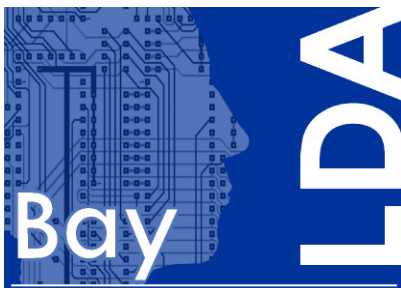




Checkliste Datensicherheit

Stand August 2011



Impressum:

Bayerisches Landesamt
für Datenschutzaufsicht
Promenade 27
91522 Ansbach

Telefon: (0981) 53-1300
Telefax: (0981) 53-5300
E-Mail: poststelle@lda.bayern.de
Internet: <http://www.lda.bayern.de>

Notwendig sind technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (§ 9 BDSG und Anlage dazu).

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Prüfpunkte:

Welche technischen bzw. organisatorischen Maßnahmen werden zur Zutrittskontrolle, insbesondere auch zur Legitimation, eingesetzt?

- Lage der Räume, Zugänge ausreichend abgesichert (Türen, Türschlösser, Lichtschächte, Lüftungsöffnungen, Fenster, Verglasungsart, Rollos gegen Hochschieben gesichert, Feuerleiter, Feuerterasse, elektrische Türöffner), Bewachung (z. B. Werkschutz), bewohntes Gebäude, besetzte Pforte
- Auf- und Abschließen der Räume bei Arbeitsbeginn bzw. -ende, Schlüsselregelung, Quittierung der Schlüsselausgabe, Generalschlüssel
- Überwachungseinrichtung (Alarmanlage, Videoüberwachung)
- Schriftliche Festlegungen zur Zugangsberechtigung, Ausweisregelungen, Trennung von Bearbeitungs- und Publikumszonen, Besucherregelungen, Besucherbuch, Kundenabfertigung (Schalterbetrieb), Zutrittskontrollsystem (Ausweisleser, Magnetkarte)
- Reinigungs- und Wartungsarbeiten
- Anwesenheitskontrollen (Stechuhren, Schichtbuch, Protokollierung kurzzeitiger Abwesenheit)
- Sicherheit bei Heimarbeiten/Telearbeiten
- Ggf. Beratung durch kriminalpolizeiliche Beratungsstelle, usw.

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern

Prüfpunkte:

Welche Maßnahmen sind hinsichtlich der Benutzeridentifikation und Authentisierung technisch und organisatorisch vorhanden?

- Firewall, Virenschutz (zentral/Server, dezentral/Arbeitsplätze)
- Geeignete Benutzeridentifikation und Passwortverfahren (u. a. keine Eigennamen und Wörter aus dem Wörterbuch, auch Sonderzeichen verwenden, Mindestlänge acht Stellen, regelmäßiger Wechsel des Passworts, z. B. alle drei Monate)
- Automatische Sperrung der Bildschirme mit Passwortschutz bei Pausen, Sperren eines Zugangs bei mehr als drei Anmelde-Fehlversuchen
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von Datenträgern
- Geschlossene PC, ohne USB-Steckplätze bzw. DVD/CD-Laufwerke

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Prüfpunkte:

Die unerlaubte Tätigkeit in DV-Systemen außerhalb eingeräumter Berechtigungen ist zu verhindern.

- Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen, differenzierte Berechtigungen für Auswertungen, Kenntnisnahme, Veränderung, Löschung
- Schutz gegen unberechtigte interne und externe Zugriffe, Verschlüsselung, Firewall
- Überwachung und Protokollierung der Zugriffe bzw. Zugriffsversuche, Auswertung der Protokolle, Aufbewahrung der Protokolle mindestens ein Jahr
- Art und Anzahl der Datenträger dokumentieren, Lagerung von Datenträgern prüfen (dauernd/zeitweise), Lagerung nach Dienstschluss (abschließbare Schränke, Schlüsselregelung), Auslagerung von Sicherungsdaträgern (Durchführung)
- Datenträgerverwaltung, Nachweis über Eingang, Ausgang sowie Bestand von Datenträgern (Bestandsverzeichnisse), Datenträgerinventuren
- Festlegung der Bereiche, in denen sich Datenträger befinden dürfen, und der Personen, die Datenträger befugt entnehmen dürfen; Festlegung der Datenempfänger, Quittierverfahren, Datenträgerbegleitpapiere
- Äußerliche Kennzeichnung der eigenen Datenträger zur Unterscheidung von fremden, Trennung der Datenträger verschiedener Auftraggeber, eigener Datenträger-Pool für jeden Kunden, Regelung/Verbot des Einsatzes privater Datenträger
- Vollständige Löschung verwendeter Datenträger vor neuer Verwendung bzw. vor Weitergabe
- Entsorgung/Vernichtung von Fehldrucken, veralteten Datenträgern (entsprechende Lagerung zu vernichtender Datenträger, Reißwolf, Datenträgerlöschgeräte, Verbrennen/Zerstören), Kontrolle der tatsächlichen Vernichtung (zuverlässiges Entsorgungsunternehmen, vertragliche Regelung, Entsorgungsbescheinigung)
- Regelung für das Kopieren von Datenträgern, Taschenverbot bzw. -kontrollen
- Regelung für USB-Sticks, PDA's, externe Festplatten, Smartphones
- Regelung und Kontrolle von externer Wartung und Fernwartung

4. Weitergabekontrolle

Maßnahmen, die 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.

Prüfpunkte:

Sämtliche Aspekte der Weitergabe personenbezogener Daten: elektronische Übertragung, Datentransport, Übermittlungskontrolle

- Welche Datenträgertransporte (innerhalb des Unternehmens, zur Auslagerung, zwischen Auftraggeber/-nehmer, zu Dritten)
- Welche Versendungsarten (Datenleitung, Post, Bahn, Kuriere, Taxi)
- Schriftliche Transportregelungen und Festlegung der Wege, der Transportverfahren, der Empfänger von Daten und der zur Weitergabe Berechtigten, Vollständigkeitsüberprüfung bei Rücklieferung vom Auftragnehmer
- Transportsicherung, verschlossene Transportbehälter, zuverlässige Boten bzw. Transportunternehmen, sichere Versendungsformen (z. B. Wertpaket, Einschreibesendung, Datentransport-/E-Mail-Verschlüsselung, elektronische Signatur, VPN/Virtual Private Network)
- Dokumentation der Abruf- und Übermittlungsprogramme

- Lieferscheine/Quittierverfahren bei Eingang und Ausgang von Datenträgern
- Legitimation der Abholer, Empfangsbestätigungen, Ein-/Ausgangsbücher, Lieferscheine, Protokollierung

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Prüfpunkte:

- Protokollierungs- und Protokollauswertungssysteme, wer erfasst, wer hat wann was eingegeben, auch Heimarbeiter, Kennzeichnung der erfassten Belege oder Laufzettel mit Namenszeichen/Stempel, Kennzeichnung bei Online-Eingaben bzw. Änderungen, Aufbewahrungsdauer der Protokolle
- Dokumentation der Eingabeverfahren mit Festlegung der für die Erstellung von Datenträgern und der Bearbeitung von Daten Befugten (Stellenbeschreibung, Dienstweisung, Geschäftsverteilungsplan)

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (vgl. § 11 BDSG).

Prüfpunkte:

- Sorgfältige Auswahl der Auftragnehmer, Kriterien zur Auswahl des Auftragnehmers
- Geprüftes Unternehmen selbst als Auftragnehmer tätig
- Detaillierte schriftliche Regelungen der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes, auch zum Einsatz von Subunternehmen (Erfassung, Scannen, Entsorgung), eindeutige Regelung der Zuständigkeiten und Verantwortlichkeiten (speziell auch bei der Datensicherung und beim Datenträgertransport)
- Formalisierte Auftragserteilung (Auftragsformular)
- Kontrolle der Arbeitsergebnisse (formal, inhaltlich), Kontrolle der Unterauftragnehmer (z. B. durch den DSB)

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Prüfpunkte:

- Brandschutzeinrichtungen (Feuerlöscher, Rauch- oder Brandmelder), Rauchverbot, Wasserschutzeinrichtungen
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung von Sicherungsdatenträgern, Back up Verfahren
- Spiegeln von Festplatten
- Virenschutz/Firewall
- Notfallplan

8. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Prüfpunkte:

- Regelungen/Maßnahmen zur Sicherstellung der getrennten Speicherung, Veränderung, Löschung und Übermittlung von Daten mit unterschiedlichen Vertragszwecken, z. B. getrennte DV-Systeme für unterschiedliche Verarbeitungszwecke
- Interne Mandantenfähigkeit/Zweckbindung
- Funktionstrennung (Produktion und Test)

9. Organisationskontrolle

Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird.

Prüfpunkte:

- IT-Sicherheitskonzept/schriftliche Regelungen über den Betrieb und die Abläufe der Datenverarbeitung sowie zu den verschiedenen Datensicherheitsmaßnahmen (Richtlinien, Arbeitsanweisungen, Stellenbeschreibungen usw.)
- Standards für die IT-Sicherheit bzw. zur Abwicklung von IT-Projekten (IT-Grundschutz, ISO 27001, etc.)
- Vollverschlüsselung mobiler Datenträger als Standard
- Mitbenutzung der Anlagen durch Fremdfirmen
- Urlaubsvertretung/Krankheitsvertretung des Inhabers
- DV-Revision, interne Revision, Auswertung der Protokollierungen/Log-Dateien
- Ausreichende Funktionstrennung/4-Augen-Prinzip
- Schriftliches Programmfreigabeverfahren
- Regelungen über Sicherung des Datenbestandes
- Regelmäßige Hinweise und Ermahnungen, um das Problembewusstsein zu fördern
- Gelegentliche unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen