



Dokumentation der technischen und organisatorischen Maßnahmen (TOM) nach Art. 32 DSGVO

dab: Daten- Analysen & Beratung GmbH

dab: data driven services GmbH

(nachfolgend **dab: Gruppe** genannt)

Hans-Obser-Straße 12

94469 Deggendorf

Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

der
dab: Gruppe
Hans-Obser-Straße 12
94469 Deggendorf

Stand: 12/2023

Erläuterung:

Technische und organisatorische Maßnahmen (TOM) sind die nach Art. 32 Datenschutzgrundverordnung (DSGVO) vorgeschriebenen Maßnahmen, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Nach Art. 32 DSGVO sind Verantwortliche und der Auftragsverarbeiter verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs und der Zwecke der Verarbeitung, sind die Maßnahmen zu bestimmen.

Aus Art. 24 Abs. 1 bzw. Art. 32 Abs. 1 ergibt sich zusätzlich die Pflicht zur regelmäßigen Überprüfung sowie einer, wenn nötig, erforderlichen Aktualisierung des Dokumentes.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Der Zutritt Unbefugter zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, wird durch verschiedene technische und organisatorische Maßnahmen verhindert.

An den Eingängen kommen personalisierte RFID-Transponder zum Einsatz, die dem Stand der Technik entsprechen und mit individuellen Zugangsberechtigungen ausgestattet sind. Das dokumentierte Berechtigungskonzept zum Einsatz der Transponder wird regelmäßig auf

Aktualität überprüft. Dabei werden vergebene Zutrittsberechtigungen auf Notwendigkeit überprüft und bei Bedarf angepasst. Änderungen, die sich zwischen den Überprüfungszyklen ergeben, werden sofort behandelt und umgesetzt.

Durch automatisch verschließbare Türen wird sichergestellt, dass der Zutritt zum Unternehmen permanent eingeschränkt und nur für berechtigte Personen mittels Transponder möglich ist.

Diensträume und Büros, in denen vertrauliche Daten verarbeitet werden (u.a. Geschäftsleitung) werden bei Abwesenheit, auch während der Geschäftszeiten, stets verschlossen.

Besucher des Unternehmens werden von der Verwaltung in Empfang genommen und im Rahmen eines internen Besucherprozesses erfasst. Die Protokollierung der Besucher erfolgt stets datenschutzkonform.

Der Zutritt zum Serverraum wird ebenfalls durch ausreichende technische und organisatorische Maßnahmen geschützt. Der Zutritt ist nur für autorisiertes, technisches Personal mit personalisiertem Schlüssel möglich. Zudem wird sichergestellt, dass die eigene IT-Hardware im Serverraum stets in verschlossenen Schränken aufbewahrt und abgeschlossen wird.

Die Haupteingänge der Geschäftsräume sind während der Öffnungszeiten durchgehend durch abgeschlossene Türen gesichert.

1.2 Zugangskontrolle

Im Unternehmen wird sichergestellt, dass nur berechtigte Mitarbeiter oder Vorgesetzte Zugang zu Anwendungen und Systemen erhalten, in denen personenbezogene Daten verarbeitet werden. Aus technischer Sicht wird hierzu für jeden Mitarbeiter eine individuelle Identifikation mittels Benutzername und Passwort sichergestellt. Passwörter besitzen eine Komplexität, welche dem Stand der

Technik entspricht. (Mindestens 10 Zeichen, Großbuchstaben, Kleinbuchstaben, Sonderzeichen). Die Einhaltung der Komplexität wird durch technische Maßnahmen erzwungen. Zudem sind Mitarbeiter darauf sensibilisiert für jedes Portal ein unterschiedliches Kennwort zu verwenden. Computer müssen außerdem bei vorübergehendem Verlassen des Arbeitsplatzes stets durch die Aktivierung des passwortgeschützten Bildschirmschoners gesperrt werden. Hierzu existieren organisatorische Richtlinien im Unternehmen. Technisch betrachtet tritt die Sperre der Computer nach 5 Minuten automatisch ein.

