Technische und organisatorische Maßnahmen der TMC GmbH, TMC Amplio GmbH und TMC Live GmbH mit Stand vom 1. März 2024

Diese vereinbarten technisch-organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und Weiterentwicklung. Insoweit ist es dem Auftragnehmer – sofern in der Vereinbarung zur Auftragsdatenverarbeitung vereinbart – gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

Die jeweils aktuelle Version der technisch-organisatorischen Maßnahmen (Anlage A) ist auf der Webseite zu finden:
https://tmc-gmbh.de/datenschutz/subunternehmen **(Passwort: Auf Anfrage erhältlich)**

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:

- Elektronisches Schließsystem mit individuell zugeordneten RFID Tags
- Zutritt zum Büro entweder mit RFID Tag oder nach Klingeln
- Die Vergabe von RFID Tags und VPN-Token erfolgt ausschließlich an Mitarbeiter. Die Vergabe erfolgt erst nach Unterzeichnung eines Übergabeprotokolls, in welchem die Vergabe mit Datum festgehalten wird.
- Die Rückgabe von RFID Tags und VPN-Token erfolgt mit Unterzeichnung eines Übergabeprotokolls, in welchem die Abgabe mit Datum festgehalten wird.
- Der Zutritt zum Serverraum ist ausschließlich ausgewählten Mitarbeitern mittels RFID Tag mit „Sonderberechtigung“ gestattet
- Ein Zutritt zum Serverraum ist Externen nur in Begleitung von ausgewählten Mitarbeitern gestattet

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:

- Mitarbeiter und Beschäftigte sind angewiesen, beim Verlassen des PCs den Bildschirm zu sperren
- Automatisches Sperren von PCs, Einsatz automatischer Bildschirmschoner
- Einsatz von Firewalls: Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt.

- Zentrale Verwaltung von Benutzerzugangsdaten (Netzwerk: Active Directory)
- Nutzung von i. d. R. personenbezogenen Benutzerprofilen
- Regelmäßige Überprüfung der Berechtigungen
- Definierte Passwortregeln: Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern mit mind. 10 Stellen, sofern vom System zulässig
- Passwortfreigabeverfahren
- Passwortrücksetzungsverfahren
- Authentifikation mit Benutzer-Passwort; teilw. Authentifikation mit biometrischen Daten
- Zwei-Faktor-Authentifizierung bei bestimmten Anwendungen
- Einsatz von VPN-Technologie mit Token
- Einsatz von Anti-Viren-Software auf PC-Clients und Server mit regelmäßiger Aktualisierung

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:

- Administrative-Zugriffe nur für erforderliche Personen vorhanden
- Zugriffe über Berechtigungen / Rollen festgelegt
- Geregelte Verwaltung der Benutzerrechte durch Geschäftsleitung bzw. deren Vertretung
- Entsorgung von Datenträger über Fachunternehmen
- Sperrung von Zugängen beim Austritt von Mitarbeitern; Verlässt ein Mitarbeiter das Unternehmen, so erfolgt noch vor dessen Austritt die Sperrung bzw. Löschung aller ihm zugewiesenen Zugänge für interne und externe Systeme.
- Verwendung eines Datenschutztresors; Zur Sicherung von datenschutzrelevanten Dokumenten wird ein Tresor eingesetzt. Dieser dient zur besonders sicheren Aufbewahrung von Dokumenten oder Datenträgern mit personenbezogenem Inhalt.
- Verwendung sicherer und individueller Passwörter
- Zentrale Verwaltung von Benutzerzugängen und -rechten

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:

- Beauftragung zuverlässiger Transportunternehmen
- Beim Versand von Daten auf dem Postweg oder beim Transport von Servern wird

darauf geachtet, dass nur zuverlässige und vertrauenswürdige Transportunternehmen eingesetzt werden.

