Direktwerbeversand GmbH
Siemensstr. 3
91161 Hilpoltstein

Übersicht der technischen und organisatorischen Maßnahmen nach § Art. 32 DS-GVO

Welche technische und organisatorische Maßnahmen sind im Einzelfall getroffen worden um:

Unbefugten den Zutritt zu solchen Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden, (1. Zutrittskontrolle):

- Ausschließlich zutrittsberechtigte Personen können in das Firmengebäude gelangen.
- Alle Personalzugangstüren können von außen nur mit Schlüssel geöffnet werden. Mitarbeiter werden bei Arbeitsbeginn von einem berechtigten Mitarbeiter über die Eingangstür eingelassen.
- Besucher und Betriebsfremde können nur über einen „Besuchereingang“ ins Gebäude gelangen. Die Tür wird nach läuten der Klingel von einem Mitarbeiter geöffnet und steht ansonsten, wie alle weiteren Türen unter Verschluss.
- Regelungen für Besucher, Lieferanten und Wartungspersonal sind vorhanden (Die Registrierung aller externen Personen erfolgt auf Besucherscheinen).
- Der Serverraum ist mit einem Sicherheitsschloss versehen. Nur autorisierte Mitarbeiter haben Zugang. Ein Ersatzschlüssel ist im Firmensafe deponiert.
- Alle Türen und Fenster werden nach Arbeitsende verschlossen. Eine Überprüfung des Verschlusses von Fenster und Türen wird durch autorisiertes Personal vorgenommen.
- Fremdkräfte (z.B. Wartungspersonal) sind nur mit Genehmigung zum Serverraum zugangsberechtigt. Und müssen sich grundsätzlich in Begleitung befinden.

zu verhindern, dass die Datenverarbeitungssysteme von Unbefugten genutzt werden können, (2. Zugangskontrolle)

- Der Zugang zu Datenverarbeitungsanlagen im Bereich der EDV ist nur berechtigten Mitarbeitern gestattet.

- Die Zugangsberechtigungen sind im System hinterlegt. Die Vergabe erfolgt durch die Systemadministration. Für die Vergabe von Berechtigungen an Mitarbeiter ist die Geschäftsleitung zuständig. Diese erfolgt mittels schriftlicher Anweisung und Zuweisung in der Active Directory.

- Die Passwörter sind mind. 8 stellig und beinhalten wenigsten je ein Sonderzeichen, eine Zahl und Groß/Kleinschreibung. Die Passwörter müssen nach 60 Tagen vom User geändert werden. Passwörter werden vom Anwender selbst vergeben. Voraussetzung dazu ist die einmalig anzuwendende einheitliche Einstiegsprozedur für neue Mitarbeiter. Nach drei fehlgeschlagenen Anmeldeversuchen wird das Konto gesperrt. Genaueres wird in den IT/Passwörter Richtlinien beschrieben.

- Nur Netzwerkdosen die zurzeit verwendet werden sind im Netzwerkverteiler gepatcht. Alle 3 Monate wird dies kontrolliert.

- Das Netzwerk befindet sich hinter einer Firewall. Genaueres wird in den IT/Firewall Richtlinien beschrieben.

- Auf allen Clients und Servern ist ein Virenscanner installiert. Genaueres wird in den IT Richtlinien beschrieben.

- Die Bildschirmarbeitsplätze sind durch kennwortgesicherte Bildschirmschoner geschützt. Diese werden nach Untätigkeit aktiviert.

- Das Passwort ist geheim zu halten (Datengeheimnis). Jeder Mitarbeiter wird mit Beginn seiner Tätigkeit bei der Direktwerbeversand GmbH per Verpflichtungserklärung auf das Daten-, Fernmelde-, Privat-, Bank- und Geschäftsgeheimnisses verpflichtet.

zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegende Daten zugreifen können, (3. Zugriffskontrolle)

- Benutzer können Daten nur speichern oder auf gespeicherte Daten zugreifen, sofern sie dafür über das Active Directory berechtigt sind.

- Zur Anmeldung / Identifizierung am System muss der Benutzer seinen Anmeldenamen und sein persönliches Passwort vorgeben. Im Active Directory sind die Zugriffsberechtigungen hinterlegt.

- Nach 3 Fehleingaben beim Login wird das User-Konto gesperrt.

- Es erfolgt eine datenschutzgerechte Entsorgung nicht mehr benötigter bzw. verwendeter Datenträger. Die Entsorgung wird dokumentiert.

zu gewährleisten, dass Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (4.Weitergabekontrolle):

- Die Datenübertragung erfolgt per Internet (SFTP, FTP) oder per Datenträger (CD ROM oder

DVD). Falls Daten in einem physischen Datenträger angeliefert werden, wird der Datenträger sofort nach Erhalt in den Safe gesperrt. Vor der Verwendung werden die Datenträger auf Viren überprüft.

- Eine Datenverschlüsselung nach aktuellen Kryptographischen Standard bei der Übertragung ist möglich falls nur ein nicht gesicherter Übertragungsweg möglich ist.

- Alle Datenübertragungen werden protokolliert. Bei Dateneingang werden diese auf Vollständigkeit und Richtigkeit überprüft.

- Datenträger werden nur an autorisierte Personen mit Begleitpapieren ausgegeben. Die Lagerung erfolgt im Tresor. Die Datenträgervernichtung erfolgt kontrolliert vor Ort im 4 Augenprinzip. Die Vernichtung wird dokumentiert.

- Unserer Systemadministration unterliegen verantwortlich auch alle Arbeiten in Bezug auf datenschutzgerechte Einrichtung, Pflege und Kündigung von Datenleitungen und -einrichtungen.

- Die Art der Weitergabe von Daten richtet sich nach der Klassifizierung der Daten und deren Schutzbedarf.

zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (5.Eingabekontrolle)

- Nur Mitarbeiter des Auftragsmanagements dürfen Daten bearbeiten. Änderungen in den Adressbeständen von Kundenaufträgen dürfen nur nach schriftlicher Anweisung des Kunden getätigt werden. Diese Anweisungen werden im Auftragsordner dokumentiert.

- Für die Produktion werden die Adressdaten auf einem verschlüsselten USB Stick kopiert. Der Schichtführer übernimmt den Stick mit einem Datenträgerlaufzettel und spielt diese Datei auf sein System ein. Die Daten werden nach dem Kopieren vom Schichtführer auf dem Stick gelöscht. Nach Produktionsende löscht der Schichtführer noch die Datei auf dem Produktionssystem. Alle Vorgänge werden auf den Datenträgerlaufzettel dokumentiert den der Schichtführer nach Produktionsende ausgefüllt ans Auftragsmanagement zurück gibt.

Der USB-Stick ist nach FIPS 140-2, Stufe 2, zertifiziert und auf Hardware-Ebene mit CBC-AES mit einer Tiefe von 256-Bit verschlüsselt. Im Gegensatz zur Authentisierung und Verschlüsselung mit Software erfolgt die Hardwareverschlüsselung direkt auf dem USB-Stick, ohne dass Informationen darüber an den Computer weitergegeben werden. Für zusätzliche Sicherheit sorgen ein komplexes Kennwort(mindestens 8 Zeichen, Zahlen, Sonderzeichen und Groß/Kleinschreibung) und die Sperrung des Flashspeichers nach einer konfigurierbaren Anzahl fehlgeschlagener Anmeldeversuche. Das Kennwort wird alle 3 Monate geändert. Das Kennwort ist nur autorisiertem Personal bekannt.

- Alle Daten werden mit einem Tool „durch mehrfaches Überschreiben“ gelöscht, damit keine Wiederherstellung der Daten möglich ist.

zu gewährleisten, dass Daten, die im Auftrag verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet oder genutzt werden können (6. Auftragskontrolle)

- Verträge und Auftragsbestätigungen liegen schriftlich vor und beinhalten alle Aufgaben und Pflichten von Auftraggeber und Auftragnehmer.

- Aus den Angebots-/Vertragsunterlagen wird über die Bestellung des Kunden durch das Auftragsmanagement der Auftrag angelegt. Darin enthalten sind alle am Prozess beteiligten, auftragsbezogenen Materialien und Arbeitsschritte.

- Für die einbezogenen Abteilungen gibt es detaillierte Auftragsunterlagen, nach denen sich die Produktion richten muss, z. B. Betriebsauftrag, Musterstandsvorgaben, Layouts

- Spezielle Anforderungen des Kunden werden mit den am Produktionsprozess beteiligten Mitarbeitern besprochen.

- Besteht die Notwendigkeit, so werden spezielle Arbeits-, Verfahrens- und Prüfanweisungen erstellt.

- Im Rahmen des QM-Systems werden die Arbeitsergebnisse regelmäßig durch Qualitätsaufzeichnungen der Produktion und Stichproben des Auftragsmanagements überprüft.

- Es existiert ein dokumentiertes Verfahren zur Lieferantenauswahl und Bewertung.

- Makulatur wird in einem gesicherteren Behälter gesammelt und von einem zertifizierten Entsorger abgeholt und sicher vernichtet.

- Die Auftragsdaten werden nach 90 Tagen, falls vom Kunden nicht anderes gewünscht, gelöscht. Gesetzliche Vorgaben werden eingehalten.

- Ein Datenschutzbeauftragter ist bestellt.

- Subdienstleister werden zur Einhaltung der DS-GVO verpflichtet.

zu gewährleisten, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind (7. Verfügungskontrolle)

- Durch den Einsatz redundant ausgelegten DV-Systemen wie z.B. mit Plattenspiegelung(Raid 1 + Raid5) in einer gesicherten IT-Umgebung sowie einer täglichen Datensicherung kann ein Verlust der Daten auf ein Restrisiko minimiert werden. Regelmäßige Recoverytests werden durchgeführt.
  Genaueres wird in den IT-Richtlinien beschrieben.

- Ein Notfallkonzept befindet sich in den IT/Backup Richtlinien.

- Es ist ein firmenweiter Virenschutz im Einsatz, der das Einschleusen von „bösartiger" Software verhindert.

- Server und Kernkomponenten der DV sind an USV angeschlossen.

- Test und Entwicklungsumgebungen sind strikt getrennt. Es werden keine Kundendaten in der Entwicklungsumgebung verwendet.

zu gewährleisten, dass zu unterschiedlichen Zwecken Daten getrennt verarbeitet werden können, (8.Trennungsgebot.)

- Es existiert eine differenzierte Datenverwaltung (Kunde; Auftragsnummer) um zu gewährleisten dass die Daten auch sauber getrennt gehalten werden und damit keine Möglichkeit der Verwechselung, Vermischung oder zufälligen Löschung durch die Adressbearbeiter oder Programmierer besteht.
- Durch interne Auftragsnummern

- Über die Vergabe von Berechtigungen an bestimmte Mitarbeiter wird sichergestellt, dass ausschließlich autorisierte Mitarbeiter durch Trennung über Berechtigungen auch Zugriff auf diese Daten haben.

- Die temporäre Speicherung der Verarbeitungsdateien erfolgt in einer logischen Trennung. Verarbeitete Dateien werden entsprechend der Vorgaben des Auftraggebers gelöscht. Eine dauerhafte Datenhaltung am Standort erfolgt nicht.