DS-GVO Dokumentation / TOMs

Technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO

Technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO

TOMs

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.

Die technischen und organisatorische Maßnahmen gemäß der Datenschutz-anforderung unterliegen einem kontinuierlichen Verbesserungsprozess (PDCA-Zyklus) und können sich daher verändern.

Unter https://www.meeta-x.com/download (Passwort: meeta-x) können Sie jederzeit die aktuelle Version einsehen.

Die oben genannte Organisation erfüllt diesen Anspruch durch folgende Maßnahmen

Inhaltsverzeichnis

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

(1 a) **Zutrittskontrolle:**
• ISO 27.001 zertifizierte Rechenzentren. • Zutrittskontrolle zum RZ mittels Wachschutz, der 24 Stunden vor Ort ist. Dieser erlaubt nach persönlicher Authentifizierung des Zutrittssuchenden und Abgleich mit der vom Auftragnehmer gepflegten Zugangsliste den Zugang zum RZ-Bereich. Das RZ ist in verschiedene Bereiche eingeteilt. • Es existieren Dienstanweisungen des RZ-Betreibers zur Handhabung von Zutrittskontrollen und Zutrittsberechtigungen. Zutrittsberechtigungen werden vom Aufragnehmer nur an Personen verteilt, die dieses Recht für ihre Arbeit benötigen. • Zutritt für Externe (z.B. für Wartung) erfolgt nur nach schriftlicher Anmeldung beim Rechenzentrum durch den Auftragnehmer und in Begleitung • Die Server sind in Serverschränken verschlossen, welche ebenfalls zutrittsgesicherte sind. Die Kombinationen der Zahlenschlösser sind nur berechtigten Personen des Auftragnehmers und berechtigten Personen des Rechenzentrumsbetreibers bekannt. • Physikalische Sicherung des Rechenzentrums durch Alarmanlage und Wachschutz mit regelmäßigen Kontrollgängen, sowie Überwachungskameras.

(1 b) **Zugangskontrolle:**
Die Identifizierung bei Anmeldung im MICE Channel Manager erfolgt über eine individuell vergebene Benutzerkennung und ein Passwort. Das Passwort wird von jedem berechtigten User selbst vergeben. Zur gesicherten Zugangskontrolle existiert eine unternehmensweite, an die ISO 27.001 angelehnte Passwortrichtlinie.

(1 c) **Zugriffskontrolle:**
Die Identifizierung bei Anmeldung im MICE Channel Manager erfolgt über eine individuell durch den User selbst vergebene Benutzerkennung und ein Passwort. Benutzern werden verschiedene Rollen bzw. Rechte eingeräumt, die Sie zum täglichen Arbeiten benötigen umso den Zugriff auf Daten auf ein Minimum zu beschränken. Folgende Grund- Rollen sind vorgegeben: - Administrator - User mit Leserechten - User mit Lese- und Schreibrechten

(1 d) **Trennungskontrolle:**
Durch systembedingte Vorgaben bzw. Zugriffssteuerung, ist eine Trennung bei Nutzung, Verarbeitung und Speicherung der mandantenseitigen Daten sichergestellt. Die im Zusammenhang erhobenen und verarbeiteten Daten werden mit einem gesonderten Schlüsselkennzeichen versehen, die eine zweckfremde Verwendung (z.B. Einsicht durch nicht Berechtigte) ausschließt. Es erfolgt eine softwareseitige Mandantentrennung.

(1 e) **Pseudonymisierung:**
Eine Pseudonymisierung wird nicht angewendet.

2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

(2 a) **Weitergabekontrolle:**
Die Weitergabe der Daten erfolgt verschlüsselt über TLS nach aktuellem Stand der Technik.

(2 b) **Eingabekontrolle:**
Die Eingabe von Benutzern, wird dokumentiert. Im Bedarfsfall ist der jederzeitige Abruf der Anfrage-Historie möglich. Die Auswertung der Daten erfolgt von Support-Mitarbeitern mit Zugriffsberechtigung.

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

(3 a) **Verfügbarkeitskontrolle:**
Die Datensicherheit wird durch redundante Festplattensysteme gewährleistet. Zum Schutz der Daten vor Verlust werden tägliche Vollbackups auf Servern außerhalb des Rechenzentrums gespeichert. Dazu erfolgt mehrmals täglich eine Sicherung der Bewegungsdaten. Die Backup-Daten werden nach Stand der Technik verschlüsselt. Die Server werden vor unbefugtem Zugriff durch eine Firewall geschützt. Die Stromversorgung wird über unterbrechungsfreie Stromversorgung (USV) gewährleistet.

