Anlage 3
Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

Vertraulichkeit

Zutrittskontrolle

(Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren.)

- Türen in sicherheitsrelevanten Bereichen sind stets geschlossen, so dass sich kein Unbefugter Zutritt verschaffen kann.
- Betriebsfremde erhalten ausschließlich Zugang, in dem sie sich am zentralen Empfang anmelden.
- Besucher werden von dem zuständigen Mitarbeiter persönlich am Empfang abgeholt.
- Festlegung der befugten Personen durch Schlüsselvergabe.
- Kontrolle der Schlüsselvergabe in einem Schlüsselbuch.
- Serverräume sind gesondert gegen Zutritt von Unbefugten geschützt.

Zugangskontrolle

(Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.)

- Prüfung der Zugangsberechtigung durch Authentifizierung (Benutzername und Passwort): persönliches Passwort (Zeichenmix, keine zusammenhängenden Worte).
- Mitarbeiter kann sich nur einmal anmelden.
- Die Passwortnutzung wird protokolliert.
- Hardware-Firewall und Virenscanner zum Schutz vor unbefugter Nutzung von außen.
- Beim Verlassen des Arbeitsplatzes ist der PC zu sperren (Bildschirmschoner).

Zugriffskontrolle

(Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten nach der Speicherung und bei der Verarbeitung, Nutzung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können)

- Die Zugriffsrechte der Mitarbeiter sind nach Rollen vergeben, differenziert nach Daten, Programmen und Zugriffsart.
- Der berechtigte Zugriff auf bestimmte Daten ist nur im Rahmen des jeweiligen Berechtigungskonzeptes möglich.
- Benutzerspezifische, abgestufte Rechteverwaltung auf Unterverzeichnis- und Dateiebene.
- Automatisches Log-off durch Bildschirmschoner mit Passwortschutz.
- Zugriffe von außen werden durch ein Virtual Private Network (VPN) abgesichert.

Trennung

(Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden können.)

- Nur befugte Personen haben Zugriff auf Layout & Kundendatenbanken.
- Die Trennung von Kundendaten findet in verschiedenen Ordnern auf den Serversystemen statt.
- Trennung von Test- und Produktionssystemen.

Integrität

Eingabekontrolle

(Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt werden.)

Dies geschieht in der Regel durch eine automatische Protokollierung der Eingaben in Logfiles. Elemente der Protokollierung sind:

- betroffener Datensatz
- Art der Aktivität (Anlage, Veränderung, Löschung des Datensatzes)
- Zeitpunkt der Aktivität bzw. des Ereignisses
- ausführende Person (Benutzerkennzeichen)

Weitergabekontrolle

(Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.)

- Daten werden nur innerhalb des dem Auftrag entsprechenden Produktionssystems weitergegeben.
- Der Versand von Datenträgern erfolgt nach Vorgabe durch den Auftraggeber, in der Regel per „Einschreiben mit Rückschein“.

- Der Einsatz von privaten Datenträgern ist durch entsprechende Mitarbeiterregelungen untersagt.
- Die Vernichtung von Datenträgern erfolgt durch zertifizierte Unternehmen.
- Die Übertragung von Daten im Internet erfolgt auftragsbezogen über gesicherte VPN-Verbindung, per FTP Down- oder Upload (nur an berechtigte User), per verschlüsselter E-Mail (wenn möglich) oder über verschlüsselte Zipp-Container.

Verfügbarkeit und Belastbarkeit

(Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.)

- Redundante Serversysteme mit Raid-Festplatten.
- Tägliches Backup.
- Verwendung von geeigneten Tresoren.
- Unterbrechungsfreie Stromversorgung der Server.
- Klimaanlagen und Brandmeldeanlagen in den Serverräumen.
- Virenschutz und Hardware-Firewall.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Regelmäßige Schulungen der Beschäftigten zum Datenschutz.
- Verpflichtung der Beschäftigten zum vertraulichen Umgang mit personenbezogenen Daten.
- Bestellung eines Datenschutzbeauftragten.
- Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten.
- Regelmäßige Kontrollen um die Umsetzung der Vorgaben der DSGVO im Unternehmen zu gewährleisten.