Datenschutz- und Datensicherheitskonzept der Trebbau direct media GmbH

Verantwortliche Stelle:
Trebbau direct media GmbH
Schönhauser Str. 21
50968 Köln

- nachfolgend Trebbau genannt -

Geschäftsführer: Jörg Hennig – Beirat: Karl-Peter Trebbau

Unseren Datenschutzbeauftragen erreichen Sie unter:

Helsper & Helsper – Rechtsanwälte
Herrn Rudolf Helsper
Am Kielshof 18
51105 Köln
Tel: +49 221 9834240 – E-Mail: helsper@helsper-koeln.de

Präambel
Trebbau ist regelmäßig im Rahmen der Auftragsverarbeitung sowohl als Lettershop wie auch als datenverarbeitendes Unternehmen tätig. Aufgrund dieser Tätigkeitsfelder unterliegt Trebbau der EU-Verordnung 2016/79 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DS-GVO). Des Weiteren hat Trebbau sich verpflichtet, die speziellen Anforderungen der Qualitäts- und Leistungsstandards (QuLS) des Deutschen Dialogmarketing Verband e.V. (DDV) einzuhalten und damit diesen, über die Gesetze hinausgehenden Verpflichtungen unterworfen, um für seine Kunden, Geschäftspartner und Lieferanten, aber auch für Mitarbeiter ein besonders hohes Maß an Datenschutz zu gewährleisten. Im Rahmen der Verarbeitung personenbezogener Daten steht dabei auch das Verhältnis zwischen den Adressen-Eigentümern, Listeignern, Listbrokern, Werbungtreibenden und anderen Auftragsverarbeitern besonders im Focus.

Darüber hinaus fühlt sich Trebbau aber auch den Empfängern von Werbung gegenüber verpflichtet und berät seine Kunden umfassend bei der Erfüllung ihrer datenschutzrechtlichen Verpflichtungen.

1. Technisch-organisatorische Maßnahmen (TOMs)

VERTRAULICHKEIT

Zutrittskontrolle
Organisatorisch ist geregelt, dass Fremde sich im Gebäude niemals allein aufhalten oder frei bewegen dürfen. Mitarbeiter werden regelmäßig entsprechend geschult.

Die Zugänge zum Gebäude sind stets geschlossen und können von außen nur mit Sicherheitsschlüsseln oder zu den üblichen Geschäftszeiten durch an die Mitarbeiter ausgehändigten Zeiterfassungskarten geöffnet werden. Betriebsfremde melden sich am zentralen Empfang oder im Falle von Anlieferungen bei der Warenannahme. Besucher werden von einer Mitarbeiterin oder einem Mitarbeiter persönlich am Empfang abgeholt, in einem Besucherbuch erfasst und erhalten einen Besucherausweis. Der Aufenthalt von Besuchern in sensiblen Bereichen ist nur in Begleitung von Mitarbeitern, die eine Verpflichtungserklärung auf Wahrung der Vertraulichkeit abgeben haben, gestattet. Außerhalb der Arbeitszeiten erfolgt die Überwachung der Räumlichkeiten durch eine Alarmanlage gemäß VDE-Norm. Meldungen der Anlage werden durch einen Sicherheitsdienst überwacht und nach einem dokumentierten Interventionsplan verfolgt. Fenster im Erdgeschoß sind teilweise vergittert oder mit Metallrollos geschützt.

Zugangskontrolle
Unbefugten wird der Zugang zu Datenverarbeitungssystemen nicht gewährt. Der Zugang über Außenschnittstellen zu unseren EDV-Systemen ist durch eine Firewall geschützt. Öffentlich erreichbare Systeme, wie Bastion Hosts mit E-Mail oder Internetzugang werden über entsprechende Trennungen vom internen Netz gesichert (DMZ). Sämtliche PC-Systeme sind passwortgeschützt. Passwörter müssen hohen Ansprüchen genügen und werden regelmäßig zwangsweise erneuert. Alte Passwörter können nicht wiederverwendet werden. Nach zehn fehlerhaften Anmeldeversuchen wird der entsprechende Benutzerzugang automatisch gesperrt. Externe Zugriffsmöglichkeiten, beispielsweise für Mitarbeiter im Homeoffice, erfolgen ausschließlich über VPN-Tunnel auf unsere Systeme und über eine Zwei-Faktor-Authentifizierung.

Zugriffskontrolle
Der Zugriff auf Netzwerkverzeichnisse, in denen personenbezogene Daten gespeichert werden, ist auf die jeweiligen Personen beschränkt, die mit den Aufträgen beschäftigt sind, für die solche Daten verwendet werden sollen. Diese Personen müssen sich gegenüber dem System identifizieren. Insbesondere Produktionssysteme haben ausschließlich zu einem einzigen, für sie eingerichteten Netzwerkverzeichnis Zugang. Auf diesen Verzeichnissen werden Daten nur so lange gespeichert, wie sie für den unmittelbaren Produktionsprozess benötigt werden. Die Programmnutzung wird ebenso protokolliert, wie das Abrufen von Daten aus Beständen über Selektionen. Das Booten des Servers ist nur über eine Passworteingabe möglich. Datenträger werden verschlossen gelagert.

Trennungsgebot
Durch die Trennung der Aufträge voneinander, die sowohl in getrennten Auftragsmappen als auch in voneinander getrennten Netzwerkverzeichnissen erfolgt, ist gewährleistet, dass zu unterschiedlichen Zwecken erhobene Adressdaten getrennt verarbeitet werden.

Pseudonymisierung und Verschlüsselung
Als Dienstleister für Direktwerbung sind die meisten unserer Datenverarbeitungsvorgänge pseudonymisiert nicht möglich. Dort wo es möglich, sinnvoll und verhältnismäßig ist, werden Daten aber verschlüsselt vorgehalten.

INTEGRITÄT

Weitergabekontrolle
Sofern die Übermittlung von personenbezogenen Daten notwendig sein sollte, erfolgt der Datenaustausch über unseren Datenaustausch-Server (DataStore). Zur Nutzung des DataStore ist eine vorherige Registrierung erforderlich. Für den einzelnen Abruf wird zusätzlich ein eindeutiges Passwort benötigt, das lediglich dem autorisierten Nutzer, mittels eines anderen Mediums, bekannt gegeben wird. Der Versand personenbezogener Daten erfolgt ausschließlich im gesetzlich vorgesehenen Rahmen. Der Datenaustausch erfolgt verschlüsselt. Die Übertragungswege sind passwortgeschützt.

Dokumente mit Personenbezug werden in verschlossenen Containern eines spezialisierten und zertifizierten Unternehmens für Daten- und Aktenvernichtung gesammelt und von diesem anschließend datenschutzgerecht vernichtet. Die Vernichtung wird protokolliert. Das gilt auch für Makulatur im Lettershop (personalisierte Werbebriefe und Kataloge). Neben der Dokumente-Entsorgung übernimmt der beauftragte Dienstleister auch die Vernichtung von Datenbändern. CDs und DVDs werden geschreddert.

Eingabekontrolle
Das verwendete EDV-System verfügt über eine automatische Protokollierung der User-Aktivitäten. Darüber hinaus wird bei den Aufträgen in schriftlicher Form dokumentiert, dass und von wem Adressdaten auf unseren Servern wohin gespeichert wurden. Veränderungen an Adressdaten (Dubletten entfernen, Adressen qualifizieren) werden durch das Abspeichern unterschiedlicher Fertigungsstufen dokumentiert.

VERFÜGBAR- UND BELASTBARKEIT

Verfügbarkeitskontrolle / Wiederherstellbarkeit

Unsere EDV-Systeme sind durch RAID-Systeme vor Datenverlust geschützt. USV-Systeme, Virenschutz und Firewall sowie tägliche Datensicherungen garantieren, dass bei Verlust der Funktionsfähigkeit von EDV-Systemen keine Daten verloren gehen. Für den Fall von Feuer oder anderen EDV-System schädigenden Ereignissen ist die Datensicherung auch außerhalb des Serverraumes brandsicher gelagert. Um das Ausmaß möglicher Brandschäden zu minimieren, ist unser Unternehmen mit einer Brandmeldeanlage ausgestattet. Meldungen der Anlage werden durch einen Sicherheitsdienst überwacht und nach einem dokumentierten Interventionsplan verfolgt.

VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG

Auftragskontrolle

Weisungen des Auftraggebers werden schriftlich dokumentiert. Aufträge werden über eine eigene Software verwaltet und dokumentiert. Organisatorisch ist geregelt, dass Aufträge nach dem 4-Augen-Prinzip kontrolliert werden. Es finden Nachkontrollen statt.

Trebbau hat gegenüber Adresseignern die Verpflichtungserklärung des Deutschen Dialogmarketing Verbandes e.V. (DDV) unterschrieben und sie zur Veröffentlichung dem Verband überlassen.

Sofern sonstige Dienstleister bzw. Unterauftragsnehmer von Trebbau beauftragt werden und die Beauftragung den Umgang mit personenbezogenen Daten erforderlich macht, legt das beauftragte Unternehmen eine unterzeichnete Datenschutzverpflichtungserklärung nach DDV-Standard vor. Sofern die Erteilung solcher Auftragsverhältnisse die Zustimmung eines Dritten erfordert, wird Trebbau diese Zustimmung über den Auftraggeber einholen.

Schulungen und Verpflichtungen der Mitarbeiter

Sämtliche Mitarbeiterinnen und Mitarbeiter sind mit dem Arbeitsvertrag zur Vertraulichkeit und zur Meldung von Verletzungen des Schutzes personenbezogener Daten verpflichtet. Sie werden in jährlichen Schulungen auf ihre Verpflichtungen zur Wahrung des Datengeheimnisses hingewiesen und bezeugen dies durch ihre Unterschrift. Ihnen wird das Merkblatt "Datenschutz" ausgehändigt. Die Unterweisung erfolgt zu den Grundsätzen des Datenschutzes (insbesondere die Voraussetzungen der Auftragsverarbeitung), dem Einsatz der Robinsonliste, der Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse, dem sorgfältigen Umgang mit Datenträgern und Dateien, dem Fernmeldegeheimnis und den Qualitäts- und Leistungsstandards des DDV (QuLS + SVE).

Richtlinien zur Umsetzung des Datenschutzes sind zentral erfasst, von der Geschäftsführung verabschiedet und den Mitarbeitern zugänglich im Trebbau Datenschutz-Handbuch.

Datenschutzbeauftragter

Ein externer Datenschutzbeauftragter ist vom Unternehmen bestellt worden.

Kontrolle der getroffenen Maßnahmen zum Datenschutz

Halbjährlich finden Meetings des Trebbau-Datenschutz-Teams statt. Dabei werden die laufenden Verarbeitungen und die zum Schutz der Daten getroffenen Maßnahmen kontrolliert und auf Verbesserungspotenzial überprüft.

Siegel Qualitäts- und Leistungsstandards (QuLS) des Deutschen Dialogmarketing Verbandes e.V. (DDV) / Lettershop, Datenverarbeitung und Listbroking

Trebbau gibt gegenüber dem DDV jährlich eine Selbstverpflichtungserklärung (SVE) ab. In mehr als 70 Punkten und Unterpunkten werden dort die Maßnahmen, die das Unternehmen getroffen hat, um den Bestimmungen der Gesetze zu entsprechen, überprüft. In der SVE erklärt Trebbau darüber hinaus die getroffenen Maßnahmen, um die über die Gesetze hinaus gehenden Verpflichtungen des DDV-Qualitäts- und Leistungssiegels darzulegen.

Die Einhaltung der in der SVE abgegebenen Verpflichtung wird von unabhängigen Gutachtern überwacht. Als Zeichen der besonderen Güte der von Trebbau erbrachten Leistungen verlieh uns der DDV das DDV-Qualitäts- und Leistungssiegel (QuLS) 2022/2023.

Stand: Dezember 2022