Technische und organisatorische Maßnahmen der Mailingwork GmbH nach Art. 32 DSGVO

1. Vertraulichkeit (Art 32 Abs. 1 lit. b DSGVO)

1.1. ZUTRITTSKONTROLLE

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben.

Die Mailingwork GmbH hat sowohl am Unternehmenssitz als auch an den Serverstandorten technische und organisatorische Maßnahmen zur Sicherung der Zutrittskontrolle getroffen. Zutrittsberechtigt zu den Datenverarbeitungsanlagen sind nur Personen, deren Anwesenheit in den Produktionsstätten zur Durchführung oder Sicherstellung des Betriebes oder zur Wahrnehmung von Kontrollaufgaben erforderlich ist. An den Hosting-Standorten finden aktive Kontrollen der Zutrittsberechtigung für alle Mitarbeiter statt.

Am für die Versandlösung MAILINGWORK relevanten Serverstandort wird die Zutrittskontrolle über eine Vielzahl von Maßnahmen realisiert. Dazu zählen:

- spezielle Berechtigungslisten und Besucherregelungen,
- Werkschutz und Pförtner,
- Videokamera-Überwachung,
- KeyCard-Zutrittssysteme,
- Einfriedung des Geländes mit Zaunanlagen.

Folgende Maßnahmen zur Zutrittskontrolle setzt die Mailingwork GmbH am Firmensitz ein:

- die Räume sind bei Abwesenheit des Bedienungspersonals, auch wenn diese nur vorübergehend ist, gegen Zutritt gesichert,
- Wechseldatenträger, auf denen personenbezogene Daten gespeichert sind, werden ebenfalls (sofern nicht gerade mit ihnen gearbeitet wird) unter Verschluss aufbewahrt,
- Notebooks werden mit Festplattenverschlüsselungen ausgestattet,
- Server befinden sich in einem separaten, verschlossenen Raum,
- die Büroräume sind alarmgesichert,
- Türen sind mit Sicherheitsschließanlagen ausgestattet,
- die Eingangsbereiche befinden sich im Blickfeld von Mitarbeitern,
- die Ausgabe von Schlüsseln wird dokumentiert; eine unerwünschte Vervielfältigung von Schlüsseln wird durch Einsatz eines Sicherheitsschließsystems unterbunden,
- Zu- und Abgänge von Mitarbeitern sowie unternehmensfremden Personen werden protokolliert,
- Besucher werden durch Empfangspersonal hereingelassen und dürfen sich nur in Gegenwart von Mitarbeitern im Unternehmensgebäude aufhalten.

1.2. ZUGANGSKONTROLLE

Folgende Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungsanlagen haben.

- Die Benutzung der Server ist nur mit einer gültigen Benutzerkennung zusammen mit einem gültigen Passwort möglich. Die Systembenutzung wird protokolliert.
- Die Mailingwork GmbH setzt bei der Datenübertragung über das Internet dem Stand der Technik entsprechende Sicherungs- und Verschlüsselungsverfahren ein. Interne Netze sichert die Mailingwork GmbH gegen Angriffe von außen mit einer Firewall und getrennten sowie gesicherten W-Lan-Verbindungen ab. Als zusätzliche Härtungsmaßnahmen werden Virenscanner, Spam-Filter und regelmäßige Software-Updates eingesetzt.
- Im Unternehmen verwendete Passworte, die einen Zugang zu personenbezogenen Daten gestatten, bestehen aus einem Zeichen-Mix (Buchstaben, Zahlen, Sonderzeichen).
- Der Zugriff Unbefugter auf Arbeitsplätze während Pausenzeiten wird neben den beschriebenen Maßnahmen zur Zutrittskontrolle auch durch versetzte Pausenzeiten für Mitarbeiter und passwortgesicherte Bildschirmsperren unterbunden.
- Scheiden Mitarbeiter aus dem Unternehmen aus, werden deren Zugangsdaten unverzüglich gesperrt, Zutrittsberechtigungen entzogen und Arbeitsmittel eingesammelt.

1.3. ZUGRIFFSKONTROLLE

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben.

Mit dem Einsatz einer systemspezifischen Benutzerverwaltung und der Vergabe von Zugriffsberechtigungen hat die Mailingwork GmbH Maßnahmen geschaffen, durch die nur berechtigte Mitarbeiter auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Im Rahmen der Zugriffskontrolle werden u.a. folgende Sicherungsmaßnahmen praktiziert:

- Trennung von Test- und Produktionsumgebung in verschiedenen Bereichen,
- Einrichtung von Administrationsrechten,
- Dokumentierung der Zugriffsberechtigungen,
- Genehmigungsroutinen,
- Absicherung der Bereiche, in denen Datenträger aufbewahrt werden,
- nicht-reversible Löschung von Datenträgern bzw. datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger durch zertifizierte Entsorger.

1.4. TRENNUNGSKONTROLLE

Folgende Maßnahmen stellen sicher, dass die zu unterschiedlichen Zwecken erhobenen personenbezogenen Daten getrennt verarbeitet werden.

- Die Mailingwork GmbH gewährleistet durch den Einsatz von Zugriffsberechtigungen, dass nur berechtigte Nutzer auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.
- Die Trennung der unterschiedlichen Datensätze erfolgt durch Speicherung in logisch getrennten Datenbanken bzw. Verzeichnissen.
- Die Versandlösung MAILINGWORK wurde als mandantenfähige Software entwickelt,
- bei Programmentwicklungen werden Test- und Produktionsumgebung getrennt sowie Testdaten verwendet.

1.5. PSEUDONYMISIERUNG (ART. 32 ABS. 1 LIT. A DSGVO, ART. 25 ABS. 1 DSGVO)

Die Verarbeitung personenbezogener Daten kann in der Versandlösung MAILINGWORK entweder anonymisiert oder personalisiert erfolgen.

- **Anonymisiert:** Die Messung von Erfolgskennzahlen wie Öffnungs- oder Klickraten erfolgt so, dass personenbezogene Daten dauerhaft nicht mit einzelnen Nutzerdatensätzen verknüpft oder verknüpfbar gespeichert werden. Eine nachträgliche Personalisierung der Daten ist nicht möglich.

- **Personalisiert:** Die Messung von Erfolgskennzahlen wie Öffnungs- oder Klickraten erfolgt so, dass personenbezogene Daten mit einzelnen Nutzerdatensätzen verknüpft oder verknüpfbar gespeichert werden. Eine nachträgliche Anonymisierung der Daten ist möglich.

Der Auftraggeber legt als Verantwortlicher durch Weisung gegenüber dem Auftragsverarbeiter fest, welches Verfahren bei der Verarbeitung zum Einsatz kommen soll. Im Falle eine Personalisierung der Daten trägt der Auftraggeber sorge dafür, dass die Rechte der betroffenen Personen gewahrt werden.

2. Integrität (Art 32 Abs. 1 lit. b DSGVO)

2.1. WEITERGABEKONTROLLE

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können sowie überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

Der Zugriff auf die Versandlösung MAILINGWORK erfolgt verschlüsselt (TLS-Verschlüsselung zwischen Client und Server). Somit steht auch für den Import und Export von Daten in die Software bzw. aus der Software eine gesicherte Verbindung zur Verfügung.

Ist ein darüberhinausgehender Austausch von Daten zwischen der Mailingwork GmbH und dem Auftraggeber für die Zweckbestimmung des Vertragsverhältnisses erforderlich, so wird die Mailingwork GmbH einen Übertragungsweg wählen, der einen angemessenen Schutz der übermittelten Daten gewährleistet.

