatzes der Integrität und Vertraulichkeit in der {{ meta.organization }}. Personenbezogene Daten müssen sicher verarbeitet und vor unbefugtem Zugriff geschützt werden.

12.2 Grundsatz gemäß Art. 5 Abs. 1 lit. f DSGVO

Rechtliche Anforderung:
Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

12.2.1 Schutzziele

1. **Vertraulichkeit:** Schutz vor unbefugtem Zugriff
2. **Integrität:** Schutz vor unbefugter Veränderung
3. **Verfügbarkeit:** Schutz vor Verlust oder Zerstörung
4. **Belastbarkeit:** Widerstandsfähigkeit der Systeme

12.3 Technische und Organisatorische Maßnahmen (TOM)

12.3.1 Übersicht der Maßnahmenkategorien (Art. 32 DSGVO)

Kategorie	Beschreibung	Beispiele
Zutrittskontrolle	Schutz vor unbefugtem Zutritt	Zugangskontrollen, Alarmanlagen, Videoüberwachung
Zugangskontrolle	Schutz vor unbefugter Systemnutzung	Benutzerauthentifizierung, Passwortrichtlinien, MFA
Zugriffskontrolle	Schutz vor unbefugtem Datenzugriff	Berechtigungskonzept, Rollenmodell, Need-to-know
Weitergabekontrolle	Schutz bei Datenübermittlung	Verschlüsselung, VPN, sichere Protokolle
Eingabekontrolle	Nachvollziehbarkeit von Eingaben	Logging, Audit-Trails, Versionierung
Auftragskontrolle	Sicherheit bei Auftragsverarbeitung	AVV, Kontrollen, Audits
Verfügbarkeitskontrolle	Schutz vor Datenverlust	Backups, Redundanz, Disaster Recovery
Trennungskontrolle	Trennung unterschiedlicher Zwecke	Mandantenfähigkeit, Datensegmentierung

12.4 Zutrittskontrolle

12.4.1 Physische Sicherheit

Maßnahmen zum Schutz vor unbefugtem Zutritt:

Maßnahme	Beschreibung	Verantwortlich	Status
[TODO: Zugangskontrollen]	Chipkarten, Schlüssel, Codes	Facility Management	[TODO]
[TODO: Besucher-registrierung]	Anmeldung und Begleitung	Empfang	[TODO]
[TODO: Videoüberwachung]	Überwachung sensibler Bereiche	Security	[TODO]
[TODO: Alarmanlagen]	Einbruchmeldesysteme	Security	[TODO]
[TODO: Serverraum-Sicherung]	Besonderer Schutz für Server	IT	[TODO]

12.5 Zugangskontrolle

12.5.1 Authentifizierung und Autorisierung

Maßnahmen zur Systemzugangskontrolle:

Maßnahme	Beschreibung	Implementierung	Status
[TODO: Benutzer-authentifizierung]	Eindeutige Benutzerkonten	Active Directory	[TODO]
[TODO: Passwortrichtlinie]	Komplexität, Länge, Ablauf	Gruppenrichtlinien	[TODO]
[TODO: Multi-Faktor-Authentifizierung]	Zusätzlicher Authentifizierungsfaktor	MFA-System	[TODO]
[TODO: Single Sign-On]	Zentrale Authentifizierung	SSO-Lösung	[TODO]
[TODO: Automatische Sperrung]	Nach Inaktivität	Systemeinstellung	[TODO]

12.5.2 Passwortrichtlinie

Anforderungen: - Mindestlänge: [TODO: z.B. 12 Zeichen] - Komplexität: [TODO: Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen] - Ablauf: [TODO: z.B. 90 Tage] - Historie: [TODO: z.B. letzte 5 Passwörter nicht wiederverwendbar] - Sperrung: [TODO: Nach 5 Fehlversuchen]

12.6 Zugriffskontrolle

12.6.1 Berechtigungskonzept

Prinzipien: - Need-to-know: Nur erforderliche Zugriffe - Least Privilege: Minimale Berechtigungen - Rollenbased Access Control (RBAC): Rollenbasierte Zugriffe - Regelmäßige Überprüfung: Quartalsweise Rezertifizierung

12.6.2 Berechtigungsmatrix

Rolle	System/Daten	Zugriff	Begründung
[TODO: Administrator]	Alle Systeme	Vollzugriff	Systemverwaltung
[TODO: Vertrieb]	CRM	Lesen/Schreiben	Kundenbetreuung
[TODO: Buchhaltung]	Finanzsystem	Lesen/Schreiben	Rechnungswesen
[TODO: Support]	Ticketsystem	Lesen/Schreiben	Kundenservice

12.6.3 Zugriffskontrollprozesse

Prozess	Beschreibung	Verantwortlich	Frequenz
Berechtigungsvergabe	Antrag und Genehmigung	IT/Vorgesetzter	Bei Bedarf

Prozess	Beschreibung	Verantwortlich	Frequenz
Rezertifizierung	Überprüfung bestehender Rechte	IT/Vorgesetzter	Quartalsweise
Entzug bei Austritt	Sofortige Sperrung	HR/IT	Bei Austritt
Privilegierte Zugriffe	Besondere Kontrolle	IT-Sicherheit	Monatlich

12.7 Weitergabekontrolle

12.7.1 Verschlüsselung

Verschlüsselungsmaßnahmen:

Bereich	Methode	Standard	Status
[TODO: Datenübertragung]	TLS/SSL	TLS 1.2+	[TODO]
[TODO: E-Mail]	S/MIME oder PGP	-	[TODO]
[TODO: Datenträger]	Festplattenverschlüsselung	AES-256	[TODO]
[TODO: Datenbanken]	Transparent Data Encryption	AES-256	[TODO]
[TODO: Backups]	Verschlüsselte Backups	AES-256	[TODO]

12.7.2 Sichere Datenübermittlung

Maßnahmen: - [TODO: VPN für Remote-Zugriffe] - [TODO: HTTPS für Webanwendungen] - [TODO: SFTP für Dateitransfers] - [TODO: Verschlüsselte E-Mail für sensible Daten] - [TODO: Sichere Cloud-Verbindungen]

12.8 Eingabekontrolle

12.8.1 Logging und Audit-Trails

Protokollierung von:

Ereignis	Details	Aufbewahrung	Zugriff
[TODO: Anmeldungen]	Erfolg/Fehlschlag, Zeitpunkt	90 Tage	IT-Sicherheit
[TODO: Datenänderungen]	Wer, Was, Wann	1 Jahr	DSB
[TODO: Zugriffe auf sensible Daten]	Benutzer, Zeitpunkt, Daten	1 Jahr	DSB
[TODO: Systemänderungen]	Administrator, Änderung	2 Jahre	IT
[TODO: Sicherheitsereignisse]	Art, Zeitpunkt, Quelle	2 Jahre	IT-Sicherheit

12.8.2 Nachvollziehbarkeit

Maßnahmen: - Eindeutige Benutzeridentifikation - Zeitstempel für alle Aktionen - Unveränderbare Protokolle - Regelmäßige Auswertung - Langfristige Archivierung

12.9 Verfügbarkeitskontrolle

12.9.1 Backup und Recovery

Backup-Strategie:

Backup-Typ	Frequenz	Aufbewahrung	Speicherort	Verantwortlich
[TODO: Vollbackup]	Wöchentlich	4 Wochen	Offsite	IT
[TODO: Inkrementell]	Täglich	7 Tage	Onsite	IT
[TODO: Archiv]	Monatlich	1 Jahr	Offsite	IT

Recovery-Prozess: - Regelmäßige Restore-Tests - Dokumentierte Recovery-Verfahren - Recovery Time Objective (RTO): [TODO] - Recovery Point Objective (RPO): [TODO]

12.9.2 Business Continuity

Maßnahmen: - [TODO: Redundante Systeme] - [TODO: Disaster Recovery Plan] - [TODO: Notfallhandbuch] - [TODO: Regelmäßige Tests]

12.10 Incident Response

12.10.1 Sicherheitsvorfälle

Prozess bei Sicherheitsvorfällen:

1. **Erkennung und Meldung**
   - Identifikation des Vorfalls
   - Sofortige Meldung an IT-Sicherheit
   - Erste Bewertung
2. **Eindämmung**
   - Isolation betroffener Systeme
   - Schadensbegrenzung
   - Beweissicherung
3. **Analyse**
   - Ursachenanalyse
   - Umfang der Betroffenheit
   - Bewertung der Auswirkungen
4. **Behebung**
   - Beseitigung der Ursache
   - Wiederherstellung des Normalbetriebs
   - Dokumentation
5. **Nachbereitung**
   - Lessons Learned

- Verbesserungsmaßnahmen
- Schulungen

12.10.2 Datenschutzverletzungen (Art. 33-34 DSGVO)

Bei Datenschutzverletzungen zusätzlich: - Meldung an Aufsichtsbehörde (innerhalb 72 Stunden) - Benachrichtigung betroffener Personen (bei hohem Risiko) - Dokumentation im Verzeichnis von Datenschutzverletzungen

12.11 Kontrollen und Überwachung

12.11.1 Regelmäßige Überprüfungen

Kontrolle	Frequenz	Verantwortlich	Dokumentation
Sicherheitsaudit	Jährlich	IT-Sicherheit	Audit-Bericht
Penetrationstest	Jährlich	Externer Dienstleister	Testbericht
Berechtigungsprüfung	Quartalsweise	IT	Prüfprotokoll
Backup-Test	Monatlich	IT	Testprotokoll
Log-Auswertung	Wöchentlich	IT-Sicherheit	Analysebericht

12.12 Dokumentation

12.12.1 Nachweispflichten

Dokumentation der TOM: - Beschreibung aller technischen und organisatorischen Maßnahmen - Begründung der Angemessenheit - Wirksamkeitsnachweise (Tests, Audits) - Aktualisierung bei Änderungen

12.12.2 Sicherheitskonzept

Inhalte: - Schutzziele und Risikobewertung - Technische Maßnahmen - Organisatorische Maßnahmen - Verantwortlichkeiten - Kontrollen und Tests - Incident Response Plan

12.13 Verknüpfung zu anderen Dokumenten

- **Datenschutzgrundsätze (Art. 5):** Integrität und Vertraulichkeit als Grundprinzip
- **Sicherheit der Verarbeitung (Art. 32):** Detaillierte Anforderungen an TOM
- **Datenschutzverletzungen (Art. 33-34):** Meldepflichten bei Sicherheitsvorfällen
- **Verzeichnis (Art. 30):** Dokumentation der TOM
- **DSFA (Art. 35):** Risikobewertung und Maßnahmen

12.14 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Schwache Passwörter	Einfache Passwörter	Passwortrichtlinie durchsetzen

Verstoß	Beispiel	Vermeidung
Fehlende Verschlüsselung	Unverschlüsselte Übertragung	TLS/SSL implementieren
Übermäßige Berechtigungen	Alle haben Admin-Rechte	Berechtigungskonzept umsetzen
Keine Backups	Datenverlust ohne Recovery	Backup-Strategie implementieren

---

Nächste Schritte: 1. Implementieren Sie umfassende TOM gemäß Art. 32 2. Etablieren Sie Zugriffskontroll- und Berechtigungskonzept 3. Implementieren Sie Verschlüsselung für Daten in Ruhe und Übertragung 4. Richten Sie Backup- und Recovery-Prozesse ein 5. Etablieren Sie Incident Response Prozess

ewpage

Chapter 13

Transparente Information und Kommunikation

Dokument-ID: 0200
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

13.1 Zweck

Dieses Dokument beschreibt die Umsetzung der Anforderungen an transparente Information und Kommunikation in der {{ meta.organization }}. Betroffene Personen müssen ihre Rechte einfach und verständlich ausüben können.

13.2 Grundsatz gemäß Art. 12 DSGVO

Rechtliche Anforderungen:

Der Verantwortliche muss: - Transparente, verständliche und leicht zugängliche Informationen bereitstellen - In klarer und einfacher Sprache kommunizieren - Informationen unentgeltlich zur Verfügung stellen - Anfragen unverzüglich, spätestens innerhalb eines Monats beantworten - Geeignete Maßnahmen zur Identifikation treffen

13.3 Transparenzanforderungen

13.3.1 Verständliche Kommunikation

Anforderungen an Informationen:

Kriterium	Beschreibung	Umsetzung
Präzise	Konkret und spezifisch	[TODO: Klare Formulierungen]
Transparent	Offen und nachvollziehbar	[TODO: Vollständige Information]
Verständlich	Einfache Sprache	[TODO: Keine Fachbegriffe]
Leicht zugänglich	Einfach auffindbar	[TODO: Prominente Platzierung]

13.3.2 Sprachliche Anforderungen

Klare und einfache Sprache: - Vermeidung von Juristensprache - Kurze Sätze und Absätze - Erklärung von Fachbegriffen - Strukturierte Darstellung - Verwendung von Beispielen

Mehrsprachigkeit: - [TODO: Deutsch als Hauptsprache] - [TODO: Englisch für internationale Nutzer] - [TODO: Weitere Sprachen bei Bedarf]

13.4 Kommunikationskanäle

13.4.1 Bereitstellung von Informationen

Kanäle für Datenschutzinformationen:

Kanal	Zweck	Zielgruppe	Aktualisierung
[TODO: Website]	Datenschutzerklärung	Websitebesucher	Bei Änderungen
[TODO: App]	In-App-Datenschutzhinweise	App-Nutzer	Bei Änderungen
[TODO: E-Mail]	Direktinformation	Kunden	Bei Erstkontakt
[TODO: Formular]	Datenerhebung	Betroffene	Bei Erhebung
[TODO: Aushang]	Vor-Ort-Information	Besucher	Permanent

13.4.2 Kontaktmöglichkeiten

Kanäle für Betroffenenanfragen:

Kanal	Beschreibung	Bearbeitungszeit	Verantwortlich
[TODO: E-Mail]	datenschutz@organisation.de	1 Monat	DSB
[TODO: Online-Formular]	Kontaktformular auf Website	1 Monat	DSB

Kanal	Beschreibung	Bearbeitungszeit	Verantwortlich
[TODO: Schriftlich]	Postadresse	1 Monat	DSB
[TODO: Telefon]	Hotline	Sofort	Kundenservice
[TODO: Persönlich]	Vor-Ort-Termin	Nach Vereinbarung	DSB

13.5 Fristen und Verfahren

13.5.1 Bearbeitungsfristen (Art. 12 Abs. 3)

Grundfrist: - Unverzüglich, spätestens innerhalb eines Monats nach Eingang

Verlängerung: - Um weitere zwei Monate bei komplexen Anfragen - Begründung der Verlängerung erforderlich - Information der betroffenen Person innerhalb eines Monats

Faktoren für Komplexität: - Anzahl der Anfragen - Umfang der betroffenen Daten - Technische Schwierigkeit - Anzahl betroffener Systeme

13.5.2 Bearbeitungsprozess

Standardprozess für Betroffenenanfragen:

1. **Eingang der Anfrage (Tag 0)**
   - Registrierung im Anfragensystem
   - Eingangsbestätigung an betroffene Person
   - Zuweisung an Bearbeiter
2. **Identifikation (Tag 1-3)**
   - Prüfung der Identität
   - Bei Zweifeln: Zusätzliche Informationen anfordern
   - Dokumentation der Identifikation
3. **Bearbeitung (Tag 4-25)**
   - Prüfung der Anfrage
   - Zusammenstellung der Informationen
   - Abstimmung mit Fachabteilungen
   - Vorbereitung der Antwort
4. **Antwort (Tag 26-30)**
   - Übermittlung der Antwort
   - Dokumentation der Bearbeitung
   - Archivierung der Korrespondenz

13.5.3 Fristenkontrolle

Meilenstein	Frist	Verantwortlich	Eskalation
Eingangsbestätigung	2 Werktage	DSB-Team	DSB
Identifikation	5 Werktage	DSB-Team	DSB
Bearbeitung	25 Tage	Fachabteilung	DSB

Meilenstein	Frist	Verantwortlich	Eskalation
Antwort	30 Tage	DSB	Geschäftsführung

13.6 Identifikation der betroffenen Person

13.6.1 Identifikationsprozess

Maßnahmen zur Identifikation:

Methode	Beschreibung	Anwendungsfall	Sicherheitsniveau
[TODO: Kundenkonto]	Login mit Zugangsdaten	Online-Anfragen	Hoch
[TODO: Personalausweis]	Kopie des Ausweises	Schriftliche Anfragen	Sehr hoch
[TODO: Sicherheitsfragen]	Persönliche Fragen	Telefonische Anfragen	Mittel
[TODO: E-Mail-Verifikation]	Bestätigungslink	E-Mail-Anfragen	Mittel
[TODO: Persönlich]	Vor-Ort-Identifikation	Persönliche Anfragen	Sehr hoch

13.6.2 Zweifel an der Identität (Art. 12 Abs. 6)

Bei begründeten Zweifeln: - Anforderung zusätzlicher Informationen zur Identitätsbestätigung - Keine Bearbeitung bis zur Identitätsbestätigung - Information der anfragenden Person - Dokumentation der Zweifel und Maßnahmen

13.7 Unentgeltlichkeit

13.7.1 Grundsatz der Kostenfreiheit (Art. 12 Abs. 5)

Informationen und Maßnahmen sind grundsätzlich unentgeltlich.

Ausnahmen (Gebühren zulässig): - Offenkundig unbegründete Anfragen - Exzessive Anfragen (insbesondere häufige Wiederholung)

Gebührenordnung: - Angemessene Gebühr basierend auf Verwaltungskosten - Begründung der Gebühr erforderlich - Information der betroffenen Person vor Bearbeitung

13.7.2 Ablehnung von Anfragen

Anfragen können abgelehnt werden, wenn: - Offenkundig unbegründet - Exzessiv (häufige Wiederholung)

Prozess bei Ablehnung: 1. Begründung der Ablehnung 2. Information über Beschwerderecht bei Aufsichtsbehörde 3. Information über gerichtliche Rechtsbehelfe 4. Dokumentation der Ablehnung

13.8 Dokumentation

13.8.1 Anfragenregister

Dokumentation aller Betroffenenanfragen:

Datum	Betroffene Person	Art der Anfrage	Bearbeitungsstatus	Frist	Bearbeiter
[TODO]	[TODO]	[TODO: Auskunft]	[TODO: In Bearbeitung]	[TODO: 30.XX.XXXX]	[TODO]

13.8.2 Nachweispflichten

Für Accountability dokumentieren: - Alle eingegangenen Anfragen - Bearbeitungsschritte und -zeiten - Identifikationsmaßnahmen - Antworten und Ablehnungen - Gebühren und deren Begründung

13.9 Schulung und Sensibilisierung

13.9.1 Mitarbeiterschulung

Schulungsinhalte: - Betroffenenrechte und deren Bedeutung - Bearbeitungsprozesse und Fristen - Identifikationsverfahren - Kommunikationsstandards - Eskalationswege

Schulungsfrequenz: - Neue Mitarbeiter: Bei Einstellung - Alle Mitarbeiter: Jährlich - DSB-Team: Quartalsweise Updates

13.10 Verknüpfung zu anderen Dokumenten

- **Informationspflichten (Art. 13-14):** Bereitstellung von Informationen
- **Auskunftsrecht (Art. 15):** Bearbeitung von Auskunftsanfragen
- **Berichtigung (Art. 16):** Bearbeitung von Berichtigungsanfragen
- **Löschung (Art. 17):** Bearbeitung von Löschanfragen
- **Weitere Betroffenenrechte (Art. 18-22):** Bearbeitung weiterer Anfragen

13.11 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Fristüberschreitung	Antwort nach 2 Monaten	Fristenkontrolle implementieren
Unverständliche Sprache	Juristische Fachsprache	Klare Sprache verwenden
Fehlende Identifikation	Keine Prüfung der Identität	Identifikationsprozess etablieren
Kostenpflichtige Auskunft	Gebühr ohne Begründung	Grundsatz der Unentgeltlichkeit beachten

---

Nächste Schritte: 1. Etablieren Sie Kommunikationskanäle für Betroffenenanfragen 2. Implementieren Sie Bearbeitungsprozesse mit Fristenkontrolle 3. Definieren Sie Identifikationsverfahren

4. Schulen Sie Mitarbeiter zu Betroffenenrechten 5. Dokumentieren Sie alle Anfragen im Anfragenregister

ewpage

Chapter 14

Informationspflicht bei Erhebung

Dokument-ID: 0210
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

14.1 Zweck

Dieses Dokument beschreibt die Umsetzung der Informationspflichten in der {{ meta.organization }}. Betroffene Personen müssen bei Erhebung ihrer Daten umfassend informiert werden.

14.2 Informationspflicht bei direkter Erhebung (Art. 13)

14.2.1 Pflichtinformationen

Bei Erhebung personenbezogener Daten von der betroffenen Person müssen folgende Informationen bereitgestellt werden:

Information	Beschreibung	Beispiel
Identität des Verantwortlichen	Name und Kontaktdaten	[TODO: Firmenname, Adresse]
Kontaktdaten DSB	Falls vorhanden	[TODO: datenschutz@organisation.de]
Zwecke der Verarbeitung	Wofür werden Daten verwendet	[TODO: Vertragserfüllung, Marketing]
Rechtsgrundlage	Art. 6 oder Art. 9 DSGVO	[TODO: Art. 6 Abs. 1 lit. b]
Berechtigte Interessen	Bei Art. 6 Abs. 1 lit. f	[TODO: Direktwerbung]

Information	Beschreibung	Beispiel
Empfänger	Wer erhält die Daten	[TODO: Versanddienstleister]
Drittlandübermittlung	Falls zutreffend	[TODO: USA, Standard-vertragsklauseln]
Speicherdauer	Wie lange werden Daten gespeichert	[TODO: 10 Jahre]
Betroffenenrechte	Auskunft, Berichtigung, Löschung, etc.	[TODO: Alle Rechte auflisten]
Widerrufsrecht	Bei Einwilligung	[TODO: Jederzeit widerrufbar]
Beschwerderecht	Bei Aufsichtsbehörde	[TODO: Landesbeauftragte]
Pflicht zur Bereitstellung	Vertraglich/gesetzlich erforderlich	[TODO: Ja/Nein]
Automatisierte Entscheidung	Falls zutreffend	[TODO: Kein Profiling]

14.2.2 Zeitpunkt der Information

Information muss erfolgen: - Zum Zeitpunkt der Erhebung - Vor Beginn der Verarbeitung - Bei Erstkontakt mit der betroffenen Person

14.3 Informationspflicht bei indirekter Erhebung (Art. 14)

14.3.1 Zusätzliche Pflichtinformationen

Bei Erhebung von Dritten zusätzlich:

Information	Beschreibung
Kategorien personenbezogener Daten	Welche Datenarten
Quelle der Daten	Woher stammen die Daten
Öffentlich zugängliche Quelle	Falls zutreffend

14.3.2 Zeitpunkt der Information

Information muss erfolgen: - Innerhalb einer angemessenen Frist (max. 1 Monat) - Spätestens bei erster Kommunikation - Spätestens bei Offenlegung an Dritten

14.4 Ausnahmen von der Informationspflicht

14.4.1 Art. 13 Abs. 4 - Bereits informiert

Keine Information erforderlich, wenn: - Betroffene Person bereits über die Informationen verfügt

14.4.2 Art. 14 Abs. 5 - Ausnahmen bei Dritterhebung

Keine Information erforderlich, wenn:

Ausnahme	Voraussetzung
Bereits informiert	Person verfügt bereits über Informationen
Unmöglich	Unverhältnismäßiger Aufwand
Gesetzliche Pflicht	Ausdrückliche Regelung
Berufsgeheimnis	Gesetzlich geschützt
Öffentliches Interesse	Beeinträchtigung der Zwecke

Bei Unmöglichkeit/unverhältnismäßigem Aufwand: - Geeignete Maßnahmen zum Schutz der Rechte - Öffentliche Bekanntmachung - Dokumentation der Gründe

14.5 Umsetzung in unserer Organisation

14.5.1 Datenschutzerklärungen

Datenschutzerklärungen für verschiedene Kontexte:

Kontext	Dokument	Zielgruppe	Aktualisierung
[TODO: Website]	Website-Datenschutzerklärung	Websitebesucher	Bei Änderungen
[TODO: App]	App-Datenschutzerklärung	App-Nutzer	Bei Änderungen
[TODO: Kundenkonto]	Datenschutzhinweise Kundenkonto	Kunden	Bei Registrierung
[TODO: Newsletter]	Newsletter-Datenschutzhinweise	Abonnenten	Bei Anmeldung
[TODO: Bewerbung]	Bewerberdatenschutz	Bewerber	Bei Bewerbung
[TODO: Mitarbeiter]	Mitarbeiterdatenschutz	Mitarbeiter	Bei Einstellung

14.5.2 Bereitstellungsformen

Wie werden Informationen bereitgestellt:

Form	Beschreibung	Anwendungsfall
[TODO: Online]	Datenschutzerklärung auf Website	Websitebesucher
[TODO: E-Mail]	Datenschutzhinweise per E-Mail	Erstkontakt
[TODO: Formular]	Datenschutzhinweise im Formular	Datenerhebung
[TODO: Aushang]	Datenschutzhinweise vor Ort	Videoüberwachung
[TODO: Schriftlich]	Datenschutzinformation per Post	Vertragsabschluss

14.6 Checkliste für Datenschutzerklärungen

14.6.1 Vollständigkeitsprüfung

- ☐ Identität und Kontaktdaten des Verantwortlichen
- ☐ Kontaktdaten des Datenschutzbeauftragten
- ☐ Zwecke der Verarbeitung
- ☐ Rechtsgrundlage der Verarbeitung
- ☐ Berechtigte Interessen (bei Art. 6 Abs. 1 lit. f)
- ☐ Empfänger oder Kategorien von Empfängern
- ☐ Absicht der Drittlandübermittlung (falls zutreffend)
- ☐ Speicherdauer oder Kriterien
- ☐ Betroffenenrechte (Auskunft, Berichtigung, Löschung, etc.)
- ☐ Widerrufsrecht (bei Einwilligung)
- ☐ Beschwerderecht bei Aufsichtsbehörde
- ☐ Pflicht zur Bereitstellung der Daten
- ☐ Automatisierte Entscheidungsfindung (falls zutreffend)
- ☐ Bei Dritterhebung: Kategorien der Daten und Quelle

14.6.2 Qualitätsprüfung

- ☐ Verständliche Sprache
- ☐ Strukturierte Darstellung
- ☐ Leicht zugänglich
- ☐ Vollständig und aktuell
- ☐ Mehrsprachig (bei Bedarf)

14.7 Dokumentation

14.7.1 Nachweispflichten

Für Accountability dokumentieren: - Alle Datenschutzerklärungen und deren Versionen - Zeitpunkt der Bereitstellung - Art der Bereitstellung - Ausnahmen und deren Begründung - Aktualisierungen und Änderungen

14.7.2 Versionsverwaltung

Version	Datum	Änderungen	Verantwortlich
[TODO: 1.0]	[TODO]	[TODO: Ersterstellung]	[TODO]
[TODO: 1.1]	[TODO]	[TODO: Neue Verarbeitung hinzugefügt]	[TODO]

14.8 Verknüpfung zu anderen Dokumenten

- **Transparenz (Art. 12):** Modalitäten der Information
- **Datenschutzgrundsätze (Art. 5):** Transparenz als Grundprinzip

- **Rechtsgrundlagen (Art. 6):** Basis der Verarbeitung
- **Betroffenenrechte (Art. 15-22):** Information über Rechte
- **Verzeichnis (Art. 30):** Quelle für Informationen

14.9 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Unvollständige Information	Fehlende Rechtsgrundlage	Checkliste verwenden
Verspätete Information	Information nach Verarbeitung	Prozess etablieren
Unverständliche Sprache	Juristische Fachsprache	Klare Sprache verwenden
Versteckte Information	Datenschutzerklärung nicht auffindbar	Prominente Platzierung

---

Nächste Schritte: 1. Erstellen Sie vollständige Datenschutzerklärungen für alle Kontexte 2. Implementieren Sie Prozesse zur rechtzeitigen Information 3. Etablieren Sie Versionsverwaltung für Datenschutzerklärungen 4. Schulen Sie Mitarbeiter zu Informationspflichten 5. Überprüfen Sie regelmäßig Vollständigkeit und Aktualität

ewpage

Chapter 15

Auskunftsrecht

Dokument-ID: 0220
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

15.1 Zweck

Dieses Dokument beschreibt die Umsetzung des Auskunftsrechts in der {{ meta.organization }}. Betroffene Personen haben das Recht, Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu erhalten.

