Technisch-Organisatorische Maßnahmen

|  |
| --- |
| **Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO** |

Bitte geben Sie an, welche **konkreten** technischen und organisatorischen Maßnahmen Sie zur Gewährleistung von Datenschutz und Datensicherheit getroffen haben und liefern Sie uns einen Nachweis hierzu.

Die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO sind nicht für die Öffentlichkeit bestimmt. Zugriff auf diese Informationen haben nur der behördliche Datenschutzbeauftragte, die jeweils zuständigen Aufsichtsbehörden zum Datenschutz und die eigenen dazu befugten MitarbeiterInnen der jeweiligen datenverarbeitenden Stelle.

**Nach Prüfung durch den Auftraggeber** werden die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen – als Bestandteil des vorliegenden Datenschutzvertrags – verbindlich: Sie sind wie folgt zwischen Auftragnehmer und Auftraggeber festgelegt:

| **Standorte der Datenverarbeitung** | |
| --- | --- |
| Die von dem Auftragnehmer ausgeführte Datenverarbeitung findet an folgenden Standorten statt: | |
|  | |
|  | |
| **Standort der Rechenzentren des Auftragnehmers:** | |
| **Name des Rechenzentrumsbetreibers** |  |
| **RZ-Standort 1 des Dienstleisters** |  |
| **RZ-Standort 2 des Dienstleisters** |  |

|  |
| --- |
| **Vertraulichkeit** |

**Zutrittskontrolle**

Der Auftragnehmer stellt sicher, dass Unbefugte keinen Zutritt zu den Büro-, Server- und Archivräumen haben.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Gibt es einen zentralen Empfangsbereich? | ja  teilweise  nein | Pförtner  Empfang mit Videoüberwachung  Sonstiges: |
| Besteht eine Regelung / Verfahren zur Besucherführung? | ja  teilweise  nein | Empfang  Besucherbuch  Besucherausweis  Persönliche Besucherführung  Sonstiges: |
| Sind Gelände und Gebäude außer-halb der Betriebszeit gesichert? | ja  teilweise  nein | Wachpersonal  Bewegungsmelder / Alarmanlage  Videoüberwachung sensibler Bereiche des Gebäudes  Sonstiges: |
| Gibt es Regelungen für Mitarbeiter bei Nichtanwesenheit? | ja  teilweise  nein | Verschließen von Schränken und Büros bei Nichtanwesenheit |
| Sind die Zu- und Ausgänge gesichert? | ja  teilweise  nein | Gebäudeeingangstüren   Ja     Nein  Fluchttüren / Notausgänge  Ja     Nein     Entfällt  Lüftungsöffnungen  Ja     Nein     Entfällt  Feuerleitern und -treppen   Ja     Nein     Entfällt |
| Sind Zutrittssicherungen eingerichtet? | ja  teilweise  nein | Zutrittskontrollsystem  mit  ohne Sicherheitszonen  Zentrales Schließsystem  Sicherheitsschlösser  Magnetkarte  Biometrische Zugangssperren  Sonstiges: |
| Sorgfältige Auswahl des Sicherheitspersonals? | ja  teilweise  nein |  |
| Wird Fremdpersonal, z. B. Wartungs- und Servicepersonal, beaufsichtigt? | ja  teilweise  nein |  |
| Sind Sicherheitsbereiche definiert? | ja  teilweise  nein | Serverräume  TK-Anlage  Archive  Netzwerkverteiler  Sonstige: |
| Sind diese Sicherheitsbereiche gegen unbefugten Zutritt besonders geschützt? | ja  teilweise  nein | Art des Schutzes: |
| Sind die Zutrittsberechtigungen zu diesen Sicherheitsbereichen geregelt und dokumentiert? | ja  teilweise  nein | Schlüssel / Magnetkarte / Schlüsselvergabe ist zentral und organisatorisch klar geregelt.  Klare Zuweisung der Berechtigungen (Zugang Gebäude, Büro, Serverraum)  (Nur ein bestimmter Personenkreis hat Zutritt zu den Serverräumen.)  Rücknahme von Zugangsmitteln nach Ablauf der Berechtigung |
| Werden zu diesen Sicherheits-bereichen Anwesenheits-aufzeichnungen geführt? | ja  teilweise  nein | In welcher Form? |

**Zugangs-, Benutzer- und Speicherkontrolle**

Der Auftragnehmer verhindert, dass EDV-Systeme von Unbefugten genutzt werden können, sowie eine unbefugte Eingabe, Kenntnisnahme, Veränderung und Löschung von personenbezogenen Daten.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Sind Maßnahmen zur Zugangs-kontrolle zum Desktop und zu den vernetzten Systemen eingerichtet? | ja  teilweise  nein | Benutzerkonto pro Nutzer  Andere Verfahren: |
| Erfolgt die Authentifikation der mit der Datenverarbeitung befugten Personen durch ein sicheres Kennwortverfahren? | ja  teilweise  nein | Authentifikation mit Benutzer und Passwort  Benutzerberechtigungen verwalten |
| Bestehen für alle Zugriffsebenen (Netz, Server, Anwendungen) Passwortregeln zur Gewährleistung eines sicheren und vertraulichen Passworts? | ja  teilweise  nein | Passwortrichtlinie  Sicheres Passwort (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen)  Trivialpasswörter sind nicht erlaubt  Passwort Mindestlänge 8 Zeichen  Regelmäßiger Wechsel des Kennworts  Passwortwiederholungssperre nach Fehlversuchen  Voreingestellte Passwörter müssen geändert werden  Andere Verfahren: |
| Wird die Einhaltung dieser Regeln auf allen Ebenen bei der Eingabe automatisiert kontrolliert? | ja  teilweise  nein |  |
| Ist eine zeitgesteuerte passwort-geschützte Pausenschaltung (Bildschirmschoner) eingerichtet? | ja  teilweise  nein | Automatische Sperrung (z. B. Regelung zur automatischen Sperrung des Computers nach einer bestimmten Zeit der Inaktivität mit anschließendem erneutem Login). |
| Gibt es Regelungen die zusätzlich zur automatischen Sperrung eine manuelle Abmeldung beim Verlassen des Büros vorschreiben? | ja  teilweise  nein |  |
| Erfolgt eine gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk? | ja  teilweise  nein | Kerberos (AD)  TLS / HTTPS  VPN  SSH  Andere Verfahren: |
| Existieren Regelungen bei längerer Abwesenheit eines Mitarbeiters? | ja  teilweise  nein |  |
| Erfolgt eine umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern? | ja  teilweise  nein | Interne Richtlinien / Arbeitsanweisungen |
| Erfolgt eine regelmäßige Kontrolle der Gültigkeit von Berechtigungen? | ja  teilweise  nein |  |
| Werden abschließbare Schränke zur Aufbewahrung von Papierakten genutzt? | ja  teilweise  nein |  |
| Sind die Systeme gegen unbefugtes Eindringen geschützt? | ja  teilweise  nein | Firewall    Anti-Viren-Software  Schnittstellenschutz (Netzwerkschalt­ schränke, Schutz nicht benötigter Netzwerk­steckdosen etc.) |
| Sind Protokollierungen / Überwachungsmaßnahmen eingerichtet, ggf. welche? | ja  teilweise  nein | Testung, Freigabe und Einrichtung von Verfahren  Einrichtung Benutzer und Rechte    Systemänderungen    Zugriffe und Zugriffsversuche    Systemüberwachung  Protokollierung der Administrator- tätigkeiten  An- und Abmeldung an Daten­ verarbeitungsverfahren |
| Werden die Protokolldaten zeitnah und regelmäßig auf sicherheits-relevante Aktionen und Vorgänge überprüft? | ja  teilweise  nein | Automatisiert  Manuell  Durch wen? |
| Ist ein zuverlässiger und aktueller Internetschutz eingerichtet? | ja  teilweise  nein | Firewall  Virenscanner  Web Proxy für HTTP / HTTPS  Datenstrom  URL-Filter |
| Bestehen Regelungen zur sicheren  E-Mail- und Internetnutzung? | ja  teilweise  nein |  |

**Zugriffskontrolle**

Der Auftragnehmer gewährleistet, 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.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Besteht ein dokumentiertes Berechtigungsprofil, das sicherstellt, dass jeder Mitarbeiter nur über die Zugriffsbefugnisse verfügt, die er zur Aufgabenerledigung benötigt? | ja  teilweise  nein | Soweit erforderlich auch differenziert nach:  Leseberechtigung  Schreibberechtigung  Sonstigen Berechtigungen, ggf. welche |
| Ist die Vergabe von generischen Benutzerkennungen oder Gruppenkennungen bzw. Passwörtern untersagt? | ja  teilweise  nein |  |
| Gibt es Regelungen, die eine Weitergabe von Passwörtern untersagt? | ja  teilweise  nein |  |
| Ist die Urlaubsvertretung mit entsprechender Rechtegestaltung geregelt? | ja  teilweise  nein |  |
| Sind die festgelegten Berechtigungen und deren Veränderungen nachvollziehbar dokumentiert? | ja  teilweise  nein |  |
| Ist eine Rechteverwaltung eingerichtet, die bei einer Veränderung des Aufgabengebiets eine zeitnahe Aufhebung nicht mehr benötigter Rechte sicherstellt? | ja  teilweise  nein |  |
| Ist die Vermeidung der Konzentration von Funktionen - Funktionstrennung von Administratorentätigkeiten auf unterschiedliche qualifizierte Personen – gewährleistet? | ja  teilweise  nein |  |
| Wir eine Historie durchgeführter administrativer Änderungen geführt? | ja  teilweise  nein |  |
| Gibt es Regelungen zur Sicherheit der Datenträger? | ja  teilweise  nein | Datenträger sind eindeutig gekennzeichnet  Datenträger sind sicher aufbewahrt  bei Datenträgern von verschiedenen Auftraggebern eindeutige Trennung der Datenträger |
| Gibt es ein differenziertes Ordnerkonzept (z. B. alle Dateien sind einheitlich und nachvollziehbar zu benennen und so abzuspeichern, dass sie problemlos wiedergefunden werden können). | ja  teilweise  nein |  |
| Ist die Anpassung sicherheitsrelevanter Standardeinstellungen von neuen Programmen und IT-Systemen sichergestellt? | ja  teilweise  nein |  |
| Werden nicht benötigte Programme und Funktionen deaktiviert? | ja  teilweise  nein |  |

**Trennungskontrolle**

Der Auftragnehmer gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Es besteht keine Notwendigkeit zu einer physischen Trennung; eine logische Trennung der Daten ist ausreichend.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Sind die Daten der verschiedenen Kunden in geeigneter Weise voneinander getrennt, um eine getrennte Verarbeitung zu gewährleisten? | ja  teilweise  nein | Logische Trennung auf   Betriebssystemebene   Anwendungsebene  Physikalische Trennung |
| Sind die personenbezogenen Daten der jeweiligen Auftraggeber durch Zuordnung zu den jeweiligen Benutzerkennungen logisch voneinander getrennt? | ja  teilweise  nein |  |
| Erfolgt eine Kennzeichnung der erfassten Daten (Aktenzeichen, ID, Kunden / Vorgangsnummer)? | ja  teilweise  nein |  |
| Gibt es eine Trennung von Produktiv- und Testsystem? | ja  teilweise  nein |  |