Datenträger in Notebooks sind im Unternehmen durch eine Pre-Boot Verschlüsselung auf Hardwareebene durch fremde Zugriffe abgesichert. Zudem existiert als organisatorische Maßnahme ein Prozess im Unternehmen der sicherstellt, dass mögliche Verluste eines mobilen Endgerätes unverzüglich an die IT-Abteilung gemeldet und behandelt werden. Im Falle eines Verlustes wird stets der bestellte Datenschutzbeauftragte zur weiteren Behandlung und zur Meldung des Vorfalls miteinbezogen.

Client-Systeme werden durch eine Antivirensoftware vor Viren, Trojanern und weiteren Angriffen geschützt. Die notwendigen Signaturupdates der Virens Scanner erfolgen dabei in angemessenen Zeitabständen. Zusätzlich erfolgt ein zentrales Patch-Management, wodurch Client-Systeme stets mit aktuellen Sicherheitsupdates versorgt werden.

Das Unternehmensnetzwerk ist durch den Einsatz von aktuellen Firewalls und Malware-Scannern, Intrusion-Detection und Intrusion-Prevention vor Angriffen geschützt.

Zugänge zu IT-Systemen von außen sind nur kontrolliert entweder über eine zusätzliche Multifaktor-Authentifizierung oder über eine verschlüsselte VPN-Verbindung möglich. Auch bei Zugriff über VPN ist eine Multi-Faktor-

Authentifizierung erforderlich.

Zusätzlich zu den technischen Maßnahmen wird die Zugangskontrolle durch organisatorische Regelungen verstärkt. Hierzu zählen unternehmensinterne Richtlinien zum Datenschutz und zur Informationssicherheit wie der sichere Umgang mit mobilen Datenträgern und die Einhaltung der Datenschutz- und Sicherheitsvorschriften an mobilen Arbeitsplätzen. Mitarbeiter sind zur Einhaltung aller vorhandenen Richtlinien verpflichtet, sodass etablierte technische und organisatorische Maßnahmen auch am jeweiligen mobilen Arbeitsplatz des Mitarbeiters zum Einsatz kommen. Zudem werden alle Mitarbeiter schriftliche auf Vertraulichkeit verpflichtet.

1.3 Zugriffskontrolle

Das Unternehmen trifft dem Stand der Technik entsprechende Maßnahmen zur Zugriffskontrolle der Datenverarbeitungsanlagen und IT-Systeme. Die umgesetzten Maßnahmen verfolgen das Ziel, dass ein ausreichender Schutz vor unbefugtem Lesen, Verändern oder Löschen von Daten durch Unbefugte gewährleistet wird. Hierzu verwendet das Unternehmen Datenschutzcontainer zur Entsorgung von nicht mehr benötigten Informationen und Dokumenten. Die Inhalte davon werden in regelmäßigen Abständen durch einen zertifizierten Dienstleister abgeholt und nach DIN 66399 datenschutzkonform entsorgt. So wird sichergestellt, dass personenbezogene Daten auch nach der Entsorgung vor unberechtigten Zugriffen geschützt werden.

Generell werden alle Datenträger vor Außerbetriebnahme über ein angemessenes Verfahren gelöscht, bei Bedarf auch mechanisch DSGVO-konform zerstört.

Aus organisatorischer Sicht existiert für sämtliche IT-Systeme und Anwendungen ein dokumentiertes Rechte- und Rollenkonzept.

Hierzu zählen eigene Konzepte für die Dokumentenablage auf der Fileserver-Infrastruktur sowie für das eingesetzte CRM-System und weitere als relevant klassifizierte Infrastruktur. Durch das individuelle Berechtigungsmanagement wird eine differenzierte Steuerung der Zugriffe auf personenbezogene Daten ermöglicht. Die vergebenen Berechtigungen werden regelmäßig überprüft und anlassbezogen angepasst. Insbesondere bei Einstellung, unternehmensinternen Wechseln oder einer Beendigung des Arbeitsverhältnisses, erfolgt eine sofortige Änderung der Berechtigungen. Die Vergabe, die Änderung und der Entzug von Berechtigungen erfolgen nur nach ausdrücklicher Freigabe der Geschäftsleitung oder entsprechend berechnete Personen. Zugriffsberechtigungen werden ausschließlich von Administratoren verwaltet. Die Administratorkonten beschränken sich auf ein Minimum und stehen nur einem ausgewählten Personenkreis zur Verfügung. Der Zugriff auf personenbezogene Daten ist so geregelt, dass Mitarbeiter nur Zugriff auf Daten erhalten, die für die Erfüllung der jeweiligen Aufgaben erforderlich sind. Hierbei orientiert sich das Unternehmen am „need-to-know“-Prinzip.

