STUDIO MITTE
DIGITAL MEDIA GMBH

Tummelplatz 3
4020 Linz
Austria

+43 732 27 27 70
office@studiomitte.com
studiomitte.com

TECHNISCHE UND ORGANISATORISCHE STANDARDMAßNAHMEN ZUM SCHUTZ VON DATEN

gemäß Art. 28 Abs. 3 lit. c, 32 DS-GVO i.V.m. Art. 5 Abs. 1, Abs. 2 DS-GVO

---

der Studio Mitte Digital Media GmbH, im Folgenden kurz Studio Mitte genannt

Alle technisch-organisatorischen Maßnahmen werden kontinuierlich auf Aktualität und Stand der Technik evaluiert und aktualisiert.

Studio Mitte Digital Media GmbH · FN **340638p** · UID **ATU65495038** · Landesgericht Linz
Bankverbindung · Oberbank AG · IBAN **AT78 1500 0007 2138 5961** · BIC **OBKLAT2L**
Folgen Sie uns auf **twitter.com/studiomitte** oder **facebook.com/studiomitte**

INHALT

1. Vertraulichkeit 3

1.1. Zutrittskontrolle 3

1.2. Zugangskontrolle 3

1.3. Zugriffskontrolle 3

1.4. Weitergabekontrolle 4

1.5. Trennungskontrolle 4

1.6. Pseudonymisierung 5

1.7. Verschlüsselung 5

2. Integrität 6

2.1. Eingabekontrolle 6

2.2. Weitergabekontrolle 6

3. Verfügbarkeit und Belastbarkeit 6

3.1. Verfügbarkeitskontrolle 6

3.2. Rasche Wiederherstellbarkeit 7

4. Weitere Maßnahmenbereiche 7

4.1. Datenschutz-Managementsystem 7

4.2. Auftragskontrolle 7

4.3. Webserver 8

4.4. Web-Applikationen 8

4.5. Online-Kampagnen, Targeted Advertising, Newsletter / E-Mail Direktmarketing 8

Studio Mitte Digital Media GmbH · FN **340638p** · UID **ATU65495038** · Landesgericht Linz
Bankverbindung · Oberbank AG · IBAN **AT78 1500 0007 2138 5961** · BIC **OBKLAT2L**
Folgen Sie uns auf **twitter.com/studiomitte** oder **facebook.com/studiomitte**

1. VERTRAULICHKEIT

1.1. Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der ihm übertragenen Leistungen genutzten technischen Einrichtungen zu verwehren.

BEIM AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, in jedem Fall durch Schlüssel oder elektrische Türöffner (Transponder oder verschlüsselte Bluetooth-Verbindung).
- Die internen Server, Netzverteiler und TKAnlagen (exkl. Telefon) befinden sich in einem physisch versperrten Schrank und werden ausschließlich von Studio Mitte genutzt.
- Zusätzliche Schutzeinrichtungen: Schlüsselregelung; Zutrittskontrollsystem; Anwesenheitskontrolle angeschlossen; Protokollierung

1.2. Zugangskontrolle

Es ist zu verhindern, dass die zur Erbringung der in der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.

BEIM AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Schutz vor unbefugter Systembenutzung durch Benutzerkennung und Passwortverfahren mit aktuellen Standards entsprechender und validierter Policy (Zeichenzusammensetzung, Länge) oder durch aktuellen Sicherheitsstandards entsprechenden Public-Keys (SSH-Zugänge).
- Weitere Maßnahmen: Zwei-Faktor-Authentifizierung bei administrativen Benutzerkonten; Bildschirmsperre bei Pausen mit Passwort-Aktivierung; Erstanmeldeprozedur; geregelte und gesicherte Aufbewahrung von Administrator-Passwörtern; nur personalisierte Zugangskennungen; Protokollierung des Zugangs; zwingende Verschlüsselung von mobilen Datenträgern; Zugriffsberechtigungskonzepte;-Firewalls; Laufende manuelle/teilw. automatisierte und Installation von Updates und Sicherheitspatches; Aufgabenbezogene systemtechnische Trennung bei mehreren Administratoren; getrennte Benutzerkonten für Systemadministratoren; Anwendung des 4-AugenPrinzips bei kritischen Systemänderungen;

1.3. Zugriffskontrolle

Es ist sicherzustellen, 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 oder verändert werden können.

BEIM AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb der Systeme. Es gibt Standard-Berechtigungsprofile auf „need to know-Basis“, periodische Überprüfung der vergebenen Berechtigungen. Administrative Benutzerkonten sind auf den kleinstmöglichen Kreis an Administratoren begrenzt und werden mit besonderer Sorgfalt regelmäßig geprüft.

