# Datenschutz-Auditplan



## 1 Allgemeine Datenschutzanforderungen

- Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowie besonderer personenbezogener Daten
- Übermittlung personenbezogener Daten ins Ausland
- Verarbeitungsverzeichnis
- Meldepflichtige Verfahren, automatisierte Abrufverfahren
- Vertragsgestaltung mit Dritten (z.B. Auftragsdatenverarbeitungen, Fernwartungen durch externe Dienstleister)
- Belehrung, Verpflichtung und Schulung von Mitarbeitern
- Rechte von Betroffenen, (z.B. Auskunft, Löschung, Datenübertragbarkeit etc.)
- Prinzip der Datenminimierung
- Beschwerdemanagement Datenschutz, Einbindung und Unterrichtung des externen Datenschutzbeauftragten

## 1.1 Unternehmenswebsite

- Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten
- Einhaltung Informationspflichten (Information der Nutzer zu Cookies und Analysetools)
- Darstellung und Inhalt von Datenschutzinformationen
- Newsletter, E-Mailkommunikation
- Maßnahmen zur Datensicherheit

## 2 Allgemeine technische und organisatorische Maßnahmen zum Datenschutz ("TOM"): Zutrittskontrolle

**Ziel:** Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren.

- Festlegung der zutrittsberechtigten Personen
- Zutrittskontrolle mittels Karten oder Schlüssel
- Zutritt von Fremdpersonal, Dienstleistern und Besuchern
- Gestaltung des Außengeländes, Zutrittskontrolle von Sicherheitsbereichen
- Installation technischer Sicherungsanlagen (z.B. Einbruchmeldeanlagen, Alarmanlagen), Einbruchssicherungen
- Überwachung außerhalb der Betriebszeit (z.B. Wachpersonal, Alarmanlagen)
- Überwachung öffentlich zugänglicher Räume (Videoüberwachung)

## 3 TOM: Zutrittskontrolle

**Ziel:** Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

- Identifikation zugangsberechtigter Personen
- Maßnahmen zur System- und Netzwerksicherung gegen unbefugte Zugriffe von außen
- Sicherung von Bildschirmarbeitsplätzen
- Vergabe von Benutzerkennungen und Passwörtern

## 4 TOM: Zugriffskontrolle

**Ziel:** Die zur Benutzung eines Datenverarbeitungssystems Berechtigten können ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen und können personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt lesen, kopieren, verändern oder entfernen.

- Benutzerberechtigungskonzepte
- Vergabe und Entzug von Berechtigungen
- Lagerung von Datenträgern
- Löschung und Sperrung personenbezogener Daten
- Vernichtung personenbezogener Daten, Entsorgung von Datenträgern

## 5 TOM: Weitergabekontrolle

**Ziel:** Gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Elektronische Übertragung personenbezogener Daten
- Dokumentation der Abruf- und Übermittlungsprogramme
- Transport personenbezogener Daten
- Speicherung personenbezogener Daten auf optischen oder elektronischen Datenträgern (CD / DVD / USB / HDD)
- Empfänger elektronisch übertragener personenbezogener Daten

## 6 TOM: Eingabekontrolle

**Ziel:** Gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Festlegung und Protokollierung von Eingaben
- Auswertung und Überwachung von Eingaben

## 7 TOM: Auftragskontrolle

**Ziel:** Im Auftrag verarbeitete personenbezogene Daten dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

- Auswahl von Auftragnehmern
- Auftragserteilung
- Weisungsgebundene Verarbeitung und Nutzung personenbezogener Daten
- Festlegung technischer und organisatorischer Maßnahmen
- Überwachung von Auftragnehmern

## 8 TOM: Verfügbarkeitskontrolle

**Ziel:** Schutz personenbezogener Daten gegen zufällige Zerstörung oder.

- Sicherungskonzepte, Maßnahmen zur Datensicherung
- Dienstanweisungen, Sicherheitsrichtlinien
- Wiederherstellung personenbezogener Daten im Schadensfall
- Brandschutzmaßnahmen

## 9 TOM: Trennungskontrolle

**Ziel:** Getrennte Verarbeitung zu unterschiedlichen Zwecken erhobener Daten

- Organisatorische Trennungskontrolle
- Technische Trennungskontrolle
- Dokumentation der Datenerhebungszwecke

## 10 TOM: Marketing / Vertrieb

**Ziel:** Erfüllung der gesetzlichen Vorgaben für die Verarbeitung von Kundendaten.

- Maßnahmen zur Neukundengewinnung und Bestandskundenbindung (Werbung)
- Einwilligungen gem. UWG
- Informationspflichten Seitens des werbenden Unternehmens
- Social Media

## 11 Erweiterte technische und organisatorische Maßnahmen für Sicherheitsbereiche und personenbezogene Daten höherer Schutzstufen: Personalwesen

- Maßnahmen zur Überprüfung höherer Schutzstufen
- Risikobetrachtung der Verarbeitungen und ggf. Durchführung einer Datenschutzfolgeabschätzung.

**Im Datenschutz-Auditbericht sind die Bewertungen wie folgt vorzunehmen:**

✓ Alle geprüften Maßnahmen waren zum Zeitpunkt des Datenschutz-Audits ausreichend. Weitere Maßnahmen sind aktuell nicht erforderlich.

oder

− Alle geprüften Maßnahmen waren zum Zeitpunkt des Datenschutz-Audits ausreichend. Dennoch sind aufgrund einzelner Ergebnisse weitere Maßnahmen erforderlich.

oder

× Die geprüften Maßnahmen ergaben zum Zeitpunkt des Datenschutz-Audits Feststellungen. Verbesserungspotentiale zur Verbesserung der Datenschutzorganisation sind entsprechend vorhanden. Weitere Maßnahmen sind notwendig.

# Datenschutz-Auditplan



| Lfd.Nr. | Thema | Status | Maßnahme |
|---|---|---|---|
| **1.** | **Allgemeine Datenschutzanforderungen** | | |
| 1.1 | Benennung eines Datenschutzbeauftragten [DSB] | | |
| 1.2 | Einbindung und Unterrichtung eines (externen) DSB | | |
| 1.3 | Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten [pbD] | | |
| 1.4 | Wahrung der Informationspflichten bei Erhebung pbD | | |
| 1.5 | Übermittlung von pbD ins Ausland | | |
| 1.6 | Übersicht über Verarbeitungen | | |
| 1.7 | Verarbeitungsverzeichnis | | |
| 1.8 | Arbeitsanweisungen, Richtlinien zum Datenschutz | | |
| 1.9 | Meldungen bei der Aufsichtsbehörde | | |
| 1.10 | Datenschutz-Audits | | |
| 1.11 | Automatisierte Abrufverfahren | | |
| 1.12 | Belehrung und Verpflichtung von Beschäftigten auf das Datengeheimnis | | |
| 1.13 | Schulung von Beschäftigten zum Datenschutz | | |
| 1.14 | Datenerhebung, -verarbeitung und -nutzung durch Dienstleister | | |
| 1.15 | Verpflichtung auf das Datengeheimnis Dienstleister, Zeitarbeiter, Praktikanten o. ä. | | |
| 1.16 | Regelung Nutzung E-Mail- und Internetdienste durch Beschäftigte | | |
| 1.17 | Verfahren zur Wahrung der Rechte von Betroffenen; Beschwerdemanagement Datenschutz | | |
| 1.18 | Gestaltung öffentlicher Auftritte (bspw. Websites) | | |
| **2.** | **Zutrittskontrolle** | | |
| 2.1 | Maßnahmen zur Zutrittskontrolle | | |
| 2.2 | Festlegung und Dokumentation von erteilten Zutrittsberechtigungen („Berechtigungskonzept“) | | |
| 2.3 | Verfahren zur Ausgabe und Freischaltung von Mitteln zur Zutrittskontrolle (z. B. Chipkarten / Schlüssel) | | |
| 2.4 | Verfahren zur Rückgabe und Freischaltung von Mitteln zur Zutrittskontrolle (z. B. Chipkarten / Schlüssel) | | |
| 2.5 | Ungekennzeichnete Mittel (z. B. Chipkarten / Schlüssel) | | |
| 2.6 | Installation technischer Sicherungsanlagen (z. B. Einbruchmeldeanlagen, Alarmanlagen, Videoüber-wachung), Einbruchssicherungen | | |

