Kompakte Checkliste zur Umsetzung der Datenschutz-Grundverordnung

(VO [EU] 2016/679)

Version: 1.0
Stand: 24. Mai 2017

Impressum: Medieninhaber, Herausgeber und Hersteller: Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at, ZVR-Zahl 061847005, Wien, https://www.privacyofficers.at/impressum

Vorwort des Vereinsvorstands

Liebe Leserin, lieber Leser,

der Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at freut sich, diese kompakte Checkliste ein Jahr vor dem Geltungsbeginn der Datenschutz-Grundverordnung (DSGVO) am 25.5.2018 zur Verfügung stellen zu können. Unser Ziel ist es, diese Umsetzungshilfe aktuell zu halten, eine Einarbeitung des (seit 12.5.2017 als Ministerialentwurf vorliegenden) Datenschutz-Anpassungsgesetzes 2018 erfolgt spätestens nach der parlamentarischen Beschlussfassung.

Besonderer Dank für die Ausarbeitung gebührt dabei unserem Arbeitskreis Datensicherheit und allen beteiligten Vereinsmitgliedern. Frei nach dem Motto „Von Mitgliedern für Mitglieder (und darüber hinaus)“ ist hier in kurzer Zeit eine übersichtliche Praxishilfe entstanden.

Die vorliegende Checkliste ist in drei Phasen unterteilt und beschreibt die wichtigsten Inhalte der DSGVO. Mit dieser Checkliste erhalten Sie einen Leitfaden, um die Herstellung der Compliance Ihrer Organisation hinsichtlich DSGVO einzuleiten und die Übersicht über das Umsetzungsprojekt zu behalten.

Wir dürfen darauf hinweisen, dass diese Checkliste nur die wichtigsten Inhalte der DSGVO in kompakter und übersichtlicher Form zusammenfasst und keinen Anspruch auf vollständige Berücksichtigung aller Bestimmungen der DSGVO bzw. der nationalen Datenschutzbestimmungen erhebt. Die in diesem Dokument verwendeten Begriffe entsprechen jenen Definitionen, wie sie in der DSGVO verwendet werden. Abkürzungen sind im Abschnitt „Abkürzungen“ definiert.

Privacyofficers.at hofft, dass die vorliegende Checkliste viele Verantwortliche und Auftragsverarbeiter bei der Umsetzung der Anforderungen der DSGVO unterstützen kann, wir haben diese daher unter eine CC BY-NC-SA 4.0-Lizenz gestellt (siehe Näheres auf Seite 18). Anregungen und konstruktive Kritik nehmen wir gerne unter office@privacyofficers.at entgegen, aktuelle Datenschutz-News finden Sie auf unserer Homepage: https://www.privacyofficers.at/.

Der Vereinsvorstand

Abkürzungen

- **BMI:** Österreichisches Bundesministerium für Inneres
- **BSI IT-Grundschutz:** Der vom deutschen Bundesamt für Sicherheit in der Informationstechnik entwickelte IT-Grundschutz ermöglicht es, notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen
- **CERT**: Ein Computer Emergency Response Team (CERT; Deutsch „Computersicherheits-Ereignis- und Reaktionsteam“) ist eine Gruppe von EDV-Sicherheitsfachleuten, die bei der Lösung von IT-Sicherheitsvorfällen als Koordinator mitwirkt bzw. sich ganz allgemein mit Computersicherheit befasst.
- **CISO:** Informationssicherheitsbeauftragter (Chief Information Security Officer)
- **DSB:** Datenschutzbeauftragter
- **DSGVO:** Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 119 vom 4.5.2016, 1–88 (LINK zum Volltext inklusive Berichtigung vom 22.11.2016)
- **DSMS:** Datenschutz-Managementsystem
- **FMA:** Finanzmarktaufsicht
- **ISMS nach ISO/IEC 27001:** Ein Informationssicherheits-Managementsystem ist eine Aufstellung von Verfahren und Regeln, um die Informationssicherheit zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Die international anerkannte Norm ISO/IEC 27001 spezifiziert die Anforderungen für Einrichtung, Umsetzung und Aufrechterhaltung eines dokumentierten ISMS.
- **ISO/IEC 31000:** Internationale Norm „*Risk Management* - Principles and Guidelines“ welche Risikomanagement in alle Unternehmensaktivitäten integriert
- **ITIL:** Die IT Infrastructure Library (ITIL) ist eine Sammlung vordefinierter Prozesse, Funktionen und Rollen, wie sie typischerweise in jeder IT-Infrastruktur mittlerer und großer Unternehmen vorkommen
- **KVP:** Kontinuierlicher Verbesserungsprozess
- **NIS-Richtlinie:** Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informations-systemen in der Union, ABl L 194 vom 19.7.2016, 1–30 (LINK zum Volltext)
- **pb Daten:** Personenbezogene Daten (siehe die Definition in Art 4 Z 1 DSGVO)
- **RTR:** Die Rundfunk- und Telekom Regulierungs-GmbH unterstützt die Kommunikationsbehörde Austria und die Telekom-Control-Kommission bei der Erfüllung ihrer Aufgaben als deren Geschäftsstelle und nimmt verschiedene Aufgaben, insbesondere in den Bereichen Telekommunikation und Medien wahr
- **TOM**: Technische und Organisatorische Maßnahme zur Erfüllung der Sicherheits- und Schutzanforderungen

Inhaltsverzeichnis

Phase 1: Vorbereitung

1.1 Management Awareness bilden und Management Commitment einholen	in Arbeit ☐ erledigt ☐
Beschreibung	Das Management soll auf das Thema Datenschutz aufmerksam gemacht werden, da Management-Support für die erfolgreiche Umsetzung der DSGVO zwingend notwendig ist.
Zielsetzung	• Bewusstsein im Management erzeugen, dass die Umsetzung der DSGVO-Inhalte vielseitigen Mehrwert wie z.B. positive Reputation, erhöhte Marktchancen usw. bietet • Haftungsrisiken im Falle von Verstößen reduzieren • Management Commitment einholen
Tätigkeiten	• Awareness-Veranstaltung mit dem Management • Skizzierung der für Datenschutz notwendigen Inhalte und Maßnahmen gemäß dieser Checkliste • Vorschlag für die Implementierung eines DSMS • Aufzeigen von Synergie-Möglichkeiten (ISMS nach ISO/IEC 27001, DSMS, NIS-Richtlinie, ITIL usw.)
Referenzen	• Art. 77, 82 und 83 DSGVO • NIS-Richtlinie • ISO/IEC 27001

