Billomat
Wir ♥ Buchhaltung

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Es findet eine Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen) statt. Dies umfasst die folgenden Maßnahmen:

- Zutrittskontrollsystem: Ausweisleser, Magnetkarte, Chipkarte
- Schlüssel / Schlüsselvergabe
- Türsicherung (elektrische Türöffner usw.)
- Überwachungseinrichtung: Alarmanlage, Video- / Fernsehmonitor

Es findet eine Zugangskontrolle (keine unbefugte Systembenutzung) statt. Dies umfasst die folgenden Maßnahmen:

- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung (z.B. Pausenschaltung)
- Verschlüsselung von Datenträgern und Datensätzen
- Software Firewall
- Anti-Viren Software

Es findet eine Trennungskontrolle / Verwendungszweckkontrolle (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden) statt. Dies umfasst die folgenden Maßnahmen:

- „Interne Mandantenfähigkeit" ist hergestellt
- Kontrolle der Zweckbindung
- Separierung von Datenbanken
- Funktionstrennung: Produktion, Test & Sandboxing

Es findet eine Pseudonymisierung von Datensätzen statt. Dies umfasst die folgenden Maßnahmen:

- Identifizierung von Datensätzen mit IDs anstatt Klarnamen und anderen persönlichen Daten
- Kontrolle der Bestimmbarkeit bei Kumulation von Datensätzen

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

Es findet eine Weitergabekontrolle (kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport) statt. Dies umfasst die folgenden Maßnahmen:

- Prüfung der Rechtmäßigkeit der Weitergabe von Daten
- Protokollierung

Es findet eine Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind) statt. Dies umfasst die folgenden Maßnahmen:

- Protokollierungs- und Protokollauswertungssysteme
- Sicherung von Protokolldaten gegen Verlust oder Veränderung

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

Es findet eine Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust) statt. Dies umfasst die folgenden Maßnahmen:

- Backup-Strategie (online, z.B. Cloud)
- Unterbrechungsfreie Stromversorgung (USV)
- Getrennte Aufbewahrung
- Überspannungsschutz
- Schutz vor Diebstahl
- Virenschutz / Firewall

Es ist eine rasche Wiederherstellbarkeit gegeben. Dies wird durch folgenden Maßnahmen gewährleistet:

- Notfallmanagement inkl. Notfallpläne
- Testen der Wiederherstellungssysteme
- Szenarioübungen (incl. worst-case)

Technische und organisatorische Umsetzung des Rechts auf Löschung, „Recht auf Vergessenwerden“ (Art. 17 DS-GVO)

Folgende Maßnahmen wurden getroffen:

- Einfache Datenlöschung (ohne Überschreiben)
- Schreddern / mechanische Deformierung von Datensätzen auf Papier / DVD / CD oder
- sonstigen Datenträgern
- Automatische Löschung von Datensätzen nach einem festgelegten Ablaufdatum
- Klassifikation der Daten in Schutzklassen
- Protokollierung von Löschvorgängen

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

Die technischen und organisatorischen Maßnahmen wurden zuletzt an folgendem Datum evaluiert:

15.05.2018

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sind im Einsatz. Dies wird durch folgende Maßnahmen unterstützt:

- Datenschutz-Management
- Regelmäßige Datenschutzschulungen
- Auftragskontrolle für Auftagsverarbeiter (AV)
- Eindeutige Vertragsgestaltung

Es liegen folgende Anweisungen, Regeln oder Analysen schriftlich vor:

- Interne Verhaltensregeln
- Risikoanalyse
- Allgemeine Datensicherheitsbeschreibung
- Datensicherheitskonzept
- Auftragskontrolle für Auftagsverarbeiter (AV)
- Es liegt ein Sicherheitszertifikat vor:

  PIO Security GmbH
  c/o Rheingau Founders
  Oranienstraße 185
  10999 Berlin

Hiermit bestätige ich, dass ich die allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach besten Wissen und Gewissen erstellt habe und die gemachten Angaben den tatsächlichen Gegebenheiten in dem von mir vertretenen Unternehmen entsprechen.

Paul-A. Thies	15.05.2018	Paul-A. Thies
Verantwortlicher	Datum	Unterschrift