**Übertragungskontrolle**

Überprüfung und Feststellung an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Ist sichergestellt, dass nur freigegebene Hard-/ Software zum Einsatz kommt? | ja  teilweise  nein |  |
| Gibt es Regelungen und Verfahren, die eine Weiterleitung von E-Mails an private E-Mail-Accounts von Mitarbeitern verbietet bzw. im  E-Mailsystem verhindert? | ja  teilweise  nein |  |
| Gibt es Regelungen zum vertraulichen Umgang mit Backup-Bändern und Datenträgern? | ja  teilweise  nein |  |
| Gibt es eine Richtlinie bzgl. dem Ausdrucken von geheimen Unterlagen (Sicherstellung, dass kein anderer Einsicht in die Ausdrucke bekommt)? | ja  teilweise  nein |  |
| Gibt es Regelungen zum Einsatz von mobilen Datenträgern, wie USB-Sticks und CD-ROMs? | ja  teilweise  nein |  |
| Erfolgt eine Protokollierung der Empfänger von Daten und der Zeitspanne der geplanten Überlassung bzw. vereinbarter Löschfristen? | ja  teilweise  nein |  |

**Datenträgerkontrolle**

Der Auftragnehmer verhindert das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Sind die Festplatten von Laptop / Datenträgern / Smartphones verschlüsselt? | ja  teilweise  nein |  |
| Ist eine Mobile Device Management Lösung im Einsatz? | ja  teilweise  nein |  |
| Ist die Möglichkeit der Fernlöschung von Smartphones bei Verlust sichergestellt? | ja  teilweise  nein |  |
| Werden technische Lösungen zum Sperren von externen Schnittstellen (z.B. USB-Anschlüsse) verwendet? | ja  teilweise  nein |  |

|  |
| --- |
| **Integrität** |

**Weitergabe- / Transportkontrolle**

Der Auftragnehmer gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Gibt es Festlegungen der zur Übermittlung bzw. den Transport (elektronisch, manuell) befugten Personen? | ja  teilweise  nein |  |
| Werden die Daten bei ihrer Übertragung vor unbefugter Kenntnisnahme geschützt? | ja  teilweise  nein | Verschlüsselung  Sichere Verbindungen, z. B. VPN  E-Mail Verschlüsselung / Elektronische Signatur  Sonstige Maßnahmen: |
| Erfolgt die Weitergabe von Daten in anonymisierter oder pseudonymisierter Form? | ja  teilweise  nein |  |
| Werden Datenübermittlungen nachvollziehbar protokolliert und kontrolliert? | ja  teilweise  nein |  |
| Erfolgt eine Prüfung der Daten auf Vollständigkeit nach Datentransport, -übertragung und Datenübermittlung oder –speicherung? | ja  teilweise  nein |  |
| Werden bei Datenträgertransporten die erforderlichen Sicherheits-vorkehrungen beachtet? | ja  teilweise  nein | Verschlüsselung der Daten  Sicherheitsbehälter  Übergabeprotokolle, Lieferscheine  Sicherer Versand, nur eigene oder geprüfte Kuriere  Vollständigkeitskontrollen  Ein- und Ausgangsbücher  Sonstiges: |
| Werden Schnittstellen von PCs und externe Laufwerke (mobile Fest-platten, USB-Sticks etc.) gegen Missbrauch geschützt? | ja  teilweise  nein | Sperrung unbefugter Geräte  Protokollierung der Nutzung der Geräte  Überwachung / Protokollierung des Datenstroms an USB-Schnittstellen  Sicherheitsrichtlinien  Sonstiges: |
| Ist die sichere Nutzung mobiler Datenträger geregelt? | ja  teilweise  nein | Sicherheitsrichtlinie  Mobile Datenträger werden verschlüsselt  Datenträger (USB-Sticks, CD-ROMs) mit vertraulichem Material dürfen nicht offen herumliegen  Nur vom Unternehmen freigegebene Datenträger sind erlaubt |
| Ist die ordnungsgemäße Löschung von Daten bzw. Entsorgung nicht mehr benötigter Datenträger gewährleistet? | ja  teilweise  nein | Sicherheitsrichtlinie  Sicheres Überschreiben nicht mehr benötigter Datenträger  Zertifizierter Dienstleister zu Akten- und Datenvernichtung  Protokollierung der Vernichtung von Daten  Protokolle werden mindestens 12 Monate revisionssicher aufbewahrt |
| Falls die Löschung / Vernichtung von Datenträgern an ein Dienstleistungs-Unternehmen vergeben sind, besteht hierzu ein Vertrag / Auftrag nach den Vorgaben des Art. 28 DSGVO? | ja  teilweise  nein |  |
| Ist die sichere und vertrauliche Außerbetriebnahme von Geräten mit Datenträgern (z.B. Server, Multifunktionsgeräte etc.) geregelt? | ja  teilweise  nein | Art und Inhalt der Regelungen: |
| Sind Sicherheitsgateways an den Netzübergabepunkten implementiert? | ja  teilweise  nein | Firewall Fortigate 3200D |
| Erfolgt bei Fernwartung der Zugriff auf die Kundendaten und Kunden-systeme nur über sichere Leitungen? | ja  teilweise  nein | Wie sind die Leitungen gesichert?  VPN      Verschlüsselung  Sonstiges: SSH, TLS |
| Ist bei Fernwartung eine sichere Identifizierung/Authentifizierung gewährleistet? | ja  teilweise  nein | Bitte das Verfahren kurz beschreiben: |
| Werden bei Fernwartung die Leitungen durch geeignete Sicherheitseinrichtungen, z. B. Protokollierung und Protokoll-auswertung, überwacht? | ja  teilweise  nein | Art der Maßnahmen: |

**Datenintegrität**

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Gibt es eine regelmäßige Integritätsprüfungen der Datenbanken, in denen personenbezogene Daten gespeichert sind? | ja  teilweise  nein |  |
| Gibt es Integritätschecks der IT-Systeme / Anwendungen, mit denen personenbezogene Daten verarbeitet werden? | ja  teilweise  nein |  |

**Eingabekontrolle**

Der Auftragnehmer gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Werden die Einwahlvorgänge in Kundensysteme nachvollziehbar protokolliert und überwacht? | ja  teilweise  nein |  |
| Ist sichergestellt, dass der Zugriff auf Datenverarbeitungssysteme nur nach einem Login erfolgt? | ja  teilweise  nein |  |
| Gibt es eine Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können? | ja  teilweise  nein |  |
| Werden die Benutzung von Datenverarbeitungssystemen und die Eingabe von Daten protokolliert? | ja  teilweise  nein | Protokollierung der Dateibenutzung:  Ja      Nein  Protokollierung von Eingaben und Veränderungen:  Datenfeldbezogen  Datensatzbezogen  Dateibezogen  Keine Protokollierung |
| Erfolgt eine Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten? | ja  teilweise  nein |  |
| Werden die Protokolldaten revisions-sicher und zugriffsgeschützt gespeichert? | ja  teilweise  nein |  |

|  |
| --- |
| **Verfügbarkeit und Belastbarkeit** |

**Verfügbarkeitskontrolle**

Der Auftragnehmer gewährleistet, dass personenbezogene Daten gegen zufällige oder vorsätzliche Zerstörung oder Verlust geschützt sind.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Sind die Kundendaten durch geeignete Sicherungsverfahren vor Zerstörung und Verlust geschützt? | ja  teilweise  nein | Gespiegelter Datenbestand (Storage / RAID Verfahren)  Regelmäßige Sicherungskopien  Back-up-Lösungen  Sonstiges: |
| Gibt es ein Sicherungskonzept, in dem die Art und Weise einer regelmäßigen Sicherung und die Rekonstruktion der Daten festgelegt ist? | ja  teilweise  nein |  |
| Gibt es eine getrennte Aufbewahrung von Daten / Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort? | ja  teilweise  nein |  |
| Werden die Sicherungsbestände sicher verwahrt? | ja  teilweise  nein |  |
| Besteht ein geregeltes Verfahren zur Datenträgerverwaltung mit einer Nachweisführung über Eingang, Ausgang, Versand und Bestand von Datenträgern? | ja  teilweise  nein |  |
| Sind Maßnahmen zur Sicherung des Betriebs des Serverraums und der IT-Infrastruktur zum Schutz gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall eingerichtet? | ja  teilweise  nein | Unterbrechungsfreie Stromversorgung (USV) mit Überspannungsschutz  Notstromversorgung  Klimaanlage mit Überwachung der Funktionen  Branderkennung  Brandschutz, Feuerlöscheinrichtungen  Schutzsteckdosenleisten  Automatischer Shutdown (Notabschaltung) der Systeme  Automatische Stromabschaltung  Sonstiges: |
| Gibt es technische Systeme die eine Alarmmeldung bei unberechtigten Zutritten zu Serverräumen auslösen? | ja  teilweise  nein |  |
| Gibt es ein Notfallhandbuch mit Alarmierungs- und Wiederanlaufplan? | ja  teilweise  nein |  |
| Ist das Notfallhandbuch transportabel und schnell erreichbar, z. B. auf einem mobilen Datenträger, oder sicher ausgelagert? | ja  teilweise  nein |  |
| Wird der bestehende Notfallplan regelmäßig geübt? | ja  teilweise  nein |  |

**Wiederherstellbarkeit**

Der Auftragnehmer gewährleistet die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu diesen bei einem physischen oder technischen Zwischenfall durch die folgenden Maßnahmen rasch wiederherzustellen:

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Gibt es ein Backup- und Disaster Recovery Konzept? | ja  teilweise  nein |  |
| Es gibt ein Backup-Verfahren zur täglichen, wöchentlichen, monatlichen und jährlichen Sicherung der Daten? | ja  teilweise  nein |  |
| Erfolgt die Aufbewahrung der Backup-Daten in Datensicherungsschränken oder Tresoren in einem anderen Brandabschnitt? | ja  teilweise  nein |  |
| Die Datenwiederherstellung wird regelmäßig getestet? | ja  teilweise  nein |  |

**Zuverlässigkeit**

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Gibt es eine Inventarliste zur Nachvollziehbarkeit bei Verlust? | ja  teilweise  nein |  |
| Erfolgt ein Monitoring der für die Verarbeitung der personenbezogenen Daten erforderlichen Dienste mit Meldefunktion bei Fehlfunktionen? | ja  teilweise  nein |  |
| Werden die Installations- und Systemdokumentationen regelmäßig aktualisiert? | ja  teilweise  nein |  |
| Erfolgt eine regelmäßige Wartung? | ja  teilweise  nein | . |

|  |
| --- |
| **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** |

**Datenschutzmanagement**

Der Auftragnehmer gewährleistet die Einhaltung der Datenschutzvorgaben.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Gibt es ein Datenschutzkonzept bzw. ein Datenschutzhandbuch zur Regelung und Umsetzung des Datenschutzes im Unternehmen? | ja  teilweise  nein |  |
| Existiert ein vollständiges Verzeichnis von Verarbeitungstätigkeiten? | ja  teilweise  nein |  |
| Gibt es ein Sicherheitskonzept? | ja  teilweise  nein |  |
| Erfolgt eine Verpflichtung der Mitarbeiter\*innen auf die Wahrung der Vertraulichkeit der Daten? | ja  teilweise  nein |  |
| Werden die Mitarbeiter\*innen laufend in die Anforderungen des Datenschutzes eingewiesen? | ja  teilweise  nein |  |
| Ist sichergestellt, dass Dritte eine Verschwiegenheitserklärung abgeben müssen? | ja  teilweise  nein |  |
| Wenn aus organisatorischen Gründen Funktionsüberschneidungen bestehen, wird das Vier-Augen-Prinzip angewendet und dokumentiert? | ja  teilweise  nein |  |
| Existiert eine definierte Vertreterregelung innerhalb der Funktionsgruppen? | ja  teilweise  nein |  |

**Auftragskontrolle**

Der Auftragnehmer gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers und zur Erfüllung des vertraglich definierten Verwendungszweckes verarbeitet werden. Der Auftraggeber kann dies durch ein gemäß Art. 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO nachweisen. Sollte keine Zertifizierung vorliegen geschieht der Nachweis durch:

