Anlage 3 (Technische und organisatorische Maßnahmen, einschließlich zur Gewährleistung der Sicherheit der Daten)

Darstellung der Datensicherheitsmaßnahmen iSd Art 32 DSGVO

1. Pseudonymisierung von Daten

Das Unternehmen stellt sicher, dass - soweit die technischen Abläufe dies zulassen - bei personenbezogenen Daten wesentliche Identifizierungsmerkmale durch einen Schlüssel ersetzt werden (Pseudonymisierung).

Soweit zusätzlich zu den übermittelten Daten eigene Dokumente durch das Unternehmen erstellt werden (z. B. tabellarische Übersichten über abgewickelte Bestellungen), sind dort die Namen der Endkunden nicht angegeben. Es werden ausschließlich andere Zuordnungsdaten wie beispielsweise Bestellnummer oder Kunden-ID verwendet.

2. Verschlüsselung personenbezogener Daten

Das Unternehmen gewährleistet, dass personenbezogene Daten nur gesichert gespeichert werden, indem eine angemessene Verschlüsselung erfolgt.

Bei der Übertragung von Daten kommen besonders gesicherte Verbindungen zum Einsatz (beispielsweise VPN-Verbindung mit Passwortschutz).

3. Vertraulichkeit der Datenverarbeitung

3. 1 Zutrittskontrolle

Das Unternehmen trifft Maßnahmen um zu verhindern, dass unbefugte Personen Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden.

Das Gebäude ist durch angemessene Schutzmaßnahmen wie Sicherheitsschlösser, Sicherheitsverglasung und Alarmanlagen angemessen gesichert.

Die Computer, die zur Abwicklung der Bestellung genutzt werden, sind in abgeschlossenen Räumen.

Das eingesetzte Personal ist sorgfältig ausgewählt, eine Vergabe von Schlüsseln erfolgt nur an vertrauenswürdige Personen.

Es existiert eine Videoüberwachung zur Absicherung der Räume.

3.2 Zugangskontrolle

Das Unternehmen trifft Maßnahmen um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können.

Eine Nutzung der Computer ist nur mit entsprechenden Zugangsdaten (Benutzername und Passwort) möglich.

Auf den Computern ist eine aktuelle Software/Konfiguration zum Schutz der Applikationen vorhanden.

Die Zugangsdaten (siehe oben) sind nicht öffentlich bekannt und werden regelmäßig gewechselt.

3.3 Zugriffskontrolle

Das Unternehmen gewährleistet, dass die zur Benutzung von IT-Infrastruktur berechtigten Nutzer ausschließlich auf Inhalte zugreifen können für welche sie berechtigt sind und das personenbezogene Daten bei der Verarbeitung und Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

Es gibt nur eine beschränkte Anzahl von Mitarbeitern, die Zugang zu den Rechnern haben und auf die Daten für die Bestellabwicklung zugreifen können.

Eine Übertragung der Daten auf externe Speichermedien (USB-Stick, externe Festplatte, etc.) erfolgt nicht.

Fehldrucke und nicht mehr benötigte Ausdrucke mit Daten über Endkunden werden sicher vernichtet (Aktenvernichter).

3.4. Weitergabekontrolle

Das Unternehmen verhindert, dass personenbezogenen Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und das festgestellt werden kann an welchen Stellen eine Übermittlung solcher Daten im IT-System vorgesehen ist.

Eine Weitergabe von Daten außer der hierfür vorgesehenen Möglichkeiten erfolgt nicht.

Es gibt eine Anweisung, wonach Informationen mit Endkundendaten nicht über ungesicherte E-Mails versendet werden dürfen.

4. Integrität der Datenverarbeitung

4.1. Eingabekontrolle

Das Unternehmen stellt sicher, dass nachträglich überprüft werden kann ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.

Jeder Mitarbeiter verfügt über eigene Zugangsdaten.

Alle Mitarbeiter sind angewiesen, ausschließlich ihre eigenen Zugangsdaten zu verwenden, damit die Aktivitäten einem konkreten Nutzer zugeordnet werden können.

4.2. Auftragskontrolle

Das Unternehmen stellt sicher, dass personenbezogene Daten die im Auftrag verarbeitet werden, gemäß den Weisungen des Auftraggebers verarbeitet werden.

Alle Mitarbeiter sind auf das Datengeheimnis (§ 5 BDSG) verpflichtet. Alle Mitarbeiter, die mit Endkundendaten in Berührung kommen, kennen die wesentlichen datenschutzrechtlichen Regelungen.

5. Verfügbarkeit von personenbezogenen Daten

Der Auftragnehmer stellt sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.

Durch angemessene Maßnahmen ist sichergestellt, dass die eingesetzten Computer und die benötigte Datenverbindung durchgängig nutzbar sind (Brandschutz, Überspannungsschutz und/oder Klimaanlage).

Der PC ist so aufbewahrt, dass er nicht frei zugänglich ist oder leicht gestohlen werden kann (Diebstahlschutz).

6. Belastbarkeit der Systeme und Dienste

Der Auftragnehmer gewährleistet, dass seine Systeme und Dienste so ausgelegt sind, dass sie eine angemessene Datenverarbeitung ermöglichen.

Die eigene Infrastruktur des Unternehmens (PC und Datenanbindung) sind so dimensioniert, dass eine angemessene Arbeit möglich ist.

Es wird in regelmäßigen Abständen geprüft, inwieweit eine Erneuerung der Infrastruktur erforderlich ist.

7. Wiederherstellung von Daten

Der Auftragnehmer stellt sicher, dass für den Fall eines Datenverlustes der verlorenen Daten wiederbeschafft werden können.

Dem Unternehmen ist bekannt, wie Daten, die im eigenen Bereich verloren gehen, wieder beschafft werden können.

8. Überprüfung, Bewertung und Evaluation

8.1. Überprüfung der Maßnahmen

Die getroffenen Maßnahmen müssen regelmäßig auf einen Anpassungsbedarf geprüft werden.

In regelmäßigen Abständen wird überprüft, inwieweit die getroffenen Maßnahmen noch angemessen sind.

Mitarbeiter sind angehalten, bei Anhaltspunkten für Störungen, Bedrohungen oder mögliche Angriffe die notwendigen Maßnahmen zu ergreifen und Meldungen zu erstatten.

8.2. Bewertung und Evaluation der Maßnahmen

Das Ergebnis der Überprüfung (siehe oben) muss bewertet werden; über die bestehenden Maßnahmen hinaus sind etwaige Anpassungen zu bewerten und umzusetzen.

In regelmäßigen Abständen erfolgt eine Überprüfung, inwieweit Anpassungen erforderlich sind.

Das Unternehmen informiert sich ggf. (etwa über DFR) über relevante gesetzliche und technische Änderungen.

9. Zertifizierungen und Audits

Für den betroffenen Bereich der Verarbeitung personenbezogener Daten besteht keine gesetzliche Verpflichtung, die Systeme oder einzelne Maßnahmen zertifizieren oder auditieren zu lassen. Eine Zertifizierung bzw. ein externes Audit

auf freiwilliger Basis kann zur Überprüfung der eigenen Einschätzung des Unternehmens und zum Nachweis der Einhaltung angemessener Standards dienen.

Besondere Zertifizierungen, Audits oder Gütesiegel im Zusammenhang mit dem Auftrag sind nicht vorgesehen.

10. Unterweisung der unterstellten Mitarbeiter

Durch das Unternehmen ist sicherzustellen, dass alle Mitarbeiter, die mit der Datenverarbeitung befasst sind, über die bestehenden Verpflichtungen und die einzuhaltenden Maßnahmen informiert sind (Unterweisung).

Schriftliche Verpflichtung auf das Datengeheimnis für alle Mitarbeiter

Unterrichtung der Mitarbeiter über die datenschutzrechtlichen Bestimmungen (Gesetzes- bzw. Rechtstexte)

Schulung / Unterweisung aller Mitarbeiter vor Aufnahme ihrer Tätigkeit

Regelmäßige Wiederholung von Schulungen / Unterweisungen für Mitarbeiter