



Darstellung der technischen und organisatorischen Maßnahmen (TOM)

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

movingimage EVP GmbH
Tempelhofer Ufer 1
10961 Berlin

erfüllt diesen Anspruch durch die folgenden Maßnahmen:

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage	Schlüsselregelung
Automatisches Zutrittskontrollsystem mit Ausweisleser (Magnet-/Chipkarte)	Empfang mit Anmeldung
Türsicherung	Gästebuch
Sicherheitsschlösser	Gästeausweise/ Badges
Transponder-Schließsystem	Gäste werden begleitet
Klingelanlage mit Kamera	Sorgfältige Auswahl des Reinigungspersonals
Videoüberwachung der Eingänge	Informationssicherheits-Richtlinien
Feuerfeste Türen	Arbeitsanweisungen zur Zugangskontrolle
Bewegungsmelder	Arbeitsanweisungen zur Arbeitssicherheit
Sicherheitstüren/ -fenster	Mitarbeiter- und Berechtigungsausweise

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen

Mindestanforderung bei der
Passwortvergabe

Authentifizierung mit mindestens
Username
und Passwort

Einsatz von 2-Faktor-Authentifizierung
bei allen kompatiblen Systemen

Einsatz von VPN

Automatische Sperrung des
Arbeitsplatzes
nach einer Zeit der Inaktivität

Verwendung von Antiviren- und Anti-
Malware-Software

Verwendung von Firewalls

Verschlüsselung von Datenträgern und
Servern

Verschlüsselung von Endgeräten

Single Sign-On

Nutzung separater, privilegierter
Benutzerkennungen für administrative
Tätigkeiten

Protokollierung des Zugriffs auf Systeme

Organisatorische Maßnahmen

Nutzerrechteverwaltung

Individuelle Nutzerkonten

Informationssicherheits-Richtlinien

Arbeitsanweisungen zur Zugangskontrolle

Richtlinie zur Verwendung von mobilen
Geräten

Least-privilege-Prinzip (Need-to-know)
bei der Rollenzuweisung

Segregation of Duties (SoD) im
Berechtigungsmanagement

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, 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.

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Datenvernichtungsdienstleistern unter Betrachtung von DIN 66399	Verwendung eines Berechtigungskonzeptes
Ordnungsgemäße Löschung von Datenträgern vor ihrer Vernichtung	Verwaltung von Nutzerkonten und deren Berechtigungen durch Administratoren
Verschlüsselung von Datenträgern und Servern	Anzahl der Administratoren auf ein notwendiges Minimum reduziert
Sichere Aufbewahrung von Datenträgern	Informationssicherheits-Richtlinien
Löschkonzept und Richtlinie zu Aufbewahrungs- und Löschrufen für Daten	Freigaberoutinen für die Beantragung von Zugriffsrechten
Mobile-Device-Management-System mit Remote-Wipe-Funktion	Mehr-Augen-Prinzip
	Protokollierung der Vernichtung von Datenträgern

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv-, Test- und Entwicklungssystemen	Verwendung eines Berechtigungskonzeptes
Physische Trennung von Systemen, Datenbanken und -trägern	Festlegung von Datenbankberechtigungen
Logische Mandantentrennung innerhalb der Anwendung	Aufgabenteilung
Netzwerksegmentierung	Informationssicherheits-Richtlinien
	Richtlinien zum sicheren Entwickeln von Software

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass der Personenbezug von Daten nicht vollständig, aber immerhin so weit aufgelöst wird, dass ein Rückschluss auf eine bestimmte Person nur unter „Hinzuziehung zusätzlicher Informationen“, insbes. eines Identifizierungsschlüssels, möglich ist.

Technische Maßnahmen

Logische Trennung der Echt- und pseudonymisierten Daten

Verschlüsselung und Schutz der Echtdaten

Protokolldateien sind pseudonymisiert oder anonymisiert

Organisatorische Maßnahmen

Anweisung zur Pseudonymisierung und Anonymisierung von Daten, soweit dies funktional möglich ist

Verschlüsselungsrichtlinien

Informationssicherheits-Richtlinien

Richtlinien zum sicheren Entwickeln von Software

Datenschutzrichtlinie

Datenschutzschulung der Mitarbeitenden

1.6 Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten durch kryptografische Maßnahmen so verändert werden, dass sie – insbes. während ihres Übertragungsvorgangs – ohne den Schlüssel nicht mehr lesbar sind, ein unberechtigter Zugriff Dritter mithin ausgeschlossen ist.

Technische Maßnahmen

Verschlüsselung und Schutz der Echtdaten

Verwendung moderner Verschlüsselungstechnologien

Organisatorische Maßnahmen

Schlüsselverwaltungsrichtlinien

Verschlüsselungsrichtlinien

Informationssicherheits-Richtlinien

Richtlinien zum sicheren Entwickeln von Software

Datenklassifizierungsrichtlinien

2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
Verwendung von VPN	Übertragung von Daten in pseudonymisierter oder anonymisierter Form, sofern möglich
Zugriffs- und Abrufprotokollierung	Verschlüsselung des Datenträgers vor physischem Transport
Verwendung von verschlüsselten Verbindungen und Protokollen, bspw. HTTPS zur Datenübertragung	Sorgfältige Auswahl von Transportpersonal und Fahrzeugen beim physischen Transport
Verwendung von verschlüsselter E-Mail-Kommunikation	Protokollierung der physischen Übergabe
Gesichertes WLAN	Informationssicherheits-Richtlinien
Gesicherter Datentransport	Datenklassifizierungsrichtlinien
Gesicherte Dateiübertragung	Regelung zum Umgang mit mobilen Speichermedien
Mobile-Device-Management-System mit Remote-Wipe-Funktion	Physische Transportsicherheit
Protokollierung des Kopierens, der Änderung oder Entfernung von Daten	
Nutzung gesicherter Wide-Area-Network (WAN)-Verbindungen	

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen

Protokollierung der Eingabe, Änderung oder Entfernung von Daten

Manuelle oder automatisierte Auswertung der Protokolle

Organisatorische Maßnahmen

Überprüfung der Anwendungen, die zur Eingabe, Änderung oder Entfernung von Daten verwendet werden können

Erstellung und Zuweisung von Berechtigungsprofilen zur Eingabe, Änderung oder Entfernung von Daten

Informationssicherheits-Richtlinien

Prozesse zum sicheren Löschen von Daten

Funktionale Zuständigkeiten und organisatorisch festgelegte Kompetenzen

Mehr-Augen-Prinzip

2.3 Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

Technische Maßnahmen

Versionskontrolle für Quellcode- und Konfigurationsänderungen

Verwendung von Infrastructure as Code für die nachvollziehbare Verwaltung von Infrastrukturänderungen

Organisatorische Maßnahmen

Verwendung eines Architektur-Diagramms

Datenklassifizierungsrichtlinien

Informationssicherheits-Richtlinien

3 Verfügbarkeit & Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen

Verwendung eines Cloud-Anbieters für alle von Kunden verwalteten Daten, zertifiziert nach:

- CSA STAR,
- ISO 9001,
- ISO 22301,
- ISO 27001 und
- ISO 27018

Physische und geografische Redundanz von Daten

Physische Trennung von Betriebs- und Dateisystemen

Geeignete Archivierungseinrichtungen für Papierdokumente

Organisatorische Maßnahmen

Konzept für den Katastrophenfall vorhanden

Wartungsprozesse

Datenklassifizierungsrichtlinien

Informationssicherheits-Richtlinien

Backupprozesse mit regelmäßiger Überprüfung, inkl.

Aufbewahrungsprozess

und Speicherung der Backups an geografisch getrennten Standorten

3.2 Belastbarkeit (Widerstandsfähigkeit & Resilienz von Diensten/ Systemen)

Maßnahmen, die gewährleisten, dass technische Systeme bei Störungen bzw. Teilausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden.

Technische Maßnahmen

Verwendung eines Cloud-Anbieters für alle von Kunden verwalteten Daten, zertifiziert nach:

- CSA STAR,
- ISO 9001,
- ISO 22301,
- ISO 27001 und
- ISO 27018

Physische und geografische Redundanz von Daten

Automatisierung der Infrastrukturverwaltung

Systemdesign mit Hochverfügbarkeitsansatz
Automatisierung von Ausfallszenarien

Verwendung eines CDN zum Cachen von Medieninhalten

Sicherheitskonzept für Software und IT-Anwendungen

Organisatorische Maßnahmen

Wiederherstellungsverfahren mit regelmäßiger Überprüfung

Informationssicherheits-Richtlinien

Notfallplan mit regelmäßigen Notfallübungen

Risikobasierte Bereitstellung von Sicherheitsupdates

Benannte Rolle Business/ Service Continuity Manager

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Management

Technische Maßnahmen

Zentrale Dokumentation aller Datenschutzverfahren und -regelungen mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf

Regelmäßige Schwachstellenscans und jährliche Penetrationstests durch einen unabhängigen Dritten

Organisatorische Maßnahmen

Berufung der externen Datenschutzbeauftragten: Charlotte Schieler, ISiCO Datenschutz GmbH, Am Hamburger Bahnhof 4, 10557 Berlin

Schulungen von Mitarbeitenden im Bereich Datenschutz

Einbezug des Datenschutzaspekts in die Planung und Entwicklung der Anwendungen

Berufung des internen Informationssicherheitsbeauftragten

Eine Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt

Einhaltung der Informationspflichten nach Art. 13 & 14 DSGVO

Prozess zur Bearbeitung von Auskunftsanfragen von Betroffenen

Datenschutzgrundsätze

Führung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO)

Externe Überprüfung/ Audit der Informationssicherheit, z. B. im Rahmen der ISO-27001-Zertifizierung

Formaler Änderungsmanagementprozess mit verpflichtender Prüfung und Freigabe von Änderungen an Software, Infrastruktur und IT-Diensten

Richtlinien und Anweisungen zur Sicherstellung technischer und organisatorischer Maßnahmen für die Datensicherheit

Einhaltung der internen Richtlinien und Prozesse für die unter Ziffer 5 aufgeführten Zertifizierungen

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Technische Maßnahmen	Organisatorische Maßnahmen
Verwendung von Firewalls	Prozess zur Erkennung und Meldung von Sicherheitsvorfällen
Verwendung von Spamfiltern	Prozess zum Umgang mit Sicherheitsvorfällen
Verwendung von Antiviren- und Anti-Malware-Software	Einbezug des Datenschutzbeauftragten und Informationssicherheitsbeauftragten in Sicherheitsvorfälle
Intrusion Detection System (IDS)	Prozess zur Benachrichtigung des Verantwortlichen über Verletzungen des Schutzes personenbezogener Daten ohne unangemessene Verzögerung (Art. 33 Abs. 2 DSGVO)
Intrusion Prevention System (IPS)	Dokumentation von Sicherheitsvorfällen
	Prozess zur Nachbearbeitung von Sicherheitsvorfällen
	Eigenes Playbook für die Reaktion auf Phishing-Vorfälle

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Technisch-organisatorische Maßnahmen zur Umsetzung datenschutzrechtlicher Vorgaben, d.h. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

Technische Maßnahmen	Organisatorische Maßnahmen
Reduzierung der Erhebung personenbezogener Daten auf ein angemessenes Minimum	Einbezug des Datenschutzes in die Planung und Entwicklung der Anwendungen
Einfache Ausübung des Widerrufsrechts der Einwilligung Betroffener durch technische Maßnahmen	Richtlinien zum sicheren Entwickeln von Software

4.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen

Organisatorische Maßnahmen

Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation

Dokumentiertes Verfahren zur Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten

Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln

Schriftliche Weisung an den Auftragnehmer

Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer, sofern der Auftragnehmer einer entsprechenden rechtlichen Verpflichtung unterliegt

Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer

Regelung zum Einsatz weiterer Subunternehmer

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Periodische Überprüfung des Auftragnehmers und seines Schutzniveaus

Formalisiertes Management der Verarbeitungsaufträge

Prozess zum Empfang und zur Befolgung der Weisungen des Verantwortlichen

Benennung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern

Kontrolle/ Überprüfung der weisungsgemäßen Verarbeitung

Standardisierte Prüfung der eingesetzten Zulieferer

5 Zertifizierungen

5.1 Weitergabekontrolle

Sowohl das Quality Management System nach ISO 9001 als auch das Information Security Management System nach ISO 27001 von movingimage inkl. des Datacenter-Betriebs durchliefen mehrere externe Zertifizierungen:

Maßnahme	PwC (TISAX „special data“)	TÜV Nord (ISO 9001, 20000-1, 22301, 27001)
Zutrittskontrolle	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Zugangskontrolle	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Zugriffskontrolle	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Trennungskontrolle	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Pseudonymisierung	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Verschlüsselung	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Weitergabekontrolle	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Eingabekontrolle	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Dokumentationskontrolle	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Verfügbarkeitskontrolle	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Belastbarkeit	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Datenschutz-Management	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Incident-Response-Management	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Datenschutzfreundliche Voreinstellungen	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025
Auftragskontrolle	Evaluiert am 29.11.2024	Zertifiziert am 5.10.2025