Anlage 1 zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage

I. Vertraulichkeit

Zutrittskonstrolle

- 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 Mitarbeiters
- elektronisches Zutrittskontrollsystem mit Protokollierung
- Videoüberwachung an den Ein- und Ausgängen
- Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer; 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 „Managed Server“, „Managed V-Server“, „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.

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 „Managed Server“, „Managed V-Server“, „Webhosting“
  - Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert.
  - Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen.

Webhosting Franken
Inhaber: Holger Häring
USt-ID: DE 213548458

Bonalinostr. 1, 96110 Scheßlitz
Tel: +49-9542-464 99 99
Fax: +49-9542-464 99 92
info@webhosting-franken.de

Bank: Commerzbank
IBAN: DE18 760800400 367805200
BIC/SWIFT: DRESDEFF760

II. 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 „Managed Server“, „Managed V-Server“, „Webhosting“
  - Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
  - Änderungen der Daten werden protokolliert.

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

- 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 „Managed Server“, „Managed V-Server“, „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.

Webhosting Franken
Inhaber: Holger Häring
USt-ID: DE 213548458

Bonalinostr. 1, 96110 Scheßlitz
Tel: +49-9542-464 99 99
Fax: +49-9542-464 99 92
info@webhosting-franken.de

Bank: Commerzbank
IBAN: DE18 760800400 367805200
BIC/SWIFT: DRESDEFF760

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 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 AGB enthalten detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers.

Webhosting Franken
Inhaber: Holger Häring
USt-ID: DE 213548458

Bonalinostr. 1, 96110 Scheßlitz
Tel: +49-9542-464 99 99
Fax: +49-9542-464 99 92
info@webhosting-franken.de

Bank: Commerzbank
IBAN: DE18 760800400 367805200
BIC/SWIFT: DRESDEFF760