TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN GEM. ART. 32 ABS. 1 DSGVO

Technische und organisatorische Maßnahmen (TOM)
gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g DSGVO)

Aus der Verpflichtung zum Datenschutz hat die microPLAN IT-Systemhaus GmbH, die im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, die technischen und organisatorischen Maßnahmen getroffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutz-Grundverordnung, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten.

Sofern Sie Fragen zur Auftragsverarbeitung haben, steht Ihnen unser Datenschutzbeauftragter Herr Thomas Floß oder als Vertreter Herr Guido Bakenecker telefonisch unter 02572/9365-77 gerne zur Verfügung.

Nachstehend erfolgt eine Aufstellung und Beschreibung der wesentlichen Maßnahmen, die die microPLAN IT-Systemhaus GmbH (mit Hauptsitz in Emsdetten; nachfolgend „microPLAN" genannt) zur Einhaltung der Datenschutzvorschriften gem. Art. 32 Abs. 1 DSGVO umsetzt.

1. Verschlüsselung

Eine Datenübertragung findet ausschließlich über eine verschlüsselte VPN-Verbindung statt.

2. Gewährleistung der Vertraulichkeit

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt.

Das Gebäude der microPLAN IT-Systemhaus GmbH wird durch eine Alarmanlage und einem externen Wachdienst geschützt. Die Glasscheiben des Gebäudes sind durch Sicherheitsfolien vor Einbruch gesichert.

Der Zutritt zum Serverraum ist ausschließlich berechtigten Mitarbeitern der microPLAN IT-Systemhaus GmbH, mittels Schlüsselregelung, möglich.

Besucher der microPLAN werden am Eingang in Empfang genommen und dürfen sich nur in Begleitung von Mitarbeitern innerhalb des microPLAN-Gebäudes bewegen.

- *Zugriffskontrolle*

  Maßnahmen, die gewährleisten, dass die Berechtigten zur Benutzung von IT-Systemen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass die bei der Bearbeitung verwendeten personenbezogenen Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, sind innerhalb der microPLAN getroffen.

  Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit mit

microPLAN IT-Systemhaus GmbH
Spatzenweg 2 Grevenerstr. 464
48282 Emsdetten 48159 Münster

Geschäftsführer:
Dipl. Inform. Kornelius Kreft
Dipl. Inform. Christoph Mauve

Telefon: (0 25 72) 93 65-0
Telefax: (0 25 72) 93 65-10
E-Mail: kontakt@microplan.de
Internet: www.microplan.de

Ust.-IdNr.:DE 124395089
Amtsgericht Steinfurt, HR B 4077

VerbundSparkasse Emsdetten-Ochtrup
BIC: WELADED1XXX
IBAN: DE88 4015 3768 0000 0899 35

VR-Bank Kreis Steinfurt eG
BIC: GENODEM1XXX
IBAN: DE84 4036 1906 0083 2552 00

der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen.

Alle Mitarbeiter der microPLAN sind schriftlich und mündlich auf das Datengeheimnis (Art. 28 Abs. 3 lit. b DSGVO) verpflichtet und werden in regelmäßigen Schulungen zum Thema Datenschutz sensibilisiert.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, sind bei microPLAN ebenfalls geregelt: Die Dateneingabe und die Verarbeitung der Auftragsdaten erfolgen ausschließlich nach dem mit dem Auftraggeber festgelegten Verfahren. Ausführliche Protokollierungen (inkl. Datensicherung) sind auf Wunsch des Auftraggebers möglich.

- *Zugangskontrolle*

  microPLAN setzt Maßnahmen ein, die sicherstellen, dass Unbefugte an der Benutzung der Datenverarbeitungsanlage und -verfahren gehindert werden.

  Alle Arbeitsplätze verfügen mindestens über ein Zugangskontrollsystem (User-ID, Passwort). Aufbau und Lebensdauer des Passwortes sind durch Richtlinien (entsprechend dem IT-Grundschutz-Katalog M 2.11) geregelt.

  Das Netzwerk der microPLAN ist durch Firewalls abgesichert. Alle Arbeitsplätze und alle Server verfügen über eine Anti-Viren-Software, die regelmäßig (mehrmals täglich) aktualisiert wird.

  Ein Datentransport findet ausschließlich über gesicherte / verschlüsselte VPN-Verbindungen statt.

- *Weitergabekontrolle*

  Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung finden ausschließlich über gesicherte VPN-Verbindungen oder per verschlüsselter E-Mail statt.

  Datenträger werden datenschutzkonform (gemäß DIN 66399) vernichtet.

  Ferner setzt microPLAN Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer ein. Die zur Verarbeitung eingereichten Daten werden ausschließlich im Rahmen der Weisungen des Auftraggebers verarbeitet und insbesondere auch nicht an unbefugte Dritte weitergegeben.

3. Gewährleistung der Integrität

Eine tägliche Datensicherung aller Systeme gewährleistet die Integrität.

4. Gewährleistung der Verfügbarkeit

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, sind bei microPLAN umgesetzt.

Serverraum: Damit Spannungsspitzen den Systemen nicht gefährlich werden können, sind die Ein-

microPLAN IT-Systemhaus GmbH
Spatzenweg 2 Grevenerstr. 464
48282 Emsdetten 48159 Münster

Geschäftsführer:
Dipl. Inform. Kornelius Kreft
Dipl. Inform. Christoph Mauve

Telefon: (0 25 72) 93 65-0
Telefax: (0 25 72) 93 65-10
E-Mail: kontakt@microplan.de
Internet: www.microplan.de

Ust.-IdNr.:DE 124395089
Amtsgericht Steinfurt, HR B 4077

VerbundSparkasse Emsdetten-Ochtrup
BIC: WELADED1XXX
IBAN: DE88 4015 3768 0000 0899 35

VR-Bank Kreis Steinfurt eG
BIC: GENODEM1XXX
IBAN: DE84 4036 1906 0083 2552 00

speisungen durch USV-Anlagen gepuffert. Diese übernehmen die Absicherung der Stromzufuhr (im Falle eines Ausfalls des Stromnetzes) bis der Generator gestartet ist und konstante Leistung abgibt.

Klimatisierung: Modernste Präzisionsklimageräte halten die Räumlichkeiten der microPLAN-Rechenzentren konstant bei einer Raumtemperatur von 27°C und einer Luftfeuchtigkeit von 40-60%. Um Fehlfunktionen vorzubeugen, werden die Einstellungen sowie Temperatur und Luftfeuchtigkeit ständig kontrolliert.

Alle Arbeitsplätze haben einen lokal installierten Virenscanner der täglich aktualisiert wird. Eine inkrementelle Datensicherung wird täglich durchgeführt und in unterschiedlichen Brandabschnitten aufbewahrt.

Test: Es finden regelmäßig Übungen statt, in denen Notfallsituationen (z. B. durch Wasser oder Feuer) simuliert werden und die Wiederherstellung der Daten geübt wird.

Notfallplan: Es existiert ein Plan, der festlegt wie im Falle der Zerstörung oder Beschädigung von Datenverarbeitungsanlagen der Geschäftsbetrieb aufrechterhalten werden kann.

5. Gewährleistung der Belastbarkeit der Systeme

Maßnahmen, die gewährleisten, dass die Belastbarkeit der eingesetzten Systeme die Verarbeitung der Daten auf Dauer sicherstellen können, sind bei microPLAN umgesetzt.

Es erfolgt eine laufende Überwachung der Nutzung der Dienste und Auslastung der Systeme.

Eine angepasste und konsequent weiterentwickelte IT-Architektur ermöglicht die Aufrechterhaltung des Betriebes der angebotenen Dienste auch bei ungewöhnlichen Spitzenbelastungen.

6. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Die Wiederherstellung von personenbezogenen Daten nach einem physischen oder technischen Zwischenfall ist in der Dokumentation des Datensicherungskonzeptes beschrieben.

7. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Es liegen schriftlich vor:

- ✓ interne Verhaltensregeln
- ✓ allgemeine Datensicherheitsbeschreibung
- ✓ allgemeines Datensicherheitskonzept
- ✓ Zertifikate (z. B. für Hardware)

Emsdetten, 01.05.2022
Ort und Datum


Unterschrift

microPLAN IT-Systemhaus GmbH
Spatzenweg 2 Grevenerstr. 464
48282 Emsdetten 48159 Münster

Geschäftsführer:
Dipl. Inform. Kornelius Kreft
Dipl. Inform. Christoph Mauve

Telefon: (0 25 72) 93 65-0
Telefax: (0 25 72) 93 65-10
E-Mail: kontakt@microplan.de
Internet: www.microplan.de

Ust.-IdNr.:DE 124395089
Amtsgericht Steinfurt, HR B 4077

VerbundSparkasse Emsdetten-Ochtrup
BIC: WELADED1XXX
IBAN: DE88 4015 3768 0000 0899 35

VR-Bank Kreis Steinfurt eG
BIC: GENODEM1XXX
IBAN: DE84 4036 1906 0083 2552 00