Technische und organisatorische Maßnahmen

1. Version

Version 1.0, gültig ab 31.05.2018

2. Ziel

Im Rahmen der Tätigkeit als Softwarehersteller und Dienstleister tritt die Firma ViCon GmbH (kurz „ViCon“) auch als Auftragsverarbeiter auf. Dies regelt ViCon mit seinen Kunden durch einen Vertrag zur Auftragsverarbeitung. Dieser ist in der Datenschutzvereinbarung der Internetseiten https://www.vicon.biz und https://www.viflow.de abrufbar. Gegenstand der Auftragsverarbeitung sind folgende Vorgänge:

1. Zu Support-, Schulungs- oder sonstigen Dienstleistungs-Zwecken schaltet ViCon sich per Fernwartung auf das System des Kunden bei ihm vor Ort.
2. Zu Zwecken von Einrichtung, Support, Schulungen oder sonstigen Dienstleistungen im Zusammenhang mit der ViCon-Software sind Mitarbeiter von ViCon vor Ort beim Kunden.
3. Der Kunde schickt seinen Datenbestand an ViCon, damit Mitarbeiter von ViCon einen Programm- oder Anwenderfehler finden und korrigieren können.
4. Es werden vom Kunden Daten an ViCon geschickt mit der Aufgabenstellung, diese Daten in von ViCon-Programmen nutzbare Daten zu transferieren.

Zu diesem Vertrag muss gemäß §32 (1) DSGVO eine Beschreibung der technischen und organisatorischen Maßnahmen angegeben werden. Diese werden im Folgenden aufgeführt.

3. Allgemeine Hinweise

Die Vorgänge 1 und 4 sind in der Regel keine zeitkritischen Vorgänge. Es muss nicht notwendig eine Hochverfügbarkeit und besondere Belastbarkeit der ViCon-Systeme gegeben sein.

Unabhängig von diesen prinzipiellen Bemerkungen zu der Art der Vorgänge ist ViCon für die Hochverfügbarkeit und Belastbarkeit der eigenen Systeme sehr gut aufgestellt, wie weiter unten aufgeführt wird.

Der Vorgang 2 der Gegenstände der Auftragsverarbeitung (ViCon vor Ort) findet nicht im Hause von ViCon statt. Daher spielen die im folgenden beschriebenen Maßnahmen bei ViCon nur eine untergeordnete Rolle. Vielmehr ist entscheidend, wie die Maßnahmen des Kunden vor Ort gestaltet sind.

4. Vertraulichkeit gemäß Art. 21 Abs. 1 DS-GVO

4.1. Zutrittskontrolle

Maßnahmen bei ViCon:

- Alarmanlage
- Schließanlage mit dokumentierter Schlüsselverwaltung. Zutrittsberechtigungen werden nach einem definierten Verfahren eingeräumt
- Eigenständige Zutrittsregelung für den IT-Serverraum
- Einbruchshemmung der Zugänge
- Empfang u. Begleitung betriebsfremder Personen

4.2. Zugangskontrolle

Maßnahmen bei ViCon:

- Authentifizierung mit Benutzername und Passwort
- Anti-Viren-Software Server
- Anti-Viren-Software Clients
- Firewall
- Einsatz SSL-Verschlüsselung bzw. VPN-Technologien bei Remote-Zugriffen
- Zentrale Verwaltung von Benutzerberechtigungen
- Vollverschlüsselung mobiler Endgeräte
- Sicherstellung komplexer Passwörter mit regelmäßiger Änderung
- Teilw. Login mit PIN/Fingerabdruck
- zusätzlich Richtliniendokument zur Verwendung mobiler Endgeräte

4.3. Zugriffskontrolle

Maßnahmen bei ViCon:

- Aktenvernichter (Sicherheitsstufe 4)
- Einsatz Berechtigungskonzepte
- Minimale Anzahl an Administratoren
- Verwaltung Benutzerrechte durch Administratoren

4.4. Trennungskontrolle

Maßnahmen bei ViCon:

- Dedizierte Benutzerrechte bei internen Anwendungen
- Vom Kunden im Rahmen der Auftragsbearbeitung erhaltene Daten werden an voneinander unabhängige Speicherorten gespeichert.

4.5. Pseudonymisierung (Art. 32 Abs. 1a; Art. 2 Abs.1 DS-GVO)

Maßnahmen bei ViCon:

- Als Auftragsverarbeiter trifft ViCon zusätzlich zu Maßnahmen, die sich aus den jeweiligen Leistungsbeschreibungen der Produkte / Dienstleistungen ergeben oder durch den Verantwortlichen im Rahmen der Beauftragung vorgenommen werden, keine Maßnahmen zur Pseudonymisierung.

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

5.1. Weitergabekontrolle

Maßnahmen bei ViCon:

- Verschlüsseltes Kommunikationsprotokoll (Website und OwnCloud)
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern
- Verschlüsselung von mobilen Geräten, wie Notebooks
- Verschlüsselung der Inhalte von Mail-Kommunikation nach Kundenwunsch

5.2. Eingabekontrolle

Maßnahmen bei ViCon:

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten in unserer Faktura Software und im CRM-System.

    - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
    - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

6.1. Verfügbarkeitskontrolle

Maßnahmen bei ViCon:

- Feuer- und Rauchmeldeanlagen
- Feuerlöscher Serverraum
- Feuerlöscher in den Büroräumen
- Serverraum klimatisiert
- USV
- Schutzsteckdosenleisten Serverraum
- RAID System / Festplattenspiegelung
- Virtualisierung
- Redundanz von Teilkomponenten: Firewall, zentrales Festplattensystem
- Desaster-Recovery-Verfahren mit regelmäßigen Überprüfungen der Datenwiederherstellung
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums und außerhalb des Firmengebäudes. Dies gilt aber nur für ViCon-eigene Daten. Zugesendete Kundendaten werden nicht innerhalb unseres Sicherungskonzeptes gesichert. Wenn überhaupt gibt es nur temporäre Sicherungen der Kundendaten innerhalb der Serverfarm von ViCon. Es wird daher im Sinne des Datenschutzes in Kauf genommen, dass Kundendaten durch z.B. einen Festplattenfehler unbrauchbar sind und vom Kunden erneut angefordert werden müssen.
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art 32. Abs. 1d; Art. 25 Abs. 1 DS-GVO)

Maßnahmen bei ViCon:

- Zentralle Dokumentation aller Verfahrensweisen und Regelung mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mindestens jährlich durchgeführt.
- Interner Datenschutzbeauftragter, erreichbar per Mail: datenschutz@vicon.biz
- Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich)
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
- Formalisierter Prozess zum Empfang von Kundendaten, deren Verarbeitung und Löschung im Sinne der Auftragsbearbeitung
- Formalisierter Prozess zur Bearbeitung von Sicherheitsproblemen ist vorhanden
- Incident-Response-Maßnahmen
- Datenschutzfreundliche Voreinstellungen