

# Technische und organisatorische Maßnahmen zum Datenschutz in eBuSy

productive web, Anbieter des eBuSy Buchungssystems trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

## 1. Vertraulichkeit

### Zutrittskontrolle

Sämtliche Daten werden auf Dedicated Servern bzw. Backup-Servern in einem Rechenzentrum der Firma Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen gespeichert. Die von der Firma Hetzner Online getroffenen Maßnahmen zur Zutrittskontrolle sind wie folgt:

- elektronisches Zutrittskontrollsystem mit Protokollierung
- Hochsicherheitszaun um den gesamten Datacenterpark
- dokumentierte Schlüsselvergabe
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen

### Zugangskontrolle

Die eBuSy Software wird auf Dedicated Servern bei der Firma Hetzer Online betrieben. Diese Dedicated Server verwenden Ubuntu-Linux als Betriebssystem und werden durch eine Firewall geschützt. Das Betriebssystem ist hinsichtlich Benutzern, Rechten und zugänglicher Ports auf ein Minimum reduziert. Ein Zugang zum Web-Server, der über die übliche Nutzung der Web-Applikation durch den Auftraggeber und dessen Kunden hinausgeht (Zugriff auf eBuSy via Web-Browser), ist ausschließlich den für eBuSy verantwortlichen Mitarbeitern von productive web möglich. Jeder Mitarbeiter verfügt über ein sog. RSA-Schlüsselpaar aus privatem und öffentlichem Schlüssel, das den Zugang zum eBuSy Web-Server ermöglicht. Der private Schlüssel jedes Mitarbeiters ist zusätzlich passwortgeschützt und auf einer verschlüsselten Festplatte des jeweiligen Mitarbeiters gespeichert.

Für den Zugang zur eBuSy-Software (Zugriff auf eBuSy via Web-Browser) gibt es einen Support-Zugang. Das Passwort für diesen Support-Zugang ist ausschließlich den verantwortlichen Mitarbeitern von productive web bekannt und auf einer verschlüsselten Festplatte des jeweiligen Mitarbeiters gespeichert. Das verwendete Passwort besitzt eine sehr hohe Passwort-Komplexität.

### Zugriffskontrolle

Jeder Mitarbeiter der Zugang zum eBuSy-Webserver erhält, verwendet einen eigenes RSA-Schlüsselpaar. Das Root-Passwort des Web-Servers ist nur den Eigentümern und Gesellschaftern der productive web GbR, Herrn Wolfgang Schneider und Michael Haun bekannt. Der Zugang zum Web-Server wird über die Berechtigung des RSA-Schlüssels eines Mitarbeiters gesteuert und kann so auch beim Ausscheiden eines Mitarbeiters entzogen werden.

Das Passwort für den eBuSy Support-Zugang wird regelmäßig geändert, insbesondere beim Ausscheiden eines Mitarbeiters.

## **Trennung**

Die Software eBuSy ist eine mandantenfähige Software. Zur Trennung der Daten verschiedener Mandanten werden sämtliche Datensätze des Auftraggebers parameterisiert mit einer eindeutigen, dem Auftraggeber zugeordneten Kennung. Sämtliche Zugriffe eines Mandanten auf die Software eBuSy (Zugriff auf eBuSy via Web-Browser) werden automatisch anhand der Kennung des Mandanten gefiltert. Dabei kommen spezielle Open-Source Datenbank-Technologien zum Einsatz, die für diesen Zweck entwickelt wurden und die Isolation der Daten einzelner Mandanten sicherstellen.

## **Pseudonymisierung & Verschlüsselung**

Alle Passwörter von Benutzern der eBuSy Software, werden verschlüsselt gespeichert, so dass weder der Betreiber des eBuSy Buchungssystems, noch productive web in Kenntnis der Klartext-Passwörter gelangen können.

Es erfolgt darüberhinaus keine Pseudonymisierung und/oder Verschlüsselung der Daten, da dies der Nutzung der eBuSy-Software durch den Auftraggeber und seine Kunden und im Sinne des Auftraggebers und seiner Kunden entgegen stehen würden.

## **2. Integrität**

### **Eingabekontrolle**

Sämtliche Eingaben, Änderungen und Löschungen von personenbezogenen Daten in der eBuSy-Webanwendung werden protokolliert. Sofern der Zugriff auf die eBuSy-Webanwendung durch einen angemeldeten Benutzer erfolgt, wird die Eingabe, Änderung oder Löschung unter diesem angemeldeten Benutzer protokolliert. Diese Protokolle sind mit dem Datensatz über die jeweilige Person in der Datenbank assoziiert und werden vollständig und datenschutzgerecht gelöscht, wenn der zugehörige Personen-Datensatz gelöscht wird. Der Zugriff auf diese Protokolle ist für autorisierte Mitarbeiter des Auftraggebers (die über einen Administrations-Zugang zur eBuSy-Software verfügen) und für zuständige Support-Mitarbeiter von productive web möglich.

### **Weitergabekontrolle**

Die Übertragung sämtlicher Daten vom Betreiber des eBuSy Buchungssystems (oder dessen Kunden) zu productive web erfolgt durch eine SSL-verschlüsselte Verbindung. Die eBuSy-Webanwendung ist ausschließlich via HTTPS-Protokoll aufzurufen. Ein unverschlüsselter Aufruf via HTTP-Protokoll wird sofort umgeleitet und in eine SSL-verschlüsselte Verbindung via HTTPS-Protokoll überführt.

Alle Mitarbeiter von productive web sind verpflichtet, den sicheren Umgang mit personenbezogenen Daten im Sinne des Art. 32 Abs. 4 DS-GVO sicherzustellen.

Sämtliche Daten des Auftraggebers werden nach Beendigung des Auftrags datenschutzgerecht gelöscht.

## **3. Verfügbarkeit und Belastbarkeit**

Die bei der Firma Hetzner Online angemieteten Dedicated Server sind mit einer unterbrechungsfreien Stromversorgung und einer Netzersatzanlage ausgestattet. Es ist ein dauerhafter

DDoS-Schutz aktiv. Die Daten des Auftraggebers werden einmal täglich auf speziell dafür vorgesehene, geschützte Backup-Server der Firma Hetzer Online gesichert. Dieses täglichen Sicherungen werden für maximal 31 Tage vorgehalten und anschließend datenschutzgerecht gelöscht.

#### **4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

Alle Mitarbeiter von productive web werden über die Notwendigkeiten des vertraulichen Umgangs mit personenbezogenen Daten informiert und zu deren Einhaltung verpflichtet.

Die beschriebenen technischen und organisatorischen Maßnahmen werden quartalsweise durch productive web geprüft und bewertet.