webprofi[l]

Anlage TOM

Technische und organisatorische Maßnahmen

Version 1.1 vom 01.04.2019

WEBprofil - Gernot Ploiner e.U.

Dr.-Franz-Wilhelm-Straße 2, 3500 Krems an der Donau

T: 0720 - 010 202 | office@webprofil.at www.webprofil.at

Vertraulichkeit

Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der Verarbeitung genutzten technischen Einrichtungen zu verwehren.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Die Räumlichkeiten sind versperrt, wenn nicht besetzt.
- Die Computer sind passwortgeschützt.
- Passwörter werden nur verschlüsselt gespeichert.

Zugangskontrolle

Es ist zu verhindern, dass die zur Erbringung der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Zugang zu den Datenverarbeitungsanlagen erhält ausschließlich autorisiertes und fachlich qualifiziertes Personal.
- Der Zugang erfolgt über eine Benutzerkennung und Eingabe eines Passwortes.
- Die Passwörter entsprechend einem technisch sicheren Niveau und sind durch interne Richtlinien geregelt.

Zugriffskontrolle

Es ist sicherzustellen, 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 oder verändert werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Nur die Mitarbeiter des Auftragnehmers und vom Auftraggeber berechtigte Dritte haben Zugriff auf dessen Systeme.
- Jeder Mitarbeiter wird entsprechend zur Vertraulichkeit und der Einhaltung des Datenschutzes bei Aufnahme seiner Tätigkeit verpflichtet. Ein Verstoß hätte die Entlassung, sowie eine Strafanzeige zur Folge. Betroffene Auftraggeber würden in so einem Fall selbstverständlich über den Vorfall informiert.

Weitergabekontrolle

Es muss dafür gesorgt werden, 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 welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Der Auftragnehmer überträgt personenbezogene Daten soweit technisch möglich und wirtschaftlich zumutbar elektronisch über verschlüsselte Datenverbindungen, sodass sie nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
- Erhebt, verarbeitet oder nutzt der Auftraggeber im Rahmen des Hostingvertrages personenbezogene Daten, so obliegt die Absicherung der Datenübertragung an den Auftragnehmer oder Dritte (z.B. über HTTPS) ausschließlich der Verantwortung des Auftraggebers.

Pseudonymisierung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Die Pseudonymisierung personenbezogener Daten erfolgt im Rahmen des Hostingvertrages und der dort vom Auftraggeber betriebenen Anwendungen.

Integrität

Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Die Eingabe, Änderung oder Löschung sensibler personenbezogener Daten ist nur den zugeteilten Personen zugänglich und wird dokumentiert.
- Die Eingabe, Änderung oder Löschung nicht sensibler personenbezogener Daten ist nur den zugeteilten Personen zugänglich und wird nicht dokumentiert.

Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle wie oben im Abschnitt Vertraulichkeit beschrieben, dienen auch der Sicherstellung der Integrität.

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Soweit es technisch möglich ist, sind sämtliche auf Datenverarbeitungssystemen liegende Daten im Rahmen der Ausfallsicherheit vor zufälligem Verlust oder Zerstörung geschützt. Hierzu kommen u.a. RAID Systeme zum Einsatz.
- Zusätzlich wird mindestens ein Backup des Vortages bereitgehalten.

Rasche Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beim Auftragnehmer umgesetzte Maßnahmen:

- IT-Notfallpläne und Wiederanlaufpläne
- Regelmäßige Datenwiederherstellungen