movingimage

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	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

1.2 Zugangskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
Mindestanforderung bei der Passwortvergabe	Nutzerrechteverwaltung
Authentifizierung mit mindestens Username und Passwort	Individuelle Nutzerkonten
Einsatz von 2-Faktor-Authentifizerung bei allen kompatiblen Systemen	Informationssicherheits-Richtlinien
Einsatz von VPN	Arbeitsanweisungen zur Zugangskontrolle
Automatische Sperrung des Arbeitsplatzes	Arbeitsanweisungen zur Arbeitssicherheit
Verwendung von Antiviren-Software	Richtlinie zur Verwendung von mobilen Geräte
Verwendung von Firewalls	
Verschlüsselung von Datenträgern und Servern	
Verschlüsselung von Endgeräten	

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

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 für Daten	
Protokollierung der Vernichtung von Datenträgern	

nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

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 Anwendungen	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 Mitarbeiter

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
Verwendung von VPN
Zugriff- und Abrufprotokollierung
Verwendung von verschlüsselten Verbindungen und Protokollen, bspw. HTTPS zur Datenübertragung
Verwendung von verschlüsselter E-Mail-Kommunikation

Organisatorische Maßnahmen
Übertragung von Daten in pseudonymisierter oder anonymisierter Form sofern möglich
Verschlüsselung des Datenträgers vor physischem Transport
Sorgfältige Auswahl von Transportpersonal und Fahrzeugen beim physischen Transport
Protokollierung der physischen Übergabe
Informationssicherheits-Richtlinien
Datenklassifizierungsrichtlinien

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

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	Organisatorische Maßnahmen
	Verwendung eines Architektur-Diagramms
	Standardisierte Prüfung der eingesetzten Zulieferer
	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	Organisatorische Maßnahmen
Verwendung eines Cloud Anbieters für alle von Kunden verwalteten Daten zertifiziert nach: • CSA STAR, • ISO 9001, • ISO 22301, • ISO 27001 und • ISO 27018	Konzept für Katastrophenfall vorhanden
Physische und geografische Redundanz von Daten	Backupprozesse
Physische Trennung von Betriebs- und Dateisystemen	Wartungsprozesse
	Datenklassifizierungsrichtlinien
	Informationssicherheits-Richtlinien

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	Organisatorische Maßnahmen
Verwendung eines Cloud Anbieters für alle von Kunden verwalteten Daten zertifiziert nach: • CSA STAR, • ISO 9001, • ISO 22301, • ISO 27001 und • ISO 27018	Backupprozesse und regelmäßige Überprüfung
Physische und geografische Redundanz von Daten	Wiederherstellungsplan und regelmäßige Überprüfung
Automatisierung der Infrastrukturverwaltung	Informationssicherheits-Richtlinien
Systemdesign mit Hochverfügbarkeitsansatz	
Automatisierung von Ausfallszenarien	
Verwendung eines CDN zum Cachen von Medieninhalten	

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	Organisatorische Maßnahmen
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf	Berufung der externen Datenschutzbeauftragten: Charlotte Schieler, ISiCO Datenschutz GmbH, Am Hamburger Bahnhof 4, 10557 Berlin
Einhaltung der internen Richtlinien und Prozesse zu den unter Ziffer 5.0 aufgeführten Zertifizierungen	Schulung von Mitarbeitern im Bereich Datenschutz
	Einbezug des Datenschutzaspekts in die Planung und Entwicklung der Anwendungen
	Berufung des internen Informationssicherheitsbeauftragten: Frank Dornberger
	Eine Datenschutzfolgeabschätzung (DSFA) wird bei Bedarf durchgeführt
	Einhaltung der Informationspflichten nach Art. 13 & 14 DSGVO
	Prozess zur Bearbeitung von Auskunftsanfragen von Betroffenen
	Zertifizierungen nach diversen relevanten Standards (s. Ziffer 5.0)

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-Software	Einbezug des Datenschutzbeauftragen und Informationssicherheitsbeauftragen in Sicherheitsvorfälle
Intrusion Detection System (IDS)	Dokumentation von Sicherheitsvorfällen
Intrusion Prevention System (IPS)	Prozess zur Nachbearbeitung von Sicherheitsvorfällen

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 personenbezogenen Daten auf ein zweckmäßiges Minimum	
Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	

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
	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	Schriftliche Weisung an den Auftragnehmer
	Verpflichtung der Mitarbeiter des Auftragnehmers auf 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

5 Zertifizierungen

5.1 Weitergabekontrolle

Sowohl das Quality Management System nach ISO 9001 als auch das Information Security Management System nach ISO 27001 und das Service Level Management nach ISO 20000-1 von movingimage inkl. des Datencenter-Betriebs durchliefen mehrere externe Zertifizierungen:

Maßnahme	PwC (TISAX „special data“)	TÜV Nord (ISO 9001, 20000-1 27001)
Zutrittskontrolle	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Zugangskontrolle	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Zugriffskontrolle	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Trennungskontrolle	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Pseudonymisierung	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Verschlüsselung	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Weitergabekontrolle	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Eingabekontrolle	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Dokumentationskontrolle	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Verfügbarkeitskontrolle	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Belastbarkeit	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Datenschutz-Management	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Incidence-Response-Management	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Datenschutzfreundliche Voreinstellungen	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023
Auftragskontrolle	Evaluiert am 4.10.2021	Zertifiziert am 6.10.2023