- Weitere Maßnahmen: Berechtigungskonzepte für Daten, Anwendungen und Betriebssysteme; Aufbewahrung der Protokolle für einen angemessenen Zeitraum; Synchronisierung der Uhren zur Auswertung von Protokollen; Prozesse zur Erlangung / Veränderung von Berechtigungen (Neuanlage, Aufgabenänderung, Austritt); Regelmäßige Überprüfung, ob vergebene Berechtigungen noch notwendig sind; Berechtigungen gehören wenn immer möglich nicht zu Personen sondern zu Rollen; Zugriffsschutz durch automatische oder über Funktionstasten ausgelöste Bildschirmsperre mit ausschließlicher passwortgestützter oder biometrischer Verfahren verifizierter Aufhebung; nur unternehmenseigene Geräte dürfen mit dem internen Netzwerk verbunden werden; Offene oder nicht ausschließlich intern verwendete WLAN-Segmente sind vom internen Netz getrennt; die Kommunikation in drahtlosen Netzen erfolgt verschlüsselt; Mobile Endgeräte sind verschlüsselt; Bei Internet-Anwendungen werden Anmeldedaten ausschließlich verschlüsselt übertragen; etwaige öffentlich zugängliche IT Systeme befinden sich in einer abgeschotteten DMZ;

1.4. Weitergabekontrolle

Es muss dafür gesorgt werden, 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 welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

BEIM AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung und Transport ausschließlich über verschlüsselte Verbindungen (z.B. HTTPS, SFTP, VPN). Weitere Maßnahmen: Festplattenverschlüsselung bei mobilen Endgeräten soweit technisch und organisatorisch sinnvoll; Regelungen für Remotearbeiter;

1.5. Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

BEIM AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Zugriff auf Daten und Systeme (Webserver, Projekt-Dokumente) ist durch ein Rollen- und Berechtigungskonzept sichergestellt.

Studio Mitte Digital Media GmbH · FN **340638p** · UID **ATU65495038** · Landesgericht Linz
Bankverbindung · Oberbank AG · IBAN **AT78 1500 0007 2138 5961** · BIC **OBKLAT2L**
Folgen Sie uns auf **twitter.com/studiomitte** oder **facebook.com/studiomitte**

- Remote-Zugriff auf Server und Anwendungen erfolgt ausschließlich verschlüsselt, die jeweiligen Projekte / Anwendungen / Daten sind mit eigenen Zugängen versehen.
- Trennung von internem Netzwerk und Gäste-Netzwerk
- Trennung von Live- und Entwicklungsservern

1.6. Pseudonymisierung

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

BEIM AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Daten, welche für Entwicklungs- und Testzwecke notwendig sind und den Kriterien für personenbezogene Informationen unterliegen, werden je nach System durch Zufallswerte ersetzt, sodass keine Rückschlüsse auf Personen möglich sind.
- Protokollierungsdaten wie bspw. IP Adressen in Log-Dateien oder Analyse-Tools werden pseudonymisiert gespeichert oder in regelmäßigen Abständen gelöscht.
- Trennung von Kontaktdaten und weiteren nutzerbezogenen Daten

1.7. Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

DURCH DEN AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Zugriff auf interne und externe Systeme (Webserver, Software-as-a-Service, APIs) erfolgt ausschließlich via verschlüsselter Kanäle nach Stand der Technik (SSL / TLS Verschlüsselung, Private / Public Key Verfahren)
- Festplatten-Verschlüsselung wird nach Möglichkeit eingesetzt (insbesondere auf mobilen Geräten)
- Passwörter werden ausschließlich verschlüsselt gespeichert, wenn möglich, wird 2-Faktor-Authentifizierung eingesetzt.

Studio Mitte Digital Media GmbH · FN **340638p** · UID **ATU65495038** · Landesgericht Linz
Bankverbindung · Oberbank AG · IBAN **AT78 1500 0007 2138 5961** · BIC **OBKLAT2L**
Folgen Sie uns auf **twitter.com/studiomitte** oder **facebook.com/studiomitte**

2. INTEGRITÄT

2.1. Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

BEIM AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Die verwendeten Systeme und entwickelten Anwendungen verfügen über Protokollierungs-Mechanismen, welche jede Änderung / Tätigkeit am System protokollieren und dem jeweiligen Urheber zuordbar sind.
- Verwendung personalisierter Logins im Unternehmensnetzwerk

2.2. Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle gem. 1.4 dienen auch der Sicherstellung der Integrität.

3. VERFÜGBARKEIT UND BELASTBARKEIT

3.1. Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

BEIM AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Brandschutzeinrichtungen (Rauch- oder Brandmelder); Feuerlöscher im Stiegenhaus; Rauchverbot in allen Server- und Arbeiträumen; USV und Überspannungsschutz für kritische IT-Infrastruktur; firmenweites Datensicherungskonzept für alle relevanten IT-Komponenten (Speicher-/ Löschfristen, standortunabhängige Replikation, manuelle und automatische Integrationskontrolle, rasche Wiederherstellbarkeit); zentrale Festplattensysteme mit Reservekapazitäten (RAID); automatisch aktualisierte Virenschutz / Schutz vor Schadsoftware; Spamfilter; zentrale IDS und IPS Systeme; Notfallpläne für unterschiedliche Szenarien Verfügbarkeitskontrolle
- Nutzung einer Versionskontrolle (GIT, SVN)

3.2. Rasche Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

DURCH DEN AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Dezentrale, redundante Datensicherung
- Nutzung einer Versionskontrolle (z. B. Git oder SVN) in der Entwicklung
- Testen von Datenwiederherstellungen
- Tägliche Backups & Snapshots der Live-Systeme

4. WEITERE MAßNAHMENBEREICHE

4.1. Datenschutz-Managementsystem

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.

BEIM AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Dokumentation von datenschutzrelevanten Zwischenfällen
- Löschen nicht mehr benötigter Daten (z. B. veraltete Daten, Testumgebungen)
- Sichere Entsorgung defekter/nicht mehr benötigter Hardware
- Sichere Entsorgung von Dokumenten (z. B. Aktenvernichter, Reisswolf)

4.2. Auftragskontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

BEIM AUFTRAGNEHMER UMGESETZTE MAßNAHMEN

- Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers durch formalisierte Auftragserteilung oder gesonderter Vereinbarung. Kontrolliert und dokumentiert werden in jedem Fall: Gegenstand und Dauer der Verarbeitung, Art und Zweck

Studio Mitte Digital Media GmbH · FN **340638p** · UID **ATU65495038** · Landesgericht Linz
Bankverbindung · Oberbank AG · IBAN **AT78 1500 0007 2138 5961** · BIC **OBKLAT2L**
Folgen Sie uns auf **twitter.com/studiomitte** oder **facebook.com/studiomitte**

der Verarbeitung, Art der personenbezogenen Daten, Kategorien der betroffenen Personen. Alle Mitarbeiter und Sub-Auftragnehmer sind zur Vertraulichkeit verpflichtet

- Auswahl geeigneter Dienstleister und Partner unter Datenschutzaspekten
- Abschluss von AV-Verträgen mit Dienstleistern, Partnern und Kunden
- Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter
- Regelmäßige Unterweisung und Fortbildung der Mitarbeiter zum Thema Datenschutz
- Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter
- Beratung/Aufklärung der Kunden zum Thema Datenschutz

4.3. Webserver

- Sofern die Einrichtung des Webservers ausschließlich durch Studio Mitte erfolgt werden initial die folgenden Maßnahmen ergriffen: Zugriff nur durch berechtigtes und geschultes Personal (Rollenkonzept); SoftwareFirewall (nur unbedingt notwendige Ports werden geöffnet); Shell-/ Administrationszugang nur für eingeschränkten IP Bereich und Personenkreis(Systemadministratoren); Protokollierung der Zugriffe (7 Tage Speicherdauer); Serverbetrieb ausschließlich für die beauftragte Software; Datenübertragung ausschließlich über verschlüsselte Verbindungen; Auf ausdrücklichen Wunsch des Auftragsgebers können auftragsbedingt oder anlassbezogen Änderungen an den Maßnahmen notwendig sein. Es erfolgt keine laufende Wartung der einmalig eingerichteten Maßnahmen, sofern dies nicht gesondert vertraglich geregelt ist (Wartungsvertrag).

4.4. Web-Applikationen

- Die durch Studio Mitte erstellten Web-Applikationen werden an den Auftraggeber in der Regel mit folgenden Schutzmaßnahmen initial übergeben (bei Erstellung der Applikation): Standard-Berechtigungskonzept auf Rollenbasis, passwortauthentifizierte Benutzeraccounts, personalisierte Benutzeraccounts für alle Studio MitteMitarbeiter inkl. SSO-Login, Werkzeug zur Kontrolle der Zugriffsrechte, Schutz gegen Brute-Force Attacken, Standardmechanismen zum Schutz vor ungewollten Zugriff

4.5. Online-Kampagnen, Targeted Advertising, Newsletter / E-Mail Direktmarketing

- Die Übermittlung von personenbezogenen Daten vom Auftraggeber zu Studio Mitte darf nur über verschlüsselte Übertragungsarten stattfinden. Die Daten werden bei Studio Mitte nach Abschluss des Auftrags gelöscht. Der Auftraggeber wird über die Weitergabe an zertifizierte Subauftragsverarbeiter in jedem Fall in Kenntnis gesetzt.

Studio Mitte Digital Media GmbH · FN **340638p** · UID **ATU65495038** · Landesgericht Linz
Bankverbindung · Oberbank AG · IBAN **AT78 1500 0007 2138 5961** · BIC **OBKLAT2L**
Folgen Sie uns auf **twitter.com/studiomitte** oder **facebook.com/studiomitte**