

Anhang 1

Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO

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

Zutrittskontrolle

- IT-Systeme werden ausschließlich in Deutschland, in den Rechenzentren der Hostway Deutschland GmbH, der Level 3 Communications (siehe auch Subunternehmer), und in eigenen Rechenzentren der BUSYMOUSE Business Systems GmbH, Am Mittelfelde 29, 30519 Hannover, betrieben.
- Zutritt zum Betrieb ist nur mit Sicherheitsschlüssel und PIN möglich.
- Zutrittskontrolle mit Kameras und Alarmanlage, mehrere Kameras in den Räumen. Aufzeichnung 24/7 (Datenmengenabhängige Aufbewahrung).
- Die Schutzmaßnahmen werden regelmäßig überprüft.

Zugangskontrolle

- Professionelle Virenschutzlösung und Firewall-Lösung sind vorhanden, konfiguriert und werden fortlaufend kontrolliert.
- Der Zugriff auf geschützte Teile der BUSYMOUSE-Umgebung ist nur über VPN möglich und wird protokolliert.
- Fernzugriff auf IT-Systeme ist grundsätzlich nur über passwortgeschützte VPN, IP-Sec, SSH, SFTP, SSL/TLS Verbindungen (verschlüsselte, authentifizierte Verbindungen) möglich.
- Remotezugriff für administrative Aufgaben ist nur mit Zwei-Faktor-Authentifizierung möglich.
- IT-Systeme werden mittels VLANs in separate logische Netze unterteilt. Ausgenommen hiervon sind Schnittstellen von IT-Systemen, die öffentliche IP-Adressen zugewiesen bekommen.
- Jedes IT-System ist durch Firewalls sowie Benutzername und Passwort und/oder Client-Zertifikate vor unberechtigten Zugriffen geschützt. Zugriffe auf die IT-Systeme werden im Access-Log protokolliert und nach Projektanforderung aufbewahrt.

Zugriffskontrolle

- Seitens BUSYMOUSE ist der Zugriff auf die IT-Systeme ausschließlich autorisierten und namentlich bekannten Personen der BUSYMOUSE erlaubt. Alle Administratoren arbeiten mit individuellen Zugangskennungen.
- Ein Berechtigungskonzept mit bedarfsgerechten Zugriffsrechten wurde umgesetzt.
- Alle Dienste (Konsole, Datenbanken, Webserver) werden in Form von Log-Files protokolliert.
- Nicht benötigte Dienste, Ports und Accounts werden standardmäßig deaktiviert bzw. gesperrt.

Trennungskontrolle

- Es findet eine getrennte Verarbeitung von Daten statt, die zu unterschiedlichen Zwecken erhoben wurden mit mandantenfähigen Verarbeitungsmöglichkeiten.

- BUSYMOUSE nimmt ausschließlich die Erfüllung der beauftragten Leistungen durch den Auftraggeber / Kunden vor.
- Alle Mitarbeiter von BUSYMOUSE sind auf das Datengeheimnis nach §5 BDSG bzw. §53 BDSG (neu) und der DS-GVO, das Telekommunikationsgeheimnis nach §88 TKG sowie das Sozialgeheimnis nach §35 Abs. 1 SGB I verpflichtet.

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

Weitergabekontrolle

- Die BUSYMOUSE Server werden ausschließlich in Deutschland betrieben und die Daten nur auf Servern in Deutschland gespeichert.
- Grundsätzlich werden personenbezogene Daten in kennwortgeschützten Datenbanken gespeichert. Der Fernzugriff hierauf ist nur verschlüsselt (SSL) möglich. Verlassen die Daten beim Transport über Dateitransfer das separierte Netz von BUSYMOUSE werden zusätzlich SSL/TLS-, IPsec oder VPN-Verbindungen verwendet.
- BUSYMOUSE-Server arbeiten mit Transportverschlüsselung.

Eingabekontrolle

- Alle Dienste (Konsole, Datenbanken, Webserver) werden in Form von Log-Files protokolliert. Die Logfiles werden nach Projektanforderung aufbewahrt.

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

Verfügbarkeitskontrolle

- Backups werden täglich erstellt und einmal pro Woche in einem anderen Brandabschnitt im feuerfesten Tresor gelagert.
- Eine unterbrechungsfreie Stromversorgung (USV) ist installiert und wird laufend geprüft.
- Virenschutz ist auf allen Servern und Endgeräten aktiviert und wird laufend aktualisiert.
- Professionelle Firewalls schützen die IT-Infrastruktur.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

- Der Datenschutzbeauftragte prüft mit Hilfe regelmäßiger Audits das Unternehmen.

Auftragskontrolle

- Eingesetzte Unterauftragnehmer erhalten ausschließlich solche Daten, die zur Erfüllung der Leistung im Sinne des Auftraggebers erforderlich sind.
- Arbeiten an IT-Systemen werden durch BUSYMOUSE im Changelog sowie in Systemdokumentationen dokumentiert.
- Es werden Zusatzvereinbarungen zur Auftragsverarbeitung mit allen Dienstleistern abgeschlossen.