FIRESTORM
WE HOST YOU.

Anlage 2 zum Auftrag gemäss Art. 28 DS-GVO: Technische und organisatorische Massnahmen nach Art. 32 DS-GVO und Anlage

1. Vertraulichkeit

Zutrittskontrolle

- **Rechenzentren**
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Hochsicherheitszaun um den gesamten Datacenterpark
    - dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation- Kunden für Colocation Racks (jeder Auftraggeber ausschliesslich für seinen Colocation Rack)
    - 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 FireStorm ISP GmbH Mitarbeiters
- **Verwaltung**
    - elektronisches Zutrittskontrollsystem mit Protokollierung
    - Videoüberwachung an den Ein- und Ausgängen
- **Zugangskontrolle**
    - bei Hauptauftrag „Rootserver“, „Serverhousing“
        - 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.

- bei Hauptauftrag „SiteDesigner“, „Webhosting“, „Mailhosting“, „Reseller-hosting“, „Managed Server“, „Domains“, „DNS Service“, „SMS Gate-way“, „SSL Zertifikat“ und alle anderen

  - Zugang ist passwortgeschützt, Zugriff besteht nur für berech-tigte Mitarbeiter vom Auftragnehmer; verwendete Passwörter müssen Mindestlänge haben

- **Zugriffskontrolle**

  - bei internen Verwaltungssystemen des Auftragnehmers

    - Durch regelmässige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass un-berechtigte Zugriffe verhindert werden.

    - Revisionssicheres, verbindliches Berechtigungsvergabever-fahren für Mitarbeiter des Auftragnehmers

  - bei Hauptauftrag „Rootserver“, „Serverhousing“

    - Die Verantwortung der Zugriffskontrolle obliegt dem Auftrag-geber.

  - bei Hauptauftrag „SiteDesigner“, „Webhosting“, „Mailhosting“, „Reseller-hosting“, „Managed Server“, „Domains“, „DNS Service“, „SMS Gateway“, „SSL Zertifikat“ und alle anderen

    - Durch regelmässige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass un-berechtigte Zugriffe verhindert werden.

    - Revisionssicheres, verbindliches Berechtigungsvergabever-fahren für Mitarbeiter des Auftragnehmers

    - Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig.

- **Datenträgerkontrolle**
    - Rechenzentren
        - 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 im Rechenzentrum zerstört (geschreddert).

- **Trennungskontrolle**
    - bei internen Verwaltungssystemen des Auftragnehmers
        - Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
        - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.
    - bei Hauptauftrag „Rootserver“, „Serverhousing“
        - Die Trennungskontrolle obliegt dem Auftraggeber.
    - bei Hauptauftrag „SiteDesigner“, „Webhosting“, „Mailhosting“, „Reseller-hosting“, „Managed Server“, „Domains“, „DNS Service“, „SMS Gateway“, „SSL Zertifikat“ und alle anderen
        - Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
        - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch 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 „Rootserver“, „Serverhousing““
    - Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.
  - bei Hauptauftrag „SiteDesigner“, „Webhosting“, „Mailhosting“, „Reselle-rhosting“, „Managed Server“, „Domains“, „DNS Service“, „SMS Gateway“, „SSL Zertifikat“ und alle anderen
    - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
    - Änderungen der Daten werden protokolliert.

3. 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 Rootserver, Serverhousing^
    - Datensicherung obliegt dem Auftraggeber
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage
    - Dauerhaft aktiver DDoS-Schutz
  - bei Hauptauftrag „SiteDesigner“, „Webhosting“, „Mailhosting“, „Reseller-hosting“, „Managed Server“, „Domains“, „DNS Service“, „SMS Gateway“, „SSL Zertifikat“ und alle anderen
    - Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages.
    - Einsatz von Festplattenspiegelung.
    - Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
    - Einsatz von Hard- und Softwarefirewall, Web Application Firewall (WAF) 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.

4. **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 Informationssicherheitsmanagementsystem 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. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
    - Die AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.
    - Die FireStorm ISP GmbH hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden.