

CHECKLISTE 1 – Anforderungen an die Sicherheit der Datenverarbeitung nach § 64 BDSG (neu) **u**Im Fall einer automatisierten Datenverarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung entsprechende Kontrollmaßnahmen zu ergreifen.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **1** |  | **Zugangskontrolle  technische und organisatorische Maßnahmen** Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 1 | 1 | Sind das Gebäude und relevante Räume gegen den Zutritt durch Unbefugte gesichert? |  |  |  |  |
| 1 | 2 | Gibt es am Gebäude Sicherheitsverglasung? |  |  |  |  |
| 1 | 3 | Gibt es manuelle Schließ-Systeme? |  |  |  |  |
| 1 | 4 | Wenn ja, wird Protokoll geführt, welche Personen wann über welche Schlüssel verfügen? |  |  |  |  |
| 1 | 5 | Gibt es ein Sicherheits-Schließsystem? (Sicherheits-Schlösser, Schließanlage mit Chipkarten, Code oder Fingerprint)? |  |  |  |  |
| 1 | 6 | Gibt es Serverschränke/Rechnerräume und, wenn ja, sind diese abschließbar? |  |  |  |  |
| 1 | 7 | Sind Akten in verschlossenen (Stahl-)Schränken aufbewahrt? |  |  |  |  |
| 1 | 8 | Existiert eine Alarmanlage? |  |  |  |  |
| 1 | 9 | Gibt es Bewegungsmelder und Lichtschranken? |  |  |  |  |
| 1 | 10 | Wurde das Sicherheitspersonal sorgfältig ausgewählt? |  |  |  |  |
| 1 | 11 | Wurde das Reinigungspersonal sorgfältig ausgewählt? |  |  |  |  |
| 1 | 12 | Werden Arbeiten durch Externe (z.B. Wartungs- oder Reparaturarbeiten) nur unter Aufsicht von autorisierten Personen durchgeführt? |  |  |  |  |
| 1 | 13 | Werden Mitarbeiter- und Gästeausweise ausgegeben? |  |  |  |  |
| 1 | 14 | Gibt es eine zulässige Videoüberwachung? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **2** |  | **Datenträgerkontrolle technische und organisatorische Maßnahmen** Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 2 | 1 | Werden Datenträger sicher in verschließbaren Schränken gelagert? |  |  |  |  |
| 2 | 2 | Ist der Austausch von Daten zwischen Datenträgern ausreichend gesichert, z. B. durch VPN-Tunnel oder Standleitungen? |  |  |  |  |
| 2 | 3 | Werden Datenträger nur an autorisierte Personen abgegeben? Ist dieser Empfängerkreis definiert? |  |  |  |  |
| 2 | 4 | Wird die Ausgabe von Datenträgern protokolliert und vom Empfänger quittiert? |  |  |  |  |
| 2 | 5 | Werden die Daten nur in anonymisierter oder pseudonymisierter Form weitergegeben? |  |  |  |  |
| 2 | 6 | Ist eine ordnungsgemäße Vernichtung von Datenträgern nach DIN 66399 gewährleistet? |  |  |  |  |
| 2 | 7 | Werden Aktenvernichter eingesetzt? |  |  |  |  |
| 2 | 8 | Werden externe, zertifizierte Dienstleister mit der Vernichtung von Datenträgern beauftragt? |  |  |  |  |
| 2 | 9 | Sind Aufbewahrungsfristen für gespeicherte Daten festgelegt? |  |  |  |  |
| 2 | 10 | Gibt es Protokolle über die Vernichtung von Daten? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **3** |  | **Speicherkontrolle technische und organisatorische Maßnahmen** Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 3 | 1 | Sind die einzelnen Berechtigungen in den IT-Systemen festgelegt? |  |  |  |  |
| 3 | 2 | Gibt es differenzierte Berechtigungen für Lesen, Ändern und Löschen? |  |  |  |  |
| 3 | 3 | Sind differenzierte Berechtigungen für Daten, Anwendungen und Betriebssysteme eingerichtet? |  |  |  |  |
| 3 | 4 | Wird die Verwaltung der Rechte durch Systemadministratoren durchgeführt? |  |  |  |  |
| 3 | 5 | Ist die Anzahl der Administratoren auf ein Minimum reduziert? |  |  |  |  |
| 3 | 6 | Gibt es eine Passwortvergabe für Dateien und Programme? |  |  |  |  |
| 3 | 7 | Existiert eine Passwortrichtlinie bezgl. Passwortlänge und Passwortwechsel? |  |  |  |  |
| 3 | 8 | Ist die Passwort-Datei gesichert? |  |  |  |  |
| 3 | 9 | Werden die Zugriffe auf Anwendungen protokolliert? |  |  |  |  |
| 3 | 10 | Werden Arbeitsabläufe pro Benutzer protokolliert? |  |  |  |  |
| **4** |  | **Benutzerkontrolle technische und organisatorische Maßnahmen** Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 4 | 1 | Sind zugangsberechtigte Mitarbeiter für die einzelnen Systeme festgelegt? |  |  |  |  |
| 4 | 2 | Wurden Benutzerprofile erstellt? |  |  |  |  |
| 4 | 3 | Wurde für die einzelnen Nutzer eine Passwortvergabe vorgenommen? |  |  |  |  |
| 4 | 4 | Erfolgt die Authentifikation mit Benutzername/Passwort? |  |  |  |  |
| 4 | 5 | Gibt es regelmäßige Kontrollen von Berechtigungen? |  |  |  |  |
| 4 | 6 | Ist die Sperrung von Berechtigungen ausscheidender Mitarbeiter gewährleistet? |  |  |  |  |
| 4 | 7 | Existiert eine Zuordnung von Benutzerprofilen zu IT-Systemen? |  |  |  |  |
| 4 | 8 | Wird Verschlüsselungs-Technologie eingesetzt? |  |  |  |  |
| 4 | 9 | Wird Anti-Viren-Software eingesetzt? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **5** |  | **Zugriffskontrolle technische und organisatorische Maßnahmen** Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 5 | 1 | Sind Berechtigungen in den IT-Systemen festgelegt? |  |  |  |  |
| 5 | 2 | Gibt es differenzierte Berechtigungen für Lesen, Ändern und Löschen? |  |  |  |  |
| 5 | 3 | Gibt es differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem? |  |  |  |  |
| 5 | 4 | Werden die Rechte durch Systemadministratoren verwaltet? |  |  |  |  |
| 5 | 5 | Ist die Anzahl der Administratoren auf ein Minimum reduziert? |  |  |  |  |
| 5 | 6 | Existiert eine Passwortrichtlinie bezgl. Passwortlänge und Passwortwechsel? |  |  |  |  |
| 5 | 7 | Gibt es eine Protokollierung von Zugriffen auf Anwendungen? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **6** |  | **Übertragungskontrolle technische und organisatorische Maßnahmen** Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 6 | 1 | Sind die für die Übertragungskontrolle verantwortlichen Personen festgelegt? |  |  |  |  |
| 6 | 2 | Gibt es eine Festlegung zugelassener Stellen und Übermittlungswege? |  |  |  |  |
| 6 | 3 | Werden für die Übertragung von Daten Standleitungen oder Verschlüsselungs-Technologien eingesetzt? |  |  |  |  |
| 6 | 4 | Gibt es eine Dokumentation über Abruf- und/oder Übertragungsprogramme? |  |  |  |  |
| 6 | 5 | Werden die Empfänger von Daten und die Zeitspannen der geplanten Überlassung bzw. vereinbarte Löschfristen dokumentiert? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **7** |  | **Eingabekontrolle technische und organisatorische Maßnahmen** Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 7 | 1 | Sind die für die Eingabekontrolle verantwortlichen Personen festgelegt? |  |  |  |  |
| 7 | 2 | Sind die zuständigen Personen für die Eingabe von Daten festgelegt? |  |  |  |  |
| 7 | 3 | Gibt es Anweisungen zur Datenerfassung? |  |  |  |  |
| 7 | 4 | Gibt es Anweisungen für den Verbleib von Eingabebelegen? |  |  |  |  |
| 7 | 5 | Werden Plausibilitätskontrollen durchgeführt? |  |  |  |  |
| 7 | 6 | Werden Erfassungsdatum, -zeit und -kraft protokolliert? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **8** |  | **Transportkontrolle technische und organisatorische Maßnahmen** Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 8 | 1 | Sind die verantwortlichen Personen zur Transportkontrolle festgelegt? |  |  |  |  |
| 8 | 2 | Sind Transport- und Übermittlungswege festgelegt? |  |  |  |  |
| 8 | 3 | Erfolgt der Transport durch Direktabholung oder Kurierdienst? |  |  |  |  |
| 8 | 4 | Erfolgt der Versand durch Wertbrief oder Wertpaket? |  |  |  |  |
| 8 | 5 | Existieren Versand- und Verpackungsvorschriften? |  |  |  |  |
| 8 | 6 | Gibt es für den Transport Liefer- und Begleitscheine? |  |  |  |  |
| 8 | 7 | Gibt es eine Übergabe-/Auslieferungsdokumentation? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **9** |  | **Wiederherstellbarkeit technische und organisatorische Maßnahmen** Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 9 | 1 | Existiert ein Backup-Konzept? |  |  |  |  |
| 9 | 2 | Werden Festplatten gespiegelt? |  |  |  |  |
| 9 | 3 | Existiert ein Recovery-Konzept? |  |  |  |  |
| 9 | 4 | Wurden Tests zur Datenwiederherstellung durchgeführt? |  |  |  |  |
| 9 | 5 | Existiert ein Notfallplan für den Fall eines Datenverlustes? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **10** |  | **Zuverlässigkeit technische und organisatorische Maßnahmen** Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 10 | 1 | Gibt es unabhängig voneinander funktionierende Systeme im Unternehmen? |  |  |  |  |
| 10 | 2 | Werden Fehlfunktionen automatisiert gemeldet? |  |  |  |  |
| 10 | 3 | Existiert ein technischer Support im Haus? |  |  |  |  |
| 10 | 4 | Gibt es einen externen technischen Support? |  |  |  |  |
| 10 | 5 | Existiert ein Notfallplan für den Ausfall von Systemen? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **11** |  | **Datenintegrität technische und organisatorische Maßnahmen** Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 11 | 1 | Ist sichergestellt, dass Daten nicht durch Fehlfunktionen des Systems beschädigt oder verändert werden? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **12** |  | **Auftragskontrolle technische und organisatorische Maßnahmen** Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 12 | 1 | Sind die für die Auftragskontrolle verantwortlichen Personen festgelegt? |  |  |  |  |
| 12 | 2 | Ist gewährleistet, dass die Auftragnehmer sorgfältig ausgewählt wurden? |  |  |  |  |
| 12 | 3 | Gibt es eine klare Kompetenz-Abgrenzung zwischen Auftraggeber- und nehmer? |  |  |  |  |
| 12 | 4 | Existiert eine Verfahrensabnehme und eine Programmfreigabe? |  |  |  |  |
| 12 | 5 | Existiert eine Vertragsgestaltung zur Datenverarbeitung im Auftrag? |  |  |  |  |
| 12 | 6 | Wird die Vertragsausführung regelmäßig kontrolliert? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **13** |  | **Verfügbarkeitskontrolle technische und organisatorische Maßnahmen** Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 13 | 1 | Existieren Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen? |  |  |  |  |
| 13 | 2 | Sind Feuer- und Rauchmeldeanlagen installiert? |  |  |  |  |
| 13 | 3 | Gibt es Feuerlöschgeräte in Serverräumen? |  |  |  |  |
| 13 | 4 | Ist die Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort gewährleistet? |  |  |  |  |
| 13 | 5 | Wird ein Alarm bei unberechtigten Zutritten zu Serverräumen ausgelöst? |  |  |  |  |
| 13 | 6 | Existiert ein Notfallplan? |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **14** |  | **Trennbarkeit technische und organisatorische Maßnahmen** Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können | **Ja** | **Nein** | **N/A** | **Bemerkung** |
| 14 | 1 | Existieren Regelungen zur Sicherstellung der getrennten Speicherung von Daten? |  |  |  |  |
| 14 | 2 | Gibt es eine physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern? |  |  |  |  |
| 14 | 3 | Gibt es getrennte DV-Systeme für unterschiedliche Verarbeitungszwecke? |  |  |  |  |
| 14 | 4 | Werden Systeme verwendet, die eine interne Mandantenaufteilung ermöglichen (Zweckbindung)? |  |  |  |  |
| 14 | 5 | Werden Daten, die zu demselben Zweck verarbeitet werden, verschlüsselt? |  |  |  |  |
| 14 | 6 | Wird bei pseudonymisierten Daten eine Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System vorgenommen? |  |  |  |  |