| Lfd.Nr. | Thema | Status | Maßnahme |
|---|---|---|---|
| 2.7 | Überwachung außerhalb der Betriebszeit (z. B. Wachpersonal, Reinigungspersonal) | | |
| **3.** | **Zugangskontrolle** | | |
| 3.1 | Zusammenfassende Dokumentation Systeme, Datenverarbeitungsanlagen, Applikationen (Zugangs- und Zugriffskontrolle) | | |
| 3.2 | Firewall und Virenschutz (Server, Einzelrechner) | | |
| 3.3 | Sicherung Zugänge zum Firmennetzwerk über Internet (VPN, SSL, Webmail) | | |
| 3.4 | Sicherung mobiler Geräte (Notebooks, Smartphones,) | | |
| 3.5 | Sicherung Heimarbeitsplätze | | |
| 3.6 | Zugang Helpdesk, IT-Support (intern, extern) | | |
| 3.7 | Spezielle Arbeitsanweisungen (Bildschirmsperrung, Logout) | | |
| 3.8 | Allgemein Authentifizierungs- und Passwortrichtlinien für Server, Datenverarbeitungsanlagen, Applikationen | | |
| 3.9 | Art und Weise der Speicherung von Passwörtern für Server, Datenverarbeitungsanlagen, Applikationen | | |
| 4. | Zugriffskontrolle | | |
| 4.1 | Festlegung und Dokumentation von erteilten Zugriffsberechtigungen („Benutzerberechtigungskonzept“) | | |
| 4.2 | Verfahren zur Freigabe und Entzug von Zugriffsberechtigungen (Neueinstellung und Ausscheiden von Beschäftigten) | | |
| 4.3 | Löschung oder Sperrung von pbD (Fristen, Verfahren) | | |
| 4.4 | Zugriffskontrolle Dienstleister Festplatten Leasing-Geräte (Kopierer, Scanner, Drucker) | | |
| 4.5 | Vernichtung von pbD, Entsorgung von Datenträgern | | |
| 5. | Weitergabekontrolle | | |
| 5.1 | Sicherung der elektronischen Übertragung von pbD (z.B. E-Mail) | | |
| 5.2 | Sicherung der Lagerung von pbD (z.B. CD / DVD / USB, Festplatten, Datensicherungen) | | |
| 5.3 | Sicherung des Transports von pbD (z.B. Datensicherungen) | | |
| 5.4 | Erlaubnis der Speicherung von pbD auf optischen oder elektronischen Datenträgern (CD / DVD / USB, Notebooks) | | |
| 5.5 | Sicherung Speicherung von pbD auf optischen oder elektronischen Datenträgern (CD / DVD / USB, Notebooks) | | |
| 5.6 | Dokumentation der Abruf- und Übermittlungsprogramme, Empfänger elektronisch übertragener pbD | | |
| 5.7 | Poststelle (Öffnung Postsendungen geschäftlich, privat, Zustellung an Beschäftigte) | | |