(3 b) **Rasche Wiederherstellbarkeit:**
Wir haben ein nach ISO 27.001 ausgerichtetes Business Continuity Management etabliert. Alle Systeme verfügen über ein Fall Back System, welches sich im Stand By befindet.

(3 c) **Belastbarkeit:**
Um die Sicherheit und die Belastbarkeit zu kontrollieren, werden regelmäßig Schwachstellen Analysen durchgeführt und alle Systeme unterliegen einem 24/7 Monitoring.

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

(4 a) **Datenschutz-Management:**
Die eingesetzten Maßnahmen unterliegen einem konstanten Review und Anpassungszyklus (PDCA). Überprüfung der Maßnahmen in Absprache mit dem DSB.

(4 b) **Incident-Response-Management:**
Es ist ein Incident-Response-Management installiert. Alle Störungen und Vorfälle werden in einem System gesammelt und abgearbeitet. Für die Entgegennahme und Überwachung der Tickets sind die Mitarbeiter zuständig und berechtigt.

(4 c) **Datenschutzfreundliche Voreinstellungen:** (Art. 25 Abs. 1 DS-GVO)
Es werden nur Daten erhoben und gespeichert, die zur Auftragserfüllung notwendig sind. Alle Daten werden regelmäßig auf Notwendigkeit geprüft und nach Ablauf der nötigen Aufbewahrungsfrist anonymisiert. Das Programmierteam ist auf Datensparsamkeit und Privacy-by-Prinzipien geschult.

(4 d) **Auftragskontrolle:**
digitise-IT wählt seine Auftragnehmer sorgfältig aus. Die Abgrenzung der Verantwortlichkeiten und die Festlegung der durchzuführenden Kontrollmaßnahmen werden vertraglich vereinbart und der Auftragnehmer vor Vergabe geprüft. Der Einsatz von Unterauftragsunternehmen ist auf ein Minimum reduziert und wird nur durch weisungsbefugte Personen vergeben. Alle Mitarbeiter sind dem Datengeheimnis schriftlich verpflichtet.

(4 e) **Informationssicherheits-Managementsystem (ISMS):**
digitise-IT sieht sich in der Pflicht, seine IT und die Daten der Kunden nach besten Möglichkeiten zu sichern und baut zur Kontrolle ein nach ISO 27.0001 angelegtes Informationssicherheits-Managementsystem. Hierdurch sind alle technischen Maßnahmen an die ISO27.001 angelehnt und erfüllen so ein Höchstmaß an Sicherheit. Alle Prozesse und Maßnahmen unterliegen einem kontinuierlichen Verbesserungsprozess.

5 Datenschutzbeauftragter der MEETA-X GmbH

Vorname Name:	Kontaktdaten:
Bodo Hoffmann	IT Future Aktiengesellschaft c/o BFD Frankfurter Straße 151B D-63303 Dreieich E-Mail: datenschutz@meeta-x.com

6 Auflistung gebilligter weiterer Auftragsverarbeiter (Subunternehmer)

Kurzbeschreibung der Tätigkeit:	Name der Firma:	Sitz der Firma, Ort der Daten-verarbeitung:	Datenschutzbeauftragter / für den Datenschutz verantwortliche Person (Vorname Name, Kontaktdaten):
Hosting	IONOS SE	Elgendorfer Str. 57 56410 Montabaur	Der Datenschutzbeauftragte datenschutz@ionos.de
Abrufs von Buchungs- und Reservierungsaufträge	hivr solutions GmbH	Gerberau 17 79098 Freiburg im Breisgau	info@hivr.ai
Accounting	digitise-IT GmbH	Kaiserstr. 68 | 72184 Eutingen im Gäu	jochen.zimmermann@digitise-it.de
CRM System	HubSpot Germany GmbH	Am Postbahnhof 17, 10243 Berlin	Legal.hubspot.com, privacy@hubspot.com

Die technischen und organisatorische Maßnahmen gemäß der Datenschutz-anforderung unterliegen einem kontinuierlichen Verbesserungsprozess (PDCA-Zyklus) und können sich daher verändern.

Dieses Dokument ist in seiner aktuellen Form jederzeit abzurufen unter www.meeta-x.com/download (Passwort: meeta-x)