Dokumentation

Technische und organisatorische Maßnahmen

Folgende Maßnahmen zur Einhaltung der Anforderungen an die Sicherheit der Datenverarbeitung werden ergriffen:

1. Pseudonymisierung

   Jeder Kunde ist einer festen Kundennummer zugeordnet.
   Falls Dateien gespeichert werden, erfolgt dies in einem zahlenbasierten Ordnungssystem. Dokumente werden nur gespeichert, wenn dies im Rahmen eines Auftrags notwendig ist.

2. Verschlüsselung

   Es wird derzeit kein Serversystem für die Dokumentenablage verwendet. Die Daten von Kunden werden auf einer lokalen Hardware (HP PRODESK 600 G6 DM CI7-10700 und HP Notebook) für die Dauer der Nutzung gespeichert und nach Projektabschluss gelöscht.
   Die Computer sind sowohl durch ein BIOS- Passwort als auch durch ein Microsoft-Konto abgesichert. Die Passwörter (mind. 14-stellig) werden in regelmäßigen Abständen geändert.
   Das an den PCs derzeit eingesetzte Betriebssystem Windows 11 Pro und die Office-Anwendungen werden durch regelmäßige Sicherheitsupdates auf dem aktuellen Stand gehalten.
   Der Zugriff auf das derzeit genutzte Samsung Smartphone Galaxy S20+ ist sowohl durch eine PIN als auch mittels biometrischer Daten abgesichert.
   Das Smartphone wird durch regelmäßige Sicherheitsupdates auf aktuellem Stand gehalten.
   PCs und Smartphone werden zusätzlich durch Bitdefender Total Security abgesichert.

3. Gewährleistung der Vertraulichkeit

   Der genutzte Büroraum befindet sich im privaten Einfamilienhaus. Der Büroraum ist abschließbar. Eventuelle Kundentermine und Besprechungen finden in einem separaten Raum statt. Der benutzte Onlinezugang (Vodafone) ist vom privat genutzten Zugang (Telekom) getrennt. Ungesicherte WLan- Zugänge werden nicht genutzt (z.B. in Hotels oder Bahn). Hierfür wird stets ein privater Hotspot über das eigene Smartphone genutzt.
   Eine Einwahl auf die Computersysteme beim Kunden erfolgen über gesicherte Zugänge (SSL mit OPEN VPN), Teamviewer oder DATEV Fernbetreuung.
   Sitzungen über Teamviewer können auf Kundenwunsch aufgezeichnet werden.
   Sitzungen mit DATEV Fernbetreuung werden immer aufgezeichnet.
   Der Zugriff auf Computersysteme des Kunden erfolgt über ein vom Kunden festzulegendes Benutzerkonto und Passwort.

Der Zugriff auf die genutzte Warenwirtschaft (DATEV Unternehmen Online – Auftragswerken) erfolgt abgesichert über DATEV SmartLogin oder DATEV MIdentity Compact.

4. Gewährleistung der Integrität

   Die Weitergabe von Daten erfolgt über abgesichert über VPN, Teamviewer, DATEV Fernbetreuung. Eine Weitergabe auf mobilen Datenträgern erfolgt nicht.
   Die Eingabe und Kontrolle der Daten erfolgen ausschließlich durch mich.

5. Gewährleistung der Verfügbarkeit

   Die Daten werden täglich über eine Sicherungssoftware auf wechselnde Datenträger gesichert. Die Datenträger werden räumlich getrennt verwahrt.
   Der PC ist über eine USV abgesichert.
   Ein Rauchmelder im Büroraum ist vorhanden

6. Gewährleistung der Belastbarkeit der Systeme und Dienste

   Die Widerstandsfähigkeit der IT im Fehlerfall, bei Störungen oder bei hoher Beanspruchung der Systeme und Dienste, die in Zusammenhang mit der Verarbeitung stehen, sind gewährleistet.

7. Die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall kann durch folgende Maßnahmen rasch wiederhergestellt werden:

   Die Verfügbarkeit der Daten wird durch regelmäßige Sicherungen sowie durch die Nutzung von DATEV Unternehmen – Online gewährleistet. DATEV Unternehmen Online funktioniert plattformunabhängig und ist somit über Windows- oder Android-Endgeräte, außer in kurzen Wartungszeiträumen verwendbar.

8. Durch folgende Maßnahmen werden die Bewertung und Evaluierung der Wirksamkeit der o.g. Maßnahmen sichergestellt

   Die TOM werden regelmäßig auf ihre Vollständigkeit überprüft und sofern erforderlich an die Geschäftsprozesse angepasst.