Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

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

Informationen zum Standort von Datenverarbeitungsanlagen und Rechenzentren

Daten der Billomat GmbH & Co. KG , die im Auftrag verarbeitet werden, werden ausschließlich im AWS-Rechenzentrum von Amazon in Frankfurt gespeichert.
Dort sind folgende Maßnahmen zur Zutrittskontrolle getroffen:

Das AWS-Rechenzentrum und die dort verwendeten Systeme sind in unscheinbaren Gebäuden untergebracht, die von außen nicht sofort als Rechenzentrum zu erkennen sind.

Das Rechenzentrum selbst ist durch physische Sicherheitsmaßnahmen geschützt, um den unberechtigten Zutritt sowohl weiträumig (z. B. Zaun, Wände) als auch in den Gebäuden selbst zu verhindern.

Der Zutritt zum Rechenzentrum wird durch elektronische Zugangskontrollen verwaltet und durch Alarmanlagen gesichert, die einen Alarm auslösen, sobald die Tür aufgebrochen oder aufgehalten wird.

Die Zutrittsberechtigung wird von einer berechtigten Person genehmigt und innerhalb von 24 Stunden entzogen, nachdem ein Mitarbeiter- oder Lieferantendatensatz deaktiviert wurde.

Alle Besucher müssen sich ausweisen und registrieren und werden stets von berechtigten Mitarbeitern begleitet.

Zutritt zu sensiblen Bereichen wird durch Videoüberwachung überwacht.
Ausgebildete Sicherheitskräfte bewachen das AWS-Rechenzentrum und die unmittelbare Umgebung davon 24 Stunden am Tag, 7 Tage die Woche.

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.)
- Gebäudesicherung (Zäune, Pforten)
- Werkschutz, Pförtner
- Alarmsicherung