Anlage zur AV-Vereinbarung:

Allgemeine technische und organisatorische Maßnahmen

gemäß Art. 32 Abs. 1 DSGVO

Firma: Billomat GmbH & Co. KG

Datum der Erstellung: 29.09.2020

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

1.1. Zutrittskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verhindern:

- Alarmanlage
- Automatisches Zutrittskontrollsystem
- Chipkarten / Transpondersysteme
- Manuelles Schließsystem
- Sicherheitsschlösser und einbruchshemmende Türen
- Türen mit Knauf an der Außenseite
- Notausgang nur von innen zu öffnen
- Schlüsselregelung / Schlüsselbuch
- Dongle-Vergaberegelung
- Besucher / Externe in Begleitung durch Mitarbeiter
- Sorgfältige Auswahl des Externen Reinigungsdienstes
- Maßnahmen bei Verlust von Schlüssel / Dongle

1.2. Zugangskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um Unbefugten den Zugang zu den Datenverarbeitungssystemen zu verhindern:

- Login mit Benutzername + Passwort
- Anti-Viren-Software Server
- Anti-Virus-Software Clients
- Firewall - Server
- Firewall - Clients
- Externer Zugang durch Mobile- / Homeoffice (bspw. PC / Laptop)
- Automatische Desktopsperre
- Verschlüsselung bei WLAN-Benutzung (WPA2)
- Richtlinie „Sicheres Passwort“
- Richtlinie „Löschen / Vernichten“
- Richtlinie „Clean desk“
- Allg. Richtlinie Datenschutz und/oder Sicherheit
- Mobile Device Policy
- Anleitung „Manuelle Desktopsperre“

1.3. Zugriffskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um Unbefugten das Lesen, Kopieren, Verändern oder Löschen innerhalb der Datenverarbeitungssysteme zu verhindern:

- Aktenschredder
- Protokollierung von Zugriffen auf Anwendungen in Log-Dateien
- Berechtigungskonzept(e)
- Minimale Anzahl an Administratoren

1.4. Trennungskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um die zu unterschiedlichen Zwecken erhobenen personenbezogenen Daten zu trennen:

- Trennung von Produktiv- und Testumgebung
- Mandantenfähigkeit relevanter Anwendungen
- Bedarfsgerechte Zugriffsberechtigungen der Mitarbeiter
- Festlegung von Datenbankrechten
- Datensätze sind mit Zweckattributen versehen

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a) & Art. 25 Abs. 1 DSGVO)

Die Pseudonymisierung von Datensätzen wird durch folgende Maßnahmen umgesetzt:

- Trennung der Zuordnungsdaten und Aufbewahrung in einem getrennten und abgesicherten System
- Interne Anweisung, personenbezogene Daten möglichst zu pseudonymisieren / anonymisieren

2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

2.1. Weitergabekontrolle

Personenbezogene Daten müssen bei der elektronischen Übermittlung ausreichend geschützt werden, um nicht unbefugt gelesen, kopiert, verändert oder entfernt zu werden. Folgende technische und organisatorische Maßnahmen haben wir hierfür ergriffen:

- Email-Verschlüsselung
- Bereitstellung von Tunnelverbindungen (VPN)
- Bereitstellung verschlüsselter Verbindungen
- Elektronische Signaturverfahren
- Protokollierung der Zugriffe und Abrufe in Log-Dateien

- Weitergabe in anonymisierter oder pseudonymisierter Form
- Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen

2.2. Eingabekontrolle

Zur Kontrolle, ob und von wem personenbezogene Daten in das Datenverarbeitungssystem eingegeben, geändert, gesperrt oder gelöscht werden, setzen wir folgende Maßnahmen ein:

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Softwareliste mit Datenverarbeitungsprogrammen
- Vergabe individueller Benutzernamen
- Berechtigungskonzept mit Vergabe von bedarfsgerechten Benutzerrechten
- Sichere Aufbewahrung von Dokumenten in Papierform
- Löschkonzept

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO)

Zur Gewährleistung der Verfügbarkeit personenbezogener Daten gegen zufällige oder mutwillige Zerstörung oder Verlust, setzen wir folgende Maßnahmen ein:

- Regelmäßige Archivierung / Backup der Daten
- Backup-Konzept (online) (ausformuliert)
- Recovery-Konzept (ausformuliert)
- Kontrolle des Sicherungsvorgangs
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

4. Verfahren zur regelmäßigen Überwachung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit d) DSGVO & Art. 25 Abs. 1 DSGVO)

Datum der Evaluierung der technischen und organisatorischen Maßnahmen:
28.09.2020

4.1. Datenschutz-Management

Zur Gewährleistung des Datenschutzes in unserem Unternehmen setzen wir folgende Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung ein:

- Software-Lösungen für Datenschutz-Management im Einsatz
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- Interner / externer Datenschutzbeauftragter, (wenn ja, bitte angeben):
- Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- "Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach"
- Formalisierter Prozess zur Bearbeitung von Auskunfts-, Löschungs- und Datenübertragungsanfragen seitens Betroffener

4.2. Incident-Response-Management (gemäß Art. 33 DSGVO)

Im Falle des Erkennens und der Meldung von Datenschutzverletzungen setzen wir folgende Maßnahmen ein:

- Einsatz von Firewall und regelmäßige Aktualisierung
- "Einsatz von Spamfilter und regelmäßige Aktualisierung"
- "Einsatz von Virenscanner und regelmäßige Aktualisierung"
- Intrusion Prevention System (IPS)
- "Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen "
- "Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen"
- Einbindung von DSB in Sicherheitsvorfällen und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen
- Formaler Prozeß und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3. Datenschutzfreundliche Voreinstellungen

Im Rahmen datenschutzfreundlicher Voreinstellungen (Art. 25 Abs. 2 DSGVO) setzen wir folgende Maßnahmen ein:

- Datenminimierung und Zweckbindung
- Einfache (technische) Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

4.4. Auftragskontrolle (Outsourcing)

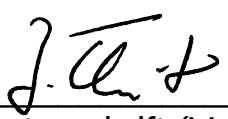
Im Rahmen des Outsourcings der Verarbeitung personenbezogener Daten durch Auftragsverarbeiter setzen wir für die Gewährleistung eines angemessenen Schutzniveaus folgende Maßnahmen ein:

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- "Auswahl des Auftragnehmers unter Sorgfalts-Gesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)"
- "Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln"
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen der Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- "Bei längerer Zusammenarbeit:
  Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus"

Hiermit bestätige ich, dass ich die Beschreibung der technischen und organisatorischen Maßnahmen nach bestem Wissen und Gewissen erstellt habe und die angegebenen Maßnahmen dem tatsächlichem Stand in dem von mir vertretenen Unternehmen entspricht.

29.09.2020, Nürnberg

Datum, Ort



Unterschrift (Verantwortlicher)