Gemäß AVV-Vertrag technische und organisatorische Maßnahmen (TOM) zur Datensicherheit (Stand 28.05.2019)

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind:

1. **Vertraulichkeit**
   Es soll verhindert werden, dass es zu einer unbefugten oder unrechtmäßigen Verarbeitung der Daten kommt.

- Zutrittskontrolle
  Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, verwehrt wird:
  - Regelung für die Vergabe von Zutrittsberechtigungen
  - Elektronisches Zugangskontrollsystem
  - Einbruchmeldeanlage mit Aufschaltung auf Sicherheitsunternehmen
  - Videoüberwachung von Eingängen und Serverräumen
  - Für die Mitarbeiter gelten abgestufte Zutrittsregelungen
  - Besucher dürfen nur in Begleitung von berechtigten Mitarbeitern die Sicherheits-bereiche betreten
  - Wartungstechniker arbeiten grundsätzlich unter Aufsicht
  - Die Reinigung der Sicherheitsbereiche erfolgt unter Aufsicht

- Zugangskontrolle
  Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:
  - Userbezogene Passwortvergabe
  - Vorgaben zur Passwortgestaltung (Mindestens 8 Zeichen, Kombination aus Buchstaben und Sonderzeichen, Groß-/Kleinschreibung und Ziffern)
  - Externer Zugang für Mitarbeiter nur über gesicherte und verschlüsselte VPN-Anbindungen
  - Regelmäßiger Passwortwechsel
  - Identifikation und Authentifikation von Benutzern

- Zugriffskontrolle
  Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:
  - Vernichtung von Fehldrucken in hauseigener Industrieschredderanlage und Vvernichtung von elektronischen Datenträgern sowie Entsorgung von geschreddertem Papier durch zertifizierte Unternehmen (vertragliche Regelung, Entsorgungsbescheinigung)
  - Funktionelle userbezogene Zuordnung
  - Getrennte Benutzerkonten für Administratortätigkeit und Sachbearbeitung
  - Hinterlegte Notfallpassworte
  - Test- oder Entwicklungsumgebung
  - Protokollierung der Systemnutzung

- Trennungsgebot
  Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Datenübertragung durch den Auftraggeber in dedizierte Ordner
- Verarbeitung in Auftraggeber bezogenen Ordnern

- Pseudonymisierung
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechend technischen und organisatorischen Maßnahmen unterliegen:
  - Eine Pseudonymisierung der Daten muss vom Auftraggeber selbst durchgeführt werden, da nur der Eigentümer der Daten diese in geeigneter Form verändert darf. Nur mit der Zustimmung und Beauftragung des Eigentümers kann der Auftragnehmer die Pseudonymisierung übernehmen (kostenpflichtig)

2. Integrität

Es soll verhindert werden, dass daten unbeabsichtigt geändert oder zerstört werden. Gewährleistung der Echtheit, Vollständigkeit und Zurechenbarkeit.

- 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:
  - Festgelegte Wege und Verfahren des Transports/der Übermittlung
  - Abgesicherter Transport/abgesicherte Übermittlung
  - Übergabeprotokolle/Empfangsbestätigungen
  - Prüfung auf Vollständigkeit
  - Identifizierung und Authentifizierung der Beteiligten
  - Protokollierung der Übertragung

- Eingabekontrolle
  Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind. Die inhaltliche Veränderung von Daten bzw. händische Dateneingaben in elektronische Systeme gehört nicht zur Serviceerbringung der Paragon CC Weingarten. In der erweiterten Begriffsbetrachtung gilt:
  - geregelte Zugriffsberechtigung
  - Aufbewahrungsfristen für Revision und Nachweiszwecke
  - Protokollierung der Datenaufbereitung

- Auftragskontrolle
  Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:
  - Durchführung von Aufträgen anhand von Arbeitsanweisungen und nach Terminplan
  - Dokumentation sämtlicher Aufträge
  - Eindeutige Regelung der Zuständigkeiten und Verantwortlichkeiten

3. Verfügbarkeit und Belastbarkeit

Um die Daten bzw. Datenverarbeitungssysteme verfügbar und belastbar zu halten, sind sie bestmöglich gegen innere und äußere Einflüsse zu schützen.

- Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimatisierung der Serverräume
- Virenschutz
- Firewalls
- Lizenzüberwachung
- Brandschutzeinrichtungen (Feuerlöscher, Rauch- oder Brandmelder), Rauchverbot
- Regelmäßige Sicherung der zur Verarbeitung der Daten erforderlichen Programme und Skripte
- Plan für zu ergreifende Sofortmaßnahmen bei einem Notfall

Der Auftragnehmer gewährt dem Auftraggeber auf dessen Wunsch die Einsicht in sein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsdatenverarbeitung.

Paragon Customer Communications
Weingarten GmbH
Josef-Bayer-Str. 5
88250 Weingarten

T +49 751 5695 0
F +49 751 5695 4402
E info@paragon-cc.de
www.paragon-cc.de

Handelsregister Ulm HRB 552722
USt.-Id-Nr. DE 176062543
Geschäftsführer Thomas Simon, Alexander Schäfer
Steuer-Nr.102/107/16691 | IBAN DE40650700840340445600 | SWIFT DEUTDESS650