



Getroffene technisch organisatorische
Maßnahmen nach EU-DSGVO & BDSG

Vertraulichkeit (Art. 32 Abs. 1 Lit. B DS-GVO)

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- ⇒ Das Bürogebäude sowie auch die Büro-Eingangstür verfügt über Zylinderschlösser. Die automatische Glas-Schiebe-Besucher-Eingangstür wird nach Büroschluss verriegelt und durch zusätzliche Sicherheitsriegel gesichert.
- ⇒ Der Zugang ist – außer Besuchern während der Öffnungszeiten – nur Befugten möglich.
- ⇒ Datensicherungen auf portablen Sicherungsmedien sind in zutrittsgeschützten Räumen untergebracht bzw. werden extern gelagert.

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ⇒ Alle Rechner verfügen mindestens über ein Zugangskontrollsystem (UserID, Passwort).
- ⇒ Grundsätzlich verfügt jeder Mitarbeiter über ein individuelles Benutzerkonto in der Infrastruktur.
- ⇒ Nicht mehr benötigte Zugangsberechtigungen werden umgehend entzogen.
- ⇒ Das Passwort ist nur dem jeweiligen Mitarbeiter bekannt.

Zugriffskontrolle

Maßnahmen, die gewährleisten, 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, verändert oder entfernt werden können.

- ⇒ Die zur Benutzung von IT-Systemen Berechtigten dürfen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen. Im Auftrag verarbeitete Daten dürfen bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.
- ⇒ Die Infrastruktur ist durch eine Firewall und Anti-Viren-Software geschützt.
- ⇒ Externe Zugriffe werden nicht zur Verfügung gestellt.
- ⇒ Die persönliche Verantwortung jedes Mitarbeiters für die Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen wird durch Schulungsmaßnahmen gestärkt.

Hausanschrift:

Klosterstr. 17
33428 Marienfeld

Postanschrift:

Postfach 21 47
33429 Marienfeld

Kommunikation:

☎ 0 52 47 - 40 42 30
☎ 0 52 47 - 40 42 329

E-Mail:

info@romavers.de

Internet:

www.romavers.de

Bankverbindung:

Sparkasse Gütersloh
BLZ 478 500 65
Kto.Nr. 29 017 416

Iban:

DE04 4785 0065 0029 0174 16

BIC: WELADED1GTL

Registrierungsnummer:

D-ADWL-EG713-74
IHK Bielefeld

Steuernummer:

351/5765/1765



Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Im Hinblick auf personenbezogene Daten verschiedener Auftraggeber erfolgt softwareseitig eine logische Trennung der Daten (Mandantenprinzip).

Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Hierzu setzt das Unternehmen für den elektronischen Transport Verschlüsselungsverfahren ein, die dem Stand der Technik entsprechen und ein Schutzniveau erreichen, das den Anforderungen und dem Schutz von Versicherungs- und Finanzprodukten angemessen ist.

Integrität (Art. 32 Abs. 1 Lit. B DS-GVO)

Weitergabekontrolle

Maßnahmen, die gewährleisten, 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ⇒ Datenübertragungen erfolgen verschlüsselt.
- ⇒ Der Zugriff auf die einzelnen Mandantendaten ist über Berechtigungen reglementiert.
- ⇒ Eine datenschutzkonforme Datenvernichtung ist gewährleistet. Für Papierdokumente steht ein der Schutzstufe angemessener Papierreißwolf zur Verfügung.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ⇒ Benutzeranmeldungen werden durch die Portal-Software protokolliert.
- ⇒ Gruppen- sowie Einzelberechtigungen schränken die Möglichkeiten von Veränderungen und das Löschen von Daten ein.
- ⇒ Durch den Einsatz eines Dokumentenmanagementsystems (DMS) ist die Nachvollziehbarkeit hinsichtlich Eingabe, Änderung und Löschung von Daten gewährleistet.

Hausanschrift: Klosterstr. 17 33428 Marienfeld	Kommunikation: ☎ 0 52 47 - 40 42 30 ☎ 0 52 47 - 40 42 329	Bankverbindung: Sparkasse Gütersloh BLZ 478 500 65 Kto.Nr. 29 017 416	Registrierungsnummer: D-ADWL-EG713-74 IHK Bielefeld
Postanschrift: Postfach 21 47 33429 Marienfeld	E-Mail: info@romavers.de Internet: www.romavers.de	Iban: DE04 4785 0065 0029 0174 16 BIC: WELADED1GTL	Steuernummer: 351/5765/1765



Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle (Art. 32 Abs. 1 Lit. B DS-GVO)

Verfahrenseigene Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ⇒ Alle elektronischen Daten befinden sich in der redundanten Rechenzentrums Umgebung (Server). Durch tägliche Backups auf unterschiedlichen Medien, die darüber hinaus an unterschiedlichen Orten und u.a. extern gelagert sind, ist der Zugang zu den Daten gewährleistet.
- ⇒ Alle Clientgeräte und anhängende Infrastrukturen verfügen über Virenschutz.
- ⇒ Es gibt ein Backup- und Recovery-Konzept.
- ⇒ Die Backups werden regelmäßig daraufhin getestet, ob ein reibungsloses Zurücksichern möglich ist.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 Lit. C DS-GVO)

Durch die verteilten Backup-Datenträger ist eine hohe Verfügbarkeit garantiert.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM (Art. 32 Abs. 1 Lit. D DS-GVO; ART. 25 ABS. 1 DS-GVO)

Datenschutz-Management

- ⇒ Auf Grundlage eines PDCA-Zyklus unterliegen alle datenschutzrelevanten Bereiche einem ständigen Monitoring durch das Datenschutz-Team.
- ⇒ Aktuell erfolgen – soweit gesetzlich erforderlich - Vorabkontrollen gemäß § 4d Abs. 5 BDSG bei der Einführung neuer Software-Systeme. Grundsätzlich erfolgen zyklische Überprüfungen der Verfahren und der technischen und organisatorischen Maßnahmen. Ab spätestens 25. Mai 2018 wird durch das Unternehmen – soweit gesetzlich erforderlich – eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchgeführt und im Rahmen von einem PDCA-Zyklus die Angemessenheit und Wirksamkeit der Maßnahmen überprüft und optimiert.
- ⇒ Im Rahmen der DS-GVO wird das DSMS erweitert. Es beinhaltet u. a. Prozesse, Rollenzuordnungen, Schulungskonzepte, Prüfverfahren und deren Ergebnisse, Dokumentationen, Begutachtungen und Abwägungen etc.

Hausanschrift: Klosterstr. 17 33428 Marienfeld	Kommunikation: ☎ 0 52 47 - 40 42 30 ☎ 0 52 47 - 40 42 329	Bankverbindung: Sparkasse Gütersloh BLZ 478 500 65 Kto.Nr. 29 017 416	Registrierungsnummer: D-ADWL-EG713-74 IHK Bielefeld
Postanschrift: Postfach 21 47 33429 Marienfeld	E-Mail: info@romavers.de Internet: www.romavers.de	Iban: DE04 4785 0065 0029 0174 16 BIC: WELADED1GTL	Steuernummer: 351/5765/1765



Incident-Response-Management

Das Incident-Response-Management wird durch die hiermit beauftragten Ansprechpartner des Unternehmens gewährleistet. Diese ist aktuell der interne Datenschutz-Koordinator in Abstimmung mit weiteren internen Stellen.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Mit der DS-GVO wird in Art. 25 gefordert, dass die eingesetzten Systeme „datenschutzfreundliche“ Voreinstellungen ermöglichen und diese Einstellungen dann auch in angemessenem Maße vorgenommen werden. Dies wird durch den Auftragnehmer im Rahmen seiner Verantwortung gewährleistet.

Auftragskontrolle

Der Auftragnehmer stellt sicher, dass alle Personen und nachgelagerten Einrichtungen (im Falle von Unter-Auftragnehmern) die Verarbeitung der personenbezogenen Daten des Auftraggebers nur nach dessen Auftrag vornehmen. Hierzu werden intern angemessene Schulungsmaßnahmen durchgeführt, Mitarbeiter verpflichtet und angemessene Maßnahmen auch bei möglichen Unter-Auftragnehmern sichergestellt (z. B. durch das Schließen einer AV-Vereinbarung nach Art. 28 DS-GVO).

Hausanschrift: Klosterstr. 17 33428 Marienfeld	Kommunikation: 0 52 47 - 40 42 30 0 52 47 - 40 42 329	Bankverbindung: Sparkasse Gütersloh BLZ 478 500 65 Kto.Nr. 29 017 416	Registrierungsnummer: D-ADWL-EG713-74 IHK Bielefeld
Postanschrift: Postfach 21 47 33429 Marienfeld	E-Mail: info@romavers.de Internet: www.romavers.de	Iban: DE04 4785 0065 0029 0174 16 BIC: WELADED1GTL	Steuernummer: 351/5765/1765