1.2 Projektauftrag für Umsetzungsprojekt einholen	in Arbeit ☐ erledigt ☐
Beschreibung	Ein Projektauftrag ist Voraussetzung für den offiziellen Start eines jeden Projektes. Er kann als Vereinbarung zwischen Projektleiter und Projektauftraggeber gesehen werden. Sowohl die Zusammenarbeit als auch die klare Definition der Ziele sollte im Projektauftrag festgehalten sein.
Zielsetzung	• Schaffung einer verbindlichen Vereinbarung zwischen allen Betroffenen und Definition der Projektinhalte • Informationsgrundlage für später hinzukommende Teammitglieder schaffen
Tätigkeiten	• Ziele des Projekts festlegen • Was soll/darf NICHT passieren? (Nicht-Ziele) • Start- und Endtermin festlegen (Timeline) • Projektteam und Budget festlegen • Nicht beeinflussbare Rahmenbedingungen identifizieren • Kritische Erfolgsfaktoren identifizieren • Unterschrift Projektleiter und Projektauftraggeber
Referenzen	• Art. 24 und 25 DSGVO

1.3 Benötigte Ressourcen bereitstellen	in Arbeit ☐ erledigt ☐
Beschreibung	Die Organisation muss Ressourcen ermitteln und bereitstellen, um das DSMS aufzubauen, zu erhalten und in weiterer Folge zu optimieren.
Zielsetzung	• Der Erfolg des Projekts kann nur sichergestellt werden, wenn qualifiziertes Personal und ausreichende materielle Ressourcen zur Verfügung stehen
Tätigkeiten	• Abhängig von der Größe und Art der Organisation sind entsprechende personelle Ressourcen für die geplante Datenschutz-Organisation bereitzustellen (z.B. Datenschutzbeauftragter, Datenschutzkoordinatoren je Fachabteilung / Bereich / Gesellschaft) • Notwendigkeit externer Ressourcen abklären • Zurverfügungstellung der erforderlichen finanziellen Mittel (Budget), um die definierten Projektziele zu erreichen • Nach Abschluss des Projektes ist sicherzustellen, dass entsprechende Ressourcen auch im Anschluss an das Umsetzungsprojekt zum laufenden Betrieb des DSMS bereitstehen
Referenzen	• Art. 24 DSGVO • ISO/IEC 27001 Kapitel 5.2

1.4 Schlüsselpersonal initial schulen	in Arbeit ☐ erledigt ☐
Beschreibung	Das Schlüsselpersonal muss Schulungen in den Bereichen Datenschutz und Datensicherheit erhalten. Mit einem kompakten Überblick über die neuen Anforderungen kann sich das Schlüsselpersonal zu wichtigen Multiplikatoren für Datenschutz und Datensicherheit in der Organisation entwickeln. Gleichzeitig wird dadurch sichergestellt, dass das Schlüsselpersonal im Umsetzungsprojekt zur DSGVO selbstständig Arbeitspakete übernehmen bzw. an Arbeitspaketen mitwirken kann.
Zielsetzung	• Das Schlüsselpersonal ist in der Lage, die Bedeutung der Themen Datenschutz und Datensicherheit für die eigene Organisation zu erläutern • Das Schlüsselpersonal ist in der Lage, eine Verarbeitungstätigkeit zu dokumentieren bzw. die dazu notwendigen Informationen einzuholen
Tätigkeiten	Mögliche Schulungsinhalte: • Grundsätze und Schutzziele • Was sind pb Daten? • Was sind besonders schutzwürdige Daten (Besondere Kategorien pb Daten)? • Aufgaben und Pflichten des Schlüsselpersonals • Betroffenenrechte (Anfragen zu Auskunft usw.) • Verschwiegenheitspflichten / Datengeheimnis • Organisationsinterne Konsultationswege (Datenschutz in internen Projekten, Einführung neuer Software usw.)
Referenzen	• Art. 13, 28, 30 und 39 DSGVO

1.5 Prüfen, ob Datenschutzbeauftragter (DSB) notwendig ist	in Arbeit ☐ erledigt ☐
Beschreibung	Unter bestimmten Umständen ist die Bestellung eines DSB vorgeschrieben. Eine Organisation muss daher ermitteln, ob sie von dieser Regelung betroffen ist und einen DSB bestellen muss. Konzern- oder Unternehmensgruppen sowie öffentliche Behörden sollten zudem prüfen, ob ein DSB für die gesamte Gruppe ausreicht, oder ob mehrere DSBs bestellt werden müssen.
Zielsetzung	• Feststellung, ob überhaupt ein oder mehrere DSBs bestellt werden müssen
Tätigkeiten	Trifft eines der nachfolgenden Kriterien zu, ist ein DSB notwendig und zu bestellen: • Verarbeitung der Daten durch eine Behörde oder öffentliche Stelle, mit Ausnahme der Gerichte • Verarbeitung pb Daten stellt eine Kerntätigkeit der Organisation dar und/oder erfordert eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Personen • Verarbeitung Besonderer Kategorien pb Daten (z.B. Gesundheitsdaten, ethische Herkunft usw.) stellt eine Kerntätigkeit der Organisation dar
Referenzen	• Art. 9, 10 und 37 DSGVO

Phase 2: Umsetzung

2.1 Verarbeitungstätigkeiten identifizieren	in Arbeit ☐ erledigt ☐
Beschreibung	In einem ersten Schritt sollen zunächst alle Verarbeitungstätigkeiten identifiziert und zentrale Fragestellungen (Verantwortlicher, Datenarten, Datenherkunft, Datenübermittlung usw.) beantwortet werden. Anschließend können die Informationen zusammengeführt, Datenflussanalysen erstellt und die Ergebnisse ins Verfahrensverzeichnis überführt werden.
Zielsetzung	• Verarbeitungstätigkeiten identifizieren • Verarbeitungstätigkeiten dokumentieren

