BAYERISCHES LANDESAMT
FÜR DATENSCHUTZAUFSICHT

Checkliste: Datensicherheit

Technische und organisatorische Maßnahmen nach § 9 BDSG und Anlage

Herausgeber:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach

Telefon: (0981) 53 - 1300
Telefax: (0981) 53 - 5300
E-Mail: poststelle@lda.bayern.de
Webseite: www.lda.bayern.de

Stand: Jan. 2014

Einführender Hinweis

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). Die nachfolgenden Prüfpunkte stellen einerseits einen Überblick der grundlegenden erforderlichen Maßnahmen und Fragestellungen und andererseits die wesentlichen Kriterien für Prüfungen durch die bayerische Datenschutzaufsichtsbehörde dar.

1. Zutrittskontrolle

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

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

- Lage der Räume:
  Sind die Zugänge der Räume ausreichend abgesichert (z. B. Türen, Türschlösser, Lichtschächte, Lüftungsöffnungen, Fenster, Verglasungsart, Rollos gegen Hochschieben, Feuerleiter, Feuertreppe, elektrische Türöffner)? Erfolgt eine Bewachung der Räumlichkeiten (z. B. durch einen Werkschutz)? Handelt es sich um ein bewohntes Gebäude? Existiert eine Pforte und wann ist diese besetzt?
- Verschließbarkeit der Räume:
  Erfolgt ein Auf- und Abschließen der Räume bei Arbeitsbeginn bzw. -ende? Gibt es ein geregeltes Konzept zur Schlüsselverwaltung? Findet eine Quittierung bei der Schlüsselausgabe statt? Wer besitzt einen Generalschlüssel?
- Überwachungseinrichtung:
  Sind Alarmanlagen vorhanden? Wird der Zutritt in den Serverraum über Videokameras überwacht? Werden Bewegungssensoren eingesetzt?
- Schriftliche Festlegungen zur Zugangsberechtigung:
  Tragen die Mitarbeiter den Ausweis sichtbar? Existieren hierfür klar Ausweisregelungen? Wird auf die Trennung von Bearbeitungs- und Publikumszonen geachtet? Sind schriftliche Besucherregelungen vorhanden? Werden Besuche in einem Besucherbuch dokumentiert? Wie findet die Kundenbetreuung statt (Schalterbetrieb)? Welches Zutrittskontrollsystem wird eingesetzt (z. B. Ausweisleser, Magnetkarte)?
- Reinigungs- und Wartungsarbeiten:
  Ist sichergestellt, dass sowohl mit dem Reinigungspersonal als auch mit IT-Dienstleistern bei Wartungen entsprechende Regelungen getroffen sind?

- Anwesenheitskontrollen:
  Wie wird die Anwesenheit überprüft (z. B. Stechuhren, Schichtbuch)? Werden auch kurzzeitige Abwesenheiten protokolliert?
- Sicherheit bei Heimarbeiten/Telearbeiten:
  Wird auch bei fernangebundenen Arbeitsplätzen für ausreichende Sicherheit gesorgt?
- Beratung:
  Findet ggf. eine Beratung durch kriminalpolizeiliche Beratungsstellen oder spezialisierte Dienstleister statt?

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

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

- Firewall und Virenschutz:
  Welche Produkte werden eingesetzt? Existiert eine zentrale Firewall? Welche dezentralen Lösungen werden an den Arbeitsplätzen verwendet?
- Benutzeridentifikation und Passwortverfahren:
  Werden ausreichend sichere Passwörter verwendet (z. B. keine Eigennamen und Wörter aus dem Wörterbuch, auch Sonderzeichen verwenden, empfohlene Länge von zehn Stellen)? Ist ein regelmäßiger Passwortwechsel verpflichtend? Findet eine Auswertung der Protokolleinträge bei Falscheingaben des Passworts statt? Werden Verfahren zur Zwei-Faktor-Authentifizierung eingesetzt (z. B. Tokens, Smartcards)?
- Systemsperrung:
  Erfolgt eine automatische Sperrung der Bildschirme mit Passwortschutz bei Pausen? Findet ein Sperren eines Zugangs bei mehr als drei Anmelde-Fehlversuchen statt? Hat die Falscheingabe eines Passworts eine zeitliche Verzögerung für einen Neuversuch zur Folge?
- Benutzerkennungen:
  Wird auf Gruppenkennungen verzichtet? Besteht ein eigenes Benutzerkonto für jeden Mitarbeiter (d. h. Einrichtung eines Benutzerstammsatzes)?
- Verschlüsselung:
  Werden Datenträger verschlüsselt? Welche Verschlüsselungsverfahren kommen zum Einsatz?
- Geräteanschlüsse:
  Sind die relevanten PCs 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.

Prüffokus:
Welche Maßnahmen sind vorhanden, um die unerlaubte Tätigkeit in DV-Systemen außerhalb eingeräumter Berechtigungen zu verhindern?

- Berechtigungskonzept und Zugriffsrechte:
  Entspricht das Konzept sowohl für Anwender als auch für Administratoren den aufgabenbedingten und datenschutzrechtlichen Erfordernissen? Existieren differenzierte Berechtigungen für Auswertungen, Kenntnisnahme, Veränderung und Löschung?
- Schutz gegen unberechtigte Zugriffe:
  Bestehen Schutzmaßnahmen gegen unbefugte interne und externe Zugriffe (z. B. durch Verschlüsselung, Firewalls)? Werden Verfahren zur Data Leak Prevention (Erkennung unerwünschter Datenabflüsse) eingesetzt? Werden regelmäßig Penetrationstests gegen Attacken von Hackern durchgeführt?
- Überwachung und Protokollierung:
  Werden Zugriffe bzw. Zugriffsversuche protokolliert? Wann findet eine Auswertung der Protokolle statt? Wo und wie lange werden die Protokolle aufbewahrt (mindestens ein Jahr)?
- Datenträgerverwaltung:
  Sind die Datenträger inventarisiert (Art und Anzahl)? Wird die Lagerung von Datenträgern überprüft (dauernd/zeitweise, Bestandsverzeichnisse)? Werden Nachweise über Eingang, Ausgang sowie Bestand von Datenträgern festgehalten? Wo werden die Datenträger, insbesondere mobile wie USB-Festplatten, nach Dienstschluss aufbewahrt (abschließbare Schränke, Schlüsselregelung)? Findet eine Auslagerung von Sicherungsdatenträgern statt?
- Datentrennung:
  Findet eine äußerliche Kennzeichnung der eigenen Datenträger zur Unterscheidung von fremden statt? Werden Datenträger verschiedener Auftraggeber getrennt behandelt? Gibt es einen eigenen Datenträger-Pool für jeden Kunden? Besteht eine Regelung/Verbot des Einsatzes privater Datenträger?
- Datenlöschung:
  Werden Datenträger vor neuer Verwendung vollständig von bestehenden Daten bereinigt? Werden Daten auf den Datenträger vor Weitergabe, wie z. B. Verkauf, gelöscht?
- Entsorgung/Vernichtung:
  Werden auch Fehldrucke sorgfältig entsorgt? Werden veraltete Datenträgern geregelt vernichtet (entsprechende Lagerung der zu vernichtenden Datenträger, Datenträgerlöschgeräte, Verbren-

nen/Zerstören)? Findet Kontrollen der tatsächlichen Vernichtung bei Dienstleistern statt (zuverlässiges Entsorgungsunternehmen, vertragliche Regelung, Entsorgungsbescheinigung)? Welche Schredder werden im Unternehmen eingesetzt (Sicherheitsstufe)?

- Regelung für das Kopieren von Datenträgern:
  Existieren Richtlinien für das Kopieren von Datensätzen bzw. auch für das vollständige Kopieren von Datenträgern? Besteht ein Taschenverbot bzw. erfolgen Kontrollen von Taschen?
- Regelungen für mobile Geräte:
  Gibt es Anweisungen zum Umgang mit mobilen Datenträgern und Geräte (z. B. USB-Sticks, PDAs, externe Festplatten, Tablets, Smartphones)? Wird BYOD (Bring-Your-Own-Device) in der Organisation gelebt?
- Fernwartung:
  Bestehen Regelungen und gezielte Kontrollen bei Wartungsarbeiten durch Dienstleister (externe 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.

