Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (vgl. auch § 3 Abs. 2 der Vereinbarung zur Auftragsverarbeitung)

Inhaltsverzeichnis

1. Datenschutz-Management

a) Datenschutzbeauftragter

André Schoppe

Anschrift: Am Busbahnhof 1
24784 Westerrönfeld

Telefon: 04331 33323-11
Fax: 04331 33323-30
Email: as@mailwork.de

b) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Zur Einhaltung datenschutzrechtlicher Grundanforderungen gibt es eine Arbeitsanweisung zu Datenschutz und Datensicherheit.

Die Richtlinien werden regelmäßig in Hinblick auf ihre Wirksamkeit evaluiert und angepasst.

Der Datenschutzbeauftragte informiert alle Mitarbeiter in regelmäßigen Abständen über Datenschutzhinweise und führt Schulungen in Datenschutzangelegenheiten durch.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem Datenschutzbeauftragten gemeldet werden. Dieser wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.

c) Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Vor dem Einsatz neuer Software und Implementierung neuer Prozesse wird durch die frühzeitige Einbindung des Datenschutzbeauftragten Sorge dafür getragen, dass dem Grundsatz der Datenvermeidung und Datensparsamkeit gemäß Art. 25 Abs 2 DS-GVO entsprochen wird.

2. Zutrittskontrolle

Unsere Büroräume und Verarbeitungsanlagen befinden sich in einem Gebäudekomplex in Westerrönfeld.

Die Zugänge zum Gebäude und auch zu den Büroräumen von mailwork sind außerhalb der Geschäftszeiten verschlossen. Es kommt ein Schließsystem zum Einsatz, das von der Geschäftsführung von mailwork verwaltet wird.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Der Empfang kann die Eingangstür einsehen und regelt die Zutrittsberechtigung für Besucher. Jeder Besucher wird von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet.

Die Türen und Tore der Warenannahme/-ausgabe sind auch während der Geschäftszeiten immer verschlossen. Besucher (i.d.R. Mitarbeiter der Deutschen Post, Lieferanten und Spediteure) erhalten dort erst nach Tür-/Toröffnung durch einen Mitarbeiter Zutritt zu den Lagerräumen.

Besucher dürfen sich nicht ohne Begleitung in den Büro- und Lagerräumen frei bewegen. Fremde Techniker werden während der Arbeit begleitet.

Der Haupteingang des Gebäudes ist mit einer Alarmanlage gesichert. Diese wird manuell aktiviert, sobald alle Personen das Gebäude verlassen haben.

3. Zugangskontrolle

Für die Zugangskontrolle sind nachfolgende Maßnahmen von mailwork getroffen worden:

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen vom Administrator vergeben, sofern die Vergabe vom Geschäftsführer beantragt wurde.

Der Benutzer erhält einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort aus einer Kombination aus Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen (3 aus 4 Kriterien) bestehen muss.

Passwörter werden alle 90 Tage gewechselt.

Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Remote-Zugriffe auf IT-Systeme von mailwork erfolgen stets über verschlüsselte Verbindungen.

Das gesamte Netzwerk ist durch eine Firewall mit Intrusion-Prevention-System geschützt. Alle Server- und Client-Systeme verfügen über Firewall und Virenschutzsoftware, bei denen eine tagesaktuelle Versorgung mit Signaturupdates und Sicherheitspatches gewährleistet ist.

Sicherheitsvorfälle werden protokolliert und für 90 Tage aufbewahrt.

Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter werden grundsätzlich verschlüsselt gespeichert.

4. Zugriffskontrolle

Definierte Zugriffsberechtigungen schützen die Eingabe und Ausgabe der Daten. Die Vergabe von Berechtigungen erfolgt ausschließlich vom Administrator, sofern dies von der Geschäftsführung beantragt wurde.

Berechtigungen werden grundsätzlich restriktiv nach dem Need-to-know-Prinzip vergeben. Es erhalten nur die Personen Zugriff, die mit der auftragsgemäßen Datenverarbeitung betraut sind.

Die Vernichtung sensibler Papier-Datenträger erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet. Elektronische Datenträger werden durch den jeweiligen IT-Dienstleister im Haus durch physische Zerstörung vernichtet.

Alle Mitarbeiter von mailwork sind angewiesen, Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsbehältnisse einzuwerfen.

Beschäftigten ist es grundsätzlich untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren.

Daten werden zeitnah nach Auftragsende physikalisch gelöscht (soweit keine anders lautenden Vorgaben des Auftraggebers vorliegen).

Die Speicherung personenbezogender Daten auf externen Datenträgern ist - bis auf die externe Datensicherung - untersagt.

5. Trennungskontrolle

Alle Daten liegen in getrennten Ordnerstrukturen. Die Daten sind gekennzeichnet mit einem individuellen Kundenzeichen und darunter wiederum nach Auftrags- bzw. Rahmenauftragsbezeichnung abgelegt.

Für die Dauer der Verarbeitung (bspw. Adressierung) werden die personenbezogenen Daten den Maschinenführern an den jeweiligen Verarbeitungsmaschinen zur Verfügung gestellt. Zu jedem Auftrag bzw. Rahmenauftrag wird dem Maschinenführer ein pseudonymisiertes Datenblatt zur Verfügung gestellt, dass die eindeutige Zuordnung von Auftrag bzw. Rahmenauftrag zu den dazugehörigen Daten sicherstellt.

Die analogen Unterlagen werden in Auftragsmappen abgelegt.

6. Pseudonymisierung und Verschlüsselung

Eine Pseudonymisierung der personenbezogenen Adressdaten ist in Anbetracht der Verarbeitungszwecke (Adressierung) nicht möglich, da die Angaben für die postalische Zustellung der Sendungen erforderlich sind.

Die Datenübertragung ist von unserer Seite immer verschlüsselt.

7. Eingabekontrolle

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

An den Verarbeitungsmaschinen nutzen die Maschinenführer sog. Dienstkonten zur Anmeldung an den Maschinen und Verarbeitung der Daten. Eine Veränderung der Daten ist an den Maschinen nicht möglich. Sofern eine Korrektur erforderlich ist, erfolgt diese durch die Sachbearbeiter. Der jeweilige Maschinenführer protokolliert schriftlich, dass er die Einrichtung der Verarbeitungsanlage nach den Vorgabe des Auftrags bzw. Rahmenauftrags korrekt durchgeführt hat.

Die endgültige Druck- und Adressierfreigabe erfolgt wiederum durch die Sachbearbeiter, sodass das 4-Augen-Prinzip eingehalten wird.

8. Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Die Weitergabe von Daten in physikalischer Form soll dabei möglichst vermieden werden. Falls dies doch notwendig ist, werden die verschlüsselten Datenträger nach Absprache persönlich geliefert (kein Transportunternehmen).

Alle Datenverbindungen sind verschlüsselt. Die Zugänge erfolgen entweder über VPN, HTTPS oder FTPS (TLS-Verschlüsselung).

Die Nutzung von privaten Datenträgern ist den Mitarbeitern bei mailwork untersagt.

9. Verfügbarkeitskontrolle

Daten auf Serversystemen werden ausschließlich auf Festplatten im RAID-Verbund gespeichert und mindestens einmal wöchentlich auf separaten Datenträger gesichert.

Die Sicherungsmedien werden an einen physisch getrennten Ort verbracht. Das Einspielen von Backups wird regelmäßig getestet.

Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

10. Auftragskontrolle

Die Vereinbarung zur Auftragsverarbeitung regelt die Rechte und Pflichten des Auftragnehmers und Auftraggebers. Zudem gibt es eine interne Arbeitsanweisung zur Einhaltung datenschutzrechtlicher Anforderungen.

Konkrete Weisungen zur Datenverarbeitung werden wiederum im jeweiligen Auftrag bzw. Rahmenauftrag mit dem Auftraggeber vereinbart.

Der Auftrag bzw. Rahmenauftrag wird einem zuständigen Sachbearbeiter und einem Maschinenführer zugewiesen. Im Laufe der Auftragsverarbeitung werden mehrere Kontrollen durch unterschiedliche Mitarbeiter durchgeführt, um die korrekte und auftragsgemäße Verarbeitung sicherzustellen.

Der Datenschutzbeauftragte informiert alle Mitarbeiter in regelmäßigen Abständen über Datenschutzhinweise und führt Schulungen in Datenschutzangelegenheiten durch.

Alle Mitarbeiter sind zur Verschwiegenheit und Einhaltung der datenschutzrechtlichen Anforderungen nach der DS-GVO verpflichtet.

Nr.	Dokumententitel	
202	Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO	
Version	**Zuletzt aktualisiert am**	**Gültig ab**
V02	19.07.2018	19.07.2018
Kategorie	**Empfänger**	**Autor**
Datenschutz	Kunden, Interessenten, Mitarbeiter	André Schoppe