Anlage technische und organisatorische Maßnahmen (TOM)

Maßnahmen gemäß DSGVO (Sicherheit der Verarbeitung)

Stand 24.05.2018

Pseudonymisierung und Verschlüsselung

Die Pseudonymisierung und Verschlüsselung personenbezogener Daten (§ 32a DSGVO).

Pseudonymisierung

- Die Maßnahmen der Pseudonymisierung obliegt dem Verantwortlichen.

Verschlüsselung

Maßnahmen beim Produkt Uberspace:

- Verschlüsselung von Datenübertragungen beim Erstellen externer Backups.
- Verschlüsselung von Datenübertragungen zwischen Uberspace Dashboard und Uberspace Account.
- Bereitstellung verschlüsselter Übertragungswege wie sftp, ssh oder https.

Maßnahmen bei Produkten Plesk, Dedicated Hosting und Housing

- Die Maßnahmen der Verschlüsselung obliegt dem Verantwortlichen.
- Verschlüsselung von Datenübertragungen beim Erstellen externer Backups.

Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (§ 32b DSGVO).

Vertraulichkeit

Zutrittskontrolle (Räume)

Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Werkschutz, Pförtner
- Verwaltung von personengebundenen Zutrittsberechtigungen
- Festlegung Zutrittsberechtigter Personen

- Protokollierung des Zutritts
- Festlegung von Sicherheitsbereichen
- Videoüberwachung der Zugänge
- Sicherheitstüren (Chipkarten-/Transponder-Schließsystem)
- Sicherheitsschlösser Serverschränke
- Tragepflicht von Mitarbeiter- / Gästeausweisen

Zugangskontrolle (Oberflächen)

Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen bei internen Verwaltungssystemen des Auftragsverarbeiters:

- Authentifikation mit Benutzer + Passwort
- Passwortvergabe / Passwortregeln
- Zwei-Faktor-Authentifikation wenn möglich
- Individuelle Schlüssel pro Mitarbeiter und Arbeitsgerät
- Sorgfältige Auswahl von Reinigungspersonal

Maßnahmen bei Produkten Uberspace, Plesk, Dedicated Hosting und Housing

- Die Maßnahmen der Zugangskontrollen obliegen dem Verantwortlichen.

Zugriffskontrolle (Dateien)

Gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung 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.

Maßnahmen bei internen Verwaltungssystemen des Auftraggebers:

- Zertifizierte Aktenvernichtung durch Dienstleister

Maßnahmen bei Produkten Uberspace, Plesk, Dedicated Hosting und Housing

- Die Maßnahmen der Zugriffskontrolle obliegt dem Verantwortlichen.
- Bei den Produkten Uberspace, Plesk oder durch vertraglicher Vereinbarung werden regelmäßige Sicherheitsupdates eingespielt, die unberechtigte Zugriffe auf Grund von Sicherheitslücken unterbinden sollen.

Datenträgerkontrolle

Maßnahmen beim Produkt Housing:

- Beim Produkt Housing erfolgt Übergabe dekommissionierter Hardware zurück an Kunden. Die Maßnahmen der Datenträgerkontrolle obliegt dann dem Verantwortlichen.

Maßnahmen bei Produkten Uberspace, Plesk und Dedicated Hosting

- Physikalische Zerstörung von dekommissionierten Datenträgern.

Trennungsgebot

Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahmen beim Produkt Uberspace:

- Trennung Produkt, Support-Ticketsystem, Bankdaten und Kundendatenbank.

Maßnahmen bei Produkten Plesk, Dedicated Hosting und Housing

- Die Maßnahmen des Trennungsgebotes obliegen dem Verantwortlichen.

Auftragskontrolle

Gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl weiterer Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit).
- Abschluss von Auftragsverarbeitungsverträgen.
- Beauftragte Verarbeitung durch Auftragnehmer nur nach genauer Anweisung.

Integrität

Weitergabekontrolle (Transport)

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.

- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen.
- Maschinen-Authentifikation bei netzbasierten automatisierten Übertragungsvorgängen.

Verfügbarkeit

Verfügbarkeitskontrolle

Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Automatische Brandlöschung
- Feuer- und Rauchmeldeanlagen

- Unterbrechungsfreie Stromversorgung
- Überwachte Stromverteilungssysteme
- Klimaanlage in Serverräumen
- Testen der Datenwiederherstellung
- Einsatz aktueller Technologien zur Reduzierung von Ausfällen je nach Produkt (Beispiel: Clusterbetrieb)
- Erstellen von Backup- und Recoverykonzepten

Belastbarkeit

Belastbarkeitskontrolle

- Zutrittskontrolle Rechenzentrum
- Zugangskontrollen Mitarbeiter
- 24/7 Monitoring aller relevanten Systeme
- Netzwerk-Firewalls
- Rate-Limits der Netzwerkdienste

Wiederherstellbarkeit

Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (§ 32c DSGVO).

Wiederherstellbarkeit

Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?

- 24/7 Monitoring aller relevanten Systeme
- 24/7 Bereitschaftsdienst
- Regelmäßige Datensicherung (Backup- und Restorekonzept)

Überprüfung

Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (§ 32d DSGVO).

Verfahren zur regelmäßigen Überprüfung

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

- Automatische Überprüfung und Alarmierung auf Aktualität der Datensicherungen

Verarbeitung personenbezogener Daten nur nach Anweisung

Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des

Verantwortlichen verarbeitet werden?

- Benennung des Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf Vertraulichkeit