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Die Weisungsberechtigten des Auftraggebers und die zur Entgegennahme von Weisungen befugten Personen sind vertraglich definiert, Weisungen erfolgen immer schriftlich. | ja  teilweise  nein |  |
| Wird die Durchführung des Kunden-auftrags / der Serviceaktion nachvollziehbar überwacht, um eine auftragskonforme Erledigung zu gewährleisten? | ja  teilweise  nein | In welcher Form? |
| Werden Aufträge als Support-Ticket erfasst, und die durchgeführten Arbeiten dokumentiert? | ja  teilweise  nein | ☐ Es gibt eine eindeutige Zuordnung zwischen Support-Ticketnummer und Kundenauftrag. |
| Sind geeignete Protokollierungs- und Auswertungsmechanismen eingerichtet, um unzulässige Zugriffe auf Kundensysteme und Kundendaten zu überwachen? | ja  teilweise  nein | In welcher Form? |
| Werden bei einer Vergabe von Serviceaufträgen mit Unterauftragnehmern (z. B. IT-Service) die Vorgaben des Art. 28 DSGVO beachtet? | ja  teilweise  nein | Auswahl des Unterauftragnehmers gemäß DSGVO  Überprüfung der technischen und organisatorischen Maßnahmen beim Unterauftragnehmer  Abschluss eines Vertrags gemäß   Art. 28 DSGVO  Regelmäßige Überprüfung des Unterauftragnehmers |

**Beurteilung des angemessenen Schutzniveaus (Art. 32 Abs. 2 DSGVO)**

Der Auftragnehmer gewährleistet eine dokumentierte Beurteilung eines angemessenen Schutzniveaus, bezüglich der Risiken, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang - der im Auftrag verarbeiteten personenbezogenen Daten.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Erfolgt die Durchführung einer Risikoanalyse für die Verarbeitungen personenbezogener Daten? | ja  teilweise  nein |  |
| Wurden Schutzbedarfskategorien definiert? | ja  teilweise  nein |  |
| Sind die Prozesse nach „Privacy by Design & Default“ ausgerichtet? | ja  teilweise  nein |  |
| Erfolgt bei Bedarf die Durchführung einer Datenschutz-Folgenabschätzung (DSFA)? | ja  teilweise  nein |  |

**Evaluierung der Einhaltung der technisch-organisatorischen Maßnahmen**

Der Auftragnehmer überprüft die Wirksamkeit der technisch-organisatorischen Maßnahmen.

| **Anforderung** | Antwort | **Bemerkung / Erläuterung** |
| --- | --- | --- |
| Werden regelmäßige Schwachstellenscans durchgeführt? | ja  teilweise  nein |  |
| Werden regelmäßige Sicherheitsaudits durchgeführt? | ja  teilweise  nein | Interne Audits  Externer Auditor |
| Werden regelmäßige Pentests durchgeführt? | ja  teilweise  nein | Interne Pentests  Externer Auditor |
| Gibt es Zertifizierungen nach Sicherheitsstandards? | ja  teilweise  nein |  |

|  |
| --- |
| **Verpflichtungserklärung zur Umsetzung der  technischen und organisatorischen Maßnahmen** |

Der Auftragnehmer bestätigt, dass er die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten des Auftraggebers – wie beschrieben – vor Beginn der Datenverarbeitung umgesetzt hat. Der Auftragnehmer verpflichtet sich, die Erfüllung dieser Anforderungen für die Dauer der Zusammenarbeit sicherzustellen, regelmäßig zu kontrollieren, zu dokumentieren und auf Nachfrage des Auftraggebers zur Verfügung zu stellen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insofern ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber unverzüglich mitzuteilen.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Ort, Datum |  | Unterschrift / Firmenstempel |

## Dokumentenlenkung

|  |  |  |  |
| --- | --- | --- | --- |
| Dateiname | Version | Änderungsdatum | Autor/in |
|  | 1.0 |  |  |
| Vertraulichkeitsstufe | Bearbeitungsstatus | Freigabedatum | Freigabe durch |
|  |  |  |  |