| Lfd.Nr. | Thema | Status | Maßnahme |
|---|---|---|---|
| **6.** | **Eingabekontrolle** | | |
| 6.1 | Protokollierung von Eingaben oder Veränderungen von pbD in Datenverarbeitungsanlagen, Applikationen o. ä. | | |
| 6.2 | Protokollierung von (externen) Netzzugriffen | | |
| 6.3 | Auswertung und Überwachung von Protokollierungen | | |
| 6.4 | Protokollierungen Internet- und E-Mailnutzung durch Beschäftigte, Einsichtnahme in Kommunikation | | |
| 6.5 | Revisionssicherheit Archive | | |
| **7.** | **Auftragskontrolle** | | |
| 7.1 | Verfahren zur Auswahl von Auftragnehmern | | |
| 7.2 | Datenerhebung, -verarbeitung oder -nutzung im Auftrag oder Wartung oder Fernwartung | | |
| 7.3 | Auftragserteilung, Vertragsgestaltung | | |
| 7.4 | Überwachung von Auftragnehmern, Dokumentation | | |
| 7.5 | Tätigkeit als Auftragnehmer im Rahmen von Auftragsdatenverarbeitungen | | |
| **8.** | **Verfügbarkeitskontrolle** | | |
| 8.1 | Dokumentiertes Sicherheitskonzept mit Notfallplan | | |
| 8.2 | Maßnahmen gegen Ausfall (Klimaanlagen, Redundanzen, USV) | | |
| 8.3 | Maßnahmen gegen Zerstörung (Brandmeldung, Feuerschutz, Wassereinbruchsschutz) | | |
| 8.4 | Maßnahmen zur Verfügbarkeit (z. B. Erstellung von Datensicherungen der pbD, E-Mails, Serverkonfigurationen, Datenbanken) | | |
| 8.5 | Verfahren zur Erstellung von Datensicherungen | | |
| 8.6 | Wiederherstellung der pbD im Schadensfall, Erprobung | | |
| 8.7 | Protokollierung von Schadens- und Störfällen | | |
| **9.** | **Trennungskontrolle** | | |
| 9.1 | Organisatorische Trennungskontrolle | | |
| 9.2 | Technische Trennungskontrolle auf Systemebene | | |
| 9.3 | Technische Trennungskontrolle auf Applikationsebene | | |
| 9.4 | Technische Trennungskontrolle innerhalb der Applikation | | |
| 9.5 | Trennungskontrolle nach Datenarten (Kundendaten, Lieferantendaten, Beschäftigten- und Bewerberdaten) | | |
| 9.6 | Trennungskontrolle nach Mandanten | | |
| **10.** | **Marketing / Vertrieb** | | |
| 10.1 | Maßnahmen zur Bestandskundenbindung | | |
| 10.2 | Maßnahmen zur Neukundengewinnung | | |
| 10.3 | Werbemaßnahmen allgemein (Direkt-, Beipackwerbung, Brief, E-Mail, Telefon, Newsletter) | | |
| 10.4 | Verfahren zur Einwilligung zum Erhalt von Werbung (schriftlich, Textform, mündlich, Protokollierung) | | |

| Lfd.Nr. | Thema | Status | Maßnahme |
|---|---|---|---|
| 10.5 | Wahrung Informationspflichten bei Erhebung von pbD zu Werbezwecken (postalische und elektronische Werbung, Telefonwerbung) | | |
| 10.6 | Wahrung Informationspflichten bei Werbemaßnahmen | | |
| 10.7 | Nutzung und Inhalte von Kundendatenbanken, CRM-Systeme | | |
| 10.8 | Weitergabe von personenbezogenen Daten, Kauf von pbD (Adressen) | | |
| 10.9 | Nutzung Social Media | | |
| **11.** | **Personalwesen** | | |
| 11.1 | Verwendete Systeme, Applikationen | | |
| 11.2 | Übermittlung von Beschäftigtendaten, Lohn- und Gehaltsabrechnungen | | |
| 11.3 | Erweiterte Maßnahmen zur Zutrittskontrolle (Beschäftigte, externe Dienstleister, Reinigungsdienst leister) Beschäftigtendaten | | |
| 11.4 | Erweiterte Maßnahmen zur Zugangs- / Zugriffs-kontrolle Beschäftigtendaten | | |
| 11.5 | Erweiterte Maßnahmen zur Weitergabekontrolle von Beschäftigtendaten | | |
| 11.6 | Erweiterte Maßnahmen zur Eingabekontrolle Beschäftigtendaten | | |
| 11.7 | Erweiterte Maßnahmen zur Auftragskontrolle Beschäftigtendaten | | |
| 11.8 | Erweiterte Maßnahmen zur Verfügbarkeitskontrolle Beschäftigtendaten | | |
| 11.9 | Erweiterte Maßnahmen zur Trennungskontrolle Beschäftigtendaten | | |
| 11.10 | Vorgehen Krankmeldung, betriebsärztlicher Dienst, Gesundheitsvorsorge | | |
| 11.11 | Zeiterfassung | | |
| 11.12 | Leistungsbewertungen Beschäftigte, Kontrolle | | |
| 11.13 | Zustellung Lohn- und Gehaltsabrechnungen | | |
| 11.14 | Erfassung Bewerberdaten | | |
| 11.15 | Interne Weiterleitung Bewerberdaten (Kopierverbot) | | |
| 11.16 | Löschung von Bewerberdaten | | |
| 11.17 | Risikoabschätzung für die Verarbeitung von pbD | | |
| 11.18 | Durchführung einer Datenschutz-Folgeabschätzung | | |