Prüffokus:
Welche Regelungen existieren bezüglich der Weitergabe personenbezogener Daten (elektronische Übertragung, Datentransport, Übermittlungskontrolle)?

- Datenträgertransportart:
  Welche unterschiedlichen Datenträgertransporte finden statt (z. B. nur innerhalb des Unternehmens, zur Auslagerung, zwischen Auftraggeber/-nehmer, zu Dritten)?
- Versendungsarten:
  Wie werden die Daten versendet (z. B. Post, Bahn, Kuriere, Taxi, elektronisch)?
- Transportregelungen:
  Sind die Bereiche festgelegt, in denen sich Datenträger befinden dürfen? Ist definiert, welche Personen die Datenträger befugt entnehmen dürfen? Gibt es schriftliche Festlegung der Transportwege und der Transportverfahren? Werden beim Transport Datenträgerbegleitpapiere ausgestellt bzw. mitgenutzt? Existiert eine verbindliche Regelung, wer als Datenempfänger fungieren darf und wer zur Weitergabe berechtigt ist? Findet eine Vollständigkeitsüberprüfung bei Rücklieferung vom Auftragnehmer statt?

- Transportsicherung:
  Sind die Datenträger beim Transport durch verschlossene Transportbehälter ausreichend gesichert? Werden ausschließlich zuverlässige Boten bzw. Transportunternehmen eingesetzt? Werden durchgängig sichere Versendungsformen verwendet (z. B. Wertpaket, Einschreibesendung, Datentransport-/E-Mail-Verschlüsselung, elektronische Signatur, VPN/Virtual Private Network)? Werden elektronische Datentransporte Ende-zu-Ende verschlüsselt?
- Dokumentation:
  Werden die Abruf- und Übermittlungsvorgänge dokumentiert? Wird der Eingang und Ausgang von Datenträgern durch Lieferscheine/Quittierverfahren schriftlich festgehalten? Gibt es Legitimation der Abholer, Empfangsbestätigungen, Ein-/Ausgangsbücher, 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.

Prüffokus:
Welche Maßnahmen werden insbesondere zur Protokollierung bei Änderungen in den Datenverarbeitungssystemen ergriffen?

- Protokollierung:
  Welche Protokollierungs- und Protokollauswertungssysteme kommen zum Einsatz? Was wird im Rahmen der Protokollierung aufgezeichnet (z. B. wer erfasst, wer hat wann was eingegeben)? Werden auch Aktivitäten der Heimarbeiter erfasst? Findet eine Kennzeichnung der erfassten Belege oder Laufzettel mit Namenszeichen/Stempel statt? Werden auch Online-Eingaben bzw. Änderungen sorgfältig protokolliert? Welche Regelungen zur Aufbewahrungsdauer der Protokolle bestehen?
- Dokumentation:
  Erfolgt eine Dokumentation der Eingabeverfahren mit Festlegung der für die Erstellung von Datenträgern und der Bearbeitung von Daten Befugten (z. B. mit Stellenbeschreibung, Dienstanweisung, 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).

Prüffokus:
Welche Regelungen bestehen im Umgang mit Auftragnehmern?

- Auswahl von Auftragnehmer:
  Findet Auswahl der Auftragnehmer sorgfältig statt? Welche Kriterien zur Auswahl des Auftragnehmers bestehen?
- Unterauftragnehmer:
  Ist das geprüfte Unternehmen selbst als Auftragnehmer tätig? Welche Auftragnehmer werden dort nach welchen Kriterien ausgewählt?
- Schriftliches Auftragsverhältnis:
  Bestehen detaillierte schriftliche Regelungen der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes - auch zum Einsatz von Subunternehmen (Erfassung, Scannen, Entsorgung)? Gibt es eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten (speziell auch bei der Datensicherung und beim Datenträgertransport)? Erfolgt eine formalisierte Auftragserteilung (Auftragsformular)?
- Kontrolle:
  Findet eine regelmäßige Kontrolle der Arbeitsergebnisse statt (formal, inhaltlich)? Erfolgt auch eine Kontrolle der Unterauftragnehmer (z. B. durch den DSB)?

