

Datenschutz

(1) microm hat als Auftragnehmer die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [s. Anlage 1].

(2) Die nachfolgenden technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

Technisch-organisatorische Maßnahmen

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

- Zutrittskontrolle
 - Firmenräume befinden sich in einer abgeschlossenen Etage
 - Zutritt nur für Befugte
 - elektr. Türsicherung
 - Chipkarten-/Transponder-Schließsystem
 - Dokumentation der Vergabe der Zutrittsmittel
 - Personenkontrolle beim Pförtner / Empfang
 - Besucher werden in Empfang genommen und jederzeit begleitet
- Zugangskontrolle
 - Einsatz einer Passworrichtlinie zum Passwortschutz für alle eingesetzten PC-Systeme
 - vorgegebene Komplexität (Sonderzeichen, Groß-/Kleinschreibung u. Ziffern) und Mindestlänge der Passwörter
 - regelmäßig erzwungene Passwortänderung
 - Zugang nur mit individueller Benutzerkennung und Passwort
 - Verschlüsselung der mobilen Endgeräte
 - automatische Sperrung bei Abwesenheit
 - Einsatz von VPN-Technologie
- Zugriffskontrolle
 - Berechtigungskonzept
 - Zugriff auf personenbezogene Daten und vertrauliche Informationen erhalten nur die autorisierten Mitarbeiter (Projektmitglieder) sowie Administratoren
 - auftrags- und projektbezogene Benennung der Projektmitarbeiter und deren Dokumentation
 - Protokollierung der Zugriffe
- Trennungskontrolle
 - Berechtigungskonzept
 - Benutzerprofile
 - logische mandantenfähige Trennung der Daten

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

- Weitergabekontrolle
 - elektronische Übermittlung in verschlüsselter Form (sFTP, zertifikatsbasiert), PGP-Verschlüsselung auf Wunsch
 - Übermittlung von Daten bzw. Ergebnissen verschlüsselt per CD-Rom / DVD per Kurier
 - Weitergabe ist nur durch die Projektmitglieder bzw. Administratoren möglich
 - Protokollierung
- Eingabekontrolle
 - eine Datenerfassung ist nicht vorgesehen
 - Berechtigungskonzept
 - Eingang sowie der Verbleib eingehender Daten mit Personenbezug, die im Rahmen von Projekten verarbeitet bzw. analysiert werden, wird bis zur Löschung dokumentiert
 - Protokollierung der Zugriffe

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

- Verfügbarkeitskontrolle
 - Sicherungskopien an einem anderen Ort
 - Unterbrechungsfreie Stromversorgung
 - Brandschutzeinrichtungen
 - regelmäßige Aktualisierung des Betriebssystems sowie der vorhandenen Betriebs- und Sicherheitssoftware (Update- und Patchmanagement),
 - Virenschutzprogramme mit täglicher Aktualisierung
 - Firewall

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

- Datenschutz-Management
 - Datenschutzbeauftragter
 - regelmäßige Auditierung
- Auftragskontrolle
 - eindeutige Vertragsgestaltung
 - formalisiertes Auftragsmanagement
 - sorgfältige Auswahl von Dienstleistern

5. Pflichten des Auftragnehmers microm

(1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(2) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen. Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden.

(3) Der Auftragnehmer hat einen Datenschutzbeauftragten schriftlich bestellt, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr Alexander Schmidt, 02131- 109 12 06, A.Schmidt@creditreform-compliance.de bestellt

(4) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Unterauftragnehmer	Anschrift/Land	Leistung
Verband der Vereine Creditreform e.V. Ecofis GmbH	Hellersbergstr. 12, 41460 Neuss	Betreuung, Wartung u. Betrieb der IT-Infrastruktur (z.B. Einrichtung u. Support der IT-Arbeitsplätze, Serverhosting, Netzwerk, Datensicherungsmaßnahmen usw.)