15.2 Auskunftsrecht gemäß Art. 15 DSGVO

15.2.1 Umfang der Auskunft

Betroffene Personen haben Recht auf Auskunft über:

Information	Beschreibung
Verarbeitungszwecke	Wofür werden die Daten verarbeitet
Kategorien personenbezogener Daten	Welche Datenarten werden verarbeitet
Empfänger	Wer hat oder wird die Daten erhalten
Speicherdauer	Wie lange werden die Daten gespeichert
Berichtigungsrecht	Recht auf Berichtigung
Löschungsrecht	Recht auf Löschung
Einschränkungsrecht	Recht auf Einschränkung
Widerspruchsrecht	Recht auf Widerspruch
Beschwerderecht	Recht auf Beschwerde bei Aufsichtsbehörde
Herkunft der Daten	Woher stammen die Daten (bei Dritterhebung)
Automatisierte Entscheidung	Profiling und Logik der Verarbeitung

Information	Beschreibung
Drittlandübermittlung	Garantien bei Übermittlung

15.2.2 Kopie der Daten (Art. 15 Abs. 3)

Betroffene Person hat Recht auf: - Kostenlose Kopie der verarbeiteten Daten - Erste Kopie unentgeltlich - Weitere Kopien: Angemessene Gebühr möglich

15.3 Bearbeitungsprozess

15.3.1 Prozess für Auskunftsanfragen

Standardprozess:

1. **Eingang der Anfrage (Tag 0)**
   - Registrierung im Anfragensystem
   - Eingangsbestätigung
   - Zuweisung an Bearbeiter
2. **Identifikation (Tag 1-5)**
   - Prüfung der Identität
   - Bei Zweifeln: Zusätzliche Informationen anfordern
   - Dokumentation
3. **Datensammlung (Tag 6-20)**
   - Identifikation aller Systeme mit Daten
   - Zusammenstellung der Informationen
   - Abstimmung mit Fachabteilungen
   - Prüfung auf Rechte Dritter
4. **Erstellung der Auskunft (Tag 21-25)**
   - Strukturierte Aufbereitung
   - Verständliche Darstellung
   - Vollständigkeitsprüfung
5. **Übermittlung (Tag 26-30)**
   - Sichere Übermittlung
   - Dokumentation
   - Archivierung

15.3.2 Fristen

Bearbeitungsfrist: - Unverzüglich, spätestens 1 Monat - Verlängerung um 2 Monate bei Komplexität möglich - Begründung der Verlängerung erforderlich

15.4 Format der Auskunft

15.4.1 Strukturierte Darstellung

Empfohlene Struktur:

```
1. Allgemeine Informationen
```

```
   - Verantwortlicher
   - Datenschutzbeauftragter
   - Kontaktdaten

2. Verarbeitete Daten
   - Kategorien personenbezogener Daten
   - Konkrete Datensätze (Kopie)

3. Verarbeitungszwecke
   - Zweck 1: [Beschreibung]
   - Zweck 2: [Beschreibung]

4. Rechtsgrundlagen
   - Rechtsgrundlage je Zweck

5. Empfänger
   - Liste der Empfänger oder Kategorien

6. Speicherdauer
   - Dauer oder Kriterien

7. Betroffenenrechte
   - Berichtigung, Löschung, Einschränkung, Widerspruch
   - Beschwerde bei Aufsichtsbehörde

8. Herkunft der Daten
   - Quelle bei Dritterhebung

9. Automatisierte Entscheidungen
   - Falls zutreffend: Logik und Tragweite
```

15.4.2 Übermittlungsformen

Form	Beschreibung	Anwendungsfall
[TODO: E-Mail]	PDF-Dokument per E-Mail	Standard
[TODO: Online-Portal]	Abruf im Kundenportal	Kundenkonto vorhanden
[TODO: Schriftlich]	Papierform per Post	Auf Wunsch
[TODO: Elektronisch]	Strukturiertes Format (JSON, XML)	Auf Wunsch

15.5 Besonderheiten

15.5.1 Rechte Dritter (Art. 15 Abs. 4)

Auskunft darf Rechte Dritter nicht beeinträchtigen: - Geschäftsgeheimnisse - Rechte anderer Personen - Geistiges Eigentum

Maßnahmen: - Schwärzung sensibler Informationen - Anonymisierung von Drittdaten - Begründung bei Verweigerung

15.5.2 Häufige Anfragen

Bei offenkundig unbegründeten oder exzessiven Anfragen: - Angemessene Gebühr möglich - Verweigerung möglich - Begründung erforderlich

15.6 Dokumentation

15.6.1 Auskunftsregister

Datum	Betroffene Person	Umfang	Übermittlungsform	Frist	Bearbeiter
[TODO]	[TODO]	[TODO: Vollständig]	[TODO: E-Mail]	[TODO: 30.XX.XXXX]	[TODO]

15.6.2 Nachweispflichten

Dokumentation für Accountability: - Alle Auskunftsanfragen - Bearbeitungsschritte und -zeiten - Übermittelte Informationen - Ablehnungen und Begründungen - Gebühren und deren Begründung

15.7 Verknüpfung zu anderen Dokumenten

- **Transparenz (Art. 12):** Modalitäten der Auskunft
- **Informationspflichten (Art. 13-14):** Proaktive Information
- **Weitere Betroffenenrechte (Art. 16-22):** Ergänzende Rechte
- **Verzeichnis (Art. 30):** Quelle für Auskunftsinformationen

15.8 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Unvollständige Auskunft	Nicht alle Systeme geprüft	Vollständige Datensammlung
Fristüberschreitung	Antwort nach 2 Monaten	Fristenkontrolle
Unverständliche Auskunft	Technische Rohdaten	Strukturierte Aufbereitung
Fehlende Identifikation	Keine Prüfung	Identifikationsprozess

Nächste Schritte: 1. Etablieren Sie Prozess für Auskunftsanfragen 2. Definieren Sie Format und Struktur der Auskunft 3. Implementieren Sie Fristenkontrolle 4. Schulen Sie Mitarbeiter zur Auskunftserteilung 5. Dokumentieren Sie alle Anfragen im Auskunftsregister

ewpage

Chapter 16

Berichtigung und Löschung

Dokument-ID: 0230
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

16.1 Zweck

Dieses Dokument beschreibt die Umsetzung des Rechts auf Berichtigung und Löschung in der {{ meta.organization }}. Betroffene Personen haben das Recht auf Berichtigung unrichtiger und Löschung nicht mehr erforderlicher Daten.

16.2 Recht auf Berichtigung (Art. 16)

16.2.1 Umfang des Berichtigungsrechts

Betroffene Personen haben Recht auf: - Unverzügliche Berichtigung unrichtiger Daten - Vervollständigung unvollständiger Daten - Ergänzende Erklärung

16.2.2 Berichtigungsprozess

Standardprozess:

1. **Eingang des Antrags (Tag 0)**
   - Registrierung
   - Eingangsbestätigung
   - Zuweisung
2. **Prüfung (Tag 1-10)**
   - Identifikation der betroffenen Person
   - Prüfung der Unrichtigkeit
   - Abgleich mit Nachweisen

3. **Durchführung (Tag 11-25)**
   - Berichtigung in allen Systemen
   - Benachrichtigung von Empfängern (Art. 19)
   - Dokumentation
4. **Rückmeldung (Tag 26-30)**
   - Information über durchgeführte Berichtigung
   - Liste der benachrichtigten Empfänger

16.2.3 Berichtigungsmatrix

System	Verantwortlich	Berichtigungsverfahren	Dokumentation
[TODO: CRM]	IT	Manuelle Änderung	Change-Log
[TODO: ERP]	IT	Workflow-gesteuert	Audit-Trail
[TODO: Datenbank]	IT	SQL-Update	Änderungsprotokoll
[TODO: Backup]	IT	Markierung	Backup-Log

16.3 Recht auf Löschung (Art. 17)

16.3.1 Löschgründe

Löschung ist erforderlich, wenn:

Grund	Beschreibung	Beispiel
Nicht mehr erforderlich	Zweck erfüllt	Bewerberdaten nach Absage
Widerruf der Einwilligung	Einwilligung zurückgezogen	Newsletter-Abmeldung
Widerspruch	Widerspruch eingelegt (Art. 21)	Werbewiderspruch
Unrechtmäßige Verarbeitung	Ohne Rechtsgrundlage	Daten ohne Einwilligung
Rechtliche Verpflichtung	Gesetzliche Löschpflicht	Datenschutzverstoß
Kinder	Dienste der Informationsgesellschaft	Social Media unter 16

16.3.2 Ausnahmen vom Löschrecht

Löschung nicht erforderlich bei:

Ausnahme	Beschreibung
Meinungsfreiheit	Ausübung des Rechts auf freie Meinungsäußerung
Rechtliche Verpflichtung	Erfüllung rechtlicher Verpflichtungen
Öffentliches Interesse	Aufgaben im öffentlichen Interesse
Gesundheitswesen	Gesundheitsvorsorge, Arbeitsmedizin
Archivzwecke	Archivierung im öffentlichen Interesse
Rechtsansprüche	Geltendmachung, Ausübung oder Verteidigung

16.3.3 Löschprozess

Standardprozess:

1. **Eingang des Antrags (Tag 0)**
   - Registrierung
   - Eingangsbestätigung
   - Zuweisung
2. **Prüfung (Tag 1-10)**
   - Identifikation der betroffenen Person
   - Prüfung der Löschgründe
   - Prüfung von Ausnahmen
   - Prüfung gesetzlicher Aufbewahrungsfristen
3. **Entscheidung (Tag 11-15)**
   - Löschung oder begründete Ablehnung
   - Bei Ablehnung: Prüfung der Einschränkung (Art. 18)
4. **Durchführung (Tag 16-25)**
   - Löschung in allen Systemen
   - Benachrichtigung von Empfängern (Art. 19)
   - Dokumentation
5. **Rückmeldung (Tag 26-30)**
   - Information über Löschung oder Ablehnung
   - Bei Ablehnung: Begründung und Rechtsbehelfe

16.3.4 Löschverfahren

Technische Löschung:

System	Löschmethode	Verantwortlich	Dokumentation
[TODO: Produktivsysteme]	Sofortige Löschung	IT	Löschprotokoll
[TODO: Backups]	Markierung/Überschreiben	IT	Backup-Log
[TODO: Archive]	Physische Vernichtung	IT	Vernichtungsprotokoll
[TODO: Cloud]	API-gesteuerte Löschung	IT	API-Log

16.4 Mitteilungspflicht (Art. 19)

16.4.1 Benachrichtigung von Empfängern

Bei Berichtigung oder Löschung müssen Empfänger informiert werden:

Prozess: 1. Identifikation aller Empfänger 2. Benachrichtigung über Berichtigung/Löschung 3. Dokumentation der Benachrichtigungen 4. Information der betroffenen Person über Empfänger (auf Verlangen)

Ausnahmen: - Unmöglich - Unverhältnismäßiger Aufwand

16.4.2 Empfängermatrix

Empfängertyp	Benachrichtigungspflicht	Methode	Dokumentation
[TODO: Auftragsverarbeiter]	Ja	E-Mail	Benachrichtigungslog
[TODO: Dritte Empfänger]	Ja	E-Mail/Schriftlich	Benachrichtigungslog
[TODO: Öffentliche Stellen]	Ja	Schriftlich	Benachrichtigungslog

16.5 Dokumentation

16.5.1 Berichtigungs- und Löschregister

Datum	Betroffene Person	Art	Grund	Durchgeführt	Empfänger benachrichtigt	Bearbeiter
[TODO]	[TODO]	Berichtigung	Unrichtig	Ja	Ja	[TODO]
[TODO]	[TODO]	Löschung	Nicht erforderlich	Ja	Ja	[TODO]
[TODO]	[TODO]	Löschung	Abgelehnt (Aufbewahrungsfrist)	Nein	N/A	[TODO]

16.5.2 Nachweispflichten

Dokumentation für Accountability: - Alle Berichtigungs- und Löschanträge - Durchgeführte Berichtigungen und Löschungen - Ablehnungen und deren Begründung - Benachrichtigungen an Empfänger - Ausnahmen und deren Begründung

16.6 Fristen

Bearbeitungsfrist: - Unverzüglich, spätestens 1 Monat - Verlängerung um 2 Monate bei Komplexität möglich - Begründung der Verlängerung erforderlich

16.7 Verknüpfung zu anderen Dokumenten

- **Transparenz (Art. 12):** Modalitäten der Bearbeitung
- **Richtigkeit (Art. 5 Abs. 1 lit. d):** Grundsatz der Richtigkeit
- **Speicherbegrenzung (Art. 5 Abs. 1 lit. e):** Grundsatz der Löschung
- **Mitteilungspflicht (Art. 19):** Benachrichtigung von Empfängern
- **Einschränkung (Art. 18):** Alternative zur Löschung

16.8 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Unvollständige Berichtigung	Nur in einem System	Alle Systeme prüfen
Verzögerte Löschung	Löschung nach 3 Monaten	Fristenkontrolle
Fehlende Benachrichtigung	Empfänger nicht informiert	Benachrichtigungsprozess
Unbegründete Ablehnung	Ablehnung ohne Prüfung	Sorgfältige Prüfung

---

Nächste Schritte: 1. Etablieren Sie Prozesse für Berichtigungs- und Löschanträge 2. Implementieren Sie Löschverfahren für alle Systeme 3. Definieren Sie Benachrichtigungsprozess für Empfänger 4. Schulen Sie Mitarbeiter zu Berichtigungs- und Löschrecht 5. Dokumentieren Sie alle Anträge im Register

ewpage

Chapter 17

Einschränkung und Widerspruch

Dokument-ID: 0240
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

17.1 Zweck

Dieses Dokument beschreibt die Umsetzung des Rechts auf Einschränkung der Verarbeitung und des Widerspruchsrechts in der {{ meta.organization }}.

17.2 Recht auf Einschränkung (Art. 18)

17.2.1 Gründe für Einschränkung

Einschränkung ist erforderlich, wenn:

Grund	Beschreibung	Dauer
Richtigkeit bestritten	Betroffene Person bestreitet Richtigkeit	Bis zur Überprüfung
Unrechtmäßige Verarbeitung	Verarbeitung unrechtmäßig, aber keine Löschung gewünscht	Bis zur Klärung
Nicht mehr erforderlich	Daten nicht mehr erforderlich, aber für Rechtsansprüche benötigt	Bis zur Klärung
Widerspruch eingelegt	Widerspruch nach Art. 21 Abs. 1	Bis zur Interessenabwägung

17.2.2 Bedeutung der Einschränkung

Bei Einschränkung: - Daten dürfen nur gespeichert werden - Keine weitere Verarbeitung (außer Speicherung)

Ausnahmen (Verarbeitung zulässig mit Einwilligung): - Geltendmachung von Rechtsansprüchen - Schutz der Rechte anderer Personen - Wichtige Gründe des öffentlichen Interesses

17.2.3 Technische Umsetzung

Methoden zur Einschränkung:

Methode	Beschreibung	Anwendungsfall
[TODO: Markierung]	Datensatz als "eingeschränkt" markieren	Standard
[TODO: Zugriffssperre]	Technische Zugriffsbeschränkung	Sensible Daten
[TODO: Separierung]	Verschiebung in separates System	Langfristige Einschränkung
[TODO: Pseudonymisierung]	Trennung von Identifikationsdaten	Zusätzlicher Schutz

17.2.4 Einschränkungsprozess

Standardprozess:

1. **Eingang des Antrags (Tag 0)**
   - Registrierung
   - Eingangsbestätigung
   - Zuweisung
2. **Prüfung (Tag 1-10)**
   - Identifikation der betroffenen Person
   - Prüfung der Einschränkungsgründe
   - Identifikation betroffener Daten
3. **Durchführung (Tag 11-25)**
   - Technische Einschränkung in allen Systemen
   - Benachrichtigung von Empfängern (Art. 19)
   - Dokumentation
4. **Rückmeldung (Tag 26-30)**
   - Information über durchgeführte Einschränkung
   - Information über Aufhebung der Einschränkung

17.2.5 Aufhebung der Einschränkung

Einschränkung wird aufgehoben, wenn: - Grund für Einschränkung entfällt - Betroffene Person zustimmt - Einschränkungsgrund geklärt

Vor Aufhebung: - Information der betroffenen Person erforderlich - Dokumentation der Aufhebung

17.3 Widerspruchsrecht (Art. 21)

17.3.1 Widerspruch gegen Verarbeitung (Art. 21 Abs. 1)

Widerspruchsrecht bei: - Verarbeitung aufgrund öffentlichen Interesses (Art. 6 Abs. 1 lit. e) - Verarbeitung aufgrund berechtigten Interesses (Art. 6 Abs. 1 lit. f)

Folge des Widerspruchs: - Verarbeitung muss eingestellt werden - Außer: Zwingende schutzwürdige Gründe überwiegen

17.3.2 Interessenabwägung

Prüfung nach Widerspruch:

Kriterium	Prüffrage	Bewertung
Zwingende Gründe	Gibt es zwingende schutzwürdige Gründe?	[TODO]
Rechtsansprüche	Sind Rechtsansprüche betroffen?	[TODO]
Interessen der Person	Welche Interessen hat die betroffene Person?	[TODO]
Abwägung	Überwiegen die Gründe des Verantwortlichen?	[TODO]

Ergebnis: - Überwiegen zwingende Gründe: Verarbeitung zulässig - Keine zwingenden Gründe: Verarbeitung einstellen

17.3.3 Widerspruch gegen Direktwerbung (Art. 21 Abs. 2)

Besonderheiten: - Absolutes Widerspruchsrecht - Keine Interessenabwägung erforderlich - Verarbeitung muss sofort eingestellt werden

Umsetzung: - Eintrag in Sperrliste - Keine weitere Werbung - Information an alle Marketingkanäle

17.3.4 Widerspruch gegen Profiling (Art. 21 Abs. 3)

Widerspruchsrecht bei: - Profiling im Zusammenhang mit Direktwerbung - Profiling aufgrund berechtigten Interesses

17.3.5 Widerspruchsprozess

Standardprozess:

1. **Eingang des Widerspruchs (Tag 0)**
   - Registrierung
   - Eingangsbestätigung
   - Sofortige Einstellung bei Direktwerbung
2. **Prüfung (Tag 1-15)**
   - Identifikation der betroffenen Person
   - Prüfung der Rechtsgrundlage

- Bei Art. 6 Abs. 1 lit. f: Interessenabwägung

3. **Entscheidung (Tag 16-20)**
   - Einstellung der Verarbeitung oder
   - Begründete Ablehnung (zwingende Gründe)
4. **Durchführung (Tag 21-25)**
   - Einstellung in allen Systemen
   - Benachrichtigung von Empfängern
   - Dokumentation
5. **Rückmeldung (Tag 26-30)**
   - Information über Einstellung oder Ablehnung
   - Bei Ablehnung: Begründung und Rechtsbehelfe

17.4 Benachrichtigungspflicht (Art. 19)

17.4.1 Benachrichtigung von Empfängern

Bei Einschränkung oder Widerspruch müssen Empfänger informiert werden: - Auftragsverarbeiter - Dritte Empfänger - Öffentliche Stellen

Ausnahmen: - Unmöglich - Unverhältnismäßiger Aufwand

17.5 Dokumentation

17.5.1 Einschränkungs- und Widerspruchsregister

Datum	Betroffene Person	Art	Grund	Status	Aufhebung	Bearbeiter
[TODO]	[TODO]	Einschränkung	Richtigkeit bestritten	Aktiv	[TODO]	[TODO]
[TODO]	[TODO]	Widerspruch	Direktwerbung	Umgesetzt	N/A	[TODO]
[TODO]	[TODO]	Widerspruch	Berechtigtes Interesse	Abgelehnt	N/A	[TODO]

17.5.2 Nachweispflichten

Dokumentation für Accountability: - Alle Einschränkungs- und Widerspruchsanträge - Durchgeführte Einschränkungen - Interessenabwägungen bei Widerspruch - Ablehnungen und deren Begründung - Benachrichtigungen an Empfänger - Aufhebungen von Einschränkungen

17.6 Verknüpfung zu anderen Dokumenten

- **Transparenz (Art. 12):** Modalitäten der Bearbeitung
- **Berechtigtes Interesse (Art. 6 Abs. 1 lit. f):** Interessenabwägung
- **Mitteilungspflicht (Art. 19):** Benachrichtigung von Empfängern
- **Löschung (Art. 17):** Alternative zur Einschränkung

17.7 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Keine Einschränkung	Weiterverarbeitung trotz Antrag	Sofortige Umsetzung
Fehlende Interessenabwägung	Ablehnung ohne Prüfung	Sorgfältige Abwägung
Verzögerte Umsetzung	Werbung nach Widerspruch	Sofortige Einstellung
Keine Benachrichtigung	Empfänger nicht informiert	Benachrichtigungsprozess

---

Nächste Schritte: 1. Etablieren Sie Prozesse für Einschränkungs- und Widerspruchsanträge 2. Implementieren Sie technische Einschränkungsmechanismen 3. Definieren Sie Interessenabwägungsprozess 4. Schulen Sie Mitarbeiter zu Einschränkungs- und Widerspruchsrecht 5. Dokumentieren Sie alle Anträge im Register

ewpage

Chapter 18

Datenübertragbarkeit

Dokument-ID: 0250
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

18.1 Zweck

Dieses Dokument beschreibt die Umsetzung des Rechts auf Datenübertragbarkeit in der {{ meta.organization }}. Betroffene Personen haben das Recht, ihre Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

18.2 Recht auf Datenübertragbarkeit (Art. 20)

18.2.1 Voraussetzungen

Datenübertragbarkeit gilt nur, wenn:

Voraussetzung	Beschreibung
Rechtsgrundlage	Einwilligung (Art. 6 Abs. 1 lit. a) oder Vertrag (Art. 6 Abs. 1 lit. b)
Bereitstellung	Daten wurden von betroffener Person bereitgestellt
Automatisierte Verarbeitung	Verarbeitung erfolgt automatisiert

Nicht anwendbar bei: - Verarbeitung aufgrund anderer Rechtsgrundlagen (lit. c, d, e, f) - Nicht automatisierte Verarbeitung - Daten, die nicht von betroffener Person bereitgestellt wurden

18.2.2 Umfang der Datenübertragbarkeit

Betroffene Daten:

Datenart	Übertragbar?	Begründung
Von Person bereitgestellt	Ja	Direkt eingegeben oder hochgeladen
Durch Beobachtung generiert	Ja	Nutzungsdaten, Standortdaten
Abgeleitete/berechnete Daten	Nein	Algorithmen, Analysen, Profile
Daten Dritter	Nein	Rechte Dritter betroffen

18.2.3 Zwei Varianten

1. Übertragung an betroffene Person: - Bereitstellung in strukturiertem Format - Gängiges Format (CSV, JSON, XML) - Maschinenlesbar

2. Direkte Übertragung an anderen Verantwortlichen: - Soweit technisch machbar - Direkte Übermittlung - Keine Verpflichtung bei fehlender Schnittstelle

18.3 Technische Umsetzung

18.3.1 Datenformate

Unterstützte Formate:

Format	Beschreibung	Anwendungsfall
[TODO: JSON]	JavaScript Object Notation	Standard für strukturierte Daten
[TODO: CSV]	Comma-Separated Values	Tabellarische Daten
[TODO: XML]	Extensible Markup Language	Hierarchische Daten
[TODO: PDF]	Portable Document Format	Lesbare Darstellung (zusätzlich)

18.3.2 Datenstruktur

Beispiel JSON-Struktur:

```
{
  "export_date": "2024-01-15",
  "data_subject": {
    "id": "12345",
    "name": "Max Mustermann",
    "email": "max@example.com"
  },
  "personal_data": {
    "profile": {
      "created": "2020-01-01",
      "last_updated": "2024-01-10",
      "fields": {
        "name": "Max Mustermann",
        "email": "max@example.com",
```

```
        "phone": "+49123456789"
      }
    },
    "orders": [
      {
        "order_id": "ORD-001",
        "date": "2023-12-01",
        "items": [...]
      }
    ],
    "usage_data": {
      "logins": [...],
      "page_views": [...]
    }
  }
}
```


18.3.3 Schnittstellen

Technische Übertragungsmöglichkeiten:

Methode	Beschreibung	Implementierung
[TODO: Download-Portal]	Selbstbedienungsportal	Web-Interface
[TODO: API]	Programmatische Schnittstelle	REST API
[TODO: E-Mail]	Versand als Anhang	Verschlüsselt
[TODO: Direkte Übertragung]	An anderen Verantwortlichen	API-to-API

18.4 Übertragungsprozess

18.4.1 Prozess für Datenübertragbarkeitsanfragen

Standardprozess:

1. **Eingang der Anfrage (Tag 0)**
   - Registrierung
   - Eingangsbestätigung
   - Klärung: An Person oder anderen Verantwortlichen?
2. **Prüfung (Tag 1-10)**
   - Identifikation der betroffenen Person
   - Prüfung der Voraussetzungen
   - Identifikation übertragbarer Daten
3. **Datenexport (Tag 11-20)**
   - Zusammenstellung der Daten
   - Konvertierung in gewünschtes Format
   - Qualitätsprüfung
4. **Übertragung (Tag 21-25)**

- Bereitstellung zum Download oder
- Direkte Übertragung an anderen Verantwortlichen
- Dokumentation

5. **Rückmeldung (Tag 26-30)**
   - Information über Bereitstellung
   - Zugangslink oder Bestätigung der Übertragung

18.4.2 Direkte Übertragung

Prozess für direkte Übertragung:

1. **Identifikation des Empfängers**
   - Name und Kontaktdaten
   - Technische Schnittstelle
2. **Prüfung der technischen Machbarkeit**
   - Verfügbarkeit von Schnittstellen
   - Kompatibilität der Formate
3. **Durchführung der Übertragung**
   - Sichere Übermittlung
   - Bestätigung des Empfangs
   - Dokumentation

Bei fehlender technischer Machbarkeit: - Bereitstellung an betroffene Person - Information über fehlende Schnittstelle

18.5 Ausnahmen und Einschränkungen

18.5.1 Rechte und Freiheiten Dritter (Art. 20 Abs. 4)

Datenübertragbarkeit darf nicht beeinträchtigen: - Rechte und Freiheiten anderer Personen - Geschäftsgeheimnisse - Geistiges Eigentum

Maßnahmen: - Anonymisierung von Drittdaten - Ausschluss geschützter Informationen - Begründung bei Einschränkung

18.5.2 Keine Löschpflicht

Datenübertragbarkeit bedeutet nicht: - Automatische Löschung beim Verantwortlichen - Beendigung der Verarbeitung - Separate Löschanfrage erforderlich

18.6 Dokumentation

18.6.1 Datenübertragbarkeitsregister

Datum	Betroffene Person	Format	Empfänger	Umfang	Status	Bearbeiter
[TODO]	[TODO]	JSON	Betroffene Person	Vollständig	Bereitgestellt	[TODO]

Datum	Betroffene Person	Format	Empfänger	Umfang	Status	Bearbeiter
[TODO]	[TODO]	CSV	Anderer Verant-wortlicher	Vollständig	Übertragen	[TODO]
[TODO]	[TODO]	JSON	Betroffene Person	Teilweise (Dritt-rechte)	Bereitgestellt	[TODO]

18.6.2 Nachweispflichten

Dokumentation für Accountability: - Alle Datenübertragbarkeitsanfragen - Bereitgestellte Daten und Formate - Direkte Übertragungen - Einschränkungen und deren Begründung - Technische Machbarkeitsprüfungen

18.7 Fristen

Bearbeitungsfrist: - Unverzüglich, spätestens 1 Monat - Verlängerung um 2 Monate bei Komplexität möglich - Begründung der Verlängerung erforderlich

18.8 Verknüpfung zu anderen Dokumenten

- **Transparenz (Art. 12):** Modalitäten der Übertragung
- **Rechtsgrundlagen (Art. 6):** Voraussetzungen für Übertragbarkeit
- **Informationspflichten (Art. 13-14):** Information über Recht
- **Auskunftsrecht (Art. 15):** Ergänzendes Recht

18.9 Häufige Verstöße und deren Vermeidung

Verstoß	Beispiel	Vermeidung
Unstrukturiertes Format	PDF-Scan	Maschinenlesbares Format
Unvollständige Daten	Nur Stammdaten	Alle übertragbaren Daten
Fehlende Schnittstelle	Keine direkte Übertragung	API bereitstellen
Verzögerte Bereitstellung	Bereitstellung nach 3 Monaten	Fristenkontrolle

---

Nächste Schritte: 1. Etablieren Sie Prozess für Datenübertragbarkeitsanfragen 2. Implementieren Sie Export in strukturierten Formaten 3. Entwickeln Sie Schnittstellen für direkte Übertragung 4. Schulen Sie Mitarbeiter zu Datenübertragbarkeit 5. Dokumentieren Sie alle Anfragen im Register

ewpage

Chapter 19

Verantwortlicher: Pflichten und Rechenschaftspflicht

Dokument-ID: 0300
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

19.1 Zweck

Dieses Dokument beschreibt die Pflichten des Verantwortlichen gemäß Art. 24 DSGVO und die Umsetzung der Rechenschaftspflicht bei {{ meta.organization }}. Es dokumentiert, wie wir sicherstellen, dass die Verarbeitung personenbezogener Daten im Einklang mit der DSGVO erfolgt.

19.2 Rechenschaftspflicht (Art. 24 Abs. 1)

Der Verantwortliche ist für die Einhaltung der Datenschutzgrundsätze verantwortlich und muss deren Einhaltung nachweisen können (Rechenschaftspflicht).

