Anhang 2 zur Anlage 2 zu den AGB

Technische und organisatorische Maßnahmen

A. Technische und organisatorische Maßnahmen von Timme Hosting

Das Hosting der vom Auftraggeber bereitgestellten Daten für Vulcavo erfolgt auf den Servern von Timme Hosting GmbH & Co. KG, Ovelgönner Weg 43, 21335 Lüneburg, deren technische und organisatorische Maßnahmen für die Datenverarbeitung des Kunden Anwendung finden.

B. Beschreibung der technischen und organisatorischen Maßnahmen des Auftragnehmers

B.1 Schutzziel Vertraulichkeit

Es ist sicherzustellen, dass keine Person – sowohl Mitarbeiter als auch Dritte - personenbezogene Daten unbefugt zur Kenntnis nimmt.

B.1.1 Zutrittskontrolle

Kontrolle des räumlichen Zutritts zu Datenverarbeitungsanlagen (DV-Anlage) durch Unbefugte. Durch die Zutrittskontrolle soll verhindert werden, dass Personen, die dazu nicht befugt sind, in die Nähe einer DV-Anlage gelangen können.
Zur DV-Anlage gehören neben der Zentraleinheit einschließlich der integrierten Laufwerke auch die angeschlossenen Peripherieeinheiten wie Terminals, PCs, Drucker, Plotter und Bandeinheiten usw. Eine Zutrittskontrolle zu PCs innerhalb von Büroräumen wird z.B. dadurch sichergestellt, dass Maßnahmen ergriffen werden, die verhindern, dass Betriebsfremde in die Nähe von PCs gelangen bzw. den Bildschirm einsehen können.

Maßnahmen
Zutrittsregelung für **betriebsfremde Personen**; die Umsetzung erfolgt i.d.R. durch folgende Punkte:
• Zentraler Empfangsbereich vorhanden und verschlossene Außentür
• Aufenthalt von Fremden in den Unternehmensräumen nur in Anwesenheit von Mitarbeitern
• Vermerk von Zu- und Abgang von betriebsfremden Personen am Empfang
Zutrittsregelung für **betriebsangehörige Personen**; die Umsetzung erfolgt i.d.R. durch folgende Punkte:
• Schlüssel mit Protokollierung
• Rücknahme von Zugangsmitteln nach Ablauf der Berechtigung

B.1.2 Zugangskontrolle

Die Benutzung von DV-Anlagen durch unbefugte Personen (nicht befugte Mitarbeiter oder Externe) soll verhindert werden. Bei der Zugangskontrolle geht es um die Frage der Identifikation und anschließender Authentifikation. Die Zugangskontrolle umfasst auch das Ziel, dass kein externer Zugang (z.B. aus dem Internet) auf DV-Anlagen erfolgen kann (Hackerschutz).

Maßnahmen
Authentisierung der Benutzer gegenüber dem Datenverarbeitungssystem. d.h. Identifikation durch Benutzernamen und Passwort
Regelungen zur Passwortvergabe • Persönliches Passwort • Mindestens 8 Zeichen, darunter auch Sonderzeichen/Zahlen • Vergabe durch Nutzer selbst • Automatisierte temporäre Zugangssperre nach zu vielen Fehlversuchen • Keine Weitergabe an Dritte • Regelung für Fall der Abwesenheit (Urlaub, Krankheit etc.)
Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern

Regelmäßige Kontrolle der Gültigkeit und einen möglichen Ablauf von Berechtigungen (mindestens jährlich)
Sicherung der Bildschirmarbeitsplätze bei Abwesenheit und laufendem System (Passwortschutz für Bildschirmschoner nach 5 Min. bis 15 Min, je nach Risiko des Missbrauchs)
Abschottung interner Netze gegen Zugriffe von außen (Firewall, Verschlüsselung VPN)
Regelmäßige Überprüfung der Firewall-Regeln
Verschlüsselung der Festplatten ausgegebener Notebooks, die außerhalb des Betriebsgeländes eingesetzt werden

B.1.3 Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, dass Mitarbeiter und befugte Dritte nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können. Darüber hinaus soll sichergestellt werden, dass beim Umgang mit personenbezogenen Daten diese nicht unbefugt gelesen, kopiert, verändert oder entfernt (gelöscht) werden können. Dies gilt sowohl für Daten, die in DV-Systemen gespeichert sind, als auch für solche, die sich auf maschinell lesbaren Datenträgern oder auf Papier befinden.

Maßnahmen
Erstellung eines Benutzerprofils, d.h. Festlegung von Zugriffsberechtigungen hinsichtlich personenbezogener Daten von Nutzern
Differenzierte Berechtigungen für Lesen, Verändern oder Löschen von Daten
Erstellung eines Berechtigungskonzeptes • Einrichtung von Administrationsrechten • Verwaltung der Zugriffsrechte durch Systemadministrator
Regelmäßige Überprüfung vergebener Berechtigungen mit Entzug nicht mehr benötigter Zugriffsrechte
Trennung von Test- und Produktionsbetrieb
Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger und von Makulatur (beispielsweise Fehldrucke von Arbeitslisten, Anschreiben etc.)