Tätigkeiten	1. Verarbeitungstätigkeiten identifizieren
	  ○ Applikationen
	  ○ IT-Systeme
	  ○ Dokumentenablagen (z.B. Excel-Dateien usw.)
	  ○ Physische Akte
	  ○ *Tipp:* Begriff „Verarbeitungstätigkeit“ bewusst weit fassen
	2. Erstellung einer Vorlage zur Erfassung des IST-Stands
	  ○ Soll zentrale Fragestellungen enthalten
	  ○ *Tipp:* Excel-Datei, Fragebögen oder Tool-Unterstützung
	3. Zentrale Fragestellungen je Verarbeitungstätigkeit:
	  ○ In welchen Rechtsträgern / Standorten / Abteilungen wird die Verarbeitungstätigkeit durchgeführt?
	  ○ Wer ist für die jeweilige Verarbeitungstätigkeit zuständig?
	  ○ Welche pb Daten welcher betroffenen Personen werden verarbeitet?
	  ○ Zu welchem Zweck werden die Daten verarbeitet?
	  ○ Was ist die Rechtsgrundlage (z.B. Vertragserfüllung, Einwilligungserklärung usw.)?
	  ○ Von wo kommen die Daten (Herkunft)?
	  ○ Wo gehen die Daten hin / an wen werden die Daten versendet?
	  ○ Wie lange werden die Daten benötigt / gespeichert?
	  ○ *Tipp:* „Aufräum“-Aktion:
	  ▪ Welche Verarbeitungstätigkeiten werden nicht mehr benötigt?
	  ▪ Welche Daten können gelöscht werden?
	4. Involvierte Personen:
	  ○ Ansprechpartner für das Thema Datenschutz in den einzelnen Standorten / Fachabteilungen
	  ○ DSB, IT-Leiter, CISO, Rechtsabteilung usw.
	  ○ Optional: Externe Berater (Datenschutz-Experten, IT- / Informationssicherheitsexperten)
	5. Rückmeldung der erhobenen Informationen an das Projektkernteam
	6. Zusammenführung aller erhaltenen Informationen durch das Projektkernteam
	  ○ Abklärung etwaiger Rückfragen / Ausräumen von Unklarheiten
	7. Erstellung Datenflussanalyse je Verarbeitungstätigkeit durch das Projektkernteam
	  ○ Anschließend: Überführung der Informationen in das Verfahrensverzeichnis

Referenzen	• Art. 2, 3 und 30 DSGVO

2.2 Verfahrensverzeichnis erstellen	in Arbeit ☐ erledigt ☐
Beschreibung	Das Verfahrensverzeichnis ist ein Verzeichnis aller Verarbeitungstätigkeiten. Die Pflicht zur Führung eines Verfahrensverzeichnisses trifft den Verantwortlichen, wie auch – mit geringerem Umfang – den Auftragsverarbeiter. Die Führung des Verfahrensverzeichnisses hat schriftlich zu erfolgen, wobei ein elektronisches Format benutzt werden kann. Das Verfahrensverzeichnis ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen. Anhand des Verfahrensverzeichnisses ist es für die Aufsichtsbehörde möglich, die durchgeführten Verarbeitungstätigkeiten zu kontrollieren.
Zielsetzung	• Erfassung aller Verarbeitungstätigkeiten mit pb Daten in einer Organisation, Behörde oder öffentlichen Stelle, falls die Pflicht zur Führung dieses Verfahrensverzeichnisses besteht

Tätigkeiten	• Details der Verarbeitungstätigkeiten erheben in der Rolle des Verantwortlichen:
	  ○ Name und Kontaktdaten des Verantwortlichen bzw. des DSB
	  ○ Zweck der Verarbeitungstätigkeit
	  ○ Kategorien betroffener Personen und Kategorien pb Daten (z.B. Mitarbeiter, Kunde, Lieferanten, Rechnungsdaten, Adressdaten usw.)
	  ○ Kategorien von Empfängern, gegenüber denen die pb Daten offengelegt worden sind oder

	noch offengelegt werden (z.B. Sozialversicherung, Finanzamt, Steuerberater usw.) ○ Gegebenenfalls Übermittlungen von pb Daten an Empfänger im Drittland (z.B. USA) oder an eine internationale Organisation, einschließlich der Angaben des betreffenden Drittlands oder der betreffenden internationalen Organisation (inklusive der Dokumentation geeigneter Garantien) ○ Sofern möglich: Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien ○ Sofern möglich: Allgemeine Beschreibung der TOMs (hier eignen sich auch gut Verweise auf interne Sicherheitsrichtlinien aus einem ISMS) ○ Sinnvoll: Angabe der Rechtsgrundlage (z.B. Einwilligungserklärung) für den Zweck der Verarbeitungstätigkeit • Details der Verarbeitungstätigkeiten erheben in der Rolle des Auftragsverarbeiters: ○ Name und Kontaktdaten des Auftragsverarbeiters bzw. des DSB ○ Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden ▪ Gegebenenfalls Übermittlungen von pb Daten an Empfänger im Drittland (z.B. USA) oder an eine internationale Organisation, einschließlich der Angaben des betreffenden Drittlands oder der betreffenden internationalen Organisation (inklusive der Dokumentation geeigneter Garantien) ▪ Sofern möglich: allgemeine Beschreibung der TOMs (hier eignen sich auch gut Verweise auf interne Sicherheitsrichtlinien aus einem ISMS)
Referenzen	• Art. 30 und 31 DSGVO • Erwägungsgründe 13, 75, 76, 82 und 89

2.3 Risikoanalyse durchführen	**in Arbeit ☐ erledigt ☐**
Beschreibung	In einem ersten Schritt soll eine Risikobewertung für die identifizierten Risiken der Verarbeitungstätigkeiten durchgeführt werden (Abschätzung Eintrittswahrscheinlichkeiten und Auswirkungen). Wenn aus Sicht der betroffenen Personen voraussichtlich ein hohes Risiko besteht, ist eine Datenschutz-Folgenabschätzung durchzuführen. Für bestimmte Verarbeitungstätigkeiten wird die Aufsichtsbehörde eine Liste führen, für die in jedem Fall eine Datenschutz-Folgenabschätzung notwendig sein wird. Daneben kann es auch eine Liste mit Ausnahmen geben.
Zielsetzung	• Auswirkungen und Risiken der Verarbeitungstätigkeiten für die Rechte der Betroffenen analysieren
Tätigkeiten	• Phase 1: Vorprüfungsphase ○ Prüfung des eigenen Verfahrensverzeichnisses gegen die Listen der Aufsichtsbehörde, ob verpflichtend eine Datenschutz-Folgenabschätzung notwendig ist ○ Prüfung, ob überhaupt die Voraussetzungen für die Durchführung einer verpflichtenden Datenschutz-Folgenabschätzung vorliegen (nicht abschließender Katalog des Art. 35 Abs. 3) ▪ Wird bei der beabsichtigten Verarbeitungstätigkeit neue Technologie verwendet oder besteht aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitungstätigkeit voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen? ▪ Wird eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen (Profiling) durchgeführt, die in weiterer Folge als Grundlage für Entscheidungen herangezogen werden soll, die für natürliche Personen Rechtswirkungen entfalten könnte (z.B. zur Frage der Kreditvergabe)? ▪ Werden in umfangreicher Art und Weise Besondere Kategorien pb Daten oder Daten über strafrechtliche Verurteilungen und Straftaten selbst verarbeitet? ▪ Erfolgt bei der Verarbeitungstätigkeit eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (z.B. Videoüberwachungen)? • Phase 2: Bewertungsphase ○ Risikobewertung je Verarbeitungstätigkeit durchführen ▪ Eintrittswahrscheinlichkeit ▪ Auswirkung / Schaden • Best-Practice: ISO 31000, ISO 29134, BSI IT-Grundschutz usw.
Referenzen	• Art. 35 DSGVO • Erwägungsgründe 84, 89, 90, 91, 92 und 93

