# Anlage – Technische und organisatorische Maßnahmen (TOM)

| **Nr.** | **Gebiet** | **Beschreibung** |
| --- | --- | --- |
| **0** | **Organisation** | |
|  | Wie ist die Umsetzung des Datenschutzes organisiert? | Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus dem DSGVO eingesetzt. |
|  | Nennen Sie uns bitte den Namen und die Kontaktdaten Ihres Datenschutzbeauftragten. | Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 14, 93047 Regensburg Tel: +49-941-2986930 E-Mail: c.volkmer@projekt29.de |
|  | In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen? | Regelmäßige Datenschutzschulungen aller Mitarbeiter  Verpflichtung aller Mitarbeiter auf die Datenschutzerklärung |
|  | Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert? | Ja, im Rahmen des internen Verfahrens-verzeichnisses sind die Datenströme dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach DSGVO nachgewiesen. |
| **1** | **Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)** | |
| **1.1** | **Zutrittskontrolle** | |
|  | Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert? | Alarmanlage in Gebäudeanteil der Firma. |
|  | Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert? | Sicherungskreise der Alarmanlage. Zutritt nur für Mitarbeiter per dediziertem RFID-Chip.  Benachrichtigung von Sicherheitsdienst und bestimmten Mitarbeitern bei Alarm. |
|  | Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt? | Gesonderter Sicherungskreis der Alarmanlage mit Zugang nur für Administrationspersonal. |
|  | Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft? | Im Rahmen der Kontrollen durch den externen Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft. |
| **1.2** | **Zugangskontrolle** | |
|  | Wie erfolgt die Vergabe von Benutzerzugängen? | Die Abteilungsleiter bzw. Geschäftsführer melden den Eintritt neuer Mitarbeiter an die Administration.  Mitarbeiter erhalten bei Eintritt Microsoft Active Directory (AD)-Accounts, die Berechtigungen werden über AD-Gruppen geregelt. (Abteilungs-, Team- oder individuell basierte Zugehörigkeiten) |
|  | Wie wird die Gültigkeit von Benutzerzugängen überprüft? | Die Abteilungsleiter bzw. Geschäftsführer sind verpflichtet, relevante Änderungen in Beschäftigungsverhältnissen rechtzeitig der Administration anzuzeigen. |
|  | Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert? | Anforderungen zu Benutzerzugängen können nur von den Abteilungsleitern bzw. Geschäftsführern per E-Mail beantragt bzw. genehmigt werden und werden von der Administration per E-Mail bestätigt. Der Verlauf wird über die Mail-Archivierung festgehalten. |
|  | Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird? | Administrationszugänge erhalten nur der dedizierte Systemadministrator und Vertretungen aufgrund Genehmigung durch die Geschäftsführung.  Alle betreffenden und in Frage kommenden Personen besitzen einen nachweislichen fachlichen IT-Hintergrund mit Erfahrung in der Administration. Sie sind weder temporär noch als externe Mitarbeiter beschäftigt, befinden sich nicht in Probezeit, und wurden auf die Datenschutzerklärung des Unternehmens verpflichtet. |
|  | Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet? | Der Zugriff ist über eine verschlüsselte VPN-Verbindung (L2TP) für explizit freigegebene Mitarbeiter möglich. Die Authentifizierung erfolgt über die Microsoft Active Directory-Anmeldedaten und einen Preshared Key. |
| **1.3** | **Zugriffskontrolle** | |
|  | Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind? | Es existieren keine gemeinsam genutzten Benutzerzugänge.  Die Benutzer erhalten ein individuelles Initial-Passwort. Eine Änderung des Passwortes wird bei der ersten Anmeldung technisch erzwungen.  Die Mitarbeiter werden bei der Einstellung unterwiesen, sorgsam mit Passwörtern umzugehen und diese nicht anderen Personen zugänglich zu machen. |
|  | Welche Anforderungen werden an die Komplexität von Passwörtern gestellt? | Es werden nur Kennwörter akzeptiert, die keinen Teil des Benutzer-Logons oder –Namens darstellen, 3 aus 4 verschiedenen Zeichenklassen enthalten, und mind. 8 Zeichen lang sind. |
|  | Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss? | Durch Gruppenrichtlinien (Systemeinstellungen Microsoft Active Directory) wird ein Wechsel des Passworts nach 60 Tagen erzwungen oder der Zugriff gesperrt. Das neue Passwort darf nicht einem der drei vorherigen entsprechen. |
|  | Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen? | Zugriffsfreigaben erfolgen User- und Gruppen-basiert für die mit der Verarbeitung betrauten Personen.  Die Systeme sind Passwortgeschützt. Arbeitsplätze werden automatisch bei Inaktivität gesperrt. Die Mitarbeiter sind unterwiesen, bei Verlassen des Arbeitsplatzes ihre Arbeitsplätze zu verlassen und keine sichtbaren bzw. frei zugängliche personenbezogene Daten zu hinterlassen. |
|  | Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden? | Die Geschäftsführung prüft in regelmäßigen Abständen die Rechte und Benutzerstruktur. |
|  | Wie erfolgt die Dokumentation von Zugriffsberechtigungen? | Über die Access Control Lists in den Systemen. |
|  | Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden? | Sporadische Durchsicht der Systemprotokolle durch die Geschäftsführung. |
|  | Wie lange werden Protokolle aufbewahrt?  Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet? | Keine festgelegten Fristen, meist Systemparameter,  ausschließlich die Geschäftsführung. |
| **1.4** | **Trennungskontrolle** | |
|  | Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden? | Zur Trennung der Daten wird ein dezidiertes Rechtesystem eingesetzt. |
| **1.5** | **Pseudonymisierung** | |
|  | Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt? | Regelmäßige Datenschutzschulungen aller Mitarbeiter  Verpflichtung aller Mitarbeiter auf die Datenschutzerklärung |
|  | Wie werden personenbezogene Daten verarbeitet /aufbewahrt, sodass diese nicht den betroffenen Personen zugeordnet werden können? | Die Verarbeitung personenbezogener Daten kann in den meisten Fällen einer betroffenen Person zugeordnet werden. |
| **2** | **Integrität (Art. 32 Abs. 1 lit. b DS-GVO)** | |
| **2.1** | **Weitergabekontrolle** | |
|  | Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten? | Die Weitergabe erfolgt über verschlüsselte Kanäle und/oder die Verschlüsselung der Daten selbst.  Eine Zustellung oder Bekanntgabe von Zugangsdaten erfolgt nur an den vorhergesehen Empfänger. |
|  | Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche? | Ein Versenden per E-Mail oder Bereitstellung per Internet erfolgt über Server mit Transportverschlüsselung (TLS).  Die Verschlüsselung von Daten erfolgt auf Datenträgerbasis über Microsoft Bitlocker und/oder über verschlüsselte ZIP-Archive (AES-256). |
|  | Wie wird die Weitergabe personenbezogener Daten dokumentiert? | n/a |
|  | Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt? | Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff. |
|  | Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann? | Dies wird im Rahmen der Kontrollen unter Punkt 1.3 mit geprüft. |
| **2.2.** | **Eingabekontrolle** | |
|  | Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat? | Zugriffs-Logs der Server und Systeme. |
|  | Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden? | Zugriffs-Logs der Applikationen. |
|  | Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisungen des Auftraggebers erfolgen kann? | Schulung bzw. Sensibilisierung der Mitarbeiter durch regelmäßige Veranstaltungen bzw. Personalgespräche. |
|  | Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt? | Die Datenverarbeitung von Unterauftragnehmern erfolgt mit eindeutigen Auftragsdefinitionen und einer formalisierten Auftragserteilung. |
|  | Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt? | Festlegung durch Vertragsbindung, bei Wegfall des Zweckes ist ebenfalls eine Löschung der Daten indiziert. |
| **3** | **Verfügbarkeit und Belastbarkeit** | |
| **3.1.** | **Verfügbarkeitskontrolle** | |
|  | Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind? | Die Backup-Datenträger werden in einem entsprechenden Panzerschrank aufbewahrt.  Backup-Sätze werden turnusmäßig extern durch die Geschäftsführung ausgelagert. |
|  | Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet? | Betriebssystem-Sicherheitsupdates und Antiviren-Software und –Definitionen werden zentral automatisiert ausgerollt und aktualisiert.  Antiviren- und Firewall-Lösungen werden auf den Client- und Serversystemen eingesetzt.  Eingehende Mails werden vor Zustellung durch den Mail-Transport-Server auf Schädlinge und gefälschte Absenderdaten geprüft. |
|  | Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden? | Die anfallenden Datenträger werden zentral durch die IT-Abteilung entsorgt.  Funktionsfähige Datenträger werden entsprechend geeigneter Methoden sicher gelöscht. (z.B. mehrfaches Überschreiben)  Nicht funktionsfähige Datenträger werden physikalisch vernichtet. |
| **3.2.** | **Wiederherstellbarkeit** | |
|  | Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DS-GVO) | Die Server- und Stromversorgungssysteme der Verarbeitungsanlage sind redundant ausgelegt, um einem Ausfall vorzubeugen. |
| **4.** | **Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)** | |
|  | Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)? | Der externe Datenschutzbeauftragte überprüft regelmäßig und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen. |
|  | Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)? | Einsatz eines Ticketsystems (Kayako) zweistufig (1st und 2nd Level); zusätzlich Telefonhotline und automatisierte Überwachung und Alarmierung |
|  | Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)? | Keine Vorbelegung durch Haken; bei Anmeldung im System erfolgen keine Vorbelegungen; Benutzer muss die Anmeldeinformationen jeweils eintragen |
| **4.1** | **Auftragskontrolle** | |
|  | Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)? | Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsdatenverarbeitung gestaltet. Der externe Datenschutzbeauftragte nimmt entsprechende Beratungs- und Kontrollpflichten wahr. |