19.2.1 Nachweispflicht

Dokumentation zur Nachweisführung:

Dokument	Zweck	Aktualisierung	Verantwortlich
Verzeichnis der Verarbeitungstätigkeiten	Art. 30 Compliance	Laufend	[TODO: Rolle]
Datenschutz-Folgenabschätzungen	Art. 35 Compliance	Bei Bedarf	[TODO: Rolle]

Dokument	Zweck	Aktualisierung	Verantwortlich
Auftragsverarbeiter-Verträge	Art. 28 Compliance	Bei Vertragsschluss	[TODO: Rolle]
TOM-Dokumentation	Art. 32 Compliance	Jährlich	[TODO: Rolle]
Schulungsnachweise	Art. 39 Compliance	Laufend	[TODO: Rolle]
Datenschutzverletzungs-Register	Art. 33 Compliance	Bei Vorfällen	[TODO: Rolle]

19.3 Technische und organisatorische Maßnahmen (TOM)

19.3.1 Risikobasierter Ansatz

Die Maßnahmen berücksichtigen: - **Art der Verarbeitung:** [TODO: Beschreibe Verarbeitungsarten] - **Umfang der Verarbeitung:** [TODO: Volumen, Anzahl betroffener Personen] - **Umstände der Verarbeitung:** [TODO: Kontext, Technologie] - **Zwecke der Verarbeitung:** [TODO: Verarbeitungszwecke] - **Eintrittswahrscheinlichkeit und Schwere des Risikos:** [TODO: Risikobewertung]

19.3.2 Implementierte Maßnahmen

19.3.2.1 Technische Maßnahmen

Maßnahme	Beschreibung	Implementierungsstatus	Verantwortlich
Zugangskontrolle	[TODO: Beschreibung]	Implementiert/Geplant	[TODO: Rolle]
Verschlüsselung	[TODO: Beschreibung]	Implementiert/Geplant	[TODO: Rolle]
Pseudonymisierung	[TODO: Beschreibung]	Implementiert/Geplant	[TODO: Rolle]
Logging und Monitoring	[TODO: Beschreibung]	Implementiert/Geplant	[TODO: Rolle]
Backup und Recovery	[TODO: Beschreibung]	Implementiert/Geplant	[TODO: Rolle]

19.3.2.2 Organisatorische Maßnahmen

Maßnahme	Beschreibung	Implementierungsstatus	Verantwortlich
Datenschutzrichtlinien	[TODO: Beschreibung]	Implementiert/Geplant	[TODO: Rolle]
Schulungsprogramm	[TODO: Beschreibung]	Implementiert/Geplant	[TODO: Rolle]
Incident Response Plan	[TODO: Beschreibung]	Implementiert/Geplant	[TODO: Rolle]

Maßnahme	Beschreibung	Implementierungsstatus	Verantwortlich
Zugriffsverwaltung	[TODO: Beschreibung]	Implementiert/Geplant	[TODO: Rolle]
Vertraulichkeitsverpflichtungen	[TODO: Beschreibung]	Implementiert/Geplant	[TODO: Rolle]

19.4 Datenschutz durch Technikgestaltung (Art. 25 Abs. 1)

19.4.1 Privacy by Design

Grundsätze: - Datenschutz als Standardeinstellung - Datenminimierung von Anfang an - Pseudonymisierung wo möglich - Transparenz in der Verarbeitung - Benutzerfreundliche Datenschutzfunktionen

Umsetzung in Projekten:

Projektphase	Datenschutzmaßnahmen	Verantwortlich
Anforderungsanalyse	[TODO: Maßnahmen]	[TODO: Rolle]
Design	[TODO: Maßnahmen]	[TODO: Rolle]
Implementierung	[TODO: Maßnahmen]	[TODO: Rolle]
Testing	[TODO: Maßnahmen]	[TODO: Rolle]
Deployment	[TODO: Maßnahmen]	[TODO: Rolle]

19.5 Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2)

19.5.1 Privacy by Default

Standardeinstellungen: - Nur notwendige Daten werden standardmäßig verarbeitet - Minimale Speicherdauer als Standard - Eingeschränkter Zugriff als Standard - Opt-in statt Opt-out für nicht-notwendige Verarbeitung

Beispiele:

System/Prozess	Standardeinstellung	Begründung
[TODO: System]	[TODO: Einstellung]	[TODO: Begründung]

19.6 Verhaltensregeln und Zertifizierung

19.6.1 Verhaltensregeln (Art. 40)

Status: [TODO: Teilnahme an Verhaltensregeln? Ja/Nein]
Verhaltensregeln: [TODO: Name, Referenz]

19.6.2 Zertifizierung (Art. 42)

Status: [TODO: Datenschutz-Zertifizierung vorhanden? Ja/Nein]
Zertifizierung: [TODO: Art der Zertifizierung, Gültigkeit]

19.7 Überprüfung und Aktualisierung der Maßnahmen

19.7.1 Regelmäßige Überprüfung

Überprüfungszyklen: - **Jährliche Überprüfung:** Vollständige Bewertung aller TOM - **Quartalsweise Überprüfung:** Kritische Systeme und Hochrisiko-Verarbeitungen - **Ad-hoc Überprüfung:** Bei Sicherheitsvorfällen, neuen Bedrohungen, Systemänderungen

19.7.2 Aktualisierungsprozess

1. **Identifikation:** Neue Risiken oder Schwachstellen erkennen
2. **Bewertung:** Angemessenheit bestehender Maßnahmen prüfen
3. **Planung:** Zusätzliche oder verbesserte Maßnahmen planen
4. **Umsetzung:** Maßnahmen implementieren
5. **Dokumentation:** Änderungen dokumentieren
6. **Überprüfung:** Wirksamkeit der Maßnahmen validieren

19.8 Dokumentation und Nachweisführung

19.8.1 Pflichtdokumente

- **Verzeichnis der Verarbeitungstätigkeiten (Art. 30)**
- **Datenschutz-Folgenabschätzungen (Art. 35)**
- **Auftragsverarbeiter-Verträge (Art. 28)**
- **TOM-Dokumentation (Art. 32)**
- **Einwilligungsnachweise (Art. 7)**
- **Informationsnachweise (Art. 13, 14)**

19.8.2 Aufbewahrungsfristen

Dokument	Aufbewahrungsfrist	Rechtsgrundlage
Verarbeitungsverzeichnis	Während Betrieb + 3 Jahre	Art. 30
DSFA	Während Betrieb + 3 Jahre	Art. 35
AVV	Vertragslaufzeit + 3 Jahre	Art. 28
Breach-Dokumentation	3 Jahre	Art. 33

19.9 Verantwortlichkeiten

Aufgabe	Verantwortlich	Rechenschaftspflichtig	Konsultiert	Informiert
TOM-Implementierung	[TODO]	[TODO]	[TODO]	[TODO]

Aufgabe	Verantwortlich	Rechenschaftspflichtig	Konsultiert	Informiert
TOM-Überprüfung	[TODO]	[TODO]	[TODO]	[TODO]
Dokumentation	[TODO]	[TODO]	[TODO]	[TODO]
Nachweisführung	[TODO]	[TODO]	[TODO]	[TODO]

19.10 Verknüpfung zu anderen Dokumenten

- **Datenschutzgrundsätze (Art. 5):** Grundlage für alle Maßnahmen
- **Sicherheit der Verarbeitung (Art. 32):** Detaillierte technische Maßnahmen
- **Datenschutz-Folgenabschätzung (Art. 35):** Risikobewertung
- **Auftragsverarbeitung (Art. 28):** Verantwortlichkeiten bei Auftragsverarbeitern

---

Nächste Schritte: 1. Dokumentieren Sie alle implementierten technischen und organisatorischen Maßnahmen 2. Erstellen Sie einen Überprüfungsplan für regelmäßige TOM-Audits 3. Implementieren Sie Privacy by Design und Privacy by Default in allen Projekten 4. Stellen Sie sicher, dass alle Nachweisdokumente aktuell und verfügbar sind 5. Definieren Sie klare Verantwortlichkeiten für die Rechenschaftspflicht

ewpage

Chapter 20

Auftragsverarbeitung

Dokument-ID: 0310
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

20.1 Zweck

Dieses Dokument regelt die Auftragsverarbeitung bei {{ meta.organization }} gemäß Art. 28 DSGVO. Es definiert die Anforderungen an Auftragsverarbeiter, die Vertragsgestaltung und die Kontrollmechanismen.

20.2 Auftragsverarbeiter-Verzeichnis

20.2.1 Aktive Auftragsverarbeiter

Auftragsverarbeiter	Dienstleistung	Verarbeitete Daten	AVV-Datum	Nächste Prüfung
[TODO: Name]	[TODO: Service]	[TODO: Datenkategorien]	[TODO: Datum]	[TODO: Datum]

20.2.2 Kategorien von Auftragsverarbeitern

- **IT-Dienstleister:** [TODO: z.B. Cloud-Provider, Hosting]
- **HR-Dienstleister:** [TODO: z.B. Lohnabrechnung, Recruiting]
- **Marketing-Dienstleister:** [TODO: z.B. E-Mail-Marketing, CRM]
- **Support-Dienstleister:** [TODO: z.B. Helpdesk, Call-Center]
- **Weitere:** [TODO: Weitere Kategorien]

20.3 Anforderungen an Auftragsverarbeiter (Art. 28 Abs. 1)

20.3.1 Auswahlkriterien

Der Auftragsverarbeiter muss hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen durchgeführt werden.

Bewertungskriterien:

Kriterium	Beschreibung	Bewertungsmethode
Fachkunde	Expertise im Datenschutz	Zertifikate, Referenzen
Zuverlässigkeit	Nachgewiesene Compliance	Audits, Berichte
Ressourcen	Ausreichende Kapazitäten	Dokumentation, Nachweis
TOM	Angemessene Sicherheitsmaßnahmen	TOM-Dokumentation
Zertifizierungen	ISO 27001, SOC 2, etc.	Zertifikate

20.3.2 Auswahlprozess

1. **Bedarfsanalyse:** Anforderungen definieren
2. **Marktanalyse:** Potenzielle Dienstleister identifizieren
3. **Vorauswahl:** Anhand Auswahlkriterien
4. **Due Diligence:** Detaillierte Prüfung
5. **Vertragsverhandlung:** AVV-Abschluss
6. **Freigabe:** Durch Datenschutzbeauftragten
7. **Onboarding:** Integration und Schulung

20.4 Auftragsverarbeiter-Vertrag (AVV)

20.4.1 Pflichtinhalte gemäß Art. 28 Abs. 3

Der Vertrag muss folgende Punkte regeln:

20.4.1.1 1. Gegenstand und Dauer

- **Gegenstand:** [TODO: Art der Verarbeitung]
- **Dauer:** [TODO: Vertragslaufzeit]
- **Art und Zweck der Verarbeitung:** [TODO: Beschreibung]

20.4.1.2 2. Art der personenbezogenen Daten

- **Datenkategorien:** [TODO: z.B. Kontaktdaten, Vertragsdaten]
- **Kategorien betroffener Personen:** [TODO: z.B. Kunden, Mitarbeiter]

20.4.1.3 3. Pflichten und Rechte des Verantwortlichen

- Weisungsrecht
- Kontrollrecht
- Recht auf Auskunft
- Recht auf Löschung

20.4.1.4 4. Pflichten des Auftragsverarbeiters

Gemäß Art. 28 Abs. 3 lit. a-h:

Pflicht	Beschreibung	Umsetzung
a) Weisungsgebundenheit	Nur auf dokumentierte Weisung verarbeiten	[TODO: Prozess]
b) Vertraulichkeit	Verpflichtung zur Vertraulichkeit	[TODO: Nachweis]
c) Sicherheit	Maßnahmen gemäß Art. 32	[TODO: TOM-Dokumentation]
d) Sub-Auftragsverarbeiter	Genehmigung und Bedingungen	[TODO: Prozess]
e) Betroffenenrechte	Unterstützung bei Anfragen	[TODO: Prozess]
f) Unterstützung	Bei Compliance-Pflichten	[TODO: Vereinbarung]
g) Löschung/Rückgabe	Nach Vertragsende	[TODO: Prozess]
h) Nachweispflicht	Informationen zur Verfügung stellen	[TODO: Reporting]

20.4.2 Vertragsvorlage

Standard-AVV-Vorlage: [TODO: Link zur Vorlage]
Genehmigungsprozess: [TODO: Beschreibe Freigabeprozess]

20.5 Sub-Auftragsverarbeiter (Art. 28 Abs. 2, 4)

20.5.1 Genehmigungsverfahren

Genehmigungsart: [TODO: Allgemeine oder spezifische Genehmigung]

20.5.1.1 Allgemeine Genehmigung

- Liste genehmigter Sub-Auftragsverarbeiter wird geführt
- Informationspflicht bei Änderungen
- Widerspruchsrecht des Verantwortlichen

20.5.1.2 Spezifische Genehmigung

- Einzelfallgenehmigung erforderlich
- Prüfung vor Beauftragung
- Dokumentation der Genehmigung

20.5.2 Sub-Auftragsverarbeiter-Verzeichnis

Sub-Auftragsverarbeiter	Hauptauftragsverarbeiter	Dienstleistung	Genehmigungsdatum
[TODO: Name]	[TODO: Name]	[TODO: Service]	[TODO: Datum]

20.6 Kontrolle und Überwachung

20.6.1 Kontrollrechte (Art. 28 Abs. 3 lit. h)

Kontrollmaßnahmen: - Audits vor Ort - Dokumentenprüfung - Zertifikatsprüfung - Fragebogen-Assessments - Penetrationstests

20.6.2 Kontrollplan

Auftragsverarbeiter	Kontrollart	Frequenz	Nächste Kontrolle	Verantwortlich
[TODO: Name]	[TODO: Art]	[TODO: Frequenz]	[TODO: Datum]	[TODO: Rolle]

20.6.3 Audit-Checkliste

- ☐ AVV vollständig und aktuell
- ☐ TOM-Dokumentation vorhanden und angemessen
- ☐ Sub-Auftragsverarbeiter genehmigt
- ☐ Zertifizierungen gültig
- ☐ Incident-Response-Prozess definiert
- ☐ Schulungsnachweise vorhanden
- ☐ Datenlöschung/Rückgabe geregelt
- ☐ Versicherungsschutz ausreichend

20.7 Weisungen

20.7.1 Weisungserteilung

Weisungsberechtigte Personen: - [TODO: Rolle/Name] - [TODO: Rolle/Name]

Weisungsform: - Schriftlich (E-Mail, Dokument) - Dokumentiert und nachvollziehbar - Mit Datum und Unterschrift

20.7.2 Weisungsregister

Datum	Auftragsverarbeiter	Weisung	Erteilt durch	Status
[TODO]	[TODO: Name]	[TODO: Inhalt]	[TODO: Person]	Umgesetzt/Offen

20.8 Datenschutzverletzungen

20.8.1 Meldepflicht des Auftragsverarbeiters

Der Auftragsverarbeiter muss den Verantwortlichen unverzüglich über Datenschutzverletzungen informieren.

Meldeprozess: 1. Unverzügliche Meldung an: [TODO: Kontakt] 2. Informationen: Art der Verletzung, betroffene Daten, Maßnahmen 3. Frist: Innerhalb von [TODO: z.B. 24 Stunden]

20.8.2 Incident-Response-Koordination

- Gemeinsame Incident-Response-Pläne
- Regelmäßige Tests und Übungen
- Klare Kommunikationswege
- Dokumentation von Vorfällen

20.9 Vertragsende

20.9.1 Löschung oder Rückgabe (Art. 28 Abs. 3 lit. g)

Nach Vertragsende:

Datenart	Maßnahme	Frist	Nachweis
[TODO: Datenart]	Löschung/Rückgabe	[TODO: Frist]	[TODO: Nachweis]

Löschnachweis: [TODO: Beschreibe Nachweisverfahren]

20.9.2 Offboarding-Prozess

1. Vertragsende-Mitteilung
2. Datenrückgabe oder Löschung
3. Zugangsrechte entziehen
4. Löschnachweis einholen
5. Dokumentation abschließen

20.10 Verantwortlichkeiten

Aufgabe	Verantwortlich	Rechenschaftspflichtig	Konsultiert	Informiert
AVV-Abschluss	[TODO]	[TODO]	[TODO]	[TODO]
Kontrolle	[TODO]	[TODO]	[TODO]	[TODO]
Weisungserteilung	[TODO]	[TODO]	[TODO]	[TODO]
Incident-Management	[TODO]	[TODO]	[TODO]	[TODO]

20.11 Verknüpfung zu anderen Dokumenten

- **Verantwortlicher-Pflichten (Art. 24):** Gesamtverantwortung
- **Sicherheit der Verarbeitung (Art. 32):** TOM-Anforderungen
- **Datenschutzverletzungen (Art. 33):** Meldepflichten
- **Verzeichnis der Verarbeitungstätigkeiten (Art. 30):** Dokumentation

---

Nächste Schritte: 1. Erstellen Sie ein vollständiges Verzeichnis aller Auftragsverarbeiter 2. Prüfen Sie alle bestehenden Verträge auf DSGVO-Konformität 3. Implementieren Sie einen Kontrollplan für regelmäßige Audits 4. Definieren Sie Weisungsprozesse und -berechtigungen 5. Etablieren Sie ein Weisungsregister

ewpage

Chapter 21

Verzeichnis der Verarbeitungstätigkeiten

Dokument-ID: 0320
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

21.1 Zweck

Dieses Dokument ist das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO für {{ meta.organization }}. Es dokumentiert alle Verarbeitungen personenbezogener Daten systematisch und dient als Nachweis der Compliance.

21.2 Pflicht zur Führung eines Verzeichnisses

Anwendbarkeit: [TODO: Prüfe Ausnahme für < 250 Mitarbeiter gemäß Art. 30 Abs. 5]

21.2.1 Ausnahmen (Art. 30 Abs. 5)

Die Pflicht gilt nicht für Unternehmen mit weniger als 250 Mitarbeitern, es sei denn: - Die Verarbeitung birgt ein Risiko für die Rechte und Freiheiten betroffener Personen - Die Verarbeitung ist nicht nur gelegentlich - Die Verarbeitung umfasst besondere Kategorien (Art. 9) oder strafrechtliche Daten (Art. 10)

Status für unsere Organisation: [TODO: Pflicht gilt / Ausnahme greift nicht]

21.3 Verzeichnis für Verantwortliche (Art. 30 Abs. 1)

21.3.1 Verarbeitungstätigkeit 1: [TODO: Name der Verarbeitung]

21.3.1.1 a) Name und Kontaktdaten

- **Verantwortlicher:** [TODO: Name, Adresse, Kontakt]
- **Vertreter (falls zutreffend):** [TODO: Name, Adresse, Kontakt]
- **Datenschutzbeauftragter:** [TODO: Name, Kontakt]

21.3.1.2 b) Zwecke der Verarbeitung

- **Hauptzweck:** [TODO: z.B. Kundenverwaltung]
- **Weitere Zwecke:** [TODO: z.B. Marketing, Analyse]

21.3.1.3 c) Kategorien betroffener Personen

- [TODO: z.B. Kunden]
- [TODO: z.B. Interessenten]
- [TODO: z.B. Lieferanten-Kontakte]

21.3.1.4 d) Kategorien personenbezogener Daten

- **Stammdaten:** [TODO: z.B. Name, Adresse, Geburtsdatum]
- **Kontaktdaten:** [TODO: z.B. E-Mail, Telefon]
- **Vertragsdaten:** [TODO: z.B. Kundennummer, Bestellungen]
- **Zahlungsdaten:** [TODO: z.B. Bankverbindung]
- **Besondere Kategorien (Art. 9):** [TODO: falls zutreffend]

21.3.1.5 e) Kategorien von Empfängern

- **Interne Empfänger:** [TODO: z.B. Vertrieb, Buchhaltung]
- **Externe Empfänger:** [TODO: z.B. Zahlungsdienstleister]
- **Auftragsverarbeiter:** [TODO: z.B. Cloud-Provider]
- **Drittländer:** [TODO: falls zutreffend]

21.3.1.6 f) Drittlandübermittlung

- **Drittland:** [TODO: Land]
- **Rechtsgrundlage:** [TODO: Art. 45/46/49]
- **Garantien:** [TODO: z.B. Standardvertragsklauseln, BCR]
- **Dokumentation:** [TODO: Verweis auf Dokument]

21.3.1.7 g) Fristen für Löschung

- **Regelfall:** [TODO: z.B. 3 Jahre nach Vertragsende]
- **Gesetzliche Aufbewahrungspflichten:** [TODO: z.B. 10 Jahre HGB]
- **Löschkonzept:** [TODO: Verweis auf Dokument]

21.3.1.8 h) Technische und organisatorische Maßnahmen (Art. 32)

- **Zugangskontr olle:** [TODO: Beschreibung]
- **Zugriffskontr olle:** [TODO: Beschreibung]
- **Verschlüsselung:** [TODO: Beschreibung]
- **Pseudonymisierung:** [TODO: Beschreibung]
- **Weitere Maßnahmen:** [TODO: Verweis auf TOM-Dokumentation]

21.3.2 Verarbeitungstätigkeit 2: [TODO: Name der Verarbeitung]

[TODO: Wiederhole Struktur für jede Verarbeitungstätigkeit]

21.4 Verzeichnis für Auftragsverarbeiter (Art. 30 Abs. 2)

Falls {{ meta.organization }} als Auftragsverarbeiter tätig ist:

21.4.1 Auftragsverarbeitung 1: [TODO: Name]

21.4.1.1 a) Name und Kontaktdaten

- **Auftragsverarbeiter:** [TODO: Name, Adresse, Kontakt]
- **Verantwortlicher(n):** [TODO: Name, Adresse, Kontakt]
- **Vertreter (falls zutreffend):** [TODO: Name, Adresse, Kontakt]
- **Datenschutzbeauftragter:** [TODO: Name, Kontakt]

21.4.1.2 b) Kategorien von Verarbeitungen

- [TODO: z.B. Hosting, Lohnabrechnung, E-Mail-Marketing]

21.4.1.3 c) Drittlandübermittlung

- **Drittland:** [TODO: Land]
- **Rechtsgrundlage:** [TODO: Art. 45/46/49]
- **Garantien:** [TODO: z.B. Standardvertragsklauseln]

21.4.1.4 d) Technische und organisatorische Maßnahmen (Art. 32)

- [TODO: Verweis auf TOM-Dokumentation]

21.5 Übersicht aller Verarbeitungstätigkeiten

ID	Verarbeitung	Zweck	Rechtsgrundlage	Betroffene	Datenkategorien	Löschfrist
V001	[TODO]	[TODO]	Art. 6 Abs. 1 lit. [TODO]	[TODO]	[TODO]	[TODO]

ID	Verarbeitung	Zweck	Rechtsgrundlage	Betroffene	Datenkategorien	Löschfrist
V002	[TODO]	[TODO]	Art. 6 Abs. 1 lit. [TODO]	[TODO]	[TODO]	[TODO]

21.6 Pflege und Aktualisierung

21.6.1 Aktualisierungsprozess

Auslöser für Aktualisierung: - Neue Verarbeitungstätigkeit - Änderung bestehender Verarbeitung - Beendigung einer Verarbeitung - Änderung von Auftragsverarbeitern - Änderung von Drittlandübermittlungen

Prozess: 1. Änderung identifizieren 2. Verzeichnis aktualisieren 3. Datenschutzbeauftragten informieren 4. Dokumentation ablegen 5. Version aktualisieren

21.6.2 Verantwortlichkeiten

Aufgabe	Verantwortlich	Frequenz
Pflege des Verzeichnisses	[TODO: Datenschutzkoordinator]	Laufend
Überprüfung	[TODO: Datenschutzbeauftragter]	Quartalsweise
Genehmigung	[TODO: Geschäftsführung]	Bei wesentlichen Änderungen

21.7 Bereitstellung für Aufsichtsbehörde

Das Verzeichnis wird auf Anfrage der Aufsichtsbehörde zur Verfügung gestellt.

Format: [TODO: z.B. PDF, Excel]
Bereitstellungsfrist: Unverzüglich nach Anforderung
Verantwortlich: [TODO: Datenschutzbeauftragter]

21.8 Verknüpfung zu anderen Dokumenten

- **Datenschutz-Folgenabschätzung (Art. 35):** Für Hochrisiko-Verarbeitungen
- **Auftragsverarbeiter-Verträge (Art. 28):** Details zu Auftragsverarbeitern
- **TOM-Dokumentation (Art. 32):** Detaillierte Sicherheitsmaßnahmen
- **Löschkonzept:** Detaillierte Löschfristen und -prozesse

Nächste Schritte: 1. Erfassen Sie systematisch alle Verarbeitungstätigkeiten 2. Dokumentieren Sie alle Pflichtangaben gemäß Art. 30 3. Implementieren Sie einen Aktualisierungsprozess 4. Schulen Sie Mitarbeiter zur Meldung neuer Verarbeitungen 5. Überprüfen Sie das Verzeichnis regelmäßig auf Vollständigkeit

ewpage

Chapter 22

Datenschutzverletzungen und Meldepflicht

Dokument-ID: 0330
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

22.1 Zweck

Dieses Dokument regelt den Umgang mit Datenschutzverletzungen bei {{ meta.organization }} gemäß Art. 33-34 DSGVO. Es definiert Meldepflichten, Fristen und Prozesse zur Bewältigung von Datenschutzvorfällen.

22.2 Definition Datenschutzverletzung (Art. 4 Nr. 12)

Eine Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt.

22.2.1 Kategorien von Datenschutzverletzungen

Kategorie	Beschreibung	Beispiele
Vertraulichkeitsverletzung	Unbefugte Offenlegung oder Zugang	Datenleck, Hacking, versehentliche Weitergabe
Integritätsverletzung	Unbefugte Veränderung	Manipulation, Korruption von Daten

Kategorie	Beschreibung	Beispiele
Verfügbarkeitsverletzung	Verlust oder Vernichtung	Ransomware, Hardwareausfall, versehentliche Löschung

22.3 Meldepflicht an Aufsichtsbehörde (Art. 33)

22.3.1 Grundsatz (Art. 33 Abs. 1)

Der Verantwortliche meldet eine Datenschutzverletzung unverzüglich und möglichst binnen 72 Stunden an die zuständige Aufsichtsbehörde, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.

22.3.2 Risikobewertung

Kriterien zur Bewertung des Risikos:

Kriterium	Niedriges Risiko	Hohes Risiko
Art der Daten	Allgemeine Kontaktdaten	Besondere Kategorien (Art. 9), Finanzdaten
Umfang	Wenige Betroffene	Viele Betroffene
Schwere	Geringe Auswirkungen	Schwerwiegende Auswirkungen
Schutzmaßnahmen	Verschlüsselt, pseudonymisiert	Unverschlüsselt, Klartext
Betroffene	Mitarbeiter (intern)	Kunden, Kinder, vulnerable Gruppen

Entscheidungsbaum: 1. Liegt eine Datenschutzverletzung vor? → Ja/Nein 2. Besteht ein Risiko für Rechte und Freiheiten? → Ja/Nein 3. Wenn Ja: Meldung erforderlich 4. Wenn hohes Risiko: Zusätzlich Benachrichtigung betroffener Personen

22.3.3 Meldepflichtiger Inhalt (Art. 33 Abs. 3)

Die Meldung muss mindestens folgende Informationen enthalten:

22.3.3.1 a) Art der Verletzung

- Beschreibung der Datenschutzverletzung
- Kategorien und ungefähre Anzahl betroffener Personen
- Kategorien und ungefähre Anzahl betroffener Datensätze

22.3.3.2 b) Kontaktstelle

- Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle

22.3.3.3 c) Beschreibung der Folgen

- Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung

22.3.3.4 d) Ergriffene Maßnahmen

- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und Abmilderung

22.3.4 Meldefrist

72-Stunden-Frist ab Kenntnisnahme

Zeitpunkt	Maßnahme
T+0 (Entdeckung)	Incident-Response aktivieren, erste Bewertung
T+24h	Risikobewertung abgeschlossen, Meldepflicht geklärt
T+48h	Meldung vorbereitet
T+72h	Meldung an Aufsichtsbehörde übermittelt

Bei Überschreitung der 72-Stunden-Frist: - Begründung der Verzögerung erforderlich (Art. 33 Abs. 1)

22.3.5 Zuständige Aufsichtsbehörde

Aufsichtsbehörde: [TODO: Name der zuständigen Behörde]
Adresse: [TODO: Adresse]
Melde-Portal: [TODO: URL zum Online-Meldeformular]
Kontakt: [TODO: E-Mail, Telefon]

22.4 Benachrichtigung betroffener Personen (Art. 34)

22.4.1 Benachrichtigungspflicht (Art. 34 Abs. 1)

Wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, benachrichtigt der Verantwortliche die betroffene Person unverzüglich.

22.4.2 Kriterien für hohes Risiko

- **Besondere Kategorien personenbezogener Daten (Art. 9)**
- **Finanzdaten, Zugangsdaten**
- **Große Anzahl betroffener Personen**
- **Vulnerable Gruppen (Kinder, Kranke)**
- **Schwerwiegende Folgen (Identitätsdiebstahl, finanzielle Verluste)**

22.4.3 Inhalt der Benachrichtigung (Art. 34 Abs. 2)

Die Benachrichtigung muss enthalten:

- Art der Datenschutzverletzung
- Name und Kontaktdaten des Datenschutzbeauftragten
- Wahrscheinliche Folgen der Datenschutzverletzung
- Ergriffene oder vorgeschlagene Maßnahmen zur Behebung und Abmilderung
- Empfehlungen für betroffene Personen (z.B. Passwort ändern)

22.4.4 Ausnahmen von der Benachrichtigungspflicht (Art. 34 Abs. 3)

Keine Benachrichtigung erforderlich, wenn:

a) Schutzmaßnahmen: Daten waren verschlüsselt oder anderweitig geschützt
b) Nachträgliche Maßnahmen: Maßnahmen wurden ergriffen, die hohes Risiko beseitigen
c) Unverhältnismäßiger Aufwand: Öffentliche Bekanntmachung stattdessen

22.5 Incident-Response-Prozess

22.5.1 Phase 1: Erkennung und Bewertung

Zeitrahmen: 0-4 Stunden

1. Vorfall erkennen und melden
2. Incident-Response-Team aktivieren
3. Erste Bewertung durchführen
4. Datenschutzverletzung bestätigen

Verantwortlich: [TODO: IT-Security, Datenschutzbeauftragter]

22.5.2 Phase 2: Eindämmung

Zeitrahmen: 4-12 Stunden

1. Sofortmaßnahmen zur Schadensbegrenzung
2. Betroffene Systeme isolieren
3. Weitere Datenverluste verhindern
4. Forensische Sicherung

Verantwortlich: [TODO: IT-Security]

22.5.3 Phase 3: Analyse und Risikobewertung

Zeitrahmen: 12-24 Stunden

1. Umfang der Verletzung ermitteln
2. Betroffene Daten und Personen identifizieren
3. Risikobewertung durchführen
4. Meldepflicht prüfen

Verantwortlich: [TODO: Datenschutzbeauftragter, IT-Security]

22.5.4 Phase 4: Meldung und Benachrichtigung

Zeitrahmen: 24-72 Stunden

1. Meldung an Aufsichtsbehörde (falls erforderlich)
2. Benachrichtigung betroffener Personen (falls erforderlich)
3. Interne Kommunikation
4. Externe Kommunikation (falls erforderlich)

Verantwortlich: [TODO: Datenschutzbeauftragter, Geschäftsführung]

22.5.5 Phase 5: Wiederherstellung

Zeitrahmen: 72 Stunden - Wochen

1. Systeme wiederherstellen
2. Sicherheitslücken schließen
3. Maßnahmen zur Verhinderung implementieren
4. Monitoring verstärken

Verantwortlich: [TODO: IT-Security]

22.5.6 Phase 6: Nachbereitung

Zeitrahmen: Nach Abschluss

1. Incident dokumentieren
2. Lessons Learned durchführen
3. Prozesse anpassen
4. Schulungen aktualisieren

Verantwortlich: [TODO: Datenschutzbeauftragter, IT-Security]

22.6 Dokumentationspflicht (Art. 33 Abs. 5)

Der Verantwortliche dokumentiert alle Datenschutzverletzungen, einschließlich aller Fakten, Auswirkungen und ergriffenen Abhilfemaßnahmen.

22.6.1 Breach-Register

Datum	Art der Verletzung	Betroffene Daten	Anzahl Betroffene	Risiko	Gemeldet	Benachrichtigt	Status
[TODO]	[TODO]	[TODO]	[TODO]	Niedrig/Hoch	Ja/Nein	Ja/Nein	Offen/Geschlossen

22.6.2 Aufbewahrungsfrist

Dokumentation: Mindestens 3 Jahre nach Abschluss des Vorfalls

22.7 Kommunikationspläne

22.7.1 Interne Kommunikation

Eskalationskette: 1. Entdecker → IT-Security 2. IT-Security → Datenschutzbeauftragter 3. Datenschutzbeauftragter → Geschäftsführung 4. Geschäftsführung → Aufsichtsrat (bei schwerwiegenden Vorfällen)

22.7.2 Externe Kommunikation

Stakeholder: - Aufsichtsbehörde - Betroffene Personen - Medien (bei öffentlichem Interesse) - Geschäftspartner (bei Betroffenheit) - Versicherung

Kommunikationsverantwortlicher: [TODO: Rolle]

22.8 Verantwortlichkeiten

Aufgabe	Verantwortlich	Rechenschaftspflichtig	Konsultiert	Informiert
Incident Detection	[TODO]	[TODO]	[TODO]	[TODO]
Risikobewertung	[TODO]	[TODO]	[TODO]	[TODO]
Meldung Aufsichtsbehörde	[TODO]	[TODO]	[TODO]	[TODO]
Benachrichtigung Betroffene	[TODO]	[TODO]	[TODO]	[TODO]
Dokumentation	[TODO]	[TODO]	[TODO]	[TODO]

22.9 Verknüpfung zu anderen Dokumenten

- **Sicherheit der Verarbeitung (Art. 32):** Präventive Maßnahmen
- **Auftragsverarbeitung (Art. 28):** Meldepflicht von Auftragsverarbeitern
- **Datenschutz-Folgenabschätzung (Art. 35):** Risikobewertung
- **Incident-Response-Plan:** Detaillierte technische Prozesse

---

Nächste Schritte: 1. Implementieren Sie einen Incident-Response-Prozess 2. Definieren Sie Eskalationswege und Verantwortlichkeiten 3. Erstellen Sie Vorlagen für Meldungen und Benachrichtigungen 4. Führen Sie regelmäßige Incident-Response-Übungen durch 5. Etablieren Sie ein Breach-Register

ewpage

Chapter 23

Datenschutzbeauftragter

Dokument-ID: 0340
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

23.1 Zweck

Dieses Dokument regelt die Rolle, Aufgaben und Stellung des Datenschutzbeauftragten bei {{ meta.organization }} gemäß Art. 37-39 DSGVO.

23.2 Benennungspflicht (Art. 37)

23.2.1 Prüfung der Benennungspflicht

Der Verantwortliche benennt einen Datenschutzbeauftragten, wenn:

23.2.1.1 a) Öffentliche Stelle oder Behörde (Art. 37 Abs. 1 lit. a)

Status: [TODO: Ja/Nein]
Begründung: [TODO: Beschreibung]

23.2.1.2 b) Kerntätigkeit umfasst umfangreiche regelmäßige und systematische Überwachung (Art. 37 Abs. 1 lit. b)

Kriterien: - Kerntätigkeit der Organisation - Umfangreiche Verarbeitung - Regelmäßig und systematisch - Überwachung von betroffenen Personen

Status: [TODO: Ja/Nein]
Begründung: [TODO: z.B. Online-Tracking, Profiling, Verhaltensüberwachung]

23.2.1.3 c) Kerntätigkeit umfasst umfangreiche Verarbeitung besonderer Kategorien (Art. 37 Abs. 1 lit. c)

Besondere Kategorien (Art. 9): - Gesundheitsdaten - Genetische/biometrische Daten - Rassische/ethnische Herkunft - Politische Meinungen - Religiöse Überzeugungen - Gewerkschaftszugehörigkeit - Sexualleben/sexuelle Orientierung

Status: [TODO: Ja/Nein]
Begründung: [TODO: Beschreibung der Verarbeitung]

23.2.1.4 d) Nationale Regelungen

Deutschland (§ 38 BDSG): Benennungspflicht ab 20 Personen, die ständig mit automatisierter Verarbeitung beschäftigt sind

Status: [TODO: Anzahl Personen, Benennungspflicht Ja/Nein]

23.2.2 Ergebnis der Prüfung

Benennungspflicht: [TODO: Ja/Nein]
Rechtsgrundlage: [TODO: Art. 37 Abs. 1 lit. a/b/c oder nationale Regelung]
Freiwillige Benennung: [TODO: Falls keine Pflicht, aber freiwillig benannt]

23.3 Benennung des Datenschutzbeauftragten

23.3.1 Datenschutzbeauftragter

Name: [TODO: Name]
Typ: [TODO: Intern/Extern]
Kontakt: - E-Mail: [TODO: datenschutz@organization.de] - Telefon: [TODO: Telefonnummer] - Adresse: [TODO: Postadresse]

Benennungsdatum: [TODO: Datum]
Veröffentlichung: [TODO: Intern (Intranet) und extern (Website) veröffentlicht]

23.3.2 Veröffentlichung der Kontaktdaten (Art. 37 Abs. 7)

Die Kontaktdaten des Datenschutzbeauftragten werden veröffentlicht und der Aufsichtsbehörde mitgeteilt.

Veröffentlichungsorte: - Website: [TODO: URL] - Intranet: [TODO: URL] - Datenschutzerklärung: [TODO: URL] - Aushang: [TODO: Standorte]

Mitteilung an Aufsichtsbehörde: [TODO: Datum der Mitteilung]

23.4 Qualifikation und Fachkunde (Art. 37 Abs. 5)

23.4.1 Erforderliche Qualifikationen

Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt.

Fachkunde in folgenden Bereichen:

Bereich	Qualifikation	Nachweis
Datenschutzrecht	[TODO: z.B. Zertifizierung, Studium]	[TODO: Zertifikat]
IT-Sicherheit	[TODO: Kenntnisse]	[TODO: Nachweis]
Branchenkenntnisse	[TODO: Erfahrung in der Branche]	[TODO: Referenzen]
Betriebliche Abläufe	[TODO: Verständnis der Organisation]	[TODO: Erfahrung]

Zertifizierungen: - [TODO: z.B. TÜV-zertifizierter Datenschutzbeauftragter] - [TODO: z.B. GDD-Zertifizierung] - [TODO: z.B. CIPP/E (Certified Information Privacy Professional)]

23.4.2 Fortbildung

Fortbildungsprogramm: - Regelmäßige Teilnahme an Datenschutz-Seminaren - Fachliteratur und Newsletter - Teilnahme an Fachkonferenzen - Austausch mit anderen Datenschutzbeauftragten

Budget: [TODO: Jährliches Fortbildungsbudget]

23.5 Stellung des Datenschutzbeauftragten (Art. 38)

23.5.1 Ordnungsgemäße Einbindung (Art. 38 Abs. 1)

Der Verantwortliche stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

Einbindung in: - Strategische Entscheidungen - Neue Projekte und Systeme - Vertragsverhandlungen mit Auftragsverarbeitern - Datenschutz-Folgenabschätzungen - Incident-Response

23.5.2 Unterstützung und Ressourcen (Art. 38 Abs. 2)

Bereitgestellte Ressourcen:

Ressource	Beschreibung	Status
Personal	[TODO: z.B. Datenschutz-Team]	[TODO: Anzahl Personen]
Budget	[TODO: Jährliches Budget]	[TODO: Betrag]
Räumlichkeiten	[TODO: Büro, Besprechungsräume]	[TODO: Verfügbar]
IT-Systeme	[TODO: Software, Tools]	[TODO: Verfügbar]
Fortbildung	[TODO: Schulungsbudget]	[TODO: Betrag]
Zugang zu Informationen	[TODO: Zugriff auf Systeme, Dokumente]	[TODO: Gewährt]

23.5.3 Unabhängigkeit (Art. 38 Abs. 3)

Der Datenschutzbeauftragte erhält bei der Erfüllung seiner Aufgaben keine Weisungen.

Sicherstellung der Unabhängigkeit: - Direkte Berichtslinie zur Geschäftsführung - Keine Weisungen bezüglich Datenschutzfragen - Keine Interessenkonflikte - Kündigungsschutz

Berichtslinie: [TODO: z.B. direkt an Geschäftsführung/Vorstand]

23.5.4 Verschwiegenheit und Geheimhaltung (Art. 38 Abs. 5)

Der Datenschutzbeauftragte ist bei der Erfüllung seiner Aufgaben an die Verschwiegenheit oder Vertraulichkeit gebunden.

Vertraulichkeitsverpflichtung: [TODO: Datum der Unterzeichnung]

23.5.5 Abberufung und Benachteiligung (Art. 38 Abs. 3)

Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden.

Kündigungsschutz: [TODO: Vertraglich geregelt]

23.6 Aufgaben des Datenschutzbeauftragten (Art. 39)

23.6.1 a) Unterrichtung und Beratung (Art. 39 Abs. 1 lit. a)

Zielgruppen: - Verantwortlicher und Auftragsverarbeiter - Beschäftigte, die Verarbeitungen durchführen

Themen: - Pflichten aus der DSGVO - Nationale Datenschutzvorschriften - Datenschutzgrundsätze - Betroffenenrechte

Umsetzung: - Regelmäßige Schulungen - Beratung bei Projekten - Bereitstellung von Informationsmaterialien - Datenschutz-Newsletter

23.6.2 b) Überwachung der Einhaltung (Art. 39 Abs. 1 lit. b)

Überwachungsaktivitäten: - Überprüfung von Verarbeitungstätigkeiten - Audits und Kontrollen - Überprüfung des Verzeichnisses der Verarbeitungstätigkeiten - Überwachung der Umsetzung von Datenschutzrichtlinien

Überwachungsplan: [TODO: Quartalsweise Audits, jährliche Compliance-Prüfung]

23.6.3 c) Beratung bei Datenschutz-Folgenabschätzung (Art. 39 Abs. 1 lit. c)

Rolle bei DSFA: - Beratung zur Notwendigkeit einer DSFA - Unterstützung bei der Durchführung - Überprüfung der DSFA-Ergebnisse - Empfehlungen zu Maßnahmen

23.6.4 d) Zusammenarbeit mit Aufsichtsbehörde (Art. 39 Abs. 1 lit. d)

Aufgaben: - Anlaufstelle für die Aufsichtsbehörde - Beantwortung von Anfragen - Koordination von Prüfungen - Meldung von Datenschutzverletzungen

Kontakt zur Aufsichtsbehörde: [TODO: Regelmäßiger Austausch]

23.6.5 e) Anlaufstelle für Aufsichtsbehörde (Art. 39 Abs. 1 lit. e)

Der Datenschutzbeauftragte ist Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen.

Erreichbarkeit: [TODO: Kontaktdaten, Erreichbarkeitszeiten]

23.6.6 Weitere Aufgaben

Zusätzliche Aufgaben bei {{ meta.organization }}: - [TODO: z.B. Bearbeitung von Betroffenenanfragen] - [TODO: z.B. Pflege des Verzeichnisses der Verarbeitungstätigkeiten] - [TODO: z.B. Vertragsmanagement für Auftragsverarbeiter] - [TODO: z.B. Datenschutz-Kommunikation]

23.7 Interessenkonflikte vermeiden (Art. 38 Abs. 6)

Der Datenschutzbeauftragte kann andere Aufgaben wahrnehmen, sofern diese nicht zu einem Interessenkonflikt führen.

Unvereinbare Funktionen: - Geschäftsführung - IT-Leitung (operative Verantwortung) - HR-Leitung (operative Verantwortung) - Marketing-Leitung (operative Verantwortung)

Aktuelle Funktion: [TODO: Beschreibung, Prüfung auf Interessenkonflikte]

23.8 Berichtswesen

23.8.1 Berichte an Geschäftsführung

Bericht	Frequenz	Inhalt
Quartalsberichte	Quartalsweise	Compliance-Status, Vorfälle, Maßnahmen
Jahresbericht	Jährlich	Gesamtübersicht, Entwicklungen, Empfehlungen
Ad-hoc-Berichte	Bei Bedarf	Schwerwiegende Vorfälle, dringende Maßnahmen

23.8.2 Teilnahme an Gremien

- **Management-Meetings:** [TODO: Frequenz]
- **IT-Security-Board:** [TODO: Frequenz]
- **Compliance-Committee:** [TODO: Frequenz]

23.9 Verantwortlichkeiten

Aufgabe	Datenschutzbeauftragter	Geschäftsführung	Fachabteilungen
Beratung	Verantwortlich	Konsultiert	Konsultiert
Überwachung	Verantwortlich	Informiert	Informiert
Schulung	Verantwortlich	Unterstützt	Teilnehmer
DSFA	Berät	Genehmigt	Führt durch
Meldungen	Verantwortlich	Informiert	Meldet

23.10 Verknüpfung zu anderen Dokumenten

- **Rollen und Verantwortlichkeiten (Art. 4):** Gesamtübersicht
- **Verantwortlicher-Pflichten (Art. 24):** Zusammenarbeit
- **Datenschutz-Folgenabschätzung (Art. 35):** Beratungsrolle
- **Datenschutzverletzungen (Art. 33):** Meldeverantwortung

Nächste Schritte: 1. Prüfen Sie die Benennungspflicht für Ihre Organisation 2. Benennen Sie einen qualifizierten Datenschutzbeauftragten 3. Veröffentlichen Sie die Kontaktdaten intern und extern 4. Stellen Sie ausreichende Ressourcen bereit 5. Definieren Sie klare Aufgaben und Verantwortlichkeiten

ewpage

Chapter 24

Verhaltensregeln und Zertifizierung

Dokument-ID: 0350
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

24.1 Zweck

Dieses Dokument beschreibt die Teilnahme von {{ meta.organization }} an Verhaltensregeln und Datenschutz-Zertifizierungen gemäß Art. 40-43 DSGVO. Diese dienen als Nachweis der Compliance und können die Rechenschaftspflicht unterstützen.

24.2 Verhaltensregeln (Art. 40-41)

24.2.1 Zweck von Verhaltensregeln (Art. 40 Abs. 1)

Verhaltensregeln tragen zur ordnungsgemäßen Anwendung der DSGVO bei, insbesondere unter Berücksichtigung der besonderen Merkmale der verschiedenen Verarbeitungssektoren und der besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen.

24.2.2 Vorteile der Teilnahme

- **Compliance-Nachweis:** Demonstration der DSGVO-Konformität
- **Branchenstandards:** Orientierung an Best Practices
- **Vertrauensbildung:** Gegenüber Kunden und Partnern
- **Rechtssicherheit:** Klarheit bei der Umsetzung
- **Wettbewerbsvorteil:** Differenzierung im Markt

24.2.3 Verfügbare Verhaltensregeln

24.2.3.1 Branchenspezifische Verhaltensregeln

Verhaltensregel	Herausgeber	Branche	Status	Genehmigung
[TODO: Name]	[TODO: Verband]	[TODO: Branche]	Genehmigt/In Entwicklung	[TODO: Aufsichtsbehörde]

24.2.3.2 Funktionsübergreifende Verhaltensregeln

Verhaltensregel	Thema	Herausgeber	Status
[TODO: Name]	[TODO: z.B. Cloud Computing]	[TODO: Verband]	Genehmigt/In Entwicklung

24.2.4 Teilnahme an Verhaltensregeln

Aktuelle Teilnahme:

Verhaltensregel	Beitrittsdatum	Überwachungsstelle	Nächste Überprüfung
[TODO: Name]	[TODO: Datum]	[TODO: Stelle]	[TODO: Datum]

Status: [TODO: Teilnahme Ja/Nein]

24.2.5 Überwachung der Einhaltung (Art. 41)

Überwachungsstelle: [TODO: Name der akkreditierten Stelle]
Kontakt: [TODO: Kontaktdaten]
Überprüfungsfrequenz: [TODO: z.B. jährlich]

Überwachungsmaßnahmen: - Regelmäßige Audits - Beschwerdebearbeitung - Sanktionen bei Nichteinhaltung - Berichterstattung an Aufsichtsbehörde

24.3 Zertifizierung (Art. 42-43)

24.3.1 Zweck der Zertifizierung (Art. 42 Abs. 1)

Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen dienen dazu, nachzuweisen, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.

24.3.2 Vorteile der Zertifizierung

- **Compliance-Nachweis:** Unabhängige Bestätigung der DSGVO-Konformität
- **Vertrauensbildung:** Transparenz gegenüber Betroffenen
- **Wettbewerbsvorteil:** Marktdifferenzierung
- **Vereinfachung:** Bei Auftragsverarbeiter-Auswahl
- **Internationale Anerkennung:** Grenzüberschreitende Gültigkeit

24.3.3 Verfügbare Zertifizierungen

24.3.3.1 Datenschutz-Zertifizierungen

Zertifizierung	Zertifizierungsstelle	Geltungsbereich	Gültigkeitsdauer
EuroPriSe	[TODO: Stelle]	Produkte, Dienstleistungen	2 Jahre
ISO/IEC 27701	[TODO: Stelle]	PIMS (Privacy Information Management System)	3 Jahre
TÜV-Datenschutz-Zertifikat	TÜV	Organisation, Prozesse	3 Jahre
TISAX	ENX Association	Automobilindustrie	3 Jahre

24.3.3.2 Sicherheits-Zertifizierungen (unterstützend)

Zertifizierung	Zertifizierungsstelle	Geltungsbereich	Gültigkeitsdauer
ISO/IEC 27001	[TODO: Stelle]	Informationssicherheits-Managementsystem	3 Jahre
SOC 2 Type II	[TODO: Stelle]	Service-Organisation-Kontrollen	1 Jahr
BSI C5	BSI	Cloud-Dienste	2 Jahre

24.3.4 Erhaltene Zertifizierungen

Aktuelle Zertifizierungen:

Zertifizierung	Zertifikatsnummer	Ausstellungsdatum	Gültig bis	Zertifizierungsstelle
[TODO: Name]	[TODO: Nummer]	[TODO: Datum]	[TODO: Datum]	[TODO: Stelle]

Status: [TODO: Zertifiziert Ja/Nein]

24.3.5 Zertifizierungsprozess

24.3.5.1 Phase 1: Vorbereitung

1. **Auswahl der Zertifizierung:** Relevanz und Nutzen bewerten
2. **Gap-Analyse:** Ist-Zustand mit Anforderungen abgleichen
3. **Maßnahmenplan:** Lücken schließen
4. **Dokumentation:** Nachweise vorbereiten

Dauer: [TODO: z.B. 3-6 Monate]
Verantwortlich: [TODO: Datenschutzbeauftragter, Projektteam]

24.3.5.2 Phase 2: Audit

1. **Antragstellung:** Bei Zertifizierungsstelle
2. **Dokumentenprüfung:** Vorab-Review
3. **Vor-Ort-Audit:** Überprüfung der Umsetzung
4. **Nachbesserungen:** Falls erforderlich

Dauer: [TODO: z.B. 1-2 Monate]
Verantwortlich: [TODO: Datenschutzbeauftragter]

24.3.5.3 Phase 3: Zertifizierung

1. **Zertifikatausstellung:** Bei erfolgreicher Prüfung
2. **Veröffentlichung:** Zertifikat kommunizieren
3. **Überwachungsaudits:** Regelmäßige Überprüfungen
4. **Rezertifizierung:** Vor Ablauf der Gültigkeit

Dauer: Laufend
Verantwortlich: [TODO: Datenschutzbeauftragter]

24.3.6 Gültigkeitsdauer und Rezertifizierung (Art. 42 Abs. 7)

Zertifizierungen werden für eine Höchstdauer von drei Jahren ausgestellt und können verlängert werden, sofern die Voraussetzungen weiterhin erfüllt sind.

Rezertifizierungsplan:

Zertifizierung	Ablaufdatum	Rezertifizierung geplant	Verantwortlich
[TODO: Name]	[TODO: Datum]	[TODO: Datum]	[TODO: Rolle]

24.3.7 Überwachung und Widerruf (Art. 42 Abs. 8, Art. 43 Abs. 4)

Überwachungsmaßnahmen: - Jährliche Überwachungsaudits - Stichprobenkontrollen - Beschwerdebearbeitung - Kontinuierliche Verbesserung

Widerrufsgründe: - Nichteinhaltung der Zertifizierungskriterien - Schwerwiegende Datenschutzverletzungen - Verweigerung der Überwachung - Täuschung bei der Zertifizierung

24.4 Verwendung von Siegeln und Prüfzeichen

24.4.1 Kommunikation der Zertifizierung

Verwendungsorte: - Website: [TODO: URL] - Datenschutzerklärung: [TODO: URL] - Geschäftsdokumente: [TODO: z.B. Angebote, Verträge] - Marketing-Materialien: [TODO: z.B. Broschüren]

Verwendungsrichtlinien: - Korrekte Darstellung des Siegels - Angabe der Gültigkeitsdauer - Verweis auf Zertifizierungsstelle - Keine irreführende Verwendung

24.4.2 Transparenz gegenüber Betroffenen

Betroffene Personen werden über die Zertifizierung informiert: - In der Datenschutzerklärung - Bei Vertragsabschluss - Auf Anfrage

24.5 Kosten-Nutzen-Analyse

24.5.1 Kosten

Kostenart	Einmalig	Jährlich
Zertifizierungsgebühren	[TODO: Betrag]	[TODO: Betrag]
Beratung/Vorbereitung	[TODO: Betrag]	-
Interne Ressourcen	[TODO: Personentage]	[TODO: Personentage]
Überwachungsaudits	-	[TODO: Betrag]
Rezertifizierung	-	[TODO: Betrag (alle 3 Jahre)]

24.5.2 Nutzen

- **Compliance-Nachweis:** Reduzierung des Haftungsrisikos
- **Vertrauensbildung:** Kundengewinnung und -bindung
- **Prozessverbesserung:** Optimierung der Datenschutzprozesse
- **Wettbewerbsvorteil:** Differenzierung im Markt
- **Internationale Geschäfte:** Erleichterung bei Drittlandübermittlungen

ROI-Bewertung: [TODO: Bewertung des Return on Investment]

24.6 Planung und Roadmap

24.6.1 Kurzfristig (0-12 Monate)

☐ Gap-Analyse durchführen
☐ Zertifizierung auswählen
☐ Maßnahmenplan erstellen
☐ Dokumentation vorbereiten

24.6.2 Mittelfristig (1-2 Jahre)

☐ Zertifizierungsaudit durchführen
☐ Zertifikat erhalten
☐ Erstes Überwachungsaudit
☐ Kommunikation der Zertifizierung

24.6.3 Langfristig (2-3 Jahre)

☐ Regelmäßige Überwachungsaudits
☐ Kontinuierliche Verbesserung
☐ Rezertifizierung planen
☐ Weitere Zertifizierungen evaluieren

24.7 Verantwortlichkeiten

Aufgabe	Verantwortlich	Rechenschaftspflichtig	Konsultiert	Informiert
Zertifizierungsauswahl	[TODO]	[TODO]	[TODO]	[TODO]
Gap-Analyse	[TODO]	[TODO]	[TODO]	[TODO]
Audit-Vorbereitung	[TODO]	[TODO]	[TODO]	[TODO]
Audit-Durchführung	[TODO]	[TODO]	[TODO]	[TODO]
Überwachung	[TODO]	[TODO]	[TODO]	[TODO]

24.8 Verknüpfung zu anderen Dokumenten

- **Verantwortlicher-Pflichten (Art. 24):** Rechenschaftspflicht
- **Auftragsverarbeitung (Art. 28):** Zertifizierung als Auswahlkriterium
- **Datenschutz-Folgenabschätzung (Art. 35):** Zertifizierung als Maßnahme
- **Datenübermittlung (Art. 46):** Zertifizierung als Garantie

---

Nächste Schritte: 1. Evaluieren Sie relevante Verhaltensregeln für Ihre Branche 2. Prüfen Sie verfügbare Datenschutz-Zertifizierungen 3. Führen Sie eine Gap-Analyse durch 4. Erstellen Sie einen Zertifizierungsplan 5. Kommunizieren Sie erhaltene Zertifizierungen transparent

ewpage

Chapter 25

Datenschutz-Folgenabschätzung (DSFA)

Dokument-ID: 0400
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

25.1 Zweck

Dieses Dokument beschreibt den Prozess der Datenschutz-Folgenabschätzung (DSFA) bei {{ meta.organization }} gemäß Art. 35 DSGVO. Eine DSFA ist erforderlich, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

25.2 Erforderlichkeit einer DSFA (Art. 35 Abs. 1)

25.2.1 Grundsatz

Eine DSFA ist erforderlich, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

25.2.2 Pflichtfälle (Art. 35 Abs. 3)

Eine DSFA ist insbesondere erforderlich bei:

25.2.2.1 a) Systematische und umfassende Bewertung persönlicher Aspekte (Art. 35 Abs. 3 lit. a)

Beispiele: - Profiling mit automatisierten Entscheidungen mit rechtlicher Wirkung - Scoring-Verfahren (Kreditwürdigkeit, Gesundheitsrisiko) - Verhaltensbasierte Werbung mit umfassendem

Tracking

Status für unsere Organisation: [TODO: Zutreffend Ja/Nein]

25.2.2.2 b) Umfangreiche Verarbeitung besonderer Kategorien (Art. 35 Abs. 3 lit. b)

Besondere Kategorien (Art. 9): - Gesundheitsdaten - Genetische/biometrische Daten - Rassische/ethnische Herkunft - Politische Meinungen - Religiöse Überzeugungen - Gewerkschaftszugehörigkeit - Sexualleben/sexuelle Orientierung

Status für unsere Organisation: [TODO: Zutreffend Ja/Nein]

25.2.2.3 c) Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (Art. 35 Abs. 3 lit. c)

Beispiele: - Videoüberwachung mit Gesichtserkennung - Tracking von Bewegungsprofilen - Umfassende Standortdaten-Erfassung

Status für unsere Organisation: [TODO: Zutreffend Ja/Nein]

25.2.3 Blacklist der Aufsichtsbehörde (Art. 35 Abs. 4)

Die Aufsichtsbehörde erstellt eine Liste von Verarbeitungsvorgängen, für die eine DSFA durchzuführen ist.

Relevante Einträge für unsere Organisation: - [TODO: Prüfe Liste der zuständigen Aufsichtsbehörde] - [TODO: Dokumentiere zutreffende Einträge]

25.2.4 Whitelist der Aufsichtsbehörde (Art. 35 Abs. 5)

Die Aufsichtsbehörde kann eine Liste von Verarbeitungsvorgängen erstellen, für die keine DSFA erforderlich ist.

Relevante Einträge für unsere Organisation: - [TODO: Prüfe Liste der zuständigen Aufsichtsbehörde] - [TODO: Dokumentiere zutreffende Einträge]

25.2.5 Weitere Kriterien (WP29-Leitlinien)

Zusätzliche Indikatoren für hohes Risiko:

Kriterium	Beschreibung	Zutreffend
Bewertung oder Scoring	Profiling, Vorhersage von Verhalten	Ja/Nein
Automatisierte Entscheidungen	Mit rechtlicher oder ähnlicher Wirkung	Ja/Nein
Systematische Überwachung	Kontinuierliche Beobachtung	Ja/Nein
Sensible Daten	Besondere Kategorien (Art. 9)	Ja/Nein
Datenverarbeitung in großem Umfang	Viele Betroffene oder große Datenmengen	Ja/Nein
Abgleich oder Zusammenführung	Von Datensätzen aus verschiedenen Quellen	Ja/Nein

Kriterium	Beschreibung	Zutreffend
Vulnerable Betroffene	Kinder, Arbeitnehmer, Patienten	Ja/Nein
Innovative Nutzung	Neue Technologien oder Anwendungen	Ja/Nein
Verwehrung von Rechten	Zugang zu Dienstleistung oder Vertrag	Ja/Nein

Faustregel: Bei zwei oder mehr zutreffenden Kriterien ist eine DSFA empfohlen.

25.3 DSFA-Verzeichnis

25.3.1 Übersicht durchgeführter DSFAs

DSFA-ID	Verarbeitung	Durchführungsdatum	Risiko	Status	Nächste Überprüfung
DSFA-001	[TODO: Name]	[TODO: Datum]	Hoch/Mittel/Niedrig	Abgeschlossen/In Arbeit	[TODO: Datum]

25.4 DSFA-Prozess

25.4.1 Phase 1: Schwellwertanalyse

Ziel: Feststellen, ob eine DSFA erforderlich ist

Schritte: 1. Verarbeitung beschreiben 2. Kriterien prüfen (Art. 35 Abs. 3, Blacklist, WP29-Kriterien) 3. Datenschutzbeauftragten konsultieren 4. Entscheidung dokumentieren

Verantwortlich: [TODO: Fachabteilung, Datenschutzbeauftragter]
Dauer: [TODO: z.B. 1-2 Wochen]

25.4.2 Phase 2: DSFA-Durchführung

Ziel: Systematische Bewertung der Risiken

25.4.2.1 Schritt 1: Beschreibung der Verarbeitung (Art. 35 Abs. 7 lit. a)

Zu dokumentieren: - Zwecke der Verarbeitung - Kategorien personenbezogener Daten - Kategorien betroffener Personen - Empfänger der Daten - Speicherdauer - Funktionale Beschreibung der Verarbeitung - Eingesetzte Technologien - Datenflüsse (Diagramme)

25.4.2.2 Schritt 2: Bewertung der Notwendigkeit und Verhältnismäßigkeit (Art. 35 Abs. 7 lit. b)

Zu prüfen: - Ist die Verarbeitung zur Zweckerreichung erforderlich? - Sind die Mittel angemessen? - Werden Datenschutzgrundsätze eingehalten? - Gibt es weniger invasive Alternativen?

Rechtmäßigkeit: - Rechtsgrundlage (Art. 6) - Berechtigte Interessen (falls Art. 6 Abs. 1 lit. f) - Interessenabwägung

25.4.2.3 Schritt 3: Risikobewertung (Art. 35 Abs. 7 lit. c)

Risikoidentifikation:

Risiko	Beschreibung	Betroffene Rechte	Eintrittswahrscheinlichkeit	Schwere
[TODO]	[TODO]	[TODO: z.B. Recht auf Privatsphäre]	Niedrig/Mittel/Hoch	Niedrig/Mittel/Hoch

Risikobewertungsmatrix:

Schwere / Wahrscheinlichkeit	Niedrig	Mittel	Hoch
Hoch	Mittel	Hoch	Sehr hoch
Mittel	Niedrig	Mittel	Hoch
Niedrig	Sehr niedrig	Niedrig	Mittel

Betroffene Rechte und Freiheiten: - Recht auf Privatsphäre - Recht auf Datenschutz - Recht auf Nichtdiskriminierung - Recht auf freie Meinungsäußerung - Weitere Grundrechte

25.4.2.4 Schritt 4: Maßnahmen zur Risikominimierung (Art. 35 Abs. 7 lit. d)

Technische Maßnahmen:

Maßnahme	Beschreibung	Risikominimierung	Status
Verschlüsselung	[TODO]	[TODO: Reduziert Risiko von X auf Y]	Implementiert/Geplant
Pseudonymisierung	[TODO]	[TODO]	Implementiert/Geplant
Zugangskontrollen	[TODO]	[TODO]	Implementiert/Geplant

Organisatorische Maßnahmen:

Maßnahme	Beschreibung	Risikominimierung	Status
Schulungen	[TODO]	[TODO]	Implementiert/Geplant
Richtlinien	[TODO]	[TODO]	Implementiert/Geplant
Audits	[TODO]	[TODO]	Implementiert/Geplant

Restrisiko nach Maßnahmen:

Risiko	Ursprüngliches Risiko	Maßnahmen	Restrisiko	Akzeptabel
[TODO]	[TODO: Hoch]	[TODO: Maßnahmen]	[TODO: Mittel]	Ja/Nein

25.4.3 Phase 3: Konsultation des Datenschutzbeauftragten (Art. 35 Abs. 2)

Pflicht: Der Datenschutzbeauftragte wird bei der Durchführung der DSFA um Rat gefragt.

Konsultation: - **Datum:** [TODO: Datum] - **Stellungnahme:** [TODO: Zusammenfassung der Empfehlungen] - **Berücksichtigung:** [TODO: Wie wurden Empfehlungen umgesetzt]

25.4.4 Phase 4: Einholung der Ansichten Betroffener (Art. 35 Abs. 9)

Gegebenenfalls: Ansichten der betroffenen Personen oder ihrer Vertreter einholen.

Durchgeführt: [TODO: Ja/Nein]
Methode: [TODO: z.B. Umfrage, Fokusgruppe]
Ergebnisse: [TODO: Zusammenfassung]

25.4.5 Phase 5: Dokumentation und Genehmigung

DSFA-Bericht erstellen: - Alle Schritte dokumentieren - Risikobewertung zusammenfassen - Maßnahmen auflisten - Restrisiko bewerten

Genehmigung: - **Verantwortlich:** [TODO: Geschäftsführung] - **Datum:** [TODO: Datum] - **Entscheidung:** Genehmigt / Genehmigt mit Auflagen / Abgelehnt

25.5 Vorherige Konsultation der Aufsichtsbehörde (Art. 36)

25.5.1 Konsultationspflicht (Art. 36 Abs. 1)

Wenn aus der DSFA hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, falls der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, konsultiert der Verantwortliche vor der Verarbeitung die Aufsichtsbehörde.