7. Verfügbarkeitskontrolle

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

Prüffokus:
Welche Regelungen bestehen, um die Daten dauerhaft verfügbar bereitzustellen?

- Brandschutz:
  Welche Einrichtungen zum Brandschutz sind vorhanden (z. B. Feuerlöscher, Rauch- oder Brandmelder)? Besteht Rauchverbot? Existieren effektive Wasserschutzeinrichtungen?
- Stromversorgung:
  Ist eine unterbrechungsfreie Stromversorgung (USV) etabliert?

- Sicherungen:
  Werden Sicherungsdatenträger getrennt aufbewahrt? Wo erfolgen die Backup-Verfahren? Werden Speichereinheiten redundant ausgelegt? Sind die Datensicherungen verschlüsselt? Werden Cloud-Lösungen zur Datensicherung eingesetzt?
- Virenschutz/Firewall:
  Bestehen ausreichende Schutzmaßnahmen durch Security-Werkzeuge?
- Notfallplan:
  Gibt es auch für einen Katastrophenfall entsprechende Vorkehrungen (z. B. durch Angriffe von intern/extern, Schäden durch Feuer)?

8. Trennungskontrolle

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

Prüffokus:
Wie wird gewährleistet, dass Daten getrennt voneinander verarbeitet werden können?

- Getrennte Speicherung:
  Welche Regelungen/Maßnahmen zur Sicherstellung der getrennten Speicherung existieren? Wie erfolgt die Veränderung, Löschung und Übermittlung von Daten mit unterschiedlichen Vertragszwecken (z. B. getrennte DV-Systeme für unterschiedliche Verarbeitungszwecke)? Wie werden Daten mit hohem Schutzbedarf verarbeitet?
- Mandantenfähigkeit:
  Werden Systeme verwendet, die eine interne Mandantenaufteilung ermöglichen (Zweckbindung)? Besteht ein Konzept zur Mandantentrennung?
- Funktionstrennung:
  Werden Produktion- und Testumgebungen stets voneinander getrennt? Werden personenbezogene Daten zu Entwicklungszwecken pseudonymisiert/anonymisiert?

9. Organisationskontrolle

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

Prüffokus:
Welche innerbetrieblichen Reglungen bestehen, um ein entsprechendes Datensicherheitsniveau zu gewährleisten?

- IT-Sicherheitskonzept:
  Bestehen schriftliche Regelungen über den Betrieb und die Abläufe der Datenverarbeitung sowie zu den verschiedenen Datensicherheitsmaßnahmen (z. B. Richtlinien, Arbeitsanweisungen, Stellenbeschreibungen)? Erfolgen Sicherungen des Datenbestandes nach festgelegtem Schema?
- Standards:
  Wird auf etablierte Standards für die IT-Sicherheit bzw. zur Abwicklung von IT-Projekten zurückgegriffen (IT-Grundschutz, ISO 27001, etc.)?
- Revision:
  Findet eine Revision der Datenverarbeitung statt? Besteht eine interne Revisionsabteilung? Werden Protokollierungen und Log-Dateien ausgewertet (z. B. stichprobenartig)? Werden im Falle der Mitbenutzung der Anlagen durch Fremdfirmen auch hier entsprechende Überprüfungen durchgeführt? Finden auch gelegentliche unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen statt?
- Mitarbeiter:
  Ist im Urlaub- und Krankheitsfall für eine Vertretung gesorgt (z. B. Vertreterregelungen, Freigaben, Berechtigungen)? Werden die Mitarbeiter über den sicheren Umgang mit den Daten entsprechend geschult? Gibt es regelmäßige Hinweise und Ermahnungen, um das Problembewusstsein zu fördern? Werden mobile Datenträger der Mitarbeiter standardmäßig verschlüsselt? Besteht eine ausreichende Funktionstrennung? Findet bei wichtigen Datenverarbeitungen das „4-Augen-Prizip“ Anwendung?