1.4 Trennungskontrolle

Mit Maßnahmen der Trennungskontrolle stellt das Unternehmen sicher, dass stets eine Zweckgebundenheit der Datenverarbeitung erreicht wird. Über geeignete Techniken wird gewährleistet, dass personenbezogene Daten von Kunden, Auftraggebern und eigene Daten logisch oder physikalisch getrennt verarbeitet werden. Bei relevanten Anwendungen wird auf Mandantenfähigkeit geachtet, sofern dies notwendig ist. Produktiv- und Testsysteme sind voneinander getrennt. Organisatorisch betrachtet wird die Trennungskontrolle mittels Berechtigungskonzepten und der Festlegung von Datenbankrechten erreicht. Personenbezogene Daten werden in unterschiedlichen Projektordnern von Windows

verwaltet, welche zusätzlich verschlüsselt sind. Dies ermöglicht eine strikte Trennung bei der Verarbeitung.

2. Integrität

2.1 Weitergabekontrolle

Durch Maßnahmen der Weitergabekontrolle wird sichergestellt, dass Daten vor unbefugter Veränderung, aber auch vor unbefugtem Lesen oder Kopieren geschützt sind. Um dies sicherstellen zu können, werden für die Datenübertragung ausschließlich verschlüsselte Verbindungen in Form von VPN bzw. SSL-Technologien genutzt. Bei der Nutzung von E-Mail wird auf Transportverschlüsselung geachtet. Sofern vertrauliche Daten per E-Mail weitergegeben werden, erfolgt zusätzlich eine Inhaltsverschlüsselung auf Basis von passwortgeschützten Anhängen. Die Weitergabe des Passworts an den Empfänger erfolgt dabei über einen separaten Kanal wie beispielsweise Telefon. Bei der generellen Weitergabe von personenbezogenen Daten an externe Empfänger wird die Dauer der Überlassung und ggf. notwendige Löschrufen geprüft und eingehalten. Um dieser Maßnahme nachzukommen, existiert im Unternehmen ein separates Löschkonzept, welches die Anforderungen der DSGVO berücksichtigt. Die technischen Maßnahmen zur Weitergabekontrolle werden detailliert im eingesetzten Informationssicherheitsmanagementsystem des Unternehmens beschrieben.

Bei Bedarf werden vertrauliche Daten – sofern sie auf externen Datenträgern weitergegeben werden – mit ausreichenden kryptographischen Verfahren abgesichert. Wo möglich, werden personenbezogene Daten pseudonymisiert oder anonymisiert.

Für Fremddaten die dem Unternehmen im Zuge von Datenanalyseprojekten von Kunden zur Verfügung gestellt werden, gelten besondere Vorsichtsmaßnahmen. Hierbei wird darauf geachtet, dass Daten nur auf verschlüsselten Datenträgern gespeichert

werden und die Verarbeitung stets durch explizite Vereinbarungen und Einverständniserklärungen mit dem Kunden geregelt ist.

2.2 Eingabekontrolle

Maßnahmen zur Eingabekontrolle verfolgen das Ziel, die Nachvollziehbarkeit von Eingaben, Änderungen oder Löschungen von Daten gewährleisten zu können. Durch organisatorische Maßnahmen wird dies im Unternehmen sichergestellt, in dem individuelle Benutzernamen an Stelle von Benutzergruppen eingesetzt werden. Es haben ausschließlich autorisierte Mitarbeiter die Möglichkeit, Änderungen an personenbezogenen Daten vorzunehmen, je nach ihrer Funktion und Tätigkeit.

