Technische und organisatorische Maßnahmen gemäß Artikel 32 DS-GVO
Altmann Marketing GmbH

Inhalt

1. Revisionshistorie

Datum	Änderung	Name
04.04.2018	Erstellung (Umstellung TOMs nach Anlage zu § 9 BDSG auf TOMs nach Artikel 32 DS-GVO)	Sebastian Grau (rehm Datenschutz GmbH)

2. Ziel dieses Dokumentes

Das vorliegende Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM) nach Artikel 32 DS-GVO bei der Altmann Marketing GmbH.

Der Datenschutz besitzt in unserem Unternehmen eine besondere Bedeutung und erfolgt auf der Basis der Datenschutz-Grundverordnung (DS-GVO), auf dessen Einhaltung alle in unserem Haus mit der Verarbeitung von personenbezogenen Daten befassten Mitarbeiter schriftlich verpflichtet wurden.

Um einen hohen Datenschutz garantieren zu können, wurden gemäß Artikel 32 DS-GVO folgende technische und organisatorische Maßnahmen getroffen und werden laufend gewährleistet:

3. Pseudonymisierung und Verschlüsselung

3.1 Pseudonymisierung

Eine Pseudonymisierung von Kundendaten ist nicht möglich, da komplette Adressdaten für den Versand benötigt werden. Nach Abschluss des Auftrages werden die Daten gelöscht.

Sofern Kunden eine Rückübertragung von Adressbeständen fordert, erfolgt dies, sofern gewünscht, pseudonymisiert.

3.2 Verschlüsselung

Die Übertragung von Adressdaten per E-Mail, USB-Stick, CD-ROM oder sonstige Datenträger erfolgt passwortgeschützt und verschlüsselt, wobei das Passwort von uns nicht per E-Mail, sondern telefonisch oder per Fax übermittelt wird.

Diese Art der Adressübertragung empfehlen wir auch unseren Kunden.

4. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

4.1 Vertraulichkeit und Integrität

4.1.1 Physikalische Sicherheit

Um Unbefugten den Zutritt zu unseren Geschäftsräumen, insbesondere denen, in denen die Verarbeitung oder Nutzung personenbezogener Daten erfolgt, zu verwehren, erfolgt der Zutritt nur nach Anmeldung und Einlass (Türschließsystem).

Der Zutritt zu unseren Geschäftsräumen ist nur berechtigten Personen gestattet. Betriebsfremden ist der Zutritt nur zur Wahrung berechtigter Interessen im Zusammenhang mit der Erfüllung unserer Leistungen und nur in Begleitung einer berechtigten Person unseres Hauses erlaubt.

Alle Eingangstüren unserer Geschäftsräume sind mit Sicherheitsschlössern gesichert. Alle Fenster, Türen und Tore sind außerhalb unserer Betriebszeiten fest verschlossen und im Erdgeschoß einbruchhemmend gemäß den Vorschriften der Sicherungsklasse SG1 nach Vds 2333 gesichert.

Darüber hinaus verfügen wir über eine Alarmanlage mit Anschluss an eine private Notrufzentrale und Videoüberwachung im Warenanlieferungsbereich.

Das Betreten unserer Geschäftsräume durch Betriebsfremde wird von uns für einen Zeitraum von einem Monat nach Betreten protokolliert.

Die Vergabe von Zutrittsberechtigungen und Schlüsseln wird nachvollziehbar dokumentiert.

Unser Serverraum ist durch eine abschließbare Tür geschützt. Er wird immer verschlossen gehalten und nur bei Bedarf von den hierzu berechtigten Personen geöffnet.

4.1.2 Authentifizierung

Um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können, wird jeder Rechner mit einem Passwort geschützt, das mindestens quartalsweise vom Mitarbeiter geändert wird und nur dem Mitarbeiter bekannt ist, der an diesem Rechner arbeitet.

Passwörter werden nach üblichen Sicherheitsanforderungen und einer Länge von mindestens 8 alphanumerischen Zeichen erstellt.

Bei mehrfacher Fehleingabe des Passwortes erfolgt eine Sperrung des Computers.

Geregelte Zugriffsrechte auf bestimmte Server-Partitionen gewährleisten, dass die Daten unserer Auftraggeber nur den mit der Auftragsdurchführung betrauten Mitarbeitern zugänglich sind.

4.1.3 Berechtigungskonzept

Um zu gewährleisten, dass nur die für die Leistungserbringung berechtigten Mitarbeiter auf die Daten unserer Auftraggeber zugreifen können, existiert ein internes Zugriffssystem, welches von unserem Netzadministrator verwaltet wird und bestimmten Arbeitsplätzen Zugriffsrechte zu bestimmten Serverpartitionen erlaubt oder verwehrt.
Jedem Arbeitsplatz sind nur die Laufwerke zugewiesen, die für die jeweiligen Aufgaben relevant sind.

Mitarbeiter, die Ihren Arbeitsplatz verlassen (z.B. Pause), sperren ihren Rechner und melden sich danach wieder mit Ihrem Passwort neu an.
Dass Passwort ist nur dem Inhaber des jeweiligen Arbeitsplatzes bekannt.

Wird die Nutzung eines Rechners unterbrochen, schaltet sich nach 5 Minuten automatisch ein Bildschirmschoner ein, der nur mittels Passwort wieder aufgehoben werden kann.
Auftragsunterlagen und Daten sind nur den für die Ausführung der Aufträge verantwortlichen Mitarbeitern zugänglich und vor unberechtigtem Zugriff geschützt.

4.1.4 Weitergabe von Daten

Der Auftragnehmer stellt sicher, dass Daten des Auftraggebers nicht unbefugt kopiert, weitergegeben und/oder gelöscht werden können.

Die Verwendung externer Speichermedien (zum Beispiel Festplatten, DVD, USB-Sticks) ist nur für den Zweck gestattet, dass im Auftrag des Auftraggebers hierauf Daten zur Übergabe an den Auftraggeber gespeichert werden.

Um den Datenzugriff von außen zu verwehren, ist unser Server mit einer Firewall geschützt sowie mit einem Virenschutzprogramm ausgestattet, welches laufend online gewartet wird.
Über unseren Provider (M-net) werden die Kanäle zum Server nur in festgelegten Intervallen geöffnet und am Wochenende komplett geschlossen, so dass ein externer Zugriff nicht möglich ist.

Der Versand von Datenträgern erfolgt grundsätzlich als Paket oder eingeschriebener Brief.

Werden Daten von uns an Dritte weitergegeben, so erfolgt dies nur auf schriftliche Weisung unserer Auftraggeber und wird in jedem Fall durch Lieferschein dokumentiert.

4.1.5 Trennung von Daten

Um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene oder gelieferte Daten getrennt verarbeitet werden können, speichern wir die Daten für jeden Auftrag unter einer eigenen Auftragsnummer ab.
Darüber hinaus erfolgt die Speicherung in getrennten Ordnern je Auftraggeber.

Ein Vermischen von Auftraggeber-Daten mit Daten anderer Auftraggeber oder eigenen Daten ist somit nicht möglich, Auftraggeber-Daten können jederzeit identifiziert und getrennt von Daten anderer Auftraggeber verarbeitet und gelöscht werden.

4.1.6 Protokollierung

Um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind, werden die bei der Bearbeitung personenbezogener Daten ausgeführten Bearbeitungsschritte protokolliert und dokumentiert.

Werden Datenbanken gepflegt oder Adressen erfasst, so wird das jeweilige Änderungsdatum und der Bearbeiter/in hinterlegt.

Bei jedem Auftrag werden darüber hinaus auch alle weiteren Verarbeitungsschritte so dokumentiert, dass sie ggf. nachvollziehbar sind.

4.1.7 Löschen von Daten

Es ist sichergestellt, dass sämtliche elektronischen Daten entsprechend den Regelungen des Datenschutzes spätestens sechs Monate nach der Verarbeitung unwiderruflich gelöscht werden, es sei denn, der Auftraggeber gibt uns ausdrücklich anderslautende Weisung.

Datenträger werden physisch gelöscht bzw. vernichtet, bei der Verarbeitung anfallendes adressiertes Papiermaterial wird unmittelbar nach dem Anfall in hierfür vorgesehene Tonnen verbracht, welche von einem zertifizierten Unternehmen nach Datenschutz-Richtline entsorgt werden.

4.2 Verfügbarkeit

Unser Server ist mit Wechselplatten ausgerüstet, die den Betrieb störungsfrei und datenverlustfrei, auch bei Festplattenschäden, ermöglichen. Der Server wird regelmäßig gewartet.

Um Daten zusätzlich vor Zerstörung oder Verlust zu sichern, ist unser Server mit einem Notstromaggregat ausgestattet, welches kürzere Stromunterbrechungen ausgleicht und bei längerem Stromausfall die Anlage ordnungsgemäß und ohne Datenverlust herunterfährt.

Sofern vom Kunden nicht anders gewünscht, speichern wir alle Daten (gezippt) bis zu sechs Monate nach Fertigstellung des Auftrags.

Unsere Verarbeitungssoftware ist dem aktuellen Stand der Technik angepasst und wird, insbesondere im Hinblick auf sicherheitsrelevante Updates, stets aktualisiert.

4.3 Belastbarkeit

Unsere Systeme entsprechen dem aktuellen Stand der Technik, ihre Auslastung wird laufend überwacht. Die Serverkapazität ist so ausgelegt, dass auch für den Fall vorübergehender Spitzenbelastungen genügend Leistungsreserven zur Verfügung stehen.

Virenscanner und Firewall schützen die Systeme vor Angriffen, regelmäßige Updates werden durchgeführt.

5. Wiederherstellung

Um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei Störungen datenverlustfrei wieder hergestellt werden können, wird eine tägliche Sicherung aller Daten vorgenommen.
Darüber hinaus wird in regelmäßigen Abständen eine weitere Sicherungskopie erstellt und extern in einem Safe verwahrt.

6. Überprüfung, Bewertung und Evaluierung

Um zu gewährleisten, dass die Auftragsverarbeitung personenbezogener Daten, deren Bearbeitung über die reine Adressierung mit oder ohne Anrede hinausgeht, nur entsprechend den Weisungen des Auftraggebers erfolgt, wird bei Aufträgen, für die keine detaillierte schriftliche Weisung des Auftraggebers bezüglich der Verwendung weiterer personenbezogener Merkmale vorliegt, die vorgesehene Verarbeitung dieser Daten von uns in einer Auftragsbestätigung oder sonstigen schriftlichen Mitteilung an den Auftraggeber bestätigt.

Die Wirksamkeit unserer technischen und organisatorischen Maßnahmen wird intern sowie u.a. durch unseren Externen Datenschutzbeauftragten laufend überprüft, bewertet und evaluiert.

7. Kontakt

Altmann Marketing GmbH, Stahlgruberring 22, 81829 München
Geschäftsführer: Dipl.-Kfm. Karl Gommersbach, Wulf Henrichs
altmann-service@altmann-marketing.de / Tel.: 089/697 994 0 / Fax: 089/697 994 19

8. Datenschutzbeauftragte/r

Um die Einhaltung aller datenschutzrechtlich relevanten technischen und organisatorischen Maßnahmen zu gewährleisten und den Kenntnisstand unserer Mitarbeiter durch Schulungen auf dem aktuellen Niveau zu halten, haben wir einen externen Datenschutzbeauftragten bestellt. Hierbei handelt es sich um die Firma:
rehm Datenschutz GmbH, Eugen-Sänger-Ring 13, 85649 München,
vertreten durch Frau Daniela Duda (Geschäftsführerin)
daniela.duda@rehm-datenschutz.de / Tel.: 089/6080 7600 / Fax.: 089/6080 7602

Stand: April/2018