- Einsatz von TLS/SSL bei E-Mail-Kommunikation
- Protokollierung von Operationen und Zugriffen im Firmennetzwerk; Sämtliche im Firmennetzwerk durchgeführten Operationen und Zugriffe werden protokolliert und der jeweilige Zugriff für sieben Tage gespeichert.
- Entsorgung von Datenträger über Fachunternehmen
- Verschlüsselung von E-Mail-Anhängen möglich, sofern vom Auftraggeber beauftragt
- Teilw. elektronische Signatur
- Verwendung von VPN-Systemen zum Login in das Firmennetzwerk;
- Bereitstellung von Daten online möglich statt E-Mail-Versand, z. B. OneDrive mit Kennwortschutz und
- Ablaufdatum des Zugrifflinks

1.5. Trennungskontrolle

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

Beim Auftragnehmer umgesetzte Maßnahmen:

- Trennung von internem WLAN und Gäste-WLAN; Gäste, denen ein Zugang zum Internet ermöglicht werden soll, erhalten einen individualisierten Zugang oder die Zugangsdaten zu einem eigenem WLAN. Von diesem separaten WLAN aus ist ein Zugriff auf das firmeninterne Netzwerk und alle dort hinterlegten Daten nicht möglich.
- Trennung von Produktiv- und Testsystem
- Verbot der Nutzung von privaten Endgeräten im Firmennetzwerk
- Speicherung von Daten in kunden- und/oder projektspezifischen Verzeichnissen
- Zugriff auf einzelne Verarbeitungen oder Verzeichnisse nach Erforderlichkeit

1.6. Pseudonymisierung

Maßnahmen zur Pseudonymisierung von Daten erfolgen aktuell nicht.

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.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Verwendung verschlüsselter Übertragungswege für den Austausch personenbezogener Daten
- Verwendung von SSL-Zertifikaten für Hostingumgebungen

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:

- Nutzung von Benutzer- und Rollenkonzepten für interne und externe Systeme
- Je nach Anwendung Protokollierung der Eingabe, Änderung und Löschung von Daten

2.2 a

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

3. Verfügbarkeitskontrolle und Wiederherstellbarkeit

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

Beim Auftragnehmer umgesetzte Maßnahmen:

- Regelmäßige Durchführung von Updates; die sich im Einsatz befindlichen Betriebssysteme sowie darauf installierte Anwendungen werden regelmäßig geupdatet.
- Verwendung einer Firewall
- Verwendung einer unterbrechungsfreien Stromversorgung (USV); Kritische IT-Systeme wie beispielsweise Server, auf denen Unternehmens- oder Kundendaten gespeichert werden, sind mit einer USV vor kurzzeitigen Stromausfällen geschützt.
- Verwendung und regelmäßige Aktualisierung eines Virenscanners und Spamfilters
- Speicherung von Daten in Rechenzentren (Office 365, DATEV)
- Backup bei externem Hosting (DATEV) beauftragt
- Eigenes Backup bei internen Anwendungen / Datenspeicherung
- Durchführung regelmäßiger Backup-Recovery-Tests
- Betreuung durch externes IT-Systemhaus (Auftragsverarbeiter)
- Geregelter Prozess zur IT-Beschaffung

4. Weitere Maßnahmen

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
- Sichere Entsorgung von gedruckten Dokumenten; Gedruckte Dokumente mit sensiblem Inhalt werden nicht über den normalen Papiermüll entsorgt. Stattdessen stehen für deren sichere Entsorgung spezielle Aktenvernichter bzw. abschließbare Papiersammelbehälter zur Verfügung, die von einem Spezialunternehmen nachweislich vernichtet und entsorgt werden.
- Löschen nicht mehr benötigter Daten
- Betreuung durch externes IT-Systemhaus (Auftragsverarbeiter) zwecks Austausches von Hard- und Software
- Bestellung eines Datenschutzbeauftragten

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:

- Abschluss von Verträgen zur Auftragsverarbeitung unter Berücksichtigung aller gesetzlichen Anforderungen gemäß Art. 28 DSGVO mit entsprechenden Dienstleistern
- Angebot zum Abschluss von Verträgen zur Auftragsverarbeitung unter Berücksichtigung aller gesetzlichen Anforderungen gemäß Art. 28 DSGVO mit Kunden
- Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter; Bei Eintritt in das Unternehmen werden alle wesentlichen Verhaltensrichtlinien zum Thema Datenschutz an neue Mitarbeiter kommuniziert.
- Regelmäßige Unterweisung und Fortbildung von Mitarbeitern zum Thema Datenschutz durch Webinar
- Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter; Alle Mitarbeiter unterzeichnen beim Eintritt in das Unternehmen eine gesonderte Verschwiegenheitserklärung. Darin verpflichten sich die Mitarbeiter, personenbezogene Daten vertraulich zu behandeln und diese ausschließlich auf Weisung ihrer Vorgesetzten zu verarbeiten.

Projekt- und anwendungsspezifische TOMs werden im Bedarfsfall projektbezogen ergänzt.