TOM (Technisch Organisatorische Maßnahmen)

Zur Gewährleistung der Sicherheits- und Schutzanforderungen gem. §32 DSGVO

(Anlage zum Auftragsdatenverarbeitungsvertrag Abs. 3)

der

Schelwat e.K.
Triererstraße 33, 54634 Bitburg, DEUTSCHLAND

1. Vertraulichkeit

- **Zutrittskontrolle**
  - Datacenterparks
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Hochsicherheitszaun um den gesamten Datacenterpark
    - dokumentierte Schlüsselvergabe an Mitarbeiter
    - Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
    - 24/7 personelle Besetzung der Rechenzentren
    - Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen
    - Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Datacenterpark-Mitarbeiters
  - Verwaltung
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Videoüberwachung an den Ein- und Ausgängen
- **Zugangskontrolle**
  - bei Hauptauftrag "Root Server"
    - Server-Passwörter, welche nur vom Auftraggeber nach erstmaliger Inbetriebnahme von ihm selbst geändert werden und dem Auftragnehmer nicht bekannt sind
    - Das Passwort zur Administrationsoberfläche wird vom Auftraggeber selbst vergeben - die Passwörter müssen vordefinierte Richtlinien erfüllen. Zusätzlich steht dem Auftraggeber dort eine Zwei-Faktor-Authentifizierung zur weiteren Absicherung seines Accounts zur Verfügung.
  - bei Hauptauftrag "Managed Server" und "Webhosting"
    - Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter des Auftragnehmers; verwendete Passwörter müssen Mindestlänge haben und werden in regelmäßigen Abständen erneuert
- **Zugriffskontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
    - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers

- bei Hauptauftrag "Root Server"
    - Die Verantwortung der Zugriffskontrolle obliegt dem Auftraggeber.
- bei Hauptauftrag "Managed Server" und "Webhosting"
    - Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.
    - Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Auftragnehmers
    - Für übertragene Daten/Software ist einzig der Auftragnehmer in Bezug auf Sicherheit und Updates zuständig.

- **Datenträgerkontrolle**
    - Datacenterpark in Nürnberg, Regensburg und Bitburg
        - Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt.
    - Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt vor Ort zerstört (geschreddert).
- **Trennungskontrolle**
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
        - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
    - bei Hauptauftrag "Root Server"
        - Die Trennungskontrolle obliegt dem Auftraggeber.
    - bei Hauptauftrag "Managed Server" und "Webhosting"
        - Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
        - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.
- **Pseudonymisierung**
    - Für die Pseudonymisierung ist der Auftraggeber verantwortlich

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**
    - Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
    - Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
    - Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.

- **Eingabekontrolle**
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
        - Änderungen der Daten werden protokolliert.
    - bei Hauptauftrag "Root Server"
        - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
    - bei Hauptauftrag "Managed Server" und "Webhosting"
        - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.

- Änderungen der Daten werden protokolliert.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**
  - bei internen Verwaltungssystemen des Auftragnehmers
    - Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
    - Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).
    - Einsatz von Festplattenspiegelung bei allen relevanten Servern.
    - Monitoring aller relevanten Server.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Dauerhaft aktiver DDoS-Schutz.
  - bei Hauptauftrag "Root Server"
    - Datensicherung obliegt dem Auftraggeber.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Dauerhaft aktiver DDoS-Schutz.
  - bei Hauptauftrag "Managed Server" und "Webhosting"
    - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
    - Einsatz von Festplattenspiegelung.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Einsatz von Softwarefirewall und Portreglementierungen.
    - Dauerhaft aktiver DDoS-Schutz.
- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);**
  - Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Das Datenschutz-Managementsystem und das Informationssicherheits-managementsystem wurden zu einem DIMS (Datenschutz-Informationssicherheits-Management-System) vereint.
- Incident-Response-Management ist vorhanden.
- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DS-GVO).

- **Auftragskontrolle**
  - Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers.