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:
  - Entsorgung/Vernichtung von Fehldrucken und Datenträgern durch ein zertifiziertes 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 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:
  - 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.

Technical and organisational measures (TOM) for data security in accordance with Data Processing contract (Version 28.05.2019)

The Processor undertakes towards the Customer to comply with the following technical and organisational measures necessary to satisfy the applicable data protection regulations:

1. **Privacy**
   The aim to prevent unauthorised or unlawful processing of the data.

- Physical access control
  Measures employed to prevent unauthorised persons from entering data processing sites in which personal data is processed and used:

  - Defined plan for the allocation of access authorisations
  - Electronic access control system
  - Intrusion detection system linked to security firm
  - Video surveillance of entrances and server rooms
  - Graded access rules for employees
  - Visitors may only enter security restricted areas if accompanied by authorised employees
  - Maintenance technicians operate under supervision in principle
  - Cleaning of the security restricted areas is performed under supervision

- Logical access control
  Measures that prevent the unauthorized use of the data processing systems:

  - User-based password allocation
  - Guidelines for creating passwords (at least 8 characters, combination of letters and special characters, case sensitive and digits)
  - External access for employees via secured, encrypted VPN connections only
  - Regular changing of passwords
  - Identification and authentication of users

- Data access control
  Measures that ensure that individuals entitled to use the data processing systems can solely access data that they are entitled to access in accordance with their rights of access, and that during the course of processing, use and after storage, personal data cannot be read, copied, modified or deleted without authorisation:

  - Disposal/destruction of misprints and data storage media by a certified firm (contractual framework of rules, certificate of disposal)
  - Functional user-based assignment
  - Split user accounts for administrator activities and operative tasks
  - Stored contingency password
  - Test or development environment
  - System use logging

- Separation rule
  Measures to ensure that data collected for different purposes are processed separately:

  - Data transfer by the client into dedicated folders
  - Processing in customer-related folders

- Pseudonymisation
  The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures:

  - A Pseudonymisation of the data must be carried out by the client himself, as only the true owner of the data may modify it in suitable form. Only with the consent of the owner can the contractor take over the Pseudonymisation (subject to a payment).

2. Integrity
The aim is to prevent data from being unintentionally changed or destroyed. Guarantee of authenticity, completeness and imputability.

- Transport control
  Measures that ensure that during electronic transmission, transport or storage on data carriers personal data cannot be read, copied, modified or deleted without authorisation, and that it can be established and verified to which entities a transfer of personal data by means of data transmission facilities is planned:

  - Defined channels and methods for transport/transmission
  - Secured transport/secured transmission
  - Transfer protocols/confirmations of receipt
  - Completeness check
  - Identification and authentication of the parties concerned
  - Transfer logging

- Input control
  Measures to ensure that it can be subsequently verified whether and by whom personal data have been entered, modified or removed in data processing systems:

  - Regulated access authorisation
  - Retention periods for internal audit and evidential purposes
  - Data preparation logging

- Job control
  Measures that ensure that personal data that are being processed on behalf of the Customer are processed solely in accordance with the Customer's instructions:

  - Execution of orders based on job specifications and determined schedule
  - Documentation of all orders
  - Unambiguous regulation of obligations and responsibilities

3. **Availability and resilience**
In order to keep data and data processing systems available and reliable, they must be optimally protected against internal and external influences.

- Availability / resilience control
Measures that ensure that personal data are protected against accidental destruction or loss:

    - Uninterrupted power supply (UPS)
    - Climate control of server rooms
    - Anti-virus protection
    - Firewalls
    - Licence monitoring
    - Fire safety systems (fire extinguishers, smoke and fire alarms), smoking ban
    - Regular backups of programmes and scripts necessary for processing the data
    - Emergency response plan

At the request of the Customer, the Contractor shall grant the Customer access to its comprehensive and up-to-date data protection and security concept for this order data processing.

Paragon Customer Communications GmbH
Mühlenstraße 57
41352 Korschenbroich

T +49 2161 6867 0
F +49 2161 6867 166
E info@paragon-cc.de
www.paragon-cc.de

Handelsregister Neuss Nr. B 18295
USt.-Id-Nr. DE 813 680 222
Geschäftsführer Thomas Simon, Philippe Coquelet
Steuer-Nr. 114 5842 5182 | IBAN DE34441600146467612200 | BIC GENODEM1DOR