Veränderungen von personenbezogenen Daten werden softwareseitig durch eine Stammdaten- sowie Bewegungsdatenprotokollierung inkl. Änderungsprotokoll aufzeichnet. Die Protokolle sind nur von berechtigten Personen einsehbar. Dies sorgt für eine genaue Nachvollziehbarkeit innerhalb der Systeme und gewährleistet somit eine DSGVO-konforme Eingabekontrolle.

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Das Unternehmen trifft dem Stand der Technik entsprechende Maßnahmen, um die kontinuierliche Verfügbarkeit und Belastbarkeit von personenbezogenen Daten und Informationen sicherzustellen. Das Ziel der umgesetzten Maßnahmen ist die Gewährleistung eines dauerhaften Schutzes vor Datenverlust, Zwischenfällen oder sonstigen Schadensereignissen. Um dieses Ziel zu erreichen, werden IT-Systeme in zwei Serverräumen an jeweils zwei unterbrechungsfreie Stromversorgungen (USV) angeschlossen. Die Server sind untereinander in einem High-Availability-Cluster abgesichert.

Zusätzlich sind beide Serverräume mit einer redundanten Klimaanlage ausgestattet, welche wiederum mit Temperaturkontrollen und Luftfeuchtigkeitsregelanlage versehen ist. Zum Schutz vor Feuer ist eine Brandmeldeanlage installiert.

Damit die korrekte Umsetzung der physischen Maßnahmen überprüft werden kann, wird der Serverraum in regelmäßigen Abständen durch den Datenschutzbeauftragten auditiert.

Aus organisatorischer Sicht liegt ein erprobtes Backup & Recovery-Konzept vor, mit dem betriebsnotwendige IT-Systeme und Daten in möglichst kurzem Zeitraum wiederhergestellt werden können. Sicherungsvorgänge werden kontrolliert und protokolliert. Zusätzlich finden in regelmäßigen Abständen Recovery-Tests zur Datenwiederherstellung statt. Die Redundanz der primären IT-Systeme ist zu jeder Zeit gegeben. Die Backup-Strategie ist so konzipiert, dass die Sicherungen, je nach Kritikalität des jeweiligen Systems, in regelmäßigen und dokumentierten Intervallen durchgeführt werden.

Zusätzlich sind die Systeme in eine umfassende System- und Netzwerküberwachung eingebunden, sodass im Falle einer Störung zeitnah auf Ausfälle reagiert werden kann. Zur Überprüfung der Belastbarkeit der IT-Infrastruktur werden bei Bedarf Penetrationstests durchgeführt. Ausfälle der Internetverbindung können durch eine entsprechende Backup-Leitung kompensiert werden.

3.2 Datenschutz-Management

Um den Anforderungen der Datenschutzgrundverordnung gerecht zu werden, wurden ausreichende organisatorische Datenschutz-Management-Prozesse innerhalb der Organisation etabliert. Diese verfolgen das Ziel, eine kontinuierliche Umsetzung des Datenschutzes im Unternehmen zu gewährleisten. Die etablierten Prozesse, Aufgaben und Dokumentationen pflegt das

Unternehmen in einer Datenschutz-Management-Software.

Für das Unternehmen wurde ein externer Datenschutzbeauftragter bestellt. Er berät und informiert die Verantwortlichen, die Betroffenen oder die Auftragsverarbeiter in Datenschutzfragen. Er überwacht die Einhaltung der Vorgaben der DSGVO, der internen Datenschutzvereinbarungen und arbeitet mit der zuständigen Aufsichtsbehörde zusammen. Bei Bedarf werden Datenschutzfolgenabschätzungen für notwendige Prozesse oder Technologien durchgeführt. Hierbei unterstützt der Datenschutzbeauftragte mit seiner Fachkenntnis. Das Unternehmen kommt den Informationspflichten nach Art. 13 und Art. 14 DSGVO nach.