2.4 Einhaltung der Datenschutz-Grundsätze sicherstellen	in Arbeit ☐ erledigt ☐
Beschreibung	Für sämtliche Verarbeitungstätigkeiten ist die Einhaltung der Datenschutz-Grundsätze zu gewährleisten, z.B. durch das Stellen von Kontrollfragen.
Zielsetzung	• Sicherstellung und Dokumentation der Einhaltung der Datenschutz-Grundsätze

Tätigkeiten	• Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
	  ○ Überprüfen der Rechtsgrundlage (z.B. Vertrag mit Kunden, Einwilligungserklärung, Einhaltung von Gesetzen)
	  ○ Kontrollfrage Rechtmäßigkeit: Wurde überprüft, ob diese pb Daten verarbeitet werden dürfen?
	  ○ Kontrollfrage Transparenz: Kann der betroffenen Person klar und verständlich erklärt werden, wie und welche pb Daten verarbeitet werden?
	• Datenminimierung und Zweckbindung
	  ○ Überprüfen, dass nur tatsächlich notwendige pb Daten für einen konkreten Zweck verarbeitet werden (z.B. Drehkreuz anstatt Videoüberwachung für Besucherstromanalyse)
	  ○ *Kontrollfrage Zweckbindung:* Wozu werden diese pb Daten verwendet?
	  ○ *Kontrollfrage Datenminimierung:* Werden tatsächlich alle diese pb Daten benötigt oder kann der gleiche Zwecke auch mit weniger bzw. ohne pb Daten erreicht werden?
	• Speicherbegrenzung
	  ○ Überprüfung bestehender gesetzlicher bzw. vertraglicher Aufbewahrungspflichten (z.B. Systeme so konfigurieren, dass nicht mehr benötigte Daten automatisch gelöscht werden)
	  ○ *Kontrollfrage:* Wie lange werden diese pb Daten benötigt?
	• Richtigkeit, Integrität, Vertraulichkeit und Verfügbarkeit
	  ○ Schutz der Daten vor Verlust bzw. Vernichtung (z.B. Backup), Veränderung (z.B. Checksummen) und unbefugter Zugriff bzw. Offenlegung (z.B. Berechtigungskonzept)
	  ○ Sicherstellen, dass benötigte Daten zur Verfügung stehen (z.B. durch redundante Systeme in zwei Serverräumen)
	  ○ *Kontrollfrage:* Wie wurde sichergestellt, dass diese pb Daten sachlich richtig, verfügbar und ausreichend geschützt sind?
	• Rechenschaftspflicht
	  ○ Dokumentation der Einhaltung der Datenschutz-Grundsätze
	  ○ *Kontrollfrage:* Wie wird die Einhaltung der Datenschutz-Grundsätze dokumentiert?

Referenzen	• Art. 5 DSGVO

2.5 Datensicherheitsmaßnahmen (TOMs) umsetzen	in Arbeit ☐ erledigt ☐
Beschreibung	Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen (TOMs) zu treffen, und zwar abhängig vom • Stand der Technik, • den Implementierungskosten, • dem Umfang, der Umstände und der Zwecke der Verarbeitung sowie • der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Der Stand der Technik wird üblicherweise durch (inter-)national anerkannte Normen (z.B. ISO/IEC 27001:2013, BSI IT-Grundschutz usw.) repräsentiert. Diese Vorgaben sind auf die Gegebenheiten der eigenen Organisation anzupassen.
Zielsetzung	• Sicherstellung geeigneter TOMs • Einhaltung vom Stand der Technik

Tätigkeiten	Welche TOMs sind umzusetzen? (gem. Controls der ISO/IEC 27002)
	• Zentrale Informationssicherheitsvorgaben (Annex 5)
	  ○ IT-Sicherheits- bzw. Benutzerrichtlinie erstellen (z.B. Sicherheitsrichtlinie, Datenschutz-Policy)
	• Organisation der Informationssicherheit (Annex 6)
	  ○ Rollen und Verantwortlichkeiten definieren (z.B. CISO)
	• Personalsicherheit (Annex 7)
	  ○ Prozesse für Eintritt, Teamwechsel und Austritt erstellen (z.B. Checklisten für Personalaustritt)
	• Verwaltung von Werten (Annex 8)
	  ○ Zuständigkeiten und Regelungen für die Rückgabe von Werten definieren (z.B. Geräte, Software, Berechtigungen, Schlüssel)
	  ○ Klassifizierung von Informationen (z.B. öffentlich vs. intern)
	• Zugangssteuerung (Annex 9)

	○ Regelungen für Zutritt (z.B. Schlüssel) und Zugriff (z.B. Benutzerverwaltung, Zugriff auf Systeme) definieren ○ Kennwortvorgaben erstellen (z.B. Mindestlänge, Komplexität) • Kryptografie (Annex 10) ○ Regelungen für den Umgang mit Verschlüsselung erstellen (z.B. E-Mail-Verschlüsselung) • Physische und umgebungsbezogene Sicherheit (Annex 11) ○ Sicherheitszonen definieren (z.B. Zaun oder Zutrittskontrolle für Rechenzentrum) • Betriebssicherheit (Annex 12) ○ Betriebsabläufe regeln und dokumentieren (z.B. Change Management) ○ Maßnahmen zum Schutz vor Schadsoftware ergreifen (z.B. Virenschutz) ○ Daten vor Verlust schützen (z.B. Backup) ○ Protokollierungs- und Überwachungsmechanismen einführen (z.B. Logging) ○ Regelungen zum Umgang mit Schwachstellen definieren (z.B. Einspielen von Security Patches) ○ Maßnahmen zur Installation von Software definieren (z.B. Regelung von Administratorrechten) • Kommunikationssicherheit (Annex 13) ○ Netzwerksicherheitsmaßnahmen ergreifen (z.B. Firewall, Netzwerksegmentierung, 802.1X) ○ Sichere Datenübertragung gewährleisten (z.B. Verschlüsselung von übertragenen Daten) • Anschaffung, Entwicklung und Instandhaltung von Systemen (Annex 14) ○ Trennung von Entwicklungs-, Test- und Produktivsystemen ○ Vorgaben zur sicheren Entwicklung erstellen (z.B. Verwendung von bestimmten Bibliotheken) • Lieferantenbeziehungen (Annex 15) ○ Sicherheitsvorgaben für Lieferanten erstellen und deren Einhaltung überprüfen (z.B. Fernwartungen, Vor-Ort-Services) • Handhabung von Informationssicherheitsvorfällen (Annex 16) ○ Prozess zur Behandlung von Sicherheitsvorfällen erstellen (z.B. CERT definieren) • Informationssicherheitsaspekte beim Business Continuity Management (Annex 17) ○ Regelungen definieren, dass auch im Notfall die Informationssicherheit gewährleistet ist (z.B. Einbindung CISO im Notfall) • Compliance (Annex 18) ○ Regelungen zur Einhaltung gesetzlicher und vertraglicher Anforderungen definieren Überprüfung der Einhaltung vom Stand der Technik • Ob die ergriffene Sicherheitsmaßnahme dem Stand der Technik entspricht, kann z.B. gegen die Anforderungen eines Maßnahmenkataloges des BSI IT-Grundschutzes geprüft werden ○ Beispiel: Der Maßnahmenkatalog M 2.11 „Regelung des Passwortgebrauchs“ enthält Vorgaben hinsichtlich Länge, Qualität, Komplexität usw. eines Passworts ○ Derartige Vorgaben werden vom BSI laufend aktuell gehalten und repräsentieren weitestgehend den Stand der Technik
Referenzen	• Art. 32 DSGVO • ISO/IEC 27001:2013 und Controls der ISO/IEC 27002:2013 • BSI IT-Grundschutz

2.6 Betroffenenrechte wahren	in Arbeit ☐ erledigt ☐
Beschreibung	Neben den erweiterten Pflichten des Verantwortlichen gem. Art 12, 13 und 14 DSGVO (Transparenz und Information) hat der Verantwortliche umfangreiche Rechte der Betroffenen zu beachten und die fristgerechte Erfüllung bei Geltendmachung sicherzustellen.
Zielsetzung	• Sicherstellung der Einhaltung der Verpflichtungen zur fristgerechten Erfüllung der Betroffenenrechte durch Einführung von organisatorischen, technischen und rechtlichen Maßnahmen und Prozessen

Tätigkeiten	• Recht auf Auskunft (Art. 15 DSGVO)
	  ○ Prüfung der Bereitstellung eines Fernzuganges bzw. einer Kopie der betreffenden pb Daten (Zwecke, verarbeitete Daten, Empfänger, Speicherdauer, Betroffenenrechte, Herkunft der Daten, automatisierte Entscheidungsfindung, Übermittlung in Drittländer usw.)
	• Recht auf Berichtigung (Art. 16 DSGVO)
	  ○ Richtigstellung falscher Daten
	• Recht auf Löschung bzw. Recht auf Vergessenwerden (Art. 17 DSGVO)
	  ○ Prüfung und Dokumentation allfälliger Ausnahmen
	• Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
	  ○ Prüfung und Implementierung der Markierung / Sperrung bis zur Entscheidung über die weitere Verarbeitungstätigkeit
	• Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
	  ○ Prüfung der Anwendbarkeit auf vorhandene Daten sowie Prüfung der technischen Machbarkeit und Implementierung in den Systemen
	• Recht auf Widerspruch (Art 21 DSGVO)
	• Festlegung und Dokumentation der Prozesse, insbesondere der Verantwortlichkeit
	  ○ Sicherstellung der Einhaltung der Pflichten beim Auftragsverarbeiter, sofern vorhanden

Referenzen	• Art. 15 bis 23 DSGVO • Erwägungsgründe 60 bis 73

2.7 Einwilligungsprozess einführen	in Arbeit ☐ erledigt ☐
Beschreibung	Die Rechtmäßigkeit der Verarbeitung pb Daten kann, sofern diese nicht der Erfüllung eines Vertrages oder einer rechtlichen Verpflichtung dient, insbesondere durch die Einwilligung einer natürlichen Person sichergestellt werden. Dabei sind die Vorgaben der DSGVO im Detail zu beachten.
Zielsetzung	• Die Einwilligung soll durch eine freiwillige, eindeutige Handlung erfolgen, mit der bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden pb Daten einverstanden ist • Der Verantwortliche muss nachweisen können, dass die betroffene Person ihre Einwilligung zu der Verarbeitungstätigkeit gegeben hat • Der betroffenen Person muss zur Kenntnis gebracht werden, wer der Verantwortliche ist, für welche Zwecke ihre pb Daten verarbeitet werden und dass die Einwilligung auch verweigert oder zurückgezogen werden kann
Tätigkeiten	• Eindeutiges, nachweisbares Einverständnis mit der Verarbeitung der pb Daten einholen, z.B. Ermöglichung des Anklickens eines Kästchens beim Besuch einer Internetseite (Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit sind keine Einwilligung) • Erstellung einer Einwilligungserklärung in verständlicher Form und klarer Sprache („kein Verstecken in AGBs“) • Bei noch nicht vollendetem 16. Lebensjahr (bzw. 13., 14., 15. oder 16. Lebensjahr, je nach nationaler Gesetzgebung) ist die Einwilligung des gesetzlichen Vertreters (z.B. Eltern) einzuholen ○ Sicherstellung, dass bei Widerruf der Einwilligung die Daten nicht mehr weiterverarbeitet werden
Referenzen	• Art. 7 und 8 DSGVO • Erwägungsgründe 32 und 42

2.8 Informationspflichten einführen	in Arbeit ☐ erledigt ☐
Beschreibung	Um eine faire und transparente Verarbeitung pb Daten sicherzustellen, muss der Verantwortliche den betroffenen Personen alle Informationen zur Verfügung stellen, die Art, Zweck und Umfang der Verarbeitungstätigkeit beschreiben. Dabei wird unterschieden, ob die Daten direkt beim Betroffenen erhoben werden oder auf anderem Wege zum Verantwortlichen gelangten. Der Informationspflicht muss nicht nachgekommen werden, wenn der Betroffene bereits über alle Informationen die Verarbeitung seiner Daten betreffend verfügt.
Zielsetzung	• Erstellung von präzisen, leicht zugänglichen, für Betroffene leicht verständlichen Informationen über die durchgeführte Verarbeitungstätigkeit pb Daten
Tätigkeiten	Sofern die Daten direkt beim Betroffenen erhoben werden, sollen zum Zeitpunkt der Erhebung folgende Information bereitgestellt werden: • Name und Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters und des DSB • Die Zwecke, für die die pb Daten verarbeitet werden • Die Rechtsgrundlage, auf der die Verarbeitungstätigkeit beruht • Sofern die Verarbeitungstätigkeit auf dem Interesse des Verantwortlichen beruht, die Darstellung dieses Interesses • Gegebenenfalls die Empfänger der Daten • Gegebenenfalls die Auskunft über die Übermittlung der Daten in ein Drittland und die Darstellung der Rechtsgrundlage hierfür • Die Speicherdauer der Daten bzw. die Kriterien für die Festlegung der Dauer • Einen Hinweis auf die Rechte des Betroffenen auf Auskunft, Berichtigung, Löschung, Widerspruch und Datenübertragung • Einen Hinweis auf das Beschwerderecht bei einer Aufsichtsbehörde • Bei Bestehen einer automatisierten Entscheidungsfindung, eine Beschreibung der Logik sowie der Tragweite und die angestrebte Auswirkung für den Betroffenen • Gegebenenfalls Beschreibung aller sonstigen Zwecke, für die die pb Daten zusätzlich zum eigentlichen Zweck verarbeitet werden sollen Sofern die Daten nicht direkt beim Betroffenen erhoben wurden, sollen innerhalb einer angemessenen Frist, aber spätestens nach einem Monat, obige Informationen und zusätzlich die nachfolgenden Informationen bereitgestellt werden: • Die Kategorien pb Daten, die verarbeitet werden • Die Quelle, aus der die pb Daten stammen (Herkunft der Daten) Beispiele, um der Informationspflicht nachzukommen: • Bereitstellung von Informationen im Intranet • Zurverfügungstellung eines Informationsblatts im Rahmen von Registrierungen (z.B. Webshops) • Überarbeitung der Datenschutz-Policy • Überarbeitung von Betriebsvereinbarungen
Referenzen	• Art. 12 bis 14 DSGVO • Erwägungsgründe 58, 60, 61 und 62

2.9 Auftragsverarbeiter-Rahmenbedingungen sicherstellen	in Arbeit ☐ erledigt ☐
Beschreibung	Auftragsverarbeiter ist jemand, der pb Daten im Auftrag eines Verantwortlichen verarbeitet (z.B. Cloud-Diensteanbieter, Hosting-Anbieter, Software-Provider, ausgelagerte Lohnverrechnung, Dienstleister innerhalb eines Konzerns usw.). Bei der Auswahl und Beauftragung des Auftragsverarbeiters sind bestimmte Rahmenbedingungen sicherzustellen und schriftlich zu vereinbaren.
Zielsetzung	• Auswahl eines Auftragsverarbeiters, der hinreichend Garantien bietet, dass TOMs so durchgeführt werden, dass die Verarbeitungstätigkeit im Einklang mit der DSGVO erfolgt • Schriftliche Vereinbarung aller rechtlichen Verpflichtungen, die einem Verantwortlichen durch die Zusammenarbeit mit einem Auftragsverarbeiter entstehen (durch verpflichtende Klauseln)

Tätigkeiten	• Identifikation aller Auftragsverarbeiter und Sub-Auftragsverarbeiter
	• Prüfung bestehender Verträge auf den Mindestinhalt der DSGVO und Aktualisierung derselben
	  ○ Bei Abschluss von Vereinbarungen vor dem 25.5.2018 bereits die neuen Pflichten abbilden (verhindert Neuverhandlungen ab dem 25.5.2018)
	• Sicherstellung der Einhaltung der Pflichten der Auftragsverarbeiter (z.B. Berücksichtigung Auditierungs-Recht)
	  ○ Sorgfältige Auswahl des Auftragsverarbeiters
	  ○ Regelmäßige Überprüfung, ob die rechtlichen Verpflichtungen eingehalten werden

Referenzen	• Art. 4, 28, 29 und 39 DSGVO

2.10 Privacy by Design / Privacy by Default sicherstellen	in Arbeit ☐ erledigt ☐
Beschreibung	Privacy by Design und Privacy by Default sind zwei Anforderungen, um Datenschutzgrundsätze (z.B. Datenminimierung) zu implementieren – sowohl für technische (z.B. Software) als auch organisatorische (z.B. Organisationsprozesse) Aspekte. Privacy by Design bedeutet, Datenschutzprobleme schon bei der Entwicklung neuer Technologien festzustellen und zu prüfen, und den Datenschutz von Vornherein in die Gesamtkonzeption einzubeziehen. Privacy by Default bedeutet, dass Produkte oder Dienstleistungen standardmäßig datenschutzfreundlich konfiguriert sind. Im Sinne der Rechenschaftspflicht müssen die Überlegungen und Entscheidungen dokumentiert werden.
Zielsetzung	• Implementierung geeigneter TOMs, die sicherstellen, dass die Datenschutz-Grundsätze eingehalten werden • Definition und Umsetzung einer Verarbeitung pb Daten mit dem geringsten Risiko für die betroffenen Personen
Tätigkeiten	Um eine möglichst risikoarme Verarbeitung pb Daten zu erreichen, sind z.B. folgende Schutzmaßnahmen umzusetzen (sofern anwendbar): • Menge der pb Daten minimieren • Pb Daten so früh wie möglich pseudonymisieren oder verschlüsseln • Transparenz in Bezug auf die Funktionen und die Verarbeitung pb Daten herstellen • Pb Daten so früh wie möglich löschen oder anonymisieren • Zugriffsmöglichkeiten auf pb Daten minimieren • Vorhandene Konfigurationsmöglichkeiten auf die datenschutzfreundlichsten Werte voreinstellen • Dokumentation der Bewertung der Risiken für die Betroffenen • Dokumentation der gesetzten TOMs Beispiele: • Privacy by Design: Funktionen zum Verpixeln von pb Daten auf Knopfdruck (z.B. für Fernwartungs-zugriffe, Exports usw.) • Privacy by Default: Datenschutzfreundliche Grundeinstellungen in sozialen Netzwerken
Referenzen	• Art. 25 DSGVO • Erwägungsgrund 78

2.11 Data Breach-Prozess einführen	in Arbeit ☐ erledigt ☐
Beschreibung	Es ist ein Prozess einzuführen, wie die fristgerechte Benachrichtigung bei Datenschutzverletzungen sowie die rechtzeitige Ergreifung geeigneter Gegenmaßnahmen erfolgen kann.
Zielsetzung	• Korrektes Verhalten bei Data Breach definiert • Korrekte und rechtzeitige Information an Dritte sicherstellen

Tätigkeiten	Vorbereitung Data Breach (sämtliche Tätigkeiten sind in einem ersten Schritt zu definieren, damit sie im Anlassfall rasch abgearbeitet werden können):
	• Prozessuale Abhängigkeiten und verfügbare Ressourcen identifizieren
	• Rollen und Verantwortlichkeiten festlegen
	  ○ Wer macht was wann?
	  ○ Wer muss welche Entscheidungen treffen?
	  ○ Aus welchen Rollen setzt sich das CERT zusammen?
	• Vorfall erkennen und erfassen (präventiv / reaktiv)
	  ○ Einbindung etwaiger Dritter (wie insbesondere Auftragsverarbeiter)
	• Erst-Einschätzung durchführen
	• Sofortmaßnahmen ergreifen
	• Information an den Verantwortlichen (z.B. Top Management)
	• Öffentlichkeitsarbeit sicherstellen (z.B. Einrichtung „Notfall“-Hotline)
	• Information der betroffenen Personen:
	  ○ Verfassung in klarer und einfacher Sprache
	  ○ Beschreibung der Art der Verletzung des Schutzes pb Daten
	  ○ Ungefähre Zahl der betroffenen pb Datensätze
	  ○ Namen und Kontaktdaten des DSB oder einer sonstigen Anlaufstelle für weitere Informationen
	  ○ Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes pb Daten
	  ○ Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes pb Daten
	  ○ Gegebenenfalls Beschreibung von Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
	• Information an die Aufsichtsbehörde binnen 72 Stunden
	  ○ Mindestangaben an die Aufsichtsbehörde:
	  ▪ Beschreibung der Art der Verletzung des Schutzes pb Daten, soweit möglich mit Angabe
	  • der Kategorien der betroffenen Personen,
	  • der ungefähren Zahl der betroffenen Personen,
	  • der betroffenen Kategorien der pb Datensätze und
	  • der ungefähren Zahl der betroffenen pb Datensätze
	  ▪ Name und Kontaktdaten des DSB oder einer sonstigen Anlaufstelle für weitere Informationen
	  ▪ Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes pb Daten
	  ▪ Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes pb Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
	  ▪ Dokumentation sämtlicher Verletzungen des Schutzes pb Daten einschließlich zugehöriger Fakten
	• Treffen von (Folge-)Maßnahmen
	  ○ Nachbetrachtung des Vorfalls (KVP)

Referenzen	• Art. 33 und 34 DSGVO

2.12 Die Aufgaben des Datenschutzbeauftragten (DSB)	in Arbeit ☐ erledigt ☐
Beschreibung	Der DSB stellt die Einhaltung der DSGVO sicher. Der DSB ist intern und extern erster Ansprechpartner in Datenschutzsachen, unterstützt bei Verfahrensverzeichnis und Datenschutz-Folgenabschätzung.
Zielsetzung	• Sicherstellung der Einhaltung der DSGVO • Sicherstellung eines funktionierenden DSMS • Erfüllung der Rechenschaftspflicht des Datenverarbeitenden mithilfe des DSB
Tätigkeiten	• Ansprechpartner für Aufsichtsbehörde und Betroffene • Beratung in datenschutzrechtlichen Fragen für Mitarbeiter • Beratung von Top Management, Mitarbeitern, Betroffenen • Schulung von Mitarbeitern • Überwachung bei Implementierung eines DSMS • Überwachung der und Beratung bei der Datenschutz-Folgenabschätzung • Überwachung des und Beratung beim Verfahrensverzeichnis • Berichterstattung an das Top Management ○ Durchführung von internen datenschutzrechtlichen Audits
Referenzen	• Art. 39 DSGVO

2.13 Datenschutz-Policy erstellen	in Arbeit ☐ erledigt ☐
Beschreibung	Erstellung eines High-Level-Dokuments mit verbindlichen und zentralen Datenschutzvorgaben aus Organisationssicht, welches vom Top Management in Kraft zu setzen ist.
Zielsetzung	• Festhalten und Nachweis der im Rahmen der DSGVO-Compliance etablierten Regelungen und Vorgaben • Verknüpfung der Richtlinien mit Verfahrensverzeichnis und Datenschutz-Folgenabschätzung
Tätigkeiten	• Recherche und Aktualisierung bereits bestehender Vorgaben (auch der gelebten Praxis) • Einbindung der erforderlichen Personen mit notwendigem Spezialwissen • Festlegung der Form, Anwendbarkeit und Kundmachung / Verfügbarkeit der Datenschutz-Policy • Planung und Organisation der Erstellung der Datenschutz-Policy • Gegebenenfalls Abgleich mit verfügbaren Mustern, Verhaltensregeln bzw. verbindlichen internen Datenschutzvorschriften ○ Einholung internes bzw. externes Feedback (rechtlicher und / oder technischer Natur)
Referenzen	• Art 5, 32, 39, 40, 42 und 47 DSGVO

2.14 Mitarbeiter schulen	in Arbeit ☐ erledigt ☐
Beschreibung	Schulung aller Mitarbeiter, die mit pb Daten zu tun haben, auf • das Datenschutzkonzept und die DSGVO, • wichtige Bestimmungen in der Organisation, • gesetzliche Bestimmungen, welche Mitarbeiter direkt betreffen sowie • die Konsequenzen bei Nichtbeachtung
Zielsetzung	• Mitarbeiter sollen sich bewusst sein, dass pb Daten schutzwürdig und auch Informationssicherheits-Aspekte zu berücksichtigen sind • Mitarbeiter sollen verstehen, was genau pb Daten sind, wo sie damit zu tun haben und was sie tun müssen / dürfen / nicht dürfen • Mitarbeiter sollen die Betroffenenrechte verstehen, sodass sie die Auswirkung auf ihre tägliche Arbeit und auch ihre Verantwortung erkennen • Permanente Wissens-Vermittlung durch laufende Awareness-Trainings

Tätigkeiten	• Mitarbeiter sollen eine Basis-Schulung für Datenschutz, aber auch für Informationssicherheit erhalten, wo die Verschränkung der Themen, auch in der betrieblichen Praxis dargestellt wird (z.B. welche Maßnahmen hinsichtlich Datenschutz und Informationssicherheit gibt es in dieser Organisation usw.)
	• Beispiele für Schulungsformen:
	  ○ Präsenz-Schulung, eLearning, Workshop usw.
	• Dokumentation der Schulung (z.B. Unterschriftenliste)
	  ○ Sicherstellung regelmäßiger Schulungen

Referenzen	• Art. 39 und 47 DSGVO

2.15 Datenübermittlung (EU / international)	in Arbeit ☐ erledigt ☐
Beschreibung	Pb Daten dürfen nur dann in Drittstaaten außerhalb der EU ohne angemessenes Schutzniveau übermittelt werden, wenn durch entsprechende Prozesse und Mechanismen sichergestellt ist, dass die Anforderungen der DSGVO eingehalten werden.
Zielsetzung	• Sicherstellung der Einhaltung der Rechtmäßigkeit bei der Übermittlung von pb Daten in Drittländer • Einführung von Prozessen bei geplanten Datenübermittlungen mit internationalem Bezug

Tätigkeiten	• Prüfung vorhandener Datenflüsse in Drittstaaten außerhalb der EU
	• Prüfung von Erlaubnistatbeständen gemäß DSGVO, insbesondere
	  ○ Angemessenheitsbeschluss (Art. 45)
	  ○ Geeignete Garantien prüfen oder bestehende anpassen (Art. 46 und 47) (z.B. Binding Corporate Rules, Standardvertragsklauseln der Aufsichtsbehörden, Verhaltensregeln, Zertifizierungsmechanismen)
	  ○ Prüfen von Ausnahmen für bestimmte Fälle (Art. 49), insbesondere: Einwilligung der betroffenen Person, Vertrag, wichtiges öffentliches Interesse, Rechtsansprüche, lebenswichtige Interessen, Übermittlung aus Register
	  ○ Implementierung von Prozessen zur Sicherstellung, dass bei zukünftigen Verarbeitungstätigkeiten die Übermittlung von pb Daten in Drittländer entsprechend berücksichtigt und geregelt wird

Referenzen	• Art. 44 bis 49 DSGVO • Erwägungsgründe 101 bis 115

Phase 3: Laufende Tätigkeiten

3.1 Verfahrensverzeichnis aktualisieren	in Arbeit ☐ erledigt ☐
Beschreibung	Das Verfahrensverzeichnis ist nach der erstmaligen Erstellung auf Basis einer umfassenden Datenerhebung laufend – jedoch zumindest einmal jährlich – zu aktualisieren.
Zielsetzung	• Sicherstellung, dass das Verfahrensverzeichnis stets aktuell ist • Sicherstellung, dass neue Verarbeitungstätigkeiten im Verfahrensverzeichnis aufgenommen werden

Tätigkeiten	• Überprüfung der Zuständigkeit für das Verfahrensverzeichnis
	• Überprüfung von Zuständigkeiten für die jeweiligen Verarbeitungstätigkeiten in der Organisation
	• Festlegung eines Zeitplans zur regelmäßigen Überprüfung des Verfahrensverzeichnisses
	• Sicherstellung der Berichtslinien, damit der DSB rechtzeitig bei Änderungen informiert wird über
	  ○ weitere / andere Datenarten
	  ○ weitere / andere Betroffene
	  ○ Zweckänderung bzw –erweiterung
	  ○ Hinzutreten von Empfängern
	  ○ veränderte Speicher- bzw. Löschfristen
	  ○ Änderungen von verantwortlichen Rollen (z.B. DSB)
	  ○ Anpassung der TOMs oder geeigneter Garantien
	  ○ Anpassung der zugrundeliegenden Dokumente (z.B. Einwilligungserklärung, Verträge, Betriebsvereinbarungen usw.)
	• Überprüfung der Aktualität der Risikobewertung bzw. gegebenenfalls Durchführung einer neuen Datenschutz-Folgenabschätzung
	• Neue Verarbeitungstätigkeiten in das Verfahrensverzeichnis aufnehmen bzw. nicht mehr vorhandene Verarbeitungstätigkeiten aus dem Verfahrensverzeichnis entfernen
	  ○ Regelmäßige Vorlage des Verfahrensverzeichnisses an das Top Management

Referenzen	• Art. 30 DSGVO

3.2 Audits durchführen	in Arbeit ☐ erledigt ☐
Beschreibung	Ähnlich wie bei anderen Managementsystemen ist auch die Wirksamkeit und Effizienz eines DSMS regelmäßig zu prüfen. Das inkludiert die Durchführung regelmäßiger interner bzw. externer Audits zur Überwachung sowie die Ableitung entsprechender Maßnahmen zur kontinuierlichen Verbesserung des DSMS. Beispielsweise können auch bestehende Managementsysteme (z.B. ISMS nach ISO/IEC 27001) mit dem DSMS zusammengeführt werden.
Zielsetzung	• Aufrechterhaltung und Verbesserung der Wirksamkeit des DSMS

Tätigkeiten	• Planung der regelmäßigen Audits
	  ○ Festlegung des jeweiligen Scopes
	  ○ Vereinbarung und Planung der Interviews
	  ○ Anfrage der zu prüfenden Dokumente
	• Beispielhafte Durchführung des Datenschutzaudits
	  ○ Review des Verfahrensverzeichnisses, der Datenschutz-Policy, der Prozessergebnisse und anderer relevanter Dokumente
	  ○ Durchführung der Interviews
	  ○ Gegebenenfalls Durchführung spezifischer Audits von Systemen und dem jeweiligen Datenfluss
	• Anfertigen des Berichtes
	  ○ Beschreibung identifizierte Abweichungen im DSMS
	  ○ Ableitung von Maßnahmen zum Umgang mit den identifizierten Abweichungen
	• Bericht an das Top Management
	  ○ Bericht des Status und der Verbesserungsmaßnahmen
	  ○ Schaffung bzw. Erneuerung von Awareness

Referenzen	• Art. 37 DSGVO • ISO/IEC 27001 Kapitel 9.2

3.3 Kontakt mit Behörden und betroffenen Personen pflegen	in Arbeit ☐ erledigt ☐
Beschreibung	Der Kontakt mit Behörden und betroffenen Personen sollte vorsorglich aufgebaut und gepflegt werden, um im Anlassfall entsprechende Kommunikationskanäle zur Verfügung zu haben.
Zielsetzung	• Pflege der Kontakte sowie wertschätzender Umgang mit Aufsichtsbehörde und betroffener Personen • Erwartungen sowohl der Behörden als auch der Kunden und Mitarbeiter nach transparenter und sicherer Handhabung von Daten erfüllen • Die betroffene Person hat das Recht, vom Verantwortlichen eine Bestätigung darüber zu verlangen, ob und welche pb Daten verarbeitet werden

Tätigkeiten	• Erstellung Übersicht interessierte Parteien (z.B. Stakeholder usw.)
	  ○ Aufsichtsbehörde
	  ○ Andere Behörden (z.B. NIS, RTR, BMI, FMA, verschiedene CERTs)
	  ○ Betroffene Personenkreise
	  ○ Öffentlichkeit (z.B. Medien usw.)
	  ○ Soziale Netzwerke

Referenzen	• Art. 4, 15, 51 und 57 DSGVO

3.4 KVP des Datenschutz-Managementsystems (DSMS) sicherstellen	in Arbeit ☐ erledigt ☐
Beschreibung	Fortlaufende Verbesserung der Eignung, Angemessenheit und Wirksamkeit des DSMS sowie Miteinbeziehung von rechtlichen Änderungen (z.B. Urteile, Verordnungen usw.).
Zielsetzung	• Sicherstellung der andauernden Gesetzeskonformität durch regelmäßige Anpassungen des DSMS

Tätigkeiten	• Erkennung und Behebung von Nicht-Konformitäten
	• Dokumentation der Nicht-Konformitäten sowie der Korrekturmaßnahmen (kann z.B. auch per Mail oder in einem Wiki erfolgen)
	• Fortlaufende Evaluierung bzw. Verbesserung von …
	  ○ TOMs / Stand der Technik / Bedrohungslage
	  ○ Mitarbeiter Awareness
	  ○ Datenschutz-Policy
	  ○ datenschutzrelevanten Prozessen (z.B. Auskunft, Einwilligung usw.)
	  ○ Verträgen (z.B. mit Auftragsverarbeitern, SLAs, Standardvertragsklauseln)
	  ○ internen bzw. externen Audits

Referenzen	• ISO/IEC 27001:2013 Kap. 10