Wenn vom Auftraggeber nicht anders gewünscht, erfolgt die Übertragung personenbezogener Daten in diesem Fall als verschlüsselter E-Mail Dateianhang. Das zum Öffnen der Datei notwendige Passwort wird auf einem getrennten Weg (z. B. telefonisch) übertragen.

2.2. EINGABEKONTROLLE

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

Die Systembenutzung der Versandlösung MAILINGWORK wird im Rahmen eines Access-Logs protokolliert. Protokolliert wird der eingeloggte Benutzer sowie die Bereiche von MAILINGWORK, in denen Aktivitäten stattfanden. Die Dauer der Speicherung beträgt 45 Tage.

Mit dem Eingabeprotokoll steht eine darüberhinausgehende Protokollierungsfunktion zur Verfügung, deren Dokumentationen für jeweils drei Monate als CSV- Datei abgerufen und extern gespeichert werden können.

Protokolliert werden:

- der betroffene Datensatz, die Subscriber-ID,
- die Art der Aktivität (Anlage, Veränderung, Kopie, Löschung des Datensatzes),
- der Zeitpunkt der Aktivität bzw. des Ereignisses,
- die ausführende Person (Benutzer- ID des MAILINGWORK- Users).

Aus Gründen der Systemperformance erfolgt die Aktivierung des Eingabeprotokolls auf spezielle Weisung des Auftraggebers.

3. Verfügbarkeit und Belastbarkeit (Art 32 Abs. 1 lit. b DSGVO)

VERFÜGBARKEITSKONTROLLE UND BELASTBARKEITSKONTROLLE

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

Die Mailingwork GmbH bedient sich für das Hosting der Versandlösung MAILINGWORK und der darin gehosteten Daten eines deutschen Rechenzentrums mit speziellem Verfügbarkeitskonzept.

Dieses umfasst:

- redundante USV-Anlagen, Notstrom-Dieselgeneratoren,
- Klimatechnik,
- aktive Brandschutzmaßnahmen, Rauchmelder mit Brandfrühesterkennung (VESDA)
- Netzüberwachung,
- Redundant ausgelegt Server-Komponenten,
- ein Backup-Konzept mit Datensicherung in einen getrennten Brandabschnitt des Rechenzentrums.
- Zwei Einspeisungen auf der 10 kV Ebene

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art 32 Abs. 1 lit. d DSGVO)

4.1. DATENSCHUTZ-MANAGEMENT

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Alle Mitarbeiter werden auf das Datengeheimnis verpflichtet und regelmäßig in den Bestimmungen der für Datenschutz relevanten Gesetze unterwiesen.
- Technische Dokumentationen und Arbeitsanweisungen beschreiben und regeln datenschutz-relevante Prozesse.

- Die betriebliche Datenschutzbeauftragte kontrolliert kontinuierlich die interne Einhaltung der Datenschutzbestimmungen. Ein externer Auditor ergänzt diese Tätigkeit durch regelmäßig stattfindende, unabhängige Kontrollen.
- Subunternehmen werden sorgfältig ausgewählt und regelmäßig überprüft.
- Die Übersicht der Verarbeitungstätigkeiten (Art. 30 DSGVO) wird geführt und kontinuierlich ergänzt/redigiert.
- Soweit erforderlich erfolgt die Durchführung der Datenschutzfolgeabschätzungen (Art. 35 DSGVO).

4.2. INCIDENT-RESPONSE-MANAGEMENT

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

Es erfolgt die Festlegung von Meldeprozessen für

- Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO),
- Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO).

4.3. DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN (ART. 25 ABS. 2 DSGVO)

Die folgenden Maßnahmen sollen gewährleisten, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden:

- Die Versandlösung MAILINGWORK ist so ausgelegt, dass bei Anlage neuer Accounts datenschutzfreundliche Grundeinstellungen voreingestellt sind.
- Erfolgskennzahlen werden in der Grundeinstellung der Versandlösung MAILINGWORK grundsätzlich nur in anonymisierter Form ausgewertet (z. B. Öffnungs- und Klickrate), es sei denn, eine personalisierte Auswertung ist erforderlich (z. B. Bounces). Eine darüber hinaus gehende, personalisierte Auswertung bedingt stets eine konkrete Weisung des Auftraggebers. Diese Beauftragung muss in schriftlicher Form erfolgen.
- Bei bestimmten Prozessen werden personenbezogene Daten getrennt von standardisierten Bearbeitungsabläufen verwaltet (z. B. nicht vollständig abgeschlossene Opt-Ins).
- Datenschutzfreundliche Voreinstellungen und automatisierte Prozesse innerhalb der Versandlösung gewährleisten, dass Daten anonymisiert respektive gelöscht werden, sobald der Zweck ihrer Speicherung hinfällig geworden ist (z. B. Abmeldung von Newsletter, Widerspruch der Erlaubnis zur Erhebung personenbezogener Aktivitätsdaten, Art. 5 Abs. 1 lit. e DSGVO).
- Weiterhin findet eine automatisierte Prüfung der Empfängeradressen mit anerkannten Blacklists statt (z. B. RTR-Blacklist / Robinsliste)
- Für eine erhöhte Zustellrate ist die Mailingwork GmbH Mitglied der Certified Senders Alliance (CSA)

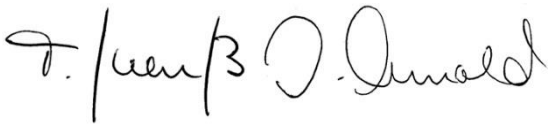
4.4. AUFTRAGSKONTROLLE

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

- Die Mailingwork GmbH handelt als Auftragnehmer entsprechend den schriftlichen Weisungen des Auftraggebers. Die Weisungen des Auftraggebers sind im Vertrag und/oder dem Produktionsauftrag enthalten.
- Insofern vereinbart wurde, dass die Mailingwork GmbH weitere Auftragsverarbeiter in Anspruch nehmen darf, erteilt die Mailingwork GmbH ihre Weisungen stets schriftlich (Art. 28 Abs. 9 DSGVO). Diese Auftragsverarbeiter werden unter besonderer Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt. Im Vertrag mit dem Auftragsverarbeiter wird für die Mailingwork GmbH ein Kontrollrecht vereinbart.

- MAILINGWORK erteilt dem Auftraggeber jederzeit Auskünfte zu Fragen, die den Vertrag betreffen und gewährt auf Anforderung Einblick in die während der Verarbeitung erzeugten Unterlagen sowie die Dokumentationen der eingesetzten Fachverfahren und der genutzten Systeme.
- MAILINGWORK benachrichtigt den Auftraggeber über technische und organisatorische Störungen bei der Verarbeitung bzw. Löschung der Daten des Auftraggebers, insbesondere insofern diese einen Meldeprozess nach Art. 33 oder 34 DSGVO erfordern.
- Alle Mitarbeiter der Mailingwork GmbH sind auf die Einhaltung des Datengeheimnisses verpflichtet. Die Mitarbeiter wurden zu den datenschutzrechtlichen Bestimmungen belehrt und werden von der Datenschutzbeauftragten regelmäßig über Neuerungen im Hinblick auf die gesetzlichen Regelungen informiert.

Chemnitz, 28.10.2019



Torsten Gneuß
Geschäftsführer

Jörg Arnold
Geschäftsführer

Mailingwork GmbH
Schönherrstraße 8
Eingang N
09113 Chemnitz

Fon: +49 (0) 371 337161 – 0
Fax: +49 (0) 371 337161 – 10
E-Mail: info@mailingwork.de
Web: www.mailingwork.de

Geschäftsführer:
Torsten Gneuß, Jörg Arnold
Amtsgericht Chemnitz, HRB 267 22
Ust-IdNr.: DE 277 964 544

Commerzbank Freiberg
IBAN: DE 36 8704 0000 0305 0010 00
BIC: COBA DEFF XXX