Kriterien für Konsultation: - Restrisiko nach Maßnahmen ist hoch - Keine weiteren Maßnahmen zur Risikominimierung möglich - Unsicherheit über Angemessenheit der Maßnahmen

Konsultation erforderlich: [TODO: Ja/Nein]

25.5.2 Konsultationsprozess

Vorzulegende Informationen (Art. 36 Abs. 3): - Verantwortlichkeiten - Zwecke und Mittel der Verarbeitung - Maßnahmen zum Schutz der Rechte und Freiheiten - Kontaktdaten des Datenschutzbeauftragten - DSFA-Bericht - Weitere relevante Informationen

Frist der Aufsichtsbehörde: 8 Wochen (verlängerbar auf 14 Wochen bei komplexen Verarbeitungen)

Konsultationsdokumentation: - **Datum der Anfrage:** [TODO: Datum] - **Stellungnahme der Aufsichtsbehörde:** [TODO: Zusammenfassung] - **Umsetzung der Empfehlungen:** [TODO: Maßnahmen]

25.6 Überprüfung und Aktualisierung

25.6.1 Überprüfungspflicht (Art. 35 Abs. 11)

Die DSFA wird überprüft, wenn: - Änderungen des Risikos der Verarbeitung - Änderungen der Verarbeitungstätigkeit - Neue Technologien eingesetzt werden - Neue Erkenntnisse über Risiken vorliegen

Überprüfungsfrequenz: [TODO: z.B. jährlich oder bei Änderungen]

25.6.2 Aktualisierungsprozess

1. Änderungen identifizieren
2. Risikobewertung aktualisieren
3. Maßnahmen anpassen
4. Datenschutzbeauftragten konsultieren
5. Dokumentation aktualisieren
6. Genehmigung einholen

25.7 DSFA-Vorlage

Standardvorlage: [TODO: Link zur DSFA-Vorlage]
Branchenspezifische Vorlagen: [TODO: Falls vorhanden]

25.8 Verantwortlichkeiten

Aufgabe	Verantwortlich	Rechenschaftspflichtig	Konsultiert	Informiert
Schwellwertanalyse	[TODO]	[TODO]	[TODO]	[TODO]
DSFA-Durchführung	[TODO]	[TODO]	[TODO]	[TODO]
Risikobewertung	[TODO]	[TODO]	[TODO]	[TODO]
Maßnahmenplanung	[TODO]	[TODO]	[TODO]	[TODO]
Genehmigung	[TODO]	[TODO]	[TODO]	[TODO]

25.9 Verknüpfung zu anderen Dokumenten

- **Verantwortlicher-Pflichten (Art. 24):** Rechenschaftspflicht
- **Sicherheit der Verarbeitung (Art. 32):** Technische Maßnahmen
- **Verzeichnis der Verarbeitungstätigkeiten (Art. 30):** Dokumentation
- **Datenschutzbeauftragter (Art. 39):** Beratungsrolle

Nächste Schritte: 1. Identifizieren Sie alle Verarbeitungen, die eine DSFA erfordern 2. Führen Sie systematische DSFAs durch 3. Dokumentieren Sie Risiken und Maßnahmen 4. Konsultieren Sie den Datenschutzbeauftragten 5. Überprüfen Sie DSFAs regelmäßig

ewpage

Chapter 26

DSFA Template - Vorlage

Dokument-ID: 0410
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

26.1 DSFA-Identifikation

DSFA-ID: [TODO: z.B. DSFA-2024-001]
Verarbeitung: [TODO: Name der Verarbeitung]
Verantwortlicher: [TODO: Name, Abteilung]
Erstellt am: [TODO: Datum]
Erstellt von: [TODO: Name, Rolle]
Status: Entwurf / In Prüfung / Genehmigt

26.2 1. Beschreibung der Verarbeitung

26.2.1 1.1 Zwecke der Verarbeitung

Hauptzweck: [TODO: Beschreibe den Hauptzweck der Verarbeitung]

Weitere Zwecke: - [TODO: Zweck 1] - [TODO: Zweck 2]

26.2.2 1.2 Kategorien personenbezogener Daten

Datenkategorie	Beispiele	Besondere Kategorie (Art. 9)
[TODO: z.B. Stammdaten]	[TODO: Name, Adresse, Geburtsdatum]	Nein
[TODO: z.B. Kontaktdaten]	[TODO: E-Mail, Telefon]	Nein
[TODO: z.B. Gesundheitsdaten]	[TODO: Diagnosen, Behandlungen]	Ja

Datenkategorie	Beispiele	Besondere Kategorie (Art. 9)

Geschätztes Datenvolumen: [TODO: z.B. 10.000 Datensätze]

26.2.3 1.3 Kategorien betroffener Personen

- [TODO: z.B. Kunden]
- [TODO: z.B. Mitarbeiter]
- [TODO: z.B. Patienten]

Geschätzte Anzahl: [TODO: z.B. 5.000 Personen]

Vulnerable Gruppen: [TODO: z.B. Kinder, Patienten - Ja/Nein]

26.2.4 1.4 Empfänger der Daten

Interne Empfänger: - [TODO: z.B. Vertrieb, Buchhaltung]

Externe Empfänger: - [TODO: z.B. Zahlungsdienstleister]

Auftragsverarbeiter: - [TODO: z.B. Cloud-Provider, IT-Dienstleister]

Drittlandübermittlung: [TODO: Ja/Nein - falls Ja, welche Länder]

26.2.5 1.5 Speicherdauer

Regelfall: [TODO: z.B. 3 Jahre nach Vertragsende]
Gesetzliche Aufbewahrungspflichten: [TODO: z.B. 10 Jahre HGB]
Löschkonzept: [TODO: Verweis auf Dokument oder Beschreibung]

26.2.6 1.6 Funktionale Beschreibung

[TODO: Beschreibe die Verarbeitung im Detail: - Wie werden Daten erhoben? - Wie werden Daten verarbeitet? - Welche Systeme sind beteiligt? - Welche Technologien werden eingesetzt? - Gibt es automatisierte Entscheidungen? - Gibt es Profiling?]

26.2.7 1.7 Datenfluss-Diagramm

[TODO: Füge ein Diagramm ein, das den Datenfluss visualisiert]

```
[Datenquelle] → [Verarbeitungssystem] → [Speicherung] → [Empfänger]
```

26.3 2. Notwendigkeit und Verhältnismäßigkeit

26.3.1 2.1 Rechtsgrundlage

Rechtsgrundlage: [TODO: Art. 6 Abs. 1 lit. a/b/c/d/e/f]

Begründung: [TODO: Erläutere, warum diese Rechtsgrundlage anwendbar ist]

Bei besonderen Kategorien (Art. 9): Rechtsgrundlage: [TODO: Art. 9 Abs. 2 lit. a-j]

26.3.2 2.2 Notwendigkeit

Ist die Verarbeitung zur Zweckerreichung erforderlich? [TODO: Ja/Nein - Begründung]

Gibt es weniger invasive Alternativen? [TODO: Ja/Nein - falls Ja, warum werden sie nicht genutzt?]

26.3.3 2.3 Verhältnismäßigkeit

Sind die Mittel angemessen? [TODO: Bewertung der Verhältnismäßigkeit]

Datenschutzgrundsätze (Art. 5):

Grundsatz	Einhaltung	Begründung
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	Ja/Nein	[TODO]
Zweckbindung	Ja/Nein	[TODO]
Datenminimierung	Ja/Nein	[TODO]
Richtigkeit	Ja/Nein	[TODO]
Speicherbegrenzung	Ja/Nein	[TODO]
Integrität und Vertraulichkeit	Ja/Nein	[TODO]

26.3.4 2.4 Interessenabwägung (bei Art. 6 Abs. 1 lit. f)

Berechtigtes Interesse des Verantwortlichen: [TODO: Beschreibe das berechtigte Interesse]

Interessen der betroffenen Personen: [TODO: Beschreibe die Interessen und Grundrechte der Betroffenen]

Abwägung: [TODO: Überwiegen die Interessen des Verantwortlichen oder der Betroffenen?]

26.4 3. Risikobewertung

26.4.1 3.1 Risikoidentifikation

Identifizierte Risiken:

26.4.1.1 Risiko 1: [TODO: Name des Risikos]

Beschreibung: [TODO: Detaillierte Beschreibung des Risikos]

Bedrohung: [TODO: z.B. Unbefugter Zugriff, Datenverlust, Manipulation]

Betroffene Rechte und Freiheiten: - [TODO: z.B. Recht auf Privatsphäre] - [TODO: z.B. Recht auf Datenschutz]

Mögliche Folgen für Betroffene: - [TODO: z.B. Identitätsdiebstahl] - [TODO: z.B. Finanzielle Verluste] - [TODO: z.B. Diskriminierung] - [TODO: z.B. Reputationsschaden]

Eintrittswahrscheinlichkeit: [TODO: Niedrig / Mittel / Hoch]

Begründung der Wahrscheinlichkeit: [TODO: Warum ist die Wahrscheinlichkeit so eingeschätzt?]

Schwere der Auswirkungen: [TODO: Niedrig / Mittel / Hoch]

Begründung der Schwere: [TODO: Warum ist die Schwere so eingeschätzt?]

Risikostufe: [TODO: Berechne aus Wahrscheinlichkeit × Schwere]

26.4.1.2 Risiko 2: [TODO: Name des Risikos]

[TODO: Wiederhole Struktur für weitere Risiken]

26.4.2 3.2 Risikobewertungsmatrix

Risiko	Wahrscheinlichkeit	Schwere	Risikostufe
Risiko 1	[TODO]	[TODO]	[TODO]
Risiko 2	[TODO]	[TODO]	[TODO]

Gesamtrisiko: [TODO: Niedrig / Mittel / Hoch / Sehr hoch]

26.5 4. Maßnahmen zur Risikominimierung

26.5.1 4.1 Technische Maßnahmen

26.5.1.1 Maßnahme 1: [TODO: Name der Maßnahme]

Beschreibung: [TODO: Detaillierte Beschreibung]

Adressiertes Risiko: [TODO: Risiko 1, Risiko 2, …]

Wirksamkeit: [TODO: Hoch / Mittel / Niedrig]

Implementierungsstatus: [TODO: Implementiert / In Umsetzung / Geplant]

Verantwortlich: [TODO: Rolle/Name]

Frist: [TODO: Datum]

26.5.1.2 Maßnahme 2: [TODO: Name der Maßnahme]

[TODO: Wiederhole Struktur für weitere Maßnahmen]

26.5.2 4.2 Organisatorische Maßnahmen

26.5.2.1 Maßnahme 1: [TODO: Name der Maßnahme]

Beschreibung: [TODO: Detaillierte Beschreibung]

Adressiertes Risiko: [TODO: Risiko 1, Risiko 2, …]

Wirksamkeit: [TODO: Hoch / Mittel / Niedrig]

Implementierungsstatus: [TODO: Implementiert / In Umsetzung / Geplant]

Verantwortlich: [TODO: Rolle/Name]

Frist: [TODO: Datum]

26.5.3 4.3 Datenschutz durch Technikgestaltung (Privacy by Design)

Umgesetzte Prinzipien: - [ ] Datenminimierung von Anfang an - [ ] Pseudonymisierung wo möglich - [ ] Verschlüsselung als Standard - [ ] Transparenz in der Verarbeitung - [ ] Benutzerfreundliche Datenschutzfunktionen

Beschreibung: [TODO: Wie wurden Privacy by Design Prinzipien umgesetzt?]

26.5.4 4.4 Datenschutz durch datenschutzfreundliche Voreinstellungen (Privacy by Default)

Umgesetzte Prinzipien: - [ ] Nur notwendige Daten werden standardmäßig verarbeitet - [ ] Minimale Speicherdauer als Standard - [ ] Eingeschränkter Zugriff als Standard - [ ] Opt-in statt Opt-out

Beschreibung: [TODO: Wie wurden Privacy by Default Prinzipien umgesetzt?]

26.6 5. Restrisikobewertung

26.6.1 5.1 Risiken nach Maßnahmen

Risiko	Ursprüngliche Risikostufe	Maßnahmen	Restrisiko	Akzeptabel
Risiko 1	[TODO: Hoch]	[TODO: Maßnahmen 1, 2]	[TODO: Mittel]	Ja/Nein
Risiko 2	[TODO: Mittel]	[TODO: Maßnahme 3]	[TODO: Niedrig]	Ja/Nein

26.6.2 5.2 Gesamtbewertung

Restrisiko nach Maßnahmen: [TODO: Niedrig / Mittel / Hoch]

Ist das Restrisiko akzeptabel? [TODO: Ja / Nein]

Begründung: [TODO: Warum ist das Restrisiko akzeptabel oder nicht akzeptabel?]

26.7 6. Konsultation des Datenschutzbeauftragten

Datenschutzbeauftragter: [TODO: Name]

Konsultationsdatum: [TODO: Datum]

Stellungnahme: [TODO: Zusammenfassung der Empfehlungen des Datenschutzbeauftragten]

Berücksichtigung der Empfehlungen: [TODO: Wie wurden die Empfehlungen umgesetzt?]

Unterschrift Datenschutzbeauftragter: _____

26.8 7. Einholung der Ansichten Betroffener

Wurden Ansichten betroffener Personen eingeholt? [TODO: Ja / Nein]

Falls Ja:

Methode: [TODO: z.B. Umfrage, Fokusgruppe, Konsultation]

Datum: [TODO: Datum]

Ergebnisse: [TODO: Zusammenfassung der Ansichten und Bedenken]

Berücksichtigung: [TODO: Wie wurden die Ansichten berücksichtigt?]

26.9 8. Vorherige Konsultation der Aufsichtsbehörde

Ist eine Konsultation der Aufsichtsbehörde erforderlich? [TODO: Ja / Nein]

Begründung: [TODO: Warum ist/ist keine Konsultation erforderlich?]

Falls Ja:

Datum der Anfrage: [TODO: Datum]

Stellungnahme der Aufsichtsbehörde: [TODO: Zusammenfassung der Stellungnahme]

Umsetzung der Empfehlungen: [TODO: Wie wurden die Empfehlungen umgesetzt?]

26.10 9. Genehmigung

Verantwortlicher: [TODO: Name, Rolle]

Datum: [TODO: Datum]

Entscheidung: [ ] Genehmigt [ ] Genehmigt mit Auflagen [ ] Abgelehnt

Auflagen (falls zutreffend): [TODO: Liste der Auflagen]

Unterschrift: _____

26.11 10. Überprüfung und Aktualisierung

Nächste Überprüfung geplant: [TODO: Datum]

Überprüfungsauslöser: - [ ] Jährliche Überprüfung - [ ] Änderung der Verarbeitung - [ ] Neue Technologien - [ ] Sicherheitsvorfall - [ ] Neue Erkenntnisse über Risiken

26.11.1 Änderungshistorie

Version	Datum	Änderung	Geändert von
1.0	[TODO]	Erstversion	[TODO]
1.1	[TODO]	[TODO: Beschreibung]	[TODO]

26.12 Anhänge

- ☐ Datenfluss-Diagramme
- ☐ TOM-Dokumentation
- ☐ Auftragsverarbeiter-Verträge
- ☐ Einwilligungserklärungen
- ☐ Weitere relevante Dokumente

Hinweis: Diese DSFA ist ein lebendes Dokument und muss bei Änderungen der Verarbeitung oder neuen Erkenntnissen über Risiken aktualisiert werden.

ewpage

Chapter 27

Datenübermittlung in Drittländer

Dokument-ID: 0500
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

27.1 Zweck

Dieses Dokument regelt die Übermittlung personenbezogener Daten in Drittländer (außerhalb EU/EWR) bei {{ meta.organization }} gemäß Art. 44-50 DSGVO. Es stellt sicher, dass auch bei internationalen Datentransfers ein angemessenes Schutzniveau gewährleistet ist.

27.2 Grundsatz (Art. 44)

Eine Übermittlung personenbezogener Daten in ein Drittland darf nur erfolgen, wenn: - Die Bedingungen der Art. 45-49 eingehalten werden - Die übrigen Bestimmungen der DSGVO eingehalten werden - Einschließlich der Betroffenenrechte und Rechtsbehelfe

27.3 Verzeichnis der Drittlandübermittlungen

27.3.1 Übersicht

ID	Empfänger	Drittland	Zweck	Rechtsgrundlage	Garantien	Volumen
T001	[TODO: Name]	[TODO: Land]	[TODO: Zweck]	Art. 45/46/49	[TODO]	[TODO: Anzahl Betroffene]

27.4 Angemessenheitsbeschluss (Art. 45)

27.4.1 Länder mit Angemessenheitsbeschluss

Die Europäische Kommission kann beschließen, dass ein Drittland ein angemessenes Schutzniveau bietet.

Aktuelle Angemessenheitsbeschlüsse (Stand 2024):

Land/Region	Beschluss	Gültig seit	Besonderheiten
Andorra	2010/625/EU	19.10.2010	-
Argentinien	2003/490/EG	30.06.2003	-
Kanada	2002/2/EG	20.12.2001	Nur kommerzielle Organisationen
Färöer	2010/146/EU	05.03.2010	-
Guernsey	2003/821/EG	21.11.2003	-
Israel	2011/61/EU	31.01.2011	-
Isle of Man	2004/411/EG	28.04.2004	-
Japan	2019/419	23.01.2019	-
Jersey	2008/393/EG	08.05.2008	-
Neuseeland	2013/65/EU	19.12.2012	-
Republik Korea	2021/2216	17.12.2021	-
Schweiz	2000/518/EG	26.07.2000	-
Vereinigtes Königreich	2021/1772	28.06.2021	Post-Brexit
Uruguay	2012/484/EU	21.08.2012	-

USA - EU-U.S. Data Privacy Framework: - **Status:** [TODO: Aktuellen Status prüfen] - **Zertifizierung erforderlich:** Ja - **Prüfung:** [TODO: Liste zertifizierter Unternehmen prüfen]

27.4.2 Übermittlungen auf Basis Angemessenheitsbeschluss

Empfänger	Land	Angemessenheitsbeschluss	Zusätzliche Prüfungen
[TODO: Name]	[TODO: Land]	[TODO: Beschluss]	[TODO: z.B. Privacy Shield Zertifizierung]

Dokumentation: [TODO: Verweis auf Nachweise]

27.5 Geeignete Garantien (Art. 46)

Ohne Angemessenheitsbeschluss ist eine Übermittlung nur zulässig, wenn geeignete Garantien vorgesehen wurden und durchsetzbare Rechte und wirksame Rechtsbehelfe für betroffene Personen verfügbar sind.

27.5.1 Standardvertragsklauseln (Art. 46 Abs. 2 lit. c)

Verfügbare Standardvertragsklauseln (SCC):

27.5.1.1 Neue SCCs (2021)

- **Modul 1:** Controller zu Controller
- **Modul 2:** Controller zu Processor
- **Modul 3:** Processor zu Processor
- **Modul 4:** Processor zu Controller

Verwendete SCCs:

Übermittlung	Modul	Datum Abschluss	Vertragspartner	Dokumentation
[TODO: Beschreibung]	[TODO: Modul]	[TODO: Datum]	[TODO: Name]	[TODO: Link]

Pflichtinhalte der SCCs: - Beschreibung der Übermittlung - Liste der Sub-Prozessoren (bei Modul 2/3) - Technische und organisatorische Maßnahmen - Docking-Klausel (optional)

27.5.2 Binding Corporate Rules (Art. 46 Abs. 2 lit. b)

Status: [TODO: BCRs vorhanden? Ja/Nein]

Falls Ja: - **Genehmigungsdatum:** [TODO: Datum] - **Genehmigende Aufsichtsbehörde:** [TODO: Behörde] - **Geltungsbereich:** [TODO: Konzerngesellschaften] - **Dokumentation:** [TODO: Link zu BCRs]

27.5.3 Verhaltensregeln und Zertifizierung (Art. 46 Abs. 2 lit. e, f)

Verhaltensregeln mit Durchsetzungsmechanismus: - **Status:** [TODO: Vorhanden? Ja/Nein] - **Verhaltensregel:** [TODO: Name]

Zertifizierung mit Durchsetzungsmechanismus: - **Status:** [TODO: Vorhanden? Ja/Nein] - **Zertifizierung:** [TODO: Name]

27.5.4 Weitere Garantien (Art. 46 Abs. 3)

Ad-hoc-Vertragsklauseln (mit Genehmigung der Aufsichtsbehörde): - **Status:** [TODO: Vorhanden? Ja/Nein] - **Genehmigungsdatum:** [TODO: Datum]

27.6 Transfer Impact Assessment (TIA)

27.6.1 Erforderlichkeit

Nach dem Schrems-II-Urteil (EuGH C-311/18) muss der Verantwortliche prüfen, ob das Schutzniveau im Drittland dem der EU gleichwertig ist.

TIA erforderlich für: - Alle Übermittlungen auf Basis von Art. 46 (Garantien) - Insbesondere bei Übermittlungen in die USA und andere Länder mit Zugriffsmöglichkeiten durch Behörden

27.6.2 TIA-Prozess

27.6.2.1 Schritt 1: Datenübermittlung kartieren

- Welche Daten werden übermittelt?

- An wen werden Daten übermittelt?
- In welches Land werden Daten übermittelt?
- Welche Rechtsgrundlage wird verwendet?

27.6.2.2 Schritt 2: Rechtslage im Drittland prüfen

Zu prüfen: - Datenschutzgesetze im Drittland - Zugriffsmöglichkeiten von Behörden (z.B. FISA 702, EO 12333) - Rechtsschutzmöglichkeiten für Betroffene - Praktische Durchsetzbarkeit von Rechten

Dokumentation: [TODO: Zusammenfassung der Rechtslage im Zielland]

27.6.2.3 Schritt 3: Zusätzliche Maßnahmen bewerten

Technische Maßnahmen: - End-to-End-Verschlüsselung - Pseudonymisierung - Anonymisierung - Verschlüsselung im Transit und at Rest

Organisatorische Maßnahmen: - Vertragliche Verpflichtungen - Transparenz gegenüber Betroffenen - Schulung des Empfängers - Audits und Kontrollen

Rechtliche Maßnahmen: - Widerspruch gegen Behördenanfragen - Benachrichtigung bei Behördenanfragen - Transparenzberichte

27.6.2.4 Schritt 4: Entscheidung

Ist ein angemessenes Schutzniveau gewährleistet? [TODO: Ja / Nein]

Falls Nein: - Übermittlung einstellen - Alternative Lösungen suchen (z.B. EU-Anbieter) - Ausnahme gemäß Art. 49 prüfen

27.6.3 TIA-Dokumentation

Übermittlung	TIA durchgeführt	Datum	Ergebnis	Zusätzliche Maßnahmen	Nächste Überprüfung
[TODO]	Ja/Nein	[TODO]	Angemessen/Nicht angemessen	[TODO]	[TODO]

27.7 Ausnahmen (Art. 49)

Ohne Angemessenheitsbeschluss oder geeignete Garantien ist eine Übermittlung nur in Ausnahmefällen zulässig.

27.7.1 Ausnahmetatbestände (Art. 49 Abs. 1)

27.7.1.1 a) Einwilligung

Voraussetzungen: - Betroffene Person wurde über mögliche Risiken informiert - Einwilligung ist freiwillig, spezifisch, informiert und unmissverständlich

Verwendung: [TODO: Ja/Nein - falls Ja, dokumentiere Einwilligungen]

27.7.1.2 b) Vertragserfüllung

Voraussetzungen: - Übermittlung ist für Erfüllung eines Vertrags erforderlich - Oder für vorvertragliche Maßnahmen auf Anfrage der betroffenen Person

Verwendung: [TODO: Ja/Nein - falls Ja, dokumentiere Fälle]

27.7.1.3 c) Öffentliches Interesse

Voraussetzungen: - Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses erforderlich

Verwendung: [TODO: Ja/Nein - falls Ja, dokumentiere Fälle]

27.7.1.4 d) Rechtliche Ansprüche

Voraussetzungen: - Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich

Verwendung: [TODO: Ja/Nein - falls Ja, dokumentiere Fälle]

27.7.1.5 e) Lebenswichtige Interessen

Voraussetzungen: - Übermittlung ist zum Schutz lebenswichtiger Interessen erforderlich - Betroffene Person ist außerstande, ihre Einwilligung zu geben

Verwendung: [TODO: Ja/Nein - falls Ja, dokumentiere Fälle]

27.7.1.6 f) Öffentliches Register

Voraussetzungen: - Übermittlung erfolgt aus einem Register, das zur Information der Öffentlichkeit bestimmt ist

Verwendung: [TODO: Ja/Nein - falls Ja, dokumentiere Fälle]

27.7.2 Ausnahme für gelegentliche Übermittlungen (Art. 49 Abs. 1 UAbs. 2)

Voraussetzungen: - Übermittlung ist nicht wiederholt - Betrifft nur begrenzte Zahl von Personen - Ist für zwingende berechtigte Interessen erforderlich - Interessen überwiegen Interessen der betroffenen Person - Verantwortlicher hat alle Umstände bewertet - Geeignete Garantien wurden vorgesehen

Verwendung: [TODO: Ja/Nein - falls Ja, dokumentiere Fälle]

Dokumentationspflicht: Übermittlung muss der Aufsichtsbehörde mitgeteilt werden

27.8 Informationspflichten

27.8.1 Information der Betroffenen

Betroffene Personen müssen über Drittlandübermittlungen informiert werden: - In der Datenschutzerklärung (Art. 13, 14) - Bei Auskunftsanfragen (Art. 15)

Zu informieren über: - Empfänger oder Kategorien von Empfängern in Drittländern - Drittland - Rechtsgrundlage der Übermittlung - Geeignete Garantien (mit Verweis auf Kopie oder Fundstelle) - Bei Ausnahmen: Zwingende berechtigte Interessen

27.8.2 Transparenz

Veröffentlichung: - Liste der Drittlandübermittlungen auf Website - Informationen zu verwendeten Garantien - Kontakt für Rückfragen

27.9 Überwachung und Überprüfung

27.9.1 Regelmäßige Überprüfung

Überprüfungsfrequenz: [TODO: z.B. jährlich]

Zu prüfen: - Sind alle Drittlandübermittlungen erfasst? - Sind die Rechtsgrundlagen noch aktuell? - Sind die Garantien noch wirksam? - Haben sich die Rechtslage oder Risiken geändert? - Sind TIAs aktuell?

27.9.2 Änderungsmanagement

Auslöser für Überprüfung: - Neue Drittlandübermittlung - Änderung der Rechtslage im Drittland - Neue Gerichtsurteile (z.B. EuGH) - Widerruf von Angemessenheitsbeschlüssen - Sicherheitsvorfälle

27.10 Verantwortlichkeiten

Aufgabe	Verantwortlich	Rechenschaftspflichtig	Konsultiert	Informiert
Identifikation Drittlandübermittlungen	[TODO]	[TODO]	[TODO]	[TODO]
TIA-Durchführung	[TODO]	[TODO]	[TODO]	[TODO]
SCC-Abschluss	[TODO]	[TODO]	[TODO]	[TODO]
Überwachung	[TODO]	[TODO]	[TODO]	[TODO]

27.11 Verknüpfung zu anderen Dokumenten

- **Verzeichnis der Verarbeitungstätigkeiten (Art. 30):** Dokumentation der Übermittlungen
- **Datenschutz-Folgenabschätzung (Art. 35):** TIA als Teil der DSFA
- **Auftragsverarbeitung (Art. 28):** SCCs bei Auftragsverarbeitern in Drittländern
- **Informationspflichten (Art. 13-14):** Transparenz gegenüber Betroffenen

---

Nächste Schritte: 1. Identifizieren Sie alle Drittlandübermittlungen 2. Prüfen Sie Angemessenheitsbeschlüsse 3. Implementieren Sie geeignete Garantien (SCCs, BCRs) 4. Führen Sie Transfer Impact Assessments durch 5. Informieren Sie betroffene Personen transparent

ewpage

Chapter 28

Standardvertragsklauseln (SCC)

Dokument-ID: 0510
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

28.1 Zweck

Dieses Dokument beschreibt die Verwendung von Standardvertragsklauseln (Standard Contractual Clauses, SCC) bei {{ meta.organization }} für die Übermittlung personenbezogener Daten in Drittländer gemäß Art. 46 Abs. 2 lit. c DSGVO.

