Technische und organisatorische Maßnahmen der

movatix GmbH

gemäß Art. 28 DSGVO

Verantwortliche Stelle	movatix GmbH
Name und Funktion des Autor des Fragebogens:	Nasser Eslami, tegos Holding GmbH Michael Horner, movatix GmbH Doris Bauer, Datenschutzbeauftragte
Version	1.2
Freigegeben von:	Michael Horner
Freigabedatum:	12.10.2023

Der Kommunikationsserver der movatix GmbH wird in der IT-Infrastruktur der Microsoft Cloud-Computing-Plattform Azure verwaltet. Der Serverstandort befindet sich in Deutschland (Zentral West). Es gelten die offiziellen Regelungen der Microsoft zum Datenschutz (Link: Datenschutz in der vertrauenswürdigen Cloud | Microsoft Azure).

Dieser Maßnahmenkatalog ist die Beschreibung der technischen und organisatorischen Maßnahmen der tegos Holding GmbH Rosenheim ergänzt um die Darstellung der notwendigen Komponenten und Konfigurationen zum Betrieb des movatix Kommunikation Servers.

Diese Dokumentation wird laufend kontrolliert und aktualisiert. Sie kann zur Vorlage für ein Vertragsverhältnis im Rahmen einer Auftragsdatenverarbeitung im Sinne des Art. 28 DSGVO verwendet werden.

Zu dieser Kurzübersicht der technischen und organisatorischen Maßnahmen werden in der tegos Holding GmbH weitere Regelungen und Dokumentationen vorgehalten und regelmäßig aktualisiert:

- IT-Schutzkonzept
- Benutzerhandbuch mit Regelungen zur IT-Infrastruktur und Datenschutz

Allgemeine technische und organisatorische Maßnahmen Art. 32 DS-GVO

A) Vertraulichkeit

1	**Zutrittskontrolle**	
	Zweck Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist. Technische bzw. organisatorische Maßnahmen zur 'körperlichen' Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten.	Im SaaS Betrieb im Rechenzentrum von Microsoft.

2	**Zugangskontrolle**	
	Zweck Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern. Technische (Kennwort- / Passwortschutz) und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung	**Maßnahme** ☒ Persönlicher und individueller User-Log-In bei der Anmeldung am System ☒ Kennwortverfahren (Angaben hinsichtlich Komplexität und Aktualisierungsintervall) ☒ Automatische Sperrung der Clients nach Zeitablauf ohne Aktivität ☒ Passwortgeschützte, automatische Pausenschaltung) ☒ Zusätzlicher System-Log-In für bestimmte Anwendungen ☒ Mehrstufige Authentifizierung (2FA) ☒ SOPHOS RED Firewall Komponenten

<u>Ergänzung movatix im SaaS Betrieb:</u>

Der Kommunikationsserver ist außerhalb der tegos Holding Netzwerkumgebung installiert und konfiguriert (Azure Administrationskonsole SaaS).

Der Kunde hat keinen direkten Zugang zur Administrationskonsole und dem Kommunikations-Server.

3	**Zugriffskontrolle**	
	Zweck Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern. Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung	**Maßnahme** ☒ Verwaltung von Berechtigungen ☒ Differenzierte Berechtigungen ☒ Profile ☒ Rollen ☒ Dokumentation der Berechtigung (auch über AD) ☒ Genehmigungsroutine tegos Holding ☒ Verschlüsselung externer Speichermedien und Laptops ☒ Aufgabenbezogene Berechtigungs-profile ☒ Passwort-Identifikation

<u>Ergänzung movatix im SaaS Betrieb:</u>

Es werden folgende Szenarien einer Anmeldung unterschieden:

- Administrations Anmeldung = Administrationskonsole, tegos Holding
- User Anmeldung = Anmeldung am mobilen Endgerät, die zugehörigen Daten werden an das mobile Gerät übertragen, Verantwortung obliegt beim Kunden

Die USER = Kommunikations-Partner werden vom Kunden im ERP-System verwaltet und mit Passwort und Kommunikationsinformationen verknüpft an den Server übertragen (SSL Verschlüsselung). Nur im ERP-System angelegte User können sich über die APP am Server anmelden. Die Verantwortung liegt diesbezüglich beim Kunden.

4	**Trennungskontrolle**	
	Zweck Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten. Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken	**Maßnahme** ☒ Getrennte Systeme ☒ Getrennte Datenbanken (Kunde / tegos Holding) ☒ Funktionstrennung (Test / Produktiv) ☒ Zugriffsberechtigungen

Ergänzung movatix:

- Trennung von Entwicklungs- und Produktivserver.
- Getrennte Datenhaltung pro movatix Kunde.

Pseudonymisierung:

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Wird eine Pseudonymisierung oder Verschlüsselung vorgenommen?

Es werden die Aspekte der Datenminimierung berücksichtigt. Das bedeutet konkret, dass die entsprechenden Datenfelder in der Datenbank und den entsprechenden Eingabemasken (z.B. Stammdaten) vorhanden sind. Eine Vergabe der Schlüssel und Werte liegt in der Verantwortung des Kunden. Es werden nur die Feldinhalte übertragen, die sich aus den Stammdaten des Kunden ergeben. Eine Übertragung von “Klarnamen” findet dementsprechend nur statt, wenn diese durch den Kunden eingepflegt werden. Das System kann auch mit Alias-Informationen genutzt werden (kein Klarname).

B) Integrität

5	**Weitergabekontrolle**	
	Zweck	**Maßnahme**
	Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle. Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung	☒ Getunnelte Datenverbindungen (VPN) ☒ Protokollierung über Firewall ☒ SSL-Verschlüsselung bei Web-Access ☒ 3 Jahre Wildcard Zertifikat von offizieller Signaturstelle.

Ergänzung movatix:

Verschlüsselte Kommunikation per SSL.

Eine verschlüsselte Ablage in der Datenbank am Server ist aus performance-Gründen nicht zu empfehlen und ist derzeit nicht aktiv.

Außerhalb des Systemdienstes sind nur dedizierte User zugelassen, die für Wartung und Support für einen Zugriff auf die Datenbank zugelassen sind.

6	**Eingabekontrolle**	
	Zweck Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten. Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind	**Maßnahme** ☒ Zugriffsrechte ☒ Systemseitige Protokollierungen ☒ Funktionelle Verantwortlichkeiten ☒ Mehraugenprinzip (Administratoren)

Ergänzung movatix:

Serverseitig findet keine Datenverarbeitung statt, reiner Kommunikationsaustausch.

Änderungen an ERP-Daten werden immer über Change-Messages abgebildet. Die entsprechenden Messages werden in den Protokollen festgehalten und sind im ERP System für den Auftraggeber einsehbar (Sendeprotokoll, Empfangsprotokoll). => Verantwortung des Kunden

Generell besteht die Möglichkeit, über den Server administrative Tätigkeiten auszuführen, diese Tätigkeiten können nur über ein direktes Login am Server erfolgen. Die Daten können am Server gelöscht werden, z.B. auf Weisung des Kunden, Änderungen an den Daten werden über diese Oberfläche nicht zugelassen. Die operativen Daten werden nach 30 Tagen automatisch gelöscht. Das Löschen der Logfiles des “movatix”-Kommunikationsservers erfolgt nach spätestens 60 Tagen. Die Logfiles befinden sich wie die operativen Daten auf einer Datenbank der Azure-Maschine.

C) Verfügbarkeit und Belastbarkeit

7	**Verfügbarkeitskontrolle**	
	Zweck Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Maßnahmen zur Datensicherung (physikalisch / logisch)	**Maßnahme**

Ergänzung movatix:

Für den Kommunikations-Server wird die IT-Infrastruktur der Microsoft Cloud-Computing-Plattform Azure genutzt. Steigerung der Verfügbarkeit und Sicherstellung der Performance und Skalierbarkeit.

Die movatix SaaS Umgebung ist in das reguläre Backup-Konzept der tegos Holding eingebunden.

Update Verantwortlichkeiten:

Tegos Holding GmbH	Admin der movatix AZURE Plattform, Zertifikatsverwaltung.
Movatix GmbH	Unicorn Server mit der IT-Abteilung der tegos Holding
	APP Anwendung mit dem Projektleiter und IT-Verantwortlichen des Kunden

Der Kunde muss bezüglich Verfügbarkeit folgende Punkte berücksichtigen:

1. Mobilfunk Vertrag mit entsprechendem Datenvolumen
2. Mobiles Gerät mit funktionsfähiger Kommunikation und möglichst gesicherter Verbindung
3. Die vorgegebenen Systemvoraussetzungen müssen eingehalten und umgesetzt werden (die Systemvoraussetzungen können aus dem Benutzerhandbuch entnommen werden)

D) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

8	**Auftragskontrolle**	
	Zweck Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten. Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer	**Maßnahme** ☒ Schriftlicher Vertrag zur ADV gem. Art. 28 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftraggebers und Auftragnehmers ☒ Verpflichtung der Beschäftigten auf Vertraulichkeit ☒ Bestimmung von Ansprechpartnern und verantwortlichen Projektmanager für den konkreten Auftrag, etc. ☒ Durchführung regelmäßiger eigener Kontrollen und deren Dokumentation ☒ Schulung aller zugriffsberechtigter Beschäftigter hinsichtlich Datenschutzes ☒ Regelmäßig stattfindende Nachschulungen

<u>Ergänzung movatix:</u>

Movatix GmbH und tegos Holding GmbH haben vertraglich die gemeinsame Verantwortung geregelt.

Die Auftragsverarbeitung mit Microsoft (OST-Vertrag) ist mit der tegos Holding geregelt.

Organisatorische Maßnahmen:

Datenschutz-Management
Die tegos Holding GmbH hat ein Datenschutz Management eingerichtet. Eine externe Datenschutz-beauftragte berät, unterstützt und führt regelmäßig Kontrollen und Prüfungen der eingesetzten Maßnahmen auf Anwendung und Aktualität durch. Die Beschäftigten werden in regelmäßig stattfindenden Schulungen oder per E-Mails zu Daten- und IT-Sicherheitsrelevanten Themen sensibilisiert. Präsenzschulungen werden per mit verpflichtender Teilnahmelisten protokolliert.

Regelmäßig findet eine sog. Löschwoche statt, in der nicht mehr erforderliche Daten von den Systemen der tegos Firmeneinheiten protokolliert entfernt werden. Ausnahme sind die Kundenordner zum Zwecke der Dokumentation der Historie. Für diverse Speicherorte wurden Verantwortliche benannt, die mit dem Datenmanagement beauftragt sind.

Daten und Informationen in Papierform werden laufend per verschlossener Datentonne fachgerecht von einem Dienstleister entsorgt.

Incident-Response-Management / Umgang mit Datenpannen
Zur Bearbeitung von Datenschutzpannen und zu Auskunftsanfragen Betroffener wurden entsprechende Teams gebildet. Die Melde- und Kommunikationswege wurden per Schulung vermittelt und sind im zentralen Dokument der organisatorischen Maßnahmen, dem tegos-Benutzerhandbuch, beschrieben. In internen Schulungsmaßnahmen wird regelmäßig darauf hingewiesen.
Auskunftsanfragen oder Meldungen von Datenpannen werden im internen Datenschutzhandbuch aufgenommen und dokumentiert.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
Daten der Kunden werden primär auf deren IT-Infrastruktur gespeichert, nur im Bedarfsfall werden Kopien von Kundendatenbanken auf dedizierten IT-Systemen der tegos Holding GmbH vorgehalten. Das Verfahren wird anhand von Formblättern dokumentiert.

Für softwaretechnische Weiterentwicklungen auf Basis von Microsoft Business Central 365 und branchenbezogener Spezial-Anwendungen müssen die tegos Firmeneinheiten das Software-technische Grundkonzept des Herstellers Microsoft anwenden. Teilweise ist ein Löschen Software-technisch nicht möglich. In diesen Fällen wird in Absprache mit den Kunden mit einer In-Aktiv Setzung gearbeitet.

Cyberversicherung
Die tegos hat eine Cyber-Versicherung abgeschlossen, die alle Firmeneinheiten beinhaltet.