B.1.4 Trennungskontrolle

Gemäß dem Trennungsgebot sind Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt zu verarbeiten. Dadurch soll gewährleistet werden, dass die Zweckbindung personenbezogener Daten durch organisatorische und technische Maßnahmen umgesetzt wird. Besondere Bedeutung hat das Trennungsgebot im Rahmen der Auftragsverarbeitung, wenn z.B. Daten mehrerer Auftraggeber auf einem System gespeichert sind. Sofern das Trennungsgebot nicht durch technische Maßnahmen, wie z.B. eine Zugriffs-Kontroll-Software, erreicht werden kann, ist eine getrennte Speicherung notwendig.

Maßnahmen
Berechtigungskonzept mit Festlegung der Zugriffsrechte
Umsetzung des Trennungsgebotes auf Datenbankebene durch Mandantentrennung bzw. logische Trennung anhand verschiedener Buchungskreise

B. 2 Schutzziel: Integrität

Es ist sicherzustellen, dass informationstechnische Prozesse und Systeme die festgelegten Spezifikationen kontinuierlich einhalten, so dass die mit ihnen zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben.

B. 2.1 Weitergabekontrolle

Umfasst sind alle Varianten der Weitergabe von personenbezogenen Daten mittels Datenträgern oder Kommunikationsnetz. Die Weitergabekontrolle soll verhindern, dass Daten bei deren Weitergabe unbefugt verwendet (gelesen, kopiert, verändert oder entfernt/gelöscht) werden können. Der Begriff der Weitergabe umfasst sowohl die Übermittlung an Dritte als auch die Weitergabe im Rahmen der Auftragsverarbeitung zwischen Auftraggeber und Auftragnehmer und an den Betroffenen.

Maßnahmen
Bei Weitergabe auf physischen Datenträgern: Dokumentation von Datenempfänger sowie der Transport-/Übermittlungswege
Soweit technisch möglich, eine elektronische Übermittlung auf gesicherten Übertragungswegen
Patch Management, das ein zeitnahes Einspielen sicherheitskritischer Patches gewährleistet
Patch Management mit rechtzeitiger Mitigation von Applikationen und Servern, zu denen vom Hersteller keine Sicherheitspatches mehr bereit gestellt werden
Einsatz eines laufend upgedateten Virenschutzes

B. 2.2 Eingabekontrolle

Durch die Eingabekontrolle soll dokumentiert werden, wer für eine unzulässige oder fehlerhafte Dateneingabe verantwortlich ist. Ziel ist die Revisionsfähigkeit der Eingabe von personenbezogenen Daten in das DV-System, zu welchem auch nicht vernetzte Einzelarbeitsplätze wie z.B. PCs gehören. Die zu kontrollierende Dateneingabe umfasst sowohl das erstmalige Speichern als auch die Veränderung und Löschung (Entfernung) von Daten.

Maßnahmen
Führung dokumentierter, nachvollziehbarer Zugriffsberechtigungen
Regelung zu Zugriffsbefugnissen auf erstellte Dokumentationen
Löschungsregelung für Dokumentationen

B. 3 Schutzziel: Verfügbarkeit

B. 3.1 Verfügbarkeitskontrolle

Schutz der Daten gegen zufällige Zerstörung oder Verlust. Mögliche Gefahren
sind z.B. Wasserschäden, Blitzschlag, Stromausfall, Brand, Sabotage oder Diebstahl.

Maßnahmen
Automatische Feuer- und Rauchmeldeanlagen
Vertretungsregelungen für Mitarbeiter

B.4 Schutzziel: Belastbarkeit

B.4.1 Auftragskontrolle

Gewährleistung der weisungsgemäßen Auftragsverarbeitung. Der Auftragnehmer hat die ihm erteilten Weisungen einzuhalten, während der Auftraggeber Sorge dafür zu tragen hat, dass seine Weisungen klar und eindeutig sind und befolgt werden.

Maßnahmen
Kontrolle der Einhaltung von Datensicherheitsbestimmungen durch Auftragnehmer und Meldung, wenn Verstöße vorliegen oder der Verdacht besteht, dass die Datensicherheitsvorgaben unzureichend sind.
Verpflichtung der Mitarbeiter des Auftragnehmers zur Wahrung der datenschutzrelevanten Vorgaben
Schriftliche Vereinbarung eines Vertrages zur Auftragsverarbeitung mit Dienstleistern

B.4.2 Verfahren zur regelmäßigen Überprüfung

Ständige Gewährleistung der Einhaltung der Vorgaben an Datenschutz und IT-Sicherheit. Der Auftragnehmer hat regelmäßig zu überprüfen und dokumentieren, dass die vertraglich geschuldeten Vorgaben eingehalten werden.

Maßnahmen
Meldung von Sicherheitsvorfällen, die im laufenden Betrieb festgestellt werden
Kontrolle der Wirksamkeit der durchgeführten Maßnahmen mindestens einmal pro Jahr