28.2 Neue Standardvertragsklauseln (2021)

28.2.1 Durchführungsbeschluss (EU) 2021/914

Verabschiedung: 4. Juni 2021
Anwendbar ab: 27. Juni 2021
Übergangszeit für alte SCCs: Bis 27. Dezember 2022

Vorteile der neuen SCCs: - Modularer Aufbau für verschiedene Übermittlungsszenarien - Berücksichtigung des Schrems-II-Urteils - Flexibilität bei komplexen Verarbeitungsketten - Docking-Klausel für weitere Parteien

28.3 SCC-Module

28.3.1 Modul 1: Controller zu Controller

Anwendungsfall: Verantwortlicher in der EU übermittelt Daten an Verantwortlichen im Drittland

Beispiele: - Übermittlung von Kundendaten an ausländischen Geschäftspartner - Datenaustausch zwischen Konzerngesellschaften (beide als Verantwortliche) - Übermittlung an ausländische Behörden (soweit zulässig)

Verwendung bei {{ meta.organization }}:

Übermittlung	Empfänger	Land	Datum Abschluss	Dokumentation
[TODO: Beschreibung]	[TODO: Name]	[TODO: Land]	[TODO: Datum]	[TODO: Link]

28.3.2 Modul 2: Controller zu Processor

Anwendungsfall: Verantwortlicher in der EU beauftragt Auftragsverarbeiter im Drittland

Beispiele: - Cloud-Hosting außerhalb EU/EWR - Outsourcing von IT-Services - Call-Center in Drittländern - Lohnabrechnung durch ausländischen Dienstleister

Verwendung bei {{ meta.organization }}:

Auftragsverarbeiter	Dienstleistung	Land	Datum Abschluss	Dokumentation
[TODO: Name]	[TODO: Service]	[TODO: Land]	[TODO: Datum]	[TODO: Link]

28.3.3 Modul 3: Processor zu Processor

Anwendungsfall: Auftragsverarbeiter beauftragt Sub-Auftragsverarbeiter im Drittland

Beispiele: - Cloud-Provider nutzt Sub-Hosting-Provider - IT-Dienstleister lagert Teile an Sub-Dienstleister aus

Verwendung bei {{ meta.organization }}:

Hauptauftragsverarbeiter	Sub-Auftragsverarbeiter	Land	Datum Abschluss	Dokumentation
[TODO: Name]	[TODO: Name]	[TODO: Land]	[TODO: Datum]	[TODO: Link]

28.3.4 Modul 4: Processor zu Controller

Anwendungsfall: Auftragsverarbeiter übermittelt Daten an Verantwortlichen im Drittland

Beispiele: - Auftragsverarbeiter übermittelt Daten an Konzernmutter im Drittland - Rückübermittlung von Daten nach Vertragsende

Verwendung bei {{ meta.organization }}:

Auftragsverarbeiter	Empfänger	Land	Datum Abschluss	Dokumentation
[TODO: Name]	[TODO: Name]	[TODO: Land]	[TODO: Datum]	[TODO: Link]

28.4 Pflichtanhänge der SCCs

28.4.1 Anhang I: Parteien und Datenübermittlung

28.4.1.1 Teil A: Liste der Parteien

Datenexporteur (EU): - Name: [TODO: {{ meta.organization }}] - Adresse: [TODO: Adresse] - Kontakt: [TODO: Name, E-Mail, Telefon] - Rolle: Verantwortlicher / Auftragsverarbeiter - Unterschrift: _____

Datenimporteur (Drittland): - Name: [TODO: Name des Empfängers] - Adresse: [TODO: Adresse] - Kontakt: [TODO: Name, E-Mail, Telefon] - Rolle: Verantwortlicher / Auftragsverarbeiter - Unterschrift: _____

28.4.1.2 Teil B: Beschreibung der Übermittlung

Kategorien betroffener Personen: - [TODO: z.B. Kunden, Mitarbeiter, Lieferanten]

Kategorien personenbezogener Daten: - [TODO: z.B. Stammdaten, Kontaktdaten, Vertragsdaten] - **Besondere Kategorien (Art. 9):** [TODO: falls zutreffend]

Sensible Daten (falls zutreffend): - [TODO: Beschreibung]

Häufigkeit der Übermittlung: - [TODO: z.B. kontinuierlich, monatlich, bei Bedarf]

Art der Übermittlung: - [TODO: z.B. E-Mail, API, Cloud-Speicher]

Zweck(e) der Datenübermittlung: - [TODO: z.B. Vertragserfüllung, IT-Services]

Speicherdauer beim Importeur: - [TODO: z.B. Vertragslaufzeit + 3 Jahre]

Für Übermittlungen an Sub-Prozessoren: - [TODO: Beschreibung der Verarbeitung durch Sub-Prozessoren]

28.4.1.3 Teil C: Zuständige Aufsichtsbehörde

Aufsichtsbehörde des Exporteurs: - Name: [TODO: z.B. Landesbeauftragter für Datenschutz] - Adresse: [TODO: Adresse] - E-Mail: [TODO: E-Mail] - Website: [TODO: URL]

28.4.2 Anhang II: Technische und organisatorische Maßnahmen (TOM)

Beschreibung der technischen und organisatorischen Maßnahmen des Datenimporteurs:

28.4.2.1 1. Zugangskontrollen

Physische Zugangskontrollen: - [TODO: z.B. Zutrittskontrollsystem, Besuchermanagement]

Logische Zugangskontrollen: - [TODO: z.B. Benutzerauthentifizierung, Multi-Faktor-Authentifizierung]

28.4.2.2 2. Zugriffskontrollen

Berechtigungskonzept: - [TODO: z.B. Rollenbasierte Zugriffskontrolle (RBAC)]

Least Privilege Prinzip: - [TODO: Beschreibung]

28.4.2.3 3. Verschlüsselung

Verschlüsselung im Transit: - [TODO: z.B. TLS 1.3]

Verschlüsselung at Rest: - [TODO: z.B. AES-256]

Schlüsselverwaltung: - [TODO: Beschreibung]

28.4.2.4 4. Pseudonymisierung

Verfahren: - [TODO: Beschreibung, falls anwendbar]

28.4.2.5 5. Logging und Monitoring

Protokollierung: - [TODO: z.B. Zugriffsprotokolle, Änderungsprotokolle]

Aufbewahrungsdauer Logs: - [TODO: z.B. 90 Tage]

Monitoring: - [TODO: z.B. SIEM, Intrusion Detection]

28.4.2.6 6. Incident Response

Incident-Response-Plan: - [TODO: Verweis auf Dokument]

Meldepflicht: - [TODO: Unverzügliche Meldung an Exporteur]

28.4.2.7 7. Backup und Recovery

Backup-Strategie: - [TODO: z.B. tägliche Backups, 30 Tage Aufbewahrung]

Recovery Time Objective (RTO): - [TODO: z.B. 24 Stunden]

Recovery Point Objective (RPO): - [TODO: z.B. 1 Stunde]

28.4.2.8 8. Datenlöschung

Löschverfahren: - [TODO: z.B. sichere Löschung nach NIST 800-88]

Löschnachweis: - [TODO: Beschreibung]

28.4.2.9 9. Schulung und Sensibilisierung

Schulungsprogramm: - [TODO: z.B. jährliche Datenschutzschulungen]

Vertraulichkeitsverpflichtung: - [TODO: Alle Mitarbeiter verpflichtet]

28.4.2.10 10. Audits und Zertifizierungen

Interne Audits: - [TODO: z.B. jährlich]

Externe Audits: - [TODO: z.B. ISO 27001, SOC 2]

Zertifizierungen: - [TODO: Liste der Zertifizierungen]

28.4.3 Anhang III: Liste der Sub-Prozessoren (nur Modul 2 und 3)

Genehmigungsverfahren: [ ] Allgemeine Genehmigung [ ] Spezifische Genehmigung

Liste der genehmigten Sub-Prozessoren:

Name	Adresse	Land	Verarbeitungstätigkeit	Garantien
[TODO]	[TODO]	[TODO]	[TODO]	[TODO: z.B. SCCs]

Informationspflicht bei Änderungen: - Frist für Widerspruch: [TODO: z.B. 30 Tage] - Benachrichtigungsmethode: [TODO: z.B. E-Mail]

28.5 Optionale Klauseln

28.5.1 Docking-Klausel (Klausel 7)

Aktiviert: [TODO: Ja/Nein]

Zweck: Ermöglicht weiteren Parteien, den SCCs beizutreten

Beigetretene Parteien:

Name	Rolle	Beitrittsdatum	Dokumentation
[TODO]	[TODO]	[TODO]	[TODO]

28.5.2 Lokale Gesetze und Praktiken (Klausel 14)

Verpflichtung des Importeurs: - Benachrichtigung bei Anfragen von Behörden - Widerspruch gegen unverhältnismäßige Anfragen - Jährliche Überprüfung der Rechtslage

Dokumentation von Behördenanfragen:

Datum	Behörde	Art der Anfrage	Maßnahmen	Benachrichtigung Exporteur
[TODO]	[TODO]	[TODO]	[TODO]	[TODO: Datum]

28.6 Transfer Impact Assessment (TIA)

28.6.1 Erforderlichkeit

Gemäß Schrems-II-Urteil muss zusätzlich zu den SCCs ein TIA durchgeführt werden.

TIA durchgeführt: [TODO: Ja/Nein]
Datum: [TODO: Datum]
Ergebnis: [TODO: Angemessenes Schutzniveau gewährleistet Ja/Nein]

28.6.2 Zusätzliche Maßnahmen

Technische Maßnahmen: - [TODO: z.B. End-to-End-Verschlüsselung] - [TODO: z.B. Pseudonymisierung]

Organisatorische Maßnahmen: - [TODO: z.B. Vertragliche Verpflichtungen] - [TODO: z.B. Transparenzberichte]

Rechtliche Maßnahmen: - [TODO: z.B. Widerspruch gegen Behördenanfragen]

Dokumentation: [TODO: Verweis auf TIA-Bericht]

28.7 Vertragsmanagement

28.7.1 Abschlussprozess

1. **Auswahl des Moduls:** Passende SCC-Vorlage wählen
2. **Ausfüllen der Anhänge:** Alle Pflichtanhänge vollständig ausfüllen
3. **TIA durchführen:** Transfer Impact Assessment
4. **Zusätzliche Maßnahmen:** Falls erforderlich implementieren
5. **Datenschutzbeauftragten konsultieren:** Stellungnahme einholen
6. **Vertragsunterzeichnung:** Beide Parteien unterzeichnen
7. **Dokumentation:** Vertrag ablegen und registrieren

28.7.2 Überwachung

Überprüfungsfrequenz: [TODO: z.B. jährlich]

Zu prüfen: - Einhaltung der SCCs durch Importeur - Aktualität der TOM - Änderungen der Rechtslage im Drittland - Sub-Prozessoren-Liste aktuell - Behördenanfragen dokumentiert

Audit-Rechte: - Recht auf Audits vor Ort - Recht auf Dokumentenprüfung - Recht auf Zertifikatsprüfung

28.7.3 Vertragsende

Bei Vertragsende: - Rückgabe oder Löschung der Daten - Löschnachweis einholen - Dokumentation abschließen

28.8 Verantwortlichkeiten

Aufgabe	Verantwortlich	Rechenschaftspflichtig	Konsultiert	Informiert
Modulauswahl	[TODO]	[TODO]	[TODO]	[TODO]
Anhänge ausfüllen	[TODO]	[TODO]	[TODO]	[TODO]

Aufgabe	Verantwortlich	Rechenschaftspflichtig	Konsultiert	Informiert
TIA durchführen	[TODO]	[TODO]	[TODO]	[TODO]
Vertragsabschluss	[TODO]	[TODO]	[TODO]	[TODO]
Überwachung	[TODO]	[TODO]	[TODO]	[TODO]

28.9 Verknüpfung zu anderen Dokumenten

- **Datenübermittlung Drittländer (Art. 44-50):** Übergeordnetes Dokument
- **Auftragsverarbeitung (Art. 28):** Bei Modul 2 und 3
- **TOM-Dokumentation (Art. 32):** Detaillierte Sicherheitsmaßnahmen
- **Transfer Impact Assessment:** Risikobewertung

Nächste Schritte: 1. Identifizieren Sie alle Drittlandübermittlungen, die SCCs erfordern 2. Wählen Sie das passende SCC-Modul 3. Füllen Sie alle Anhänge vollständig aus 4. Führen Sie ein Transfer Impact Assessment durch 5. Schließen Sie die SCCs mit allen Datenimporteuren ab

ewpage

Chapter 29

Datenschutzverletzung Response Plan (Template)

Dokument-ID: 0600
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Entwurf
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

29.1 Zweck

Dieser Response Plan definiert die Schritte zur Bewältigung von Datenschutzverletzungen bei {{ meta.organization }}. Er stellt sicher, dass Datenschutzverletzungen schnell erkannt, bewertet und gemäß DSGVO Art. 33-34 behandelt werden.

29.2 Geltungsbereich

Dieser Plan gilt für alle Datenschutzverletzungen, die personenbezogene Daten betreffen, die von {{ meta.organization }} verarbeitet werden.

29.3 Breach Response Team

29.3.1 Kernteam

Rolle	Name	Kontakt	Verantwortlichkeiten
Incident Commander	[TODO]	[TODO: Telefon, E-Mail]	Gesamtverantwortung, Entscheidungen
Datenschutzbeauftragter	[TODO]	[TODO: Telefon, E-Mail]	Rechtliche Bewertung, Meldepflicht

Rolle	Name	Kontakt	Verantwortlichkeiten
IT-Security Lead	[TODO]	[TODO: Telefon, E-Mail]	Technische Analyse, Eindämmung
Legal Counsel	[TODO]	[TODO: Telefon, E-Mail]	Rechtliche Beratung
Communications Lead	[TODO]	[TODO: Telefon, E-Mail]	Interne/externe Kommunikation

29.3.2 Erweiterte Stakeholder

Rolle	Name	Kontakt	Wann einbeziehen
Geschäftsführung	[TODO]	[TODO]	Bei hohem Risiko
HR	[TODO]	[TODO]	Bei Mitarbeiterdaten
Compliance	[TODO]	[TODO]	Bei regulatorischen Fragen
PR/Marketing	[TODO]	[TODO]	Bei öffentlicher Kommunikation

29.4 Breach Response Prozess

29.4.1 Phase 1: Erkennung und Meldung (0-2 Stunden)

29.4.1.1 1.1 Breach erkennen

Erkennungsquellen: - Monitoring-Systeme und Alerts - Mitarbeiter-Meldungen - Externe Meldungen (Kunden, Partner) - Audit-Findings - Medienberichte

29.4.1.2 1.2 Initiale Meldung

Wer meldet: - Jeder Mitarbeiter, der eine potenzielle Datenschutzverletzung entdeckt

An wen: - IT-Security: [TODO: E-Mail/Telefon] - Datenschutzbeauftragter: [TODO: E-Mail/Telefon]

Meldeformular:

```
INITIALE BREACH-MELDUNG

Melder: [Name, Abteilung, Kontakt]
Datum/Uhrzeit Entdeckung: [YYYY-MM-DD HH:MM]
Entdeckungsart: [Monitoring / Mitarbeiter / Extern / Audit / Sonstiges]

Kurzbeschreibung:
[Was ist passiert?]

Betroffene Systeme:
[Welche Systeme sind betroffen?]

Betroffene Daten (erste Einschätzung):
[Welche Art von Daten?]
```

```
Anzahl betroffener Personen (Schätzung):
[Ungefähre Anzahl]

Sofortmaßnahmen ergriffen:
[Was wurde bereits getan?]
```

29.4.1.3 1.3 Breach Response Team aktivieren

Incident Commander: - Aktiviert Kernteam - Setzt initiales Meeting an (innerhalb 2 Stunden) - Erstellt Breach-ID: `BREACH-[YYYY]-[NNN]`

29.4.2 Phase 2: Bewertung und Eindämmung (2-12 Stunden)

29.4.2.1 2.1 Initiale Bewertung

Checkliste: - [ ] Liegt tatsächlich eine Datenschutzverletzung vor? - [ ] Welche Kategorie: Vertraulichkeit / Integrität / Verfügbarkeit? - [ ] Welche Daten sind betroffen? - [ ] Wie viele Personen sind betroffen? - [ ] Sind besondere Kategorien (Art. 9) betroffen? - [ ] Wie ist die Verletzung entstanden? - [ ] Ist die Verletzung noch aktiv?

Dokumentation: - Alle Erkenntnisse im Breach-Register dokumentieren - Screenshots und Logs sichern - Forensische Sicherung bei Bedarf

29.4.2.2 2.2 Sofortige Eindämmung

Technische Maßnahmen: - [ ] Betroffene Systeme isolieren - [ ] Zugriffe sperren - [ ] Passwörter zurücksetzen - [ ] Sicherheitslücken schließen - [ ] Weitere Datenverluste verhindern

Verantwortlich: IT-Security Lead

Zeitrahmen: Innerhalb 4 Stunden

29.4.2.3 2.3 Umfangsermittlung

Zu klären: - Genaue Anzahl betroffener Personen - Genaue Datenkategorien - Zeitraum der Verletzung - Ursache der Verletzung - Potenzielle Auswirkungen

Methoden: - Log-Analyse - Datenbank-Abfragen - System-Forensik - Interviews mit Beteiligten

29.4.3 Phase 3: Risikobewertung (12-24 Stunden)

29.4.3.1 3.1 Risiko für Betroffene bewerten

Bewertungskriterien:

Kriterium	Bewertung	Punkte
Art der Daten		
- Allgemeine Kontaktdaten	Niedrig	1
- Finanzdaten, Zugangsdaten	Mittel	2
- Besondere Kategorien (Art. 9)	Hoch	3
Anzahl Betroffene		

Kriterium	Bewertung	Punkte
- < 100 Personen	Niedrig	1
- 100-1.000 Personen	Mittel	2
- > 1.000 Personen	Hoch	3
Schutzmaßnahmen		
- Verschlüsselt, pseudonymisiert	Niedrig	1
- Teilweise geschützt	Mittel	2
- Unverschlüsselt, Klartext	Hoch	3
Betroffene Personen		
- Mitarbeiter (intern)	Niedrig	1
- Kunden, Partner	Mittel	2
- Kinder, vulnerable Gruppen	Hoch	3

Gesamtrisiko: - 4-6 Punkte: Niedriges Risiko - 7-9 Punkte: Mittleres Risiko (Meldepflicht) - 10-12 Punkte: Hohes Risiko (Meldepflicht + Benachrichtigung)

29.4.3.2 3.2 Meldepflicht prüfen

Entscheidungsbaum:

```
Datenschutzverletzung bestätigt?
  Nein → Dokumentieren, kein weiterer Handlungsbedarf
  Ja → Risiko für Rechte und Freiheiten?
      Nein (< 7 Punkte) → Nur dokumentieren
      Ja (  7 Punkte) → Meldung an Aufsichtsbehörde erforderlich
          Hohes Risiko (  10 Punkte)?
              Nein → Nur Meldung
              Ja → Meldung + Benachrichtigung Betroffener
```

Verantwortlich: Datenschutzbeauftragter

29.4.4 Phase 4: Meldung und Benachrichtigung (24-72 Stunden)

29.4.4.1 4.1 Meldung an Aufsichtsbehörde (falls erforderlich)

Frist: 72 Stunden ab Kenntnisnahme

Zuständige Behörde: - Name: [TODO: z.B. Landesbeauftragte für Datenschutz] - Melde-Portal: [TODO: URL] - Kontakt: [TODO: E-Mail, Telefon]

Meldung vorbereiten: - Verwende Template 0610 (Breach Notification Template) - Stelle alle erforderlichen Informationen zusammen - Lasse durch Datenschutzbeauftragten prüfen - Hole Freigabe von Geschäftsführung

Verantwortlich: Datenschutzbeauftragter

29.4.4.2 4.2 Benachrichtigung Betroffener (falls erforderlich)

Voraussetzung: Hohes Risiko (10 Punkte)

Ausnahmen (keine Benachrichtigung): - Daten waren verschlüsselt/pseudonymisiert - Nachträgliche Maßnahmen beseitigen hohes Risiko - Unverhältnismäßiger Aufwand (dann öffentliche Bekanntmachung)

Benachrichtigung vorbereiten: - Verwende Template 0620 (Breach Communication Template) - Klare, verständliche Sprache - Konkrete Handlungsempfehlungen - Kontaktmöglichkeiten

Kommunikationskanäle: - E-Mail (bevorzugt) - Brief (bei fehlender E-Mail) - Öffentliche Bekanntmachung (bei unverhältnismäßigem Aufwand)

Verantwortlich: Communications Lead, Datenschutzbeauftragter

29.4.4.3 4.3 Interne Kommunikation

Zu informieren: - Geschäftsführung - Betroffene Abteilungen - Betriebsrat (bei Mitarbeiterdaten) - Alle Mitarbeiter (bei Bedarf)

Kommunikationsplan: - Initiale Information: Innerhalb 24 Stunden - Regelmäßige Updates: Täglich während aktiver Phase - Abschlussbericht: Nach Incident-Closure

29.4.5 Phase 5: Wiederherstellung (72 Stunden - Wochen)

29.4.5.1 5.1 Systeme wiederherstellen

Checkliste: - [ ] Sicherheitslücken geschlossen - [ ] Systeme gepatcht/aktualisiert - [ ] Zugriffskontrollen überprüft - [ ] Monitoring verstärkt - [ ] Backup-Strategie überprüft

Verantwortlich: IT-Security Lead

29.4.5.2 5.2 Präventive Maßnahmen

Zu implementieren: - Technische Verbesserungen - Prozessanpassungen - Schulungen - Verstärktes Monitoring

29.4.6 Phase 6: Nachbereitung (Nach Abschluss)

29.4.6.1 6.1 Post-Breach Review

Verwende Template 0640 (Post-Breach Review Template)

Durchzuführen innerhalb: 2 Wochen nach Incident-Closure

Teilnehmer: - Breach Response Team - Betroffene Abteilungen - Geschäftsführung

Themen: - Was lief gut? - Was lief schlecht? - Lessons Learned - Verbesserungsmaßnahmen

29.4.6.2 6.2 Dokumentation abschließen

Checkliste: - [ ] Breach-Register aktualisiert - [ ] Alle Meldungen archiviert - [ ] Timeline dokumentiert - [ ] Kosten erfasst - [ ] Maßnahmen dokumentiert

Aufbewahrungsfrist: Mindestens 3 Jahre

29.5 Kommunikationsrichtlinien

29.5.1 Interne Kommunikation

Grundsätze: - Transparent, aber vertraulich - Faktenbasiert - Regelmäßige Updates - Klare Verantwortlichkeiten

29.5.2 Externe Kommunikation

Grundsätze: - Nur durch autorisierte Sprecher - Abgestimmt mit Legal und Datenschutzbeauftragtem - Keine Spekulationen - Fokus auf Maßnahmen und Unterstützung

Medienanfragen: - Alle Anfragen an Communications Lead - Keine spontanen Statements - Vorbereitung von Q&A

29.6 Eskalation

29.6.1 Eskalationsstufen

Stufe 1: Routine - Niedriges Risiko - $<$ 100 Betroffene - Keine besonderen Kategorien - Kernteam ausreichend

Stufe 2: Erhöht - Mittleres Risiko - 100-1.000 Betroffene - Meldepflicht - Geschäftsführung informieren

Stufe 3: Kritisch - Hohes Risiko - $>$ 1.000 Betroffene - Besondere Kategorien - Benachrichtigungspflicht - Geschäftsführung aktiv einbinden - Externe Berater erwägen

Stufe 4: Krise - Sehr hohes Risiko - Massive Auswirkungen - Öffentliches Interesse - Krisenmanagement aktivieren - Externe PR-Unterstützung - Aufsichtsrat informieren

29.7 Kontakte und Ressourcen

29.7.1 Interne Kontakte

Rolle	Name	Telefon	E-Mail	Verfügbarkeit
Incident Commander	[TODO]	[TODO]	[TODO]	24/7
Datenschutzbeauftragter	[TODO]	[TODO]	[TODO]	24/7
IT-Security Lead	[TODO]	[TODO]	[TODO]	24/7
Legal Counsel	[TODO]	[TODO]	[TODO]	Werktags
Communications Lead	[TODO]	[TODO]	[TODO]	Werktags

29.7.2 Externe Kontakte

Organisation	Kontakt	Telefon	E-Mail	Zweck
Aufsichtsbehörde	[TODO]	[TODO]	[TODO]	Meldung
Forensik-Dienstleister	[TODO]	[TODO]	[TODO]	Analyse
Rechtsanwalt (extern)	[TODO]	[TODO]	[TODO]	Beratung
PR-Agentur	[TODO]	[TODO]	[TODO]	Krisenkommunikation

Organisation	Kontakt	Telefon	E-Mail	Zweck
Cyber-Versicherung	[TODO]	[TODO]	[TODO]	Schadensmeldung

29.7.3 Tools und Systeme

Tool	Zweck	Zugriff
[TODO: SIEM]	Monitoring, Log-Analyse	[TODO: URL]
[TODO: Ticketsystem]	Incident-Tracking	[TODO: URL]
[TODO: Breach-Register]	Dokumentation	[TODO: URL/Datei]
[TODO: Kommunikationsplattform]	Team-Koordination	[TODO: URL]

29.8 Anhänge

- **Template 0610:** Breach Notification Template (Aufsichtsbehörde)
- **Template 0620:** Breach Communication Template (Betroffene)
- **Template 0630:** Breach Register Template
- **Template 0640:** Post-Breach Review Template

Nächste Schritte: 1. Passe diesen Plan an deine Organisation an 2. Definiere alle Rollen und Kontakte 3. Führe Breach-Response-Übungen durch (mindestens jährlich) 4. Halte den Plan aktuell 5. Stelle sicher, dass alle Teammitglieder den Plan kennen

ewpage

Chapter 30

Breach Notification Template (Aufsichtsbehörde)

Dokument-ID: 0610
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

30.1 Meldung einer Datenschutzverletzung gemäß Art. 33 DS-GVO

An: [TODO: Name der zuständigen Aufsichtsbehörde]
Datum: [TODO: YYYY-MM-DD]
Breach-ID: [TODO: BREACH-YYYY-NNN]

30.1.1 1. Verantwortlicher

Organisation: {{ meta.organization }}
Adresse: [TODO: Vollständige Adresse]
Kontaktperson: [TODO: Name, Funktion]
Telefon: [TODO: Telefonnummer]
E-Mail: [TODO: E-Mail-Adresse]

30.1.2 2. Datenschutzbeauftragter

Name: [TODO: Name des Datenschutzbeauftragten]
Telefon: [TODO: Telefonnummer]
E-Mail: [TODO: E-Mail-Adresse]

30.2 A. Art der Verletzung (Art. 33 Abs. 3 lit. a)

30.2.1 Beschreibung der Datenschutzverletzung

Datum und Uhrzeit der Verletzung:
[TODO: YYYY-MM-DD HH:MM - YYYY-MM-DD HH:MM]

Datum und Uhrzeit der Kenntnisnahme:
[TODO: YYYY-MM-DD HH:MM]

Art der Verletzung:
[ ] Vertraulichkeitsverletzung (unbefugte Offenlegung oder Zugang)
[ ] Integritätsverletzung (unbefugte Veränderung)
[ ] Verfügbarkeitsverletzung (Verlust oder Vernichtung)

Detaillierte Beschreibung:
[TODO: Beschreibe ausführlich, was passiert ist, wie die Verletzung entstanden ist, welche Systeme betroffen sind]

Beispiel:

```
Am [Datum] um [Uhrzeit] wurde festgestellt, dass durch eine Fehlkonfiguration
des Webservers personenbezogene Daten von Kunden über einen Zeitraum von
[Zeitraum] öffentlich zugänglich waren. Die Daten waren über eine nicht
geschützte API-Schnittstelle abrufbar.
```

30.2.2 Kategorien betroffener personenbezogener Daten

Datenkategorie	Beschreibung	Besondere Kategorie (Art. 9)
[TODO: z.B. Stammdaten]	[TODO: Name, Adresse, Geburtsdatum]	[ ] Ja [X] Nein
[TODO: z.B. Kontaktdaten]	[TODO: E-Mail, Telefon]	[ ] Ja [X] Nein
[TODO: z.B. Finanzdaten]	[TODO: Kontonummer, Kreditkarte]	[ ] Ja [X] Nein

Besondere Kategorien personenbezogener Daten betroffen (Art. 9):
[ ] Ja [ ] Nein

Falls Ja, welche:
[ ] Gesundheitsdaten
[ ] Genetische Daten
[ ] Biometrische Daten
[ ] Daten über rassische/ethnische Herkunft
[ ] Politische Meinungen
[ ] Religiöse/weltanschauliche Überzeugungen

[ ] Gewerkschaftszugehörigkeit
[ ] Sexualleben/sexuelle Orientierung

30.2.3 Kategorien betroffener Personen

Anzahl betroffener Personen (ungefähr): [TODO: z.B. 1.234 Personen]

Kategorien:
[ ] Kunden
[ ] Mitarbeiter
[ ] Lieferanten/Partner
[ ] Patienten
[ ] Kinder
[ ] Sonstige: [TODO]

Vulnerable Gruppen betroffen:
[ ] Ja [ ] Nein

Falls Ja, welche: [TODO: z.B. Kinder, Patienten, Behinderte]

30.2.4 Anzahl betroffener Datensätze

Ungefähre Anzahl: [TODO: z.B. 5.000 Datensätze]

30.3 B. Kontaktstelle (Art. 33 Abs. 3 lit. b)

Name und Kontaktdaten des Datenschutzbeauftragten:

Name: [TODO: Name]
Telefon: [TODO: Telefonnummer]
E-Mail: [TODO: E-Mail-Adresse]
Verfügbarkeit: [TODO: z.B. Mo-Fr 9-17 Uhr, Notfall 24/7]

Alternative Anlaufstelle:

Name: [TODO: Name, Funktion]
Telefon: [TODO: Telefonnummer]
E-Mail: [TODO: E-Mail-Adresse]

30.4 C. Wahrscheinliche Folgen (Art. 33 Abs. 3 lit. c)

30.4.1 Beschreibung der wahrscheinlichen Folgen

Für betroffene Personen:

[TODO: Beschreibe die möglichen Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen]

Beispiele: - Identitätsdiebstahl - Finanzieller Schaden - Reputationsschaden - Diskriminierung - Verlust der Vertraulichkeit - Psychische Belastung

Risikobewertung:
[ ] Niedriges Risiko
[ ] Mittleres Risiko
[ ] Hohes Risiko
[ ] Sehr hohes Risiko

Begründung der Risikobewertung:
[TODO: Erläutere, warum das Risiko so eingeschätzt wurde, unter Berücksichtigung von Art der Daten, Anzahl Betroffener, Schutzmaßnahmen, etc.]

30.5 D. Ergriffene Maßnahmen (Art. 33 Abs. 3 lit. d)

30.5.1 Maßnahmen zur Behebung der Datenschutzverletzung

Sofortmaßnahmen (bereits ergriffen):

1. [TODO: z.B. Betroffene Systeme isoliert]
   - Zeitpunkt: [TODO: YYYY-MM-DD HH:MM]
   - Verantwortlich: [TODO: Name/Rolle]
2. [TODO: z.B. Sicherheitslücke geschlossen]
   - Zeitpunkt: [TODO: YYYY-MM-DD HH:MM]
   - Verantwortlich: [TODO: Name/Rolle]
3. [TODO: z.B. Passwörter zurückgesetzt]
   - Zeitpunkt: [TODO: YYYY-MM-DD HH:MM]
   - Verantwortlich: [TODO: Name/Rolle]

30.5.2 Maßnahmen zur Abmilderung der nachteiligen Auswirkungen

Bereits umgesetzt:

1. [TODO: z.B. Betroffene Personen benachrichtigt]
   - Zeitpunkt: [TODO: YYYY-MM-DD]
   - Methode: [TODO: E-Mail/Brief/Telefon]
2. [TODO: z.B. Monitoring verstärkt]
   - Zeitpunkt: [TODO: YYYY-MM-DD]
   - Beschreibung: [TODO]

Geplante Maßnahmen:

1. [TODO: z.B. Implementierung zusätzlicher Sicherheitsmaßnahmen]
   - Geplanter Zeitpunkt: [TODO: YYYY-MM-DD]
   - Verantwortlich: [TODO: Name/Rolle]
2. [TODO: z.B. Schulung der Mitarbeiter]
   - Geplanter Zeitpunkt: [TODO: YYYY-MM-DD]
   - Verantwortlich: [TODO: Name/Rolle]

30.6 E. Benachrichtigung betroffener Personen (Art. 34)

Wurden betroffene Personen benachrichtigt?
[ ] Ja [ ] Nein [ ] Geplant

Falls Ja: - Zeitpunkt: [TODO: YYYY-MM-DD] - Methode: [TODO: E-Mail/Brief/Öffentliche Bekanntmachung] - Anzahl benachrichtigter Personen: [TODO]

Falls Nein, Begründung:
[ ] Kein hohes Risiko für Rechte und Freiheiten
[ ] Daten waren verschlüsselt/pseudonymisiert
[ ] Nachträgliche Maßnahmen beseitigen hohes Risiko
[ ] Unverhältnismäßiger Aufwand (öffentliche Bekanntmachung geplant)

Erläuterung:
[TODO: Begründe, warum keine Benachrichtigung erfolgt oder warum die gewählte Methode angemessen ist]

30.7 F. Grenzüberschreitende Verarbeitung

Findet grenzüberschreitende Verarbeitung statt?
[ ] Ja [ ] Nein

Falls Ja: - Hauptniederlassung: [TODO: Land] - Weitere betroffene Mitgliedstaaten: [TODO: Länder] - Federführende Aufsichtsbehörde: [TODO: Name]

30.8 G. Auftragsverarbeiter betroffen

Ist ein Auftragsverarbeiter betroffen?
[ ] Ja [ ] Nein

Falls Ja:

Auftragsverarbeiter	Rolle	Benachrichtigt	Zeitpunkt
[TODO: Name]	[TODO: z.B. Cloud-Provider]	[ ] Ja [ ] Nein	[TODO: YYYY-MM-DD]

30.9 H. Zusätzliche Informationen

Frühere Datenschutzverletzungen:
[ ] Ja [ ] Nein

Falls Ja, Anzahl in den letzten 12 Monaten: [TODO]

Versicherung:
[ ] Cyber-Versicherung vorhanden
[ ] Versicherung benachrichtigt am: [TODO: YYYY-MM-DD]

Externe Unterstützung:
[ ] Forensik-Dienstleister eingebunden
[ ] Rechtsanwalt konsultiert
[ ] Sonstige: [TODO]

Medienberichterstattung:
[ ] Ja [ ] Nein [ ] Erwartet

Strafanzeige erstattet:
[ ] Ja [ ] Nein [ ] Geplant

Falls Ja: - Behörde: [TODO: z.B. Polizei, Staatsanwaltschaft] - Aktenzeichen: [TODO] - Datum: [TODO: YYYY-MM-DD]

30.10 I. Anlagen

[ ] Timeline der Ereignisse
[ ] Technischer Bericht
[ ] Forensik-Analyse
[ ] Benachrichtigung an betroffene Personen (Muster)
[ ] Sonstige: [TODO]

30.11 J. Erklärung

Hiermit bestätige ich, dass die vorstehenden Angaben nach bestem Wissen und Gewissen vollständig und wahrheitsgemäß sind.

Ort, Datum: [TODO: Ort, YYYY-MM-DD]

Name: [TODO: Name des Verantwortlichen/Datenschutzbeauftragten]

Funktion: [TODO: Funktion]

Unterschrift: _____

30.12 K. Hinweise zur Übermittlung

Übermittlung an:
[TODO: Name der Aufsichtsbehörde]
[TODO: Adresse]
[TODO: E-Mail]
[TODO: Online-Portal URL]

Frist: 72 Stunden ab Kenntnisnahme (Art. 33 Abs. 1)

Bei Überschreitung der Frist:
Begründung der Verzögerung beifügen (Art. 33 Abs. 1)

Nachreichung von Informationen:
Falls nicht alle Informationen sofort verfügbar sind, können diese schrittweise nachgereicht werden (Art. 33 Abs. 4)

Interne Vermerke:

Erstellt von: [TODO: Name]
Geprüft von: [TODO: Datenschutzbeauftragter]
Freigegeben von: [TODO: Geschäftsführung]
Übermittelt am: [TODO: YYYY-MM-DD HH:MM]
Aktenzeichen Behörde: [TODO: Nach Erhalt eintragen]

ewpage

Chapter 31

Breach Communication Template (Betroffene Personen)

Dokument-ID: 0620
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

31.1 E-Mail-Vorlage

Betreff: Wichtige Information zu Ihren Daten bei {{ meta.organization }}

Sehr geehrte/r [Anrede] [Name],

wir informieren Sie über einen Vorfall, der Ihre personenbezogenen Daten betrifft, die wir verarbeiten.

31.1.1 Was ist passiert?

[TODO: Beschreibe in klarer, verständlicher Sprache, was passiert ist. Vermeide technischen Jargon.]

Beispiel:

```
Am [Datum] haben wir festgestellt, dass durch einen technischen Fehler
personenbezogene Daten von Kunden zeitweise für Unbefugte zugänglich waren.
Der Fehler wurde am [Datum] behoben.
```

31.1.2 Welche Ihrer Daten sind betroffen?

[TODO: Liste die betroffenen Datenkategorien auf]

Beispiel: - Ihr Name - Ihre E-Mail-Adresse - Ihre Telefonnummer - [Weitere Daten]

Nicht betroffen sind: [TODO: z.B. Passwörter, Zahlungsdaten]

31.1.3 Welche Auswirkungen kann dies für Sie haben?

[TODO: Erkläre ehrlich und transparent die möglichen Folgen]

Beispiel:

```
Es besteht das Risiko, dass Dritte Ihre Kontaktdaten für unerwünschte
Werbung oder Phishing-Versuche nutzen könnten.
```

31.1.4 Was haben wir unternommen?

[TODO: Beschreibe die ergriffenen Maßnahmen]

Beispiel: 1. Wir haben den Fehler sofort behoben 2. Wir haben unsere Sicherheitsmaßnahmen verstärkt 3. Wir haben die zuständige Datenschutzbehörde informiert 4. Wir haben eine umfassende Untersuchung eingeleitet

31.1.5 Was sollten Sie jetzt tun?

[TODO: Gib konkrete, umsetzbare Handlungsempfehlungen]

Empfehlungen:

1. **Seien Sie wachsam bei verdächtigen E-Mails oder Anrufen**
   - Öffnen Sie keine Anhänge von unbekannten Absendern
   - Klicken Sie nicht auf verdächtige Links
   - Geben Sie keine persönlichen Informationen preis
2. **[Falls Passwörter betroffen] Ändern Sie Ihr Passwort**
   - Nutzen Sie ein starkes, einzigartiges Passwort
   - Ändern Sie auch Passwörter bei anderen Diensten, falls Sie dasselbe Passwort verwenden
3. **[Falls Finanzdaten betroffen] Überprüfen Sie Ihre Kontoauszüge**
   - Achten Sie auf ungewöhnliche Transaktionen
   - Kontaktieren Sie bei Auffälligkeiten sofort Ihre Bank
4. **[Falls Zugangsdaten betroffen] Aktivieren Sie Zwei-Faktor-Authentifizierung**
   - Dies bietet zusätzlichen Schutz für Ihr Konto

31.1.6 Ihre Kontaktmöglichkeiten

Wenn Sie Fragen haben oder Unterstützung benötigen, stehen wir Ihnen gerne zur Verfügung:

Datenschutzbeauftragter:
[TODO: Name]
E-Mail: [TODO: E-Mail-Adresse]
Telefon: [TODO: Telefonnummer]
Erreichbarkeit: [TODO: z.B. Mo-Fr 9-17 Uhr]

Kundenservice:
E-Mail: [TODO: E-Mail-Adresse]

Telefon: [TODO: Telefonnummer]
Erreichbarkeit: [TODO: z.B. Mo-Fr 8-18 Uhr]

31.1.7 Ihre Rechte

Sie haben das Recht: - Auskunft über die Sie betreffenden Daten zu erhalten - Die Berichtigung unrichtiger Daten zu verlangen - Die Löschung Ihrer Daten zu verlangen - Eine Beschwerde bei der Datenschutzbehörde einzureichen

Zuständige Aufsichtsbehörde:
[TODO: Name der Behörde]
Website: [TODO: URL]
E-Mail: [TODO: E-Mail-Adresse]

31.1.8 Weitere Informationen

Weitere Informationen zu diesem Vorfall finden Sie auf unserer Website:
[TODO: URL zu FAQ oder Informationsseite]

Wir nehmen den Schutz Ihrer Daten sehr ernst und bedauern diesen Vorfall. Wir haben umfassende Maßnahmen ergriffen, um sicherzustellen, dass sich ein solcher Vorfall nicht wiederholt.

Mit freundlichen Grüßen

[TODO: Name]
[TODO: Funktion]
{{ meta.organization }}

Anhang: [Optional: Detaillierte technische Informationen, FAQ]

ewpage

Chapter 32

Breach Register (Verzeichnis der Datenschutzverletzungen)

Dokument-ID: 0630
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

32.1 Zweck

Dieses Register dokumentiert alle Datenschutzverletzungen bei {{ meta.organization }} gemäß Art. 33 Abs. 5 DSGVO. Es dient der Rechenschaftspflicht und ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Meldepflichten.

32.2 Verantwortlichkeiten

Register-Verantwortlicher: [TODO: Name, Funktion]
Datenschutzbeauftragter: [TODO: Name]
Zugriffsberechtigt: [TODO: Rollen/Personen]

32.3 Aufbewahrungsfrist

Mindestens 3 Jahre nach Abschluss des Vorfalls

32.4 Breach Register

32.4.1 Breach-Eintrag: [BREACH-YYYY-NNN]

32.4.1.1 1. Grundinformationen

Feld	Wert
Breach-ID	[TODO: BREACH-2024-001]
Status	[ ] Offen [ ] In Bearbeitung [ ] Geschlossen
Datum Entdeckung	[TODO: YYYY-MM-DD HH:MM]
Datum Kenntnisnahme	[TODO: YYYY-MM-DD HH:MM]
Datum Abschluss	[TODO: YYYY-MM-DD]
Entdecker	[TODO: Name, Abteilung]
Incident Commander	[TODO: Name]

32.4.1.2 2. Art der Verletzung

Feld	Wert
Kategorie	[ ] Vertraulichkeit [ ] Integrität [ ] Verfügbarkeit
Kurzbeschreibung	[TODO: 1-2 Sätze]
Detaillierte Beschreibung	[TODO: Ausführliche Beschreibung]
Ursache	[TODO: z.B. Fehlkonfiguration, Hacking, menschliches Versagen]
Betroffene Systeme	[TODO: Liste der Systeme]

32.4.1.3 3. Betroffene Daten und Personen

Feld	Wert
Datenkategorien	[TODO: z.B. Name, E-Mail, Adresse]
Besondere Kategorien (Art. 9)	[ ] Ja [ ] Nein - Falls Ja: [TODO]
Anzahl betroffener Personen	[TODO: Zahl]
Kategorien betroffener Personen	[TODO: z.B. Kunden, Mitarbeiter]
Vulnerable Gruppen	[ ] Ja [ ] Nein - Falls Ja: [TODO]
Anzahl betroffener Datensätze	[TODO: Zahl]

32.4.1.4 4. Risikobewertung

Feld	Wert
Risiko für Betroffene	[ ] Niedrig [ ] Mittel [ ] Hoch [ ] Sehr hoch
Risikopunkte	[TODO: 4-12 Punkte]
Begründung	[TODO: Erläuterung der Risikobewertung]
Mögliche Folgen	[TODO: z.B. Identitätsdiebstahl, finanzielle Verluste]

32.4.1.5 5. Meldepflicht und Benachrichtigung

Feld	Wert
Meldepflicht Aufsichtsbehörde	[ ] Ja [ ] Nein
Begründung	[TODO: Warum Ja/Nein]
Gemeldet am	[TODO: YYYY-MM-DD HH:MM]
Frist eingehalten (72h)	[ ] Ja [ ] Nein
Aktenzeichen Behörde	[TODO: Falls vorhanden]
Benachrichtigung Betroffener	[ ] Ja [ ] Nein [ ] Nicht erforderlich
Benachrichtigt am	[TODO: YYYY-MM-DD]
Anzahl benachrichtigter Personen	[TODO: Zahl]
Benachrichtigungsmethode	[TODO: E-Mail/Brief/Öffentlich]

32.4.1.6 6. Ergriffene Maßnahmen

Sofortmaßnahmen:

Maßnahme	Zeitpunkt	Verantwortlich	Status
[TODO: z.B. Systeme isoliert]	[TODO: YYYY-MM-DD HH:MM]	[TODO: Name]	[ ] Erledigt
[TODO: z.B. Zugriffe gesperrt]	[TODO: YYYY-MM-DD HH:MM]	[TODO: Name]	[ ] Erledigt

Abhilfemaßnahmen:

Maßnahme	Zeitpunkt	Verantwortlich	Status
[TODO: z.B. Sicherheitslücke geschlossen]	[TODO: YYYY-MM-DD]	[TODO: Name]	[ ] Erledigt
[TODO: z.B. Monitoring verstärkt]	[TODO: YYYY-MM-DD]	[TODO: Name]	[ ] Erledigt

Präventivmaßnahmen:

Maßnahme	Geplant für	Verantwortlich	Status
[TODO: z.B. Schulung Mitarbeiter]	[TODO: YYYY-MM-DD]	[TODO: Name]	[ ] Geplant [ ] Umgesetzt
[TODO: z.B. Prozessanpassung]	[TODO: YYYY-MM-DD]	[TODO: Name]	[ ] Geplant [ ] Umgesetzt

32.4.1.7 7. Kosten und Auswirkungen

Feld	Wert
Direkte Kosten	[TODO: EUR]
Indirekte Kosten	[TODO: EUR]
Versicherungsleistung	[TODO: EUR]
Reputationsschaden	[ ] Ja [ ] Nein
Medienberichterstattung	[ ] Ja [ ] Nein
Beschwerden Betroffener	[TODO: Anzahl]

32.4.1.8 8. Beteiligte Parteien

Rolle	Name/Organisation	Kontakt
Datenschutzbeauftragter	[TODO]	[TODO]
IT-Security	[TODO]	[TODO]
Legal	[TODO]	[TODO]
Auftragsverarbeiter	[TODO]	[TODO]
Forensik-Dienstleister	[TODO]	[TODO]
Aufsichtsbehörde	[TODO]	[TODO]

32.4.1.9 9. Dokumentation

Dokument	Speicherort	Erstellt am
Initiale Meldung	[TODO: Pfad/URL]	[TODO: YYYY-MM-DD]
Technischer Bericht	[TODO: Pfad/URL]	[TODO: YYYY-MM-DD]
Forensik-Analyse	[TODO: Pfad/URL]	[TODO: YYYY-MM-DD]
Meldung Aufsichtsbehörde	[TODO: Pfad/URL]	[TODO: YYYY-MM-DD]
Benachrichtigung Betroffene	[TODO: Pfad/URL]	[TODO: YYYY-MM-DD]
Post-Breach Review	[TODO: Pfad/URL]	[TODO: YYYY-MM-DD]

32.4.1.10 10. Lessons Learned

Was lief gut: - [TODO: Positive Aspekte]

Was lief schlecht: - [TODO: Verbesserungsbedarf]

Verbesserungsmaßnahmen: - [TODO: Konkrete Maßnahmen]

Prozessanpassungen: - [TODO: Anpassungen an Prozessen]

32.4.1.11 11. Abschluss

Feld	Wert
Abgeschlossen am	[TODO: YYYY-MM-DD]
Abgeschlossen durch	[TODO: Name, Funktion]

Feld	Wert
Freigabe Datenschutzbeauftragter	[ ] Ja - Datum: [TODO]
Freigabe Geschäftsführung	[ ] Ja - Datum: [TODO]

32.5 Statistik und Übersicht

32.5.1 Jahresübersicht [YYYY]

Monat	Anzahl Breaches	Gemeldet	Benachrichtigt	Status
Januar	[TODO]	[TODO]	[TODO]	[TODO]
Februar	[TODO]	[TODO]	[TODO]	[TODO]
März	[TODO]	[TODO]	[TODO]	[TODO]
April	[TODO]	[TODO]	[TODO]	[TODO]
Mai	[TODO]	[TODO]	[TODO]	[TODO]
Juni	[TODO]	[TODO]	[TODO]	[TODO]
Juli	[TODO]	[TODO]	[TODO]	[TODO]
August	[TODO]	[TODO]	[TODO]	[TODO]
September	[TODO]	[TODO]	[TODO]	[TODO]
Oktober	[TODO]	[TODO]	[TODO]	[TODO]
November	[TODO]	[TODO]	[TODO]	[TODO]
Dezember	[TODO]	[TODO]	[TODO]	[TODO]
Gesamt	**[TODO]**	**[TODO]**	**[TODO]**	

32.5.2 Kategorisierung

Kategorie	Anzahl	Prozent
Vertraulichkeitsverletzung	[TODO]	[TODO]%
Integritätsverletzung	[TODO]	[TODO]%
Verfügbarkeitsverletzung	[TODO]	[TODO]%

32.5.3 Ursachen

Ursache	Anzahl	Prozent
Menschliches Versagen	[TODO]	[TODO]%
Technisches Versagen	[TODO]	[TODO]%
Externe Angriffe	[TODO]	[TODO]%
Auftragsverarbeiter	[TODO]	[TODO]%
Sonstige	[TODO]	[TODO]%

32.5.4 Trends und Erkenntnisse

[TODO: Analyse von Trends, häufigen Ursachen, Verbesserungspotenzial]

32.6 Zugriffskontrolle

32.6.1 Zugriffsprotokoll

Datum	Benutzer	Aktion	Breach-ID
[TODO]	[TODO]	[TODO: Ansicht/Bearbeitung/Export]	[TODO]

32.7 Audit-Trail

32.7.1 Änderungshistorie

Datum	Benutzer	Breach-ID	Änderung	Begründung
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Hinweise: - Dieses Register ist vertraulich und darf nur autorisierten Personen zugänglich gemacht werden - Alle Einträge müssen vollständig und wahrheitsgemäß sein - Das Register muss bei Audits und auf Anfrage der Aufsichtsbehörde vorgelegt werden können - Regelmäßige Überprüfung und Aktualisierung erforderlich

ewpage

Chapter 33

Post-Breach Review Template

Dokument-ID: 0640
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

33.1 Post-Breach Review

Breach-ID: [TODO: BREACH-YYYY-NNN]
Review-Datum: [TODO: YYYY-MM-DD]
Moderator: [TODO: Name]

33.1.1 Teilnehmer

Name	Rolle	Abteilung
[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]

33.2 1. Incident-Zusammenfassung

Kurzbeschreibung:
[TODO: 2-3 Sätze zur Beschreibung des Vorfalls]

Zeitraum:
- Beginn: [TODO: YYYY-MM-DD HH:MM] - Entdeckung: [TODO: YYYY-MM-DD HH:MM] - Abschluss: [TODO: YYYY-MM-DD HH:MM] - Gesamtdauer: [TODO: X Stunden/Tage]

Betroffene:
- Anzahl Personen: [TODO] - Datenkategorien: [TODO] - Risikostufe: [TODO: Niedrig/Mittel/Hoch]

33.3 2. Timeline-Analyse

Zeitpunkt	Ereignis	Verantwortlich	Dauer bis nächstem Schritt
[TODO: HH:MM]	Vorfall tritt ein	-	-
[TODO: HH:MM]	Entdeckung	[TODO]	[TODO: X Min/Std]
[TODO: HH:MM]	Erste Meldung	[TODO]	[TODO: X Min/Std]
[TODO: HH:MM]	Team aktiviert	[TODO]	[TODO: X Min/Std]
[TODO: HH:MM]	Eindämmung	[TODO]	[TODO: X Min/Std]
[TODO: HH:MM]	Meldung Behörde	[TODO]	[TODO: X Std]
[TODO: HH:MM]	Benachrichtigung Betroffene	[TODO]	[TODO: X Std]
[TODO: HH:MM]	Incident geschlossen	[TODO]	-

Analyse:
[TODO: Waren die Reaktionszeiten angemessen? Wo gab es Verzögerungen?]

33.4 3. Was lief gut? (Positives)

33.4.1 3.1 Erkennung und Meldung

Positive Aspekte: - [TODO: z.B. Schnelle Erkennung durch Monitoring] - [TODO: z.B. Klare Meldewege funktionierten]

33.4.2 3.2 Response und Eindämmung

Positive Aspekte: - [TODO: z.B. Team war gut vorbereitet] - [TODO: z.B. Technische Maßnahmen griffen schnell]

33.4.3 3.3 Kommunikation

Positive Aspekte: - [TODO: z.B. Klare interne Kommunikation] - [TODO: z.B. Professionelle externe Kommunikation]

33.4.4 3.4 Dokumentation

Positive Aspekte: - [TODO: z.B. Vollständige Dokumentation] - [TODO: z.B. Breach-Register aktuell]

33.5 4. Was lief schlecht? (Verbesserungsbedarf)

33.5.1 4.1 Erkennung und Meldung

Probleme: - [TODO: z.B. Verzögerte Erkennung] - [TODO: z.B. Unklare Meldewege]

Ursachen: - [TODO: Warum traten diese Probleme auf?]

33.5.2 4.2 Response und Eindämmung

Probleme: - [TODO: z.B. Verzögerte Reaktion] - [TODO: z.B. Fehlende Tools]

Ursachen: - [TODO: Warum traten diese Probleme auf?]

33.5.3 4.3 Kommunikation

Probleme: - [TODO: z.B. Verzögerte Benachrichtigung] - [TODO: z.B. Unklare Botschaften]

Ursachen: - [TODO: Warum traten diese Probleme auf?]

33.5.4 4.4 Dokumentation

Probleme: - [TODO: z.B. Lückenhafte Dokumentation] - [TODO: z.B. Fehlende Templates]

Ursachen: - [TODO: Warum traten diese Probleme auf?]

33.6 5. Root Cause Analysis

Primäre Ursache:
[TODO: Was war die Hauptursache des Vorfalls?]

Beitragende Faktoren: - [TODO: Faktor 1] - [TODO: Faktor 2] - [TODO: Faktor 3]

5-Why-Analyse:

1. Warum trat der Vorfall auf?
   [TODO: Antwort]
2. Warum [Antwort aus 1]?
   [TODO: Antwort]
3. Warum [Antwort aus 2]?
   [TODO: Antwort]
4. Warum [Antwort aus 3]?
   [TODO: Antwort]
5. Warum [Antwort aus 4]?
   [TODO: Root Cause]

33.7 6. Lessons Learned

33.7.1 6.1 Technische Erkenntnisse

- [TODO: z.B. Monitoring-Lücken identifiziert]
- [TODO: z.B. Sicherheitskonfiguration unzureichend]

33.7.2 6.2 Prozessuale Erkenntnisse

- [TODO: z.B. Response-Plan muss aktualisiert werden]
- [TODO: z.B. Eskalationswege unklar]

33.7.3 6.3 Organisatorische Erkenntnisse

- [TODO: z.B. Schulungsbedarf identifiziert]
- [TODO: z.B. Rollen müssen klarer definiert werden]

33.7.4 6.4 Kommunikative Erkenntnisse

- [TODO: z.B. Templates müssen verbessert werden]
- [TODO: z.B. Kommunikationswege optimieren]

33.8 7. Verbesserungsmaßnahmen

33.8.1 7.1 Sofortmaßnahmen (innerhalb 1 Monat)

Maßnahme	Verantwortlich	Frist	Priorität	Status
[TODO: z.B. Monitoring erweitern]	[TODO]	[TODO: YYYY-MM-DD]	Hoch	[ ] Offen
[TODO: z.B. Response-Plan aktualisieren]	[TODO]	[TODO: YYYY-MM-DD]	Hoch	[ ] Offen

33.8.2 7.2 Mittelfristige Maßnahmen (1-3 Monate)

Maßnahme	Verantwortlich	Frist	Priorität	Status
[TODO: z.B. Schulungen durchführen]	[TODO]	[TODO: YYYY-MM-DD]	Mittel	[ ] Offen
[TODO: z.B. Prozesse dokumentieren]	[TODO]	[TODO: YYYY-MM-DD]	Mittel	[ ] Offen

33.8.3 7.3 Langfristige Maßnahmen (3-12 Monate)

Maßnahme	Verantwortlich	Frist	Priorität	Status
[TODO: z.B. Neue Tools implementieren]	[TODO]	[TODO: YYYY-MM-DD]	Niedrig	[ ] Offen
[TODO: z.B. Organisationsstruktur anpassen]	[TODO]	[TODO: YYYY-MM-DD]	Niedrig	[ ] Offen

---

33.9 8. Kosten-Nutzen-Analyse

33.9.1 8.1 Kosten des Vorfalls

Kostenart	Betrag (EUR)
Direkte Kosten (Forensik, externe Berater)	[TODO]
Personalkosten (Arbeitszeit)	[TODO]
Meldungen und Benachrichtigungen	[TODO]
Reputationsschaden (geschätzt)	[TODO]
Gesamt	**[TODO]**

33.9.2 8.2 Kosten der Verbesserungsmaßnahmen

Maßnahme	Geschätzte Kosten (EUR)
[TODO: Maßnahme 1]	[TODO]
[TODO: Maßnahme 2]	[TODO]
Gesamt	**[TODO]**

33.9.3 8.3 Erwarteter Nutzen

[TODO: Beschreibe den erwarteten Nutzen der Maßnahmen, z.B. Risikoreduktion, schnellere Response-Zeiten]

33.10 9. Response-Plan-Anpassungen

Erforderliche Änderungen am Response-Plan:

Abschnitt	Änderung	Begründung
[TODO: z.B. Kontakte]	[TODO: z.B. Neue Kontakte ergänzen]	[TODO]
[TODO: z.B. Eskalation]	[TODO: z.B. Schwellenwerte anpassen]	[TODO]

33.11 10. Schulungs- und Awareness-Bedarf

Identifizierter Schulungsbedarf:

Zielgruppe	Thema	Format	Zeitrahmen
[TODO: z.B. IT-Team]	[TODO: z.B. Incident Response]	[TODO: Workshop]	[TODO: Q2 2024]
[TODO: z.B. Alle MA]	[TODO: z.B. Data Breach Awareness]	[TODO: E-Learning]	[TODO: Q2 2024]

33.12 11. Follow-up und Monitoring

Nächste Schritte:

Aktion	Verantwortlich	Frist
Maßnahmenplan erstellen	[TODO]	[TODO: YYYY-MM-DD]
Monatliches Review-Meeting	[TODO]	[TODO: Jeden 1. Montag]
Fortschrittsbericht an Geschäftsführung	[TODO]	[TODO: YYYY-MM-DD]
Follow-up Review (3 Monate)	[TODO]	[TODO: YYYY-MM-DD]

33.13 12. Abschluss und Freigabe

Zusammenfassung:
[TODO: 2-3 Sätze Zusammenfassung der wichtigsten Erkenntnisse und Maßnahmen]

Freigabe:

Rolle	Name	Datum	Unterschrift
Moderator	[TODO]	[TODO]	_____
Datenschutzbeauftragter	[TODO]	[TODO]	_____
Geschäftsführung	[TODO]	[TODO]	_____

Anhänge: - [ ] Detaillierte Timeline - [ ] Technischer Bericht - [ ] Kommunikationsmaterialien - [ ] Maßnahmenplan (detailliert)

ewpage

Chapter 34

Anhang: Verzeichnis der Verarbeitungstätigkeiten (Template)

Dokument-ID: 0700
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

34.1 Verzeichnis der Verarbeitungstätigkeiten

Organisation: {{ meta.organization }}
Verantwortlicher: [TODO: Name, Funktion]
Datenschutzbeauftragter: [TODO: Name, Kontakt]
Stand: {{ meta.date }}

34.2 Verarbeitungstätigkeit [Nr. 1]

34.2.1 1. Name und Kontaktdaten des Verantwortlichen

Verantwortlicher:
{{ meta.organization }}
[TODO: Adresse]
[TODO: Telefon]
[TODO: E-Mail]

Vertreter (falls zutreffend):
[TODO: Name, Adresse, Kontakt]

Datenschutzbeauftragter:
[TODO: Name]

[TODO: Kontakt]

34.2.2 2. Zwecke der Verarbeitung

Hauptzweck:
[TODO: z.B. Kundenverwaltung, Personalverwaltung, Marketing]

Weitere Zwecke:
- [TODO: Zweck 1] - [TODO: Zweck 2]

34.2.3 3. Kategorien betroffener Personen

- ☐ Kunden
- ☐ Interessenten
- ☐ Mitarbeiter
- ☐ Bewerber
- ☐ Lieferanten/Partner
- ☐ Website-Besucher
- ☐ Sonstige: [TODO]

34.2.4 4. Kategorien personenbezogener Daten

Allgemeine Daten: - [ ] Stammdaten (Name, Adresse, Geburtsdatum) - [ ] Kontaktdaten (E-Mail, Telefon) - [ ] Vertragsdaten - [ ] Zahlungsdaten - [ ] Nutzungsdaten - [ ] Sonstige: [TODO]

Besondere Kategorien (Art. 9): - [ ] Gesundheitsdaten - [ ] Genetische Daten - [ ] Biometrische Daten - [ ] Daten über rassische/ethnische Herkunft - [ ] Politische Meinungen - [ ] Religiöse/weltanschauliche Überzeugungen - [ ] Gewerkschaftszugehörigkeit - [ ] Sexualleben/sexuelle Orientierung

34.2.5 5. Kategorien von Empfängern

Interne Empfänger:
[TODO: z.B. Vertrieb, Buchhaltung, IT]

Externe Empfänger:
[TODO: z.B. Zahlungsdienstleister, Versanddienstleister]

Auftragsverarbeiter:
[TODO: z.B. Cloud-Provider, IT-Dienstleister]

Drittlandübermittlung:
[ ] Ja [ ] Nein

Falls Ja: - Länder: [TODO] - Garantien: [TODO: z.B. Standardvertragsklauseln, Angemessenheitsbeschluss]

34.2.6 6. Fristen für die Löschung

Regelfall:
[TODO: z.B. 3 Jahre nach Vertragsende]

Gesetzliche Aufbewahrungspflichten:
[TODO: z.B. 10 Jahre HGB, 6 Jahre AO]

Löschkonzept:
[TODO: Beschreibung oder Verweis auf Dokument]

34.2.7 7. Technische und organisatorische Maßnahmen (TOM)

Zutrittskontrolle:
[TODO: z.B. Zutrittskarten, Besucherregistrierung]

Zugangskontrolle:
[TODO: z.B. Passwörter, Zwei-Faktor-Authentifizierung]

Zugriffskontrolle:
[TODO: z.B. Berechtigungskonzept, Rollenmodell]

Weitergabekontrolle:
[TODO: z.B. Verschlüsselung, VPN]

Eingabekontrolle:
[TODO: z.B. Logging, Protokollierung]

Auftragskontrolle:
[TODO: z.B. Auftragsverarbeiter-Verträge]

Verfügbarkeitskontrolle:
[TODO: z.B. Backup, Notfallplan]

Trennungskontrolle:
[TODO: z.B. Mandantenfähigkeit, Datentrennung]

34.2.8 8. Rechtsgrundlage

Rechtsgrundlage:
[ ] Art. 6 Abs. 1 lit. a (Einwilligung)
[ ] Art. 6 Abs. 1 lit. b (Vertragserfüllung)
[ ] Art. 6 Abs. 1 lit. c (Rechtliche Verpflichtung)
[ ] Art. 6 Abs. 1 lit. d (Schutz lebenswichtiger Interessen)
[ ] Art. 6 Abs. 1 lit. e (Öffentliches Interesse)
[ ] Art. 6 Abs. 1 lit. f (Berechtigtes Interesse)

Bei besonderen Kategorien (Art. 9):
[ ] Art. 9 Abs. 2 lit. a (Ausdrückliche Einwilligung)
[ ] Art. 9 Abs. 2 lit. b (Arbeitsrecht)
[ ] Art. 9 Abs. 2 lit. c (Schutz lebenswichtiger Interessen)
[ ] Art. 9 Abs. 2 lit. d (Stiftungen, Vereine)
[ ] Art. 9 Abs. 2 lit. e (Öffentlich gemachte Daten)
[ ] Art. 9 Abs. 2 lit. f (Rechtliche Ansprüche)
[ ] Art. 9 Abs. 2 lit. g (Erhebliches öffentliches Interesse)
[ ] Art. 9 Abs. 2 lit. h (Gesundheitsvorsorge)
[ ] Art. 9 Abs. 2 lit. i (Öffentliche Gesundheit)
[ ] Art. 9 Abs. 2 lit. j (Archivzwecke, Forschung, Statistik)

Erläuterung:
[TODO: Begründung der Rechtsgrundlage]

34.2.9 9. Datenschutz-Folgenabschätzung (DSFA)

DSFA erforderlich:
[ ] Ja [ ] Nein

Falls Ja:
- DSFA-ID: [TODO] - Durchgeführt am: [TODO: YYYY-MM-DD] - Ergebnis: [TODO: Risiko akzeptabel/nicht akzeptabel]

34.2.10 10. Weitere Informationen

Datenquellen:
[TODO: z.B. Direkt vom Betroffenen, von Dritten]

Automatisierte Entscheidungsfindung:
[ ] Ja [ ] Nein

Falls Ja:
[TODO: Beschreibung der Logik, Tragweite, Auswirkungen]

Profiling:
[ ] Ja [ ] Nein

Falls Ja:
[TODO: Beschreibung]

34.3 Verarbeitungstätigkeit [Nr. 2]

[TODO: Wiederhole Struktur für weitere Verarbeitungstätigkeiten]

34.4 Übersicht aller Verarbeitungstätigkeiten

Nr.	Name	Zweck	Betroffene	Rechtsgrundlage	DSFA
1	[TODO]	[TODO]	[TODO]	[TODO]	Ja/Nein
2	[TODO]	[TODO]	[TODO]	[TODO]	Ja/Nein
3	[TODO]	[TODO]	[TODO]	[TODO]	Ja/Nein

34.5 Änderungshistorie

Version	Datum	Änderung	Geändert von
1.0	[TODO]	Erstversion	[TODO]
1.1	[TODO]	[TODO: Beschreibung]	[TODO]

Hinweise: - Dieses Verzeichnis muss bei Änderungen aktualisiert werden - Das Verzeichnis muss der Aufsichtsbehörde auf Anfrage vorgelegt werden - Regelmäßige Überprüfung (mindestens jährlich) erforderlich

ewpage

Chapter 35

Anhang: DSFA Quick Reference

Dokument-ID: 0710
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Referenz
Klassifizierung: Intern
Letzte Aktualisierung: {{ meta.date }}

35.1 Wann ist eine DSFA erforderlich?

35.1.1 Pflichtfälle (Art. 35 Abs. 3)

Eine DSFA ist **immer** erforderlich bei:

1. **Systematische und umfassende Bewertung persönlicher Aspekte**
   - Automatisierte Verarbeitung einschließlich Profiling
   - Grundlage für Entscheidungen mit Rechtswirkung oder erheblicher Beeinträchtigung
2. **Umfangreiche Verarbeitung besonderer Kategorien (Art. 9)**
   - Gesundheitsdaten, genetische Daten, biometrische Daten
   - Daten über strafrechtliche Verurteilungen und Straftaten
3. **Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche**
   - Videoüberwachung
   - Tracking und Monitoring

35.1.2 Blacklist der Aufsichtsbehörden

Zusätzlich erforderlich bei (Beispiele): - Scoring und Rating - Automatisierte Entscheidungen mit Rechtswirkung - Systematisches Monitoring - Verarbeitung sensibler Daten in großem Umfang - Datenabgleich oder Datenzusammenführung - Daten vulnerabler Personen (Kinder, Patienten, Mitarbeiter) - Innovative Technologien (KI, Biometrie) - Drittlandübermittlung ohne Angemessenheitsbeschluss

35.1.3 Schwellenwertkriterien

Anzahl betroffener Personen: - < 5.000: Meist keine DSFA erforderlich - 5.000 - 20.000: DSFA empfohlen - > 20.000: DSFA meist erforderlich

Risikofaktoren (je mehr zutreffen, desto eher DSFA): - [ ] Bewertung oder Scoring - [ ] Automatisierte Entscheidungen - [ ] Systematisches Monitoring - [ ] Besondere Kategorien (Art. 9) - [ ] Vulnerable Gruppen - [ ] Umfangreiche Verarbeitung - [ ] Datenabgleich - [ ] Innovative Technologie - [ ] Drittlandübermittlung - [ ] Verhinderung von Rechtsausübung

Faustregel: Bei 2 oder mehr Risikofaktoren → DSFA durchführen

---

35.2 DSFA-Prozess (Kurzübersicht)

35.2.1 Phase 1: Vorbereitung

1. **Prüfen:** Ist DSFA erforderlich?
2. **Team bilden:** Verantwortlicher, Datenschutzbeauftragter, IT, Fachbereich
3. **Informationen sammeln:** Verarbeitungsbeschreibung, Datenflüsse, Systeme

35.2.2 Phase 2: Durchführung

4. **Beschreibung:** Verarbeitung detailliert beschreiben
5. **Notwendigkeit:** Notwendigkeit und Verhältnismäßigkeit prüfen
6. **Risiken identifizieren:** Systematische Risikoanalyse
7. **Maßnahmen definieren:** Technische und organisatorische Maßnahmen
8. **Restrisiko bewerten:** Ist Restrisiko akzeptabel?

35.2.3 Phase 3: Konsultation

9. **Datenschutzbeauftragter:** Stellungnahme einholen
10. **Betroffene (optional):** Ansichten einholen
11. **Aufsichtsbehörde (falls erforderlich):** Bei hohem Restrisiko konsultieren

35.2.4 Phase 4: Dokumentation

12. **DSFA dokumentieren:** Template 0410 verwenden
13. **Genehmigung:** Verantwortlicher genehmigt
14. **Archivierung:** DSFA aufbewahren

35.3 Risikobewertungsmatrix

35.3.1 Eintrittswahrscheinlichkeit

Stufe	Beschreibung	Beispiel
Niedrig	Unwahrscheinlich	Verschlüsselte Daten, starke Sicherheitsmaßnahmen
Mittel	Möglich	Standardsicherheit, bekannte Schwachstellen
Hoch	Wahrscheinlich	Schwache Sicherheit, öffentlich zugänglich

35.3.2 Schwere der Auswirkungen

Stufe	Beschreibung	Beispiel
Niedrig	Geringe Beeinträchtigung	Allgemeine Kontaktdaten, keine sensiblen Daten
Mittel	Erhebliche Beeinträchtigung	Finanzdaten, Vertragsdaten
Hoch	Schwerwiegende Beeinträchtigung	Gesundheitsdaten, Identitätsdiebstahl möglich

35.3.3 Risikomatrix

	Niedrige Schwere	**Mittlere Schwere**	**Hohe Schwere**
Niedrige Wahrscheinlichkeit	Niedriges Risiko	Mittleres Risiko	Mittleres Risiko
Mittlere Wahrscheinlichkeit	Mittleres Risiko	Mittleres Risiko	Hohes Risiko
Hohe Wahrscheinlichkeit	Mittleres Risiko	Hohes Risiko	Sehr hohes Risiko

Handlungsempfehlung: - **Niedriges Risiko:** Standardmaßnahmen ausreichend - **Mittleres Risiko:** Zusätzliche Maßnahmen erforderlich - **Hohes Risiko:** Umfassende Maßnahmen, ggf. Konsultation Aufsichtsbehörde - **Sehr hohes Risiko:** Konsultation Aufsichtsbehörde erforderlich

---

35.4 Typische Maßnahmen

35.4.1 Technische Maßnahmen

- **Verschlüsselung:** Ende-zu-Ende, Transport, Speicherung
- **Pseudonymisierung:** Trennung von Identifikationsdaten
- **Anonymisierung:** Irreversible Entfernung personenbezogener Daten
- **Zugriffskontrolle:** Rollenbasiert, Least Privilege
- **Logging:** Nachvollziehbarkeit, Audit-Trails
- **Backup:** Regelmäßig, getestet
- **Monitoring:** Anomalieerkennung, Intrusion Detection

35.4.2 Organisatorische Maßnahmen

- **Richtlinien:** Datenschutzrichtlinie, Sicherheitsrichtlinie
- **Schulungen:** Regelmäßig, zielgruppenspezifisch
- **Verträge:** Auftragsverarbeiter-Verträge, NDAs
- **Prozesse:** Incident Response, Löschkonzept
- **Dokumentation:** Verarbeitungsverzeichnis, TOMs
- **Audits:** Regelmäßige Überprüfungen

35.4.3 Privacy by Design/Default

- **Datenminimierung:** Nur notwendige Daten erheben
- **Zweckbindung:** Klare Zweckdefinition
- **Speicherbegrenzung:** Automatische Löschung
- **Transparenz:** Klare Informationen für Betroffene
- **Benutzerfreundlichkeit:** Einfache Ausübung von Rechten

35.5 Checkliste: DSFA erforderlich?

☐ Systematische und umfassende Bewertung persönlicher Aspekte?
☐ Automatisierte Entscheidungen mit Rechtswirkung?
☐ Umfangreiche Verarbeitung besonderer Kategorien (Art. 9)?
☐ Systematische Überwachung öffentlich zugänglicher Bereiche?
☐ Scoring oder Rating?
☐ Verarbeitung sensibler Daten in großem Umfang?
☐ Datenabgleich oder Datenzusammenführung?
☐ Daten vulnerabler Personen (Kinder, Patienten)?
☐ Innovative Technologien (KI, Biometrie)?
☐ Drittlandübermittlung ohne Angemessenheitsbeschluss?
☐ Mehr als 20.000 betroffene Personen?
☐ 2 oder mehr Risikofaktoren treffen zu?

Wenn 1 oder mehr Fragen mit Ja beantwortet: DSFA durchführen!

35.6 Vorherige Konsultation der Aufsichtsbehörde

Erforderlich wenn: - Restrisiko trotz Maßnahmen hoch bleibt - Keine angemessenen Maßnahmen möglich - Unsicherheit über Angemessenheit der Maßnahmen

Prozess: 1. DSFA vollständig durchführen 2. Alle möglichen Maßnahmen dokumentieren 3. Anfrage an Aufsichtsbehörde mit DSFA-Dokumentation 4. Aufsichtsbehörde hat 8 Wochen Zeit (verlängerbar auf 14 Wochen) 5. Stellungnahme der Behörde umsetzen

---

35.7 Häufige Fehler vermeiden

DSFA zu spät durchführen → Vor Beginn der Verarbeitung!
Oberflächliche Risikoanalyse → Systematisch und detailliert!
Datenschutzbeauftragten nicht einbeziehen → Immer konsultieren!
Keine konkreten Maßnahmen → Spezifisch und umsetzbar!
DSFA nicht aktualisieren → Bei Änderungen überprüfen!
Keine Dokumentation → Vollständig dokumentieren!

35.8 Nützliche Ressourcen

Templates: - Template 0410: DSFA Template (Vorlage) - Template 0400: DSFA Grundlagen

Externe Ressourcen: - WP29 Guidelines on DPIA (wp248rev.01) - Blacklist der Aufsichtsbehörden - DSFA-Tools der Aufsichtsbehörden

Kontakt: - Datenschutzbeauftragter: [TODO: Kontakt] - Aufsichtsbehörde: [TODO: Kontakt]

ewpage

Chapter 36

Anhang: Auftragsverarbeitungsvertrag (DPA) Template

Dokument-ID: 0720
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Template
Klassifizierung: Vertraulich
Letzte Aktualisierung: {{ meta.date }}

36.1 Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

zwischen

Verantwortlicher (Auftraggeber):
{{ meta.organization }}
[TODO: Adresse]
[TODO: Vertretungsberechtigte Person]

nachfolgend “Auftraggeber”

und

Auftragsverarbeiter (Auftragnehmer):
[TODO: Name des Auftragsverarbeiters]
[TODO: Adresse]
[TODO: Vertretungsberechtigte Person]

nachfolgend “Auftragnehmer”

36.2 Präambel

Der Auftraggeber beauftragt den Auftragnehmer mit Dienstleistungen, bei denen der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit dieser Auftragsverarbeitung gemäß Art. 28 DSGVO.

36.3 § 1 Gegenstand und Dauer

36.3.1 1.1 Gegenstand

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen folgender Leistungen:

[TODO: z.B. Cloud-Hosting, IT-Support, Lohnbuchhaltung, Marketing-Services]

36.3.2 1.2 Dauer

Dieser Vertrag tritt mit Unterzeichnung in Kraft und gilt für die Dauer der Hauptleistung. Er endet automatisch mit Beendigung der Hauptleistung oder kann von beiden Parteien mit einer Frist von [TODO: z.B. 3 Monaten] gekündigt werden.

36.4 § 2 Art und Zweck der Verarbeitung

36.4.1 2.1 Art der Verarbeitung

[ ] Erhebung
[ ] Erfassung
[ ] Organisation
[ ] Ordnen
[ ] Speicherung
[ ] Anpassung
[ ] Veränderung
[ ] Auslesen
[ ] Abfragen
[ ] Verwendung
[ ] Offenlegung durch Übermittlung
[ ] Verbreitung
[ ] Bereitstellung
[ ] Abgleich
[ ] Verknüpfung
[ ] Einschränkung
[ ] Löschen
[ ] Vernichtung

36.4.2 2.2 Zweck der Verarbeitung

[TODO: z.B. Bereitstellung von Cloud-Speicher für Kundendaten, Verarbeitung von Lohndaten]

36.5 § 3 Umfang der Verarbeitung

36.5.1 3.1 Kategorien betroffener Personen

[TODO: z.B. Kunden, Mitarbeiter, Lieferanten]

36.5.2 3.2 Kategorien personenbezogener Daten

Allgemeine Daten:
[TODO: z.B. Name, Adresse, E-Mail, Telefon]

Besondere Kategorien (Art. 9):
[ ] Ja [ ] Nein

Falls Ja: [TODO: z.B. Gesundheitsdaten, biometrische Daten]

36.5.3 3.3 Umfang

Geschätzte Anzahl betroffener Personen: [TODO: z.B. 10.000]
Geschätztes Datenvolumen: [TODO: z.B. 100 GB]

36.6 § 4 Pflichten des Auftragnehmers

36.6.1 4.1 Weisungsgebundenheit

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach dokumentierten Weisungen des Auftraggebers. Weisungen können schriftlich, elektronisch oder mündlich (mit schriftlicher Bestätigung) erteilt werden.

Weisungsbefugte Personen beim Auftraggeber:
[TODO: Name, Funktion, Kontakt]

Weisungsempfänger beim Auftragnehmer:
[TODO: Name, Funktion, Kontakt]

36.6.2 4.2 Vertraulichkeit

Der Auftragnehmer stellt sicher, dass sich alle mit der Verarbeitung befassten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

36.6.3 4.3 Technische und organisatorische Maßnahmen (TOM)

Der Auftragnehmer implementiert und unterhält angemessene technische und organisatorische Maßnahmen gemäß Anlage 1 (TOM).

36.6.4 4.4 Unterstützungspflichten

Der Auftragnehmer unterstützt den Auftraggeber bei: - Beantwortung von Betroffenenanfragen - Meldung von Datenschutzverletzungen - Durchführung von Datenschutz-Folgenabschätzungen - Vorherigen Konsultationen mit Aufsichtsbehörden

36.6.5 4.5 Löschung und Rückgabe

Nach Beendigung der Leistungen löscht oder gibt der Auftragnehmer alle personenbezogenen Daten zurück, es sei denn, eine gesetzliche Aufbewahrungspflicht besteht.

Frist: [TODO: z.B. 30 Tage nach Vertragsende]

36.7 § 5 Unterauftragsverhältnisse

36.7.1 5.1 Genehmigung

Der Auftragnehmer darf Unterauftragsverarbeiter nur mit vorheriger schriftlicher Genehmigung des Auftraggebers einsetzen.

Bereits genehmigte Unterauftragsverarbeiter:

Name	Leistung	Standort
[TODO]	[TODO]	[TODO]

36.7.2 5.2 Informationspflicht

Der Auftragnehmer informiert den Auftraggeber über geplante Änderungen (Hinzufügung oder Ersetzung) von Unterauftragsverarbeitern. Der Auftraggeber kann innerhalb von [TODO: z.B. 14 Tagen] Einspruch erheben.

36.7.3 5.3 Pflichten

Der Auftragnehmer stellt sicher, dass Unterauftragsverarbeiter dieselben Datenschutzpflichten erfüllen wie in diesem Vertrag festgelegt.

36.8 § 6 Rechte und Pflichten des Auftraggebers

36.8.1 6.1 Weisungsrecht

Der Auftraggeber hat das Recht, jederzeit Weisungen zur Datenverarbeitung zu erteilen.

36.8.2 6.2 Kontrollrechte

Der Auftraggeber oder ein beauftragter Prüfer hat das Recht: - Auskünfte einzuholen - Inspektionen durchzuführen - Audits durchzuführen

Ankündigungsfrist: [TODO: z.B. 14 Tage]

36.8.3 6.3 Verantwortlichkeit

Der Auftraggeber bleibt für die Einhaltung der Datenschutzvorschriften verantwortlich.

36.9 § 7 Datenschutzverletzungen

36.9.1 7.1 Meldepflicht

Der Auftragnehmer meldet Datenschutzverletzungen unverzüglich, spätestens innerhalb von [TODO: z.B. 24 Stunden] an den Auftraggeber.

Kontakt beim Auftraggeber:
[TODO: Name, Telefon, E-Mail]

36.9.2 7.2 Unterstützung

Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Meldepflichten gemäß Art. 33-34 DSGVO.

36.10 § 8 Haftung und Schadensersatz

36.10.1 8.1 Haftung

Beide Parteien haften gemäß Art. 82 DSGVO für Schäden, die durch die Verarbeitung entstehen.

36.10.2 8.2 Freistellung

Der Auftragnehmer stellt den Auftraggeber von Ansprüchen Dritter frei, die aufgrund von Verstößen des Auftragnehmers gegen diesen Vertrag entstehen.

36.11 § 9 Datenschutzbeauftragte

Datenschutzbeauftragter des Auftraggebers:
[TODO: Name, Kontakt]

Datenschutzbeauftragter des Auftragnehmers:
[TODO: Name, Kontakt]

36.12 § 10 Schlussbestimmungen

36.12.1 10.1 Änderungen

Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform.

36.12.2 10.2 Salvatorische Klausel

Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

36.12.3 10.3 Anwendbares Recht

Es gilt das Recht der [TODO: z.B. Bundesrepublik Deutschland].

36.12.4 10.4 Gerichtsstand

Gerichtsstand ist [TODO: z.B. München].

36.13 Unterschriften

Auftraggeber:

Ort, Datum: _____

Name: _____

Unterschrift: _____

Auftragnehmer:

Ort, Datum: _____

Name: _____

Unterschrift: _____

36.14 Anlage 1: Technische und organisatorische Maßnahmen (TOM)

36.14.1 1. Zutrittskontrolle

[TODO: z.B. Zutrittskarten, Besucherregistrierung, Sicherheitspersonal]

36.14.2 2. Zugangskontrolle

[TODO: z.B. Passwörter, Zwei-Faktor-Authentifizierung, Biometrie]

36.14.3 3. Zugriffskontrolle

[TODO: z.B. Rollenbasierte Berechtigungen, Least Privilege, Need-to-know]

36.14.4 4. Weitergabekontrolle

[TODO: z.B. Verschlüsselung, VPN, sichere Übertragungsprotokolle]

36.14.5 5. Eingabekontrolle

[TODO: z.B. Logging, Audit-Trails, Versionierung]

36.14.6 6. Auftragskontrolle

[TODO: z.B. Klare Verträge, Weisungsdokumentation, Kontrollen]

36.14.7 7. Verfügbarkeitskontrolle

[TODO: z.B. Backup, Redundanz, Notfallplan, Disaster Recovery]

36.14.8 8. Trennungskontrolle

[TODO: z.B. Mandantenfähigkeit, Datentrennung, separate Umgebungen]

36.14.9 9. Datenschutz-Management

[TODO: z.B. Datenschutzbeauftragter, Richtlinien, Schulungen]

36.14.10 10. Incident Response

[TODO: z.B. Incident-Response-Plan, Meldewege, Eskalation]

Hinweis: Dieses Template ist eine Vorlage und muss an die spezifischen Anforderungen angepasst werden. Eine rechtliche Prüfung wird empfohlen.

ewpage

Chapter 37

Anhang: Begriffe und Abkürzungen

Dokument-ID: 0730
Owner: {{ meta.owner }}
Version: {{ meta.version }}
Status: Referenz
Klassifizierung: Öffentlich
Letzte Aktualisierung: {{ meta.date }}

37.1 Abkürzungen

Abkürzung	Bedeutung	Englisch
DSGVO	Datenschutz-Grundverordnung	GDPR (General Data Protection Regulation)
GDPR	General Data Protection Regulation	Datenschutz-Grundverordnung
DSB	Datenschutzbeauftragter	DPO (Data Protection Officer)
DPO	Data Protection Officer	Datenschutzbeauftragter
DSFA	Datenschutz-Folgenabschätzung	DPIA (Data Protection Impact Assessment)
DPIA	Data Protection Impact Assessment	Datenschutz-Folgenabschätzung
AVV	Auftragsverarbeitungsvertrag	DPA (Data Processing Agreement)
DPA	Data Processing Agreement	Auftragsverarbeitungsvertrag
TOM	Technische und organisatorische Maßnahmen	TOMs (Technical and Organizational Measures)
SCC	Standard Contractual Clauses	Standardvertragsklauseln
BCR	Binding Corporate Rules	Verbindliche interne Datenschutzvorschriften

Abkürzung	Bedeutung	Englisch
PbD	Privacy by Design	Datenschutz durch Technikgestaltung
PbD	Privacy by Default	Datenschutz durch datenschutzfreundliche Voreinstellungen
EuGH	Europäischer Gerichtshof	CJEU (Court of Justice of the European Union)
EDSA	Europäischer Datenschutzausschuss	EDPB (European Data Protection Board)
EDPB	European Data Protection Board	Europäischer Datenschutzausschuss

---

37.2 Begriffsdefinitionen (Art. 4 DSGVO)

37.2.1 Personenbezogene Daten (Art. 4 Nr. 1)

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine identifizierbare Person ist eine Person, die direkt oder indirekt identifiziert werden kann.

Beispiele: - Name, Adresse, Geburtsdatum - E-Mail-Adresse, Telefonnummer - IP-Adresse, Cookie-ID - Standortdaten, Nutzungsdaten - Foto, Video, Audioaufnahme

37.2.2 Verarbeitung (Art. 4 Nr. 2)

Jeden Vorgang im Zusammenhang mit personenbezogenen Daten, wie: - Erhebung, Erfassung, Organisation - Ordnen, Speicherung, Anpassung, Veränderung - Auslesen, Abfragen, Verwendung - Offenlegung, Übermittlung, Verbreitung - Abgleich, Verknüpfung, Einschränkung - Löschen, Vernichtung

37.2.3 Einschränkung der Verarbeitung (Art. 4 Nr. 3)

Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

37.2.4 Profiling (Art. 4 Nr. 4)

Jede Art der automatisierten Verarbeitung zur Bewertung persönlicher Aspekte, insbesondere zur Analyse oder Prognose von: - Arbeitsleistung - Wirtschaftliche Lage - Gesundheit - Persönliche Vorlieben - Interessen - Zuverlässigkeit - Verhalten - Aufenthaltsort - Ortswechsel

37.2.5 Pseudonymisierung (Art. 4 Nr. 5)

Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können.

Beispiel: Ersetzung von Namen durch Pseudonyme (IDs), wobei die Zuordnungstabelle separat gespeichert wird.

37.2.6 Dateisystem (Art. 4 Nr. 6)

Jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind.

37.2.7 Verantwortlicher (Art. 4 Nr. 7)

Die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet.

Beispiel: Unternehmen, das Kundendaten verarbeitet

37.2.8 Auftragsverarbeiter (Art. 4 Nr. 8)

Eine natürliche oder juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Beispiele: - Cloud-Provider - IT-Dienstleister - Lohnbuchhaltungsdienstleister - Marketing-Agentur

37.2.9 Empfänger (Art. 4 Nr. 9)

Eine natürliche oder juristische Person, der personenbezogene Daten offengelegt werden.

37.2.10 Dritter (Art. 4 Nr. 10)

Eine natürliche oder juristische Person außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung befugt sind, die Daten zu verarbeiten.

37.2.11 Einwilligung (Art. 4 Nr. 11)

Jede freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung.

Anforderungen: - Freiwillig - Informiert - Spezifisch - Unmissverständlich - Widerrufbar

37.2.12 Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12)

Eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt.

Kategorien: - Vertraulichkeitsverletzung (Confidentiality Breach) - Integritätsverletzung (Integrity Breach) - Verfügbarkeitsverletzung (Availability Breach)

37.2.13 Genetische Daten (Art. 4 Nr. 13)

Personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person.

37.2.14 Biometrische Daten (Art. 4 Nr. 14)

Personenbezogene Daten, die sich aus einer spezifischen technischen Verarbeitung zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person ergeben und die Identifizierung dieser Person ermöglichen.

Beispiele: - Fingerabdrücke - Gesichtserkennung - Iris-Scan - Stimmerkennung

37.2.15 Gesundheitsdaten (Art. 4 Nr. 15)

Personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und Informationen über deren Gesundheitszustand geben.

Beispiele: - Diagnosen - Behandlungen - Medikamente - Laborwerte - Krankengeschichte

37.2.16 Hauptniederlassung (Art. 4 Nr. 16)

Bei einem Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat der Ort seiner Hauptverwaltung in der Union.

37.2.17 Vertreter (Art. 4 Nr. 17)

Eine in der Union niedergelassene natürliche oder juristische Person, die von einem nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter schriftlich bestellt wurde.

37.2.18 Unternehmen (Art. 4 Nr. 18)

Eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt.

37.2.19 Unternehmensgruppe (Art. 4 Nr. 19)

Eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.

37.2.20 Verbindliche interne Datenschutzvorschriften (Art. 4 Nr. 20)

Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein Verantwortlicher oder Auftragsverarbeiter verpflichtet.

37.2.21 Aufsichtsbehörde (Art. 4 Nr. 21)

Eine von einem Mitgliedstaat eingerichtete unabhängige staatliche Stelle zur Überwachung der Anwendung der DSGVO.

Deutschland: Bundes- und Landesbeauftragte für Datenschutz

37.2.22 Betroffene Aufsichtsbehörde (Art. 4 Nr. 22)

Eine Aufsichtsbehörde, die von der Verarbeitung betroffen ist, weil: - Der Verantwortliche oder Auftragsverarbeiter im Hoheitsgebiet ihres Mitgliedstaats niedergelassen ist - Betroffene Personen in ihrem Mitgliedstaat erheblich beeinträchtigt werden - Eine Beschwerde bei ihr eingereicht wurde

37.2.23 Grenzüberschreitende Verarbeitung (Art. 4 Nr. 23)

Verarbeitung, die: - Im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder Auftragsverarbeiters in mehr als einem Mitgliedstaat stattfindet, oder - Erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat

37.2.24 Maßgeblicher und begründeter Einspruch (Art. 4 Nr. 24)

Ein Einspruch einer betroffenen Aufsichtsbehörde gegen einen Beschlussentwurf, aus dem hervorgeht, ob ein Verstoß gegen die DSGVO vorliegt.

37.2.25 Dienst der Informationsgesellschaft (Art. 4 Nr. 25)

Eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535.

Beispiele: - Online-Shops - Soziale Netzwerke - Cloud-Dienste - Streaming-Dienste

37.2.26 Internationale Organisation (Art. 4 Nr. 26)

Eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft geschaffen wurde.

37.3 Weitere wichtige Begriffe

37.3.1 Besondere Kategorien personenbezogener Daten (Art. 9)

Sensible Daten, die besonderen Schutz genießen: - Rassische und ethnische Herkunft - Politische Meinungen - Religiöse oder weltanschauliche Überzeugungen - Gewerkschaftszugehörigkeit - Genetische Daten - Biometrische Daten zur eindeutigen Identifizierung - Gesundheitsdaten - Daten zum Sexualleben oder der sexuellen Orientierung

37.3.2 Anonymisierung

Irreversible Entfernung des Personenbezugs, sodass die Daten nicht mehr einer Person zugeordnet werden können.

Unterschied zur Pseudonymisierung: Anonymisierung ist irreversibel, Pseudonymisierung ist reversibel.

37.3.3 Datenschutz durch Technikgestaltung (Privacy by Design)

Implementierung von Datenschutzprinzipien bereits bei der Entwicklung von Systemen und Prozessen.

37.3.4 Datenschutz durch datenschutzfreundliche Voreinstellungen (Privacy by Default)

Standardmäßige Einstellungen, die den Datenschutz maximieren (z.B. nur notwendige Daten werden verarbeitet).

37.3.5 Drittland

Ein Land außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums.

37.3.6 Angemessenheitsbeschluss

Entscheidung der EU-Kommission, dass ein Drittland ein angemessenes Datenschutzniveau bietet.

Beispiele: Schweiz, Vereinigtes Königreich (post-Brexit), Japan

37.3.7 Standardvertragsklauseln (SCC)

Von der EU-Kommission genehmigte Vertragsklauseln für Datenübermittlungen in Drittländer.

37.3.8 Rechenschaftspflicht (Accountability)

Pflicht des Verantwortlichen, die Einhaltung der DSGVO nachweisen zu können.

37.3.9 Datenschutz-Folgenabschätzung (DSFA)

Systematische Bewertung der Risiken einer Verarbeitung für die Rechte und Freiheiten betroffener Personen.

37.3.10 Verzeichnis von Verarbeitungstätigkeiten

Dokumentation aller Verarbeitungstätigkeiten eines Verantwortlichen oder Auftragsverarbeiters (Art. 30).

37.3.11 Betroffenenrechte

Rechte natürlicher Personen gegenüber dem Verantwortlichen: - Auskunftsrecht (Art. 15) - Berichtigungsrecht (Art. 16) - Recht auf Löschung (Art. 17) - Recht auf Einschränkung (Art. 18) - Recht auf Datenübertragbarkeit (Art. 20) - Widerspruchsrecht (Art. 21) - Recht auf Widerruf der Einwilligung (Art. 7)

37.4 Rechtsgrundlagen (Art. 6 Abs. 1)

Buchstabe	Rechtsgrundlage	Beschreibung
a	Einwilligung	Betroffene Person hat eingewilligt
b	Vertragserfüllung	Erforderlich zur Erfüllung eines Vertrags
c	Rechtliche Verpflichtung	Erforderlich zur Erfüllung einer rechtlichen Verpflichtung
d	Schutz lebenswichtiger Interessen	Erforderlich zum Schutz lebenswichtiger Interessen
e	Öffentliches Interesse	Erforderlich für Aufgabe im öffentlichen Interesse

Buchstabe	Rechtsgrundlage	Beschreibung
f	Berechtigtes Interesse	Erforderlich zur Wahrung berechtigter Interessen

---

37.5 Sanktionen und Bußgelder

37.5.1 Bußgeldkategorien

Kategorie 1 (bis zu 10 Mio. EUR oder 2% des Jahresumsatzes): - Verstöße gegen Auftragsverarbeiter-Pflichten (Art. 28-29) - Verstöße gegen Zertifizierungsstellen (Art. 42-43)

Kategorie 2 (bis zu 20 Mio. EUR oder 4% des Jahresumsatzes): - Verstöße gegen Grundsätze (Art. 5) - Verstöße gegen Rechtsgrundlagen (Art. 6) - Verstöße gegen Betroffenenrechte (Art. 12-22) - Verstöße gegen Datenübermittlung (Art. 44-49)

Hinweis: Diese Definitionen basieren auf der DSGVO und dienen als Referenz. Bei rechtlichen Fragen sollte ein Datenschutzexperte oder Rechtsanwalt konsultiert werden.

ewpage