Sämtliche Mitarbeiter sind durch eine schriftliche Vereinbarung auf Vertraulichkeit verpflichtet und dafür sensibilisiert. Getroffene Richtlinien und technische Maßnahmen sind so konzipiert, dass diese auch von Mitarbeitern vom mobilen Arbeitsplatz aus eingehalten werden. Mitarbeiter des Unternehmens werden bei Unternehmenseintritt durch eine initiale Datenschutzbildung sensibilisiert. Zusätzlich finden weiterführende und regelmäßige Sensibilisierungen unter Einbeziehung des Datenschutzbeauftragten statt.

Der intern eingesetzte Informationssicherheitsbeauftragte entwickelt zusätzlich Maßnahmen und Leitlinien, um sicherzustellen, dass angestrebte IT-Sicherheitsstrategien wirksam umgesetzt werden. Hierbei orientiert sich das Unternehmen am internationalen Standard für Informationssicherheit ISO/IEC 27001. Das etablierte IT-Sicherheitskonzept ist ausgerollt und allen Mitarbeitern bekannt.

3.3 Auftragskontrolle

Werden Dritte mit der Verarbeitung von personenbezogenen Daten beauftragt, wird durch geeignete Maßnahmen gewährleistet, dass Daten nur entsprechend den Weisungen

des Auftraggebers verarbeitet werden. Sämtliche Auftragnehmer werden unter Sorgfaltsgesichtspunkten hinsichtlich des Datenschutzes und der Datensicherheit ausgewählt. Mit allen Auftragnehmern werden stets notwendige Vereinbarungen zur Auftragsverarbeitung abgeschlossen. Die existierenden Verträge zur Auftragsverarbeitung werden regelmäßig durch den Datenschutzbeauftragten auf inhaltliche Korrektheit geprüft. Weitere Subunternehmer werden im Regelfall nicht eingesetzt. Wenn personenbezogene Daten in ein Drittland übermittelt werden, werden die Bedingungen der Art. 44 ff DSGVO eingehalten. Sollte dies notwendig sein, werden dazu ebenfalls die datenschutzrechtlichen Anforderungen geprüft und ausschließlich durch den Datenschutzbeauftragten als Empfehlung für die Geschäftsführung freigegeben. Sofern Dienstleister in einem erweiterten Bereich für das Unternehmen tätig sind (z.B. Umsetzung der Webseite), werden mit diesen stets Vertraulichkeitsvereinbarungen und Datenverarbeitungsvereinbarungen abgeschlossen.

Gemäß Artikel 25 DSGVO gewährt das eingesetzte CRM-System unter Beachtung der Implementierungskosten und dem Stand der Technik die notwendigen datenschutzfreundlichen Voreinstellungen. Dies bedeutet im Einzelnen die Wahrung der Grundsätze für die Verarbeitung von personenbezogenen Daten gemäß Artikel 5 DSGVO wie die Speicherbegrenzung und Datenminimierung. Durch diese Beachtung kann einem Datenschutzvorfall vorgebeugt werden.

4. Aktualisierung der Maßnahmen

Die technischen und organisatorischen Maßnahmen werden mindestens einmal jährlich auf Aktualität und Angemessenheit überprüft und ggf. angepasst. Das Ergebnis wird jeweils dokumentiert.

Sollten sich außerhalb des Überprüfungszyklus signifikante Änderungen an den umgesetzten Maßnahmen ergeben, wird die Dokumentation der technischen und organisatorischen Maßnahmen direkt angepasst. Bei jeder Überprüfung der eingesetzten Maßnahmen wird darauf geachtet, dass Datenschutzmaßnahmen durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen so konzipiert werden, dass stets der Stand der Technik berücksichtigt wird.

5. Änderungsnachweis

Versio n	Autor	Änderun g	Datum
1.0	Thomas Greiner	Erstellung	05.10.2020
1.1	Tobias Damasko	Änderung / Überprüfung	15.02.2022
1.1	Stefan Wenig	Freigabe	16.02.2022
2.1	Michael Paternoster	Änderung / Überprüfung	29.11.2023
2.1	Stefan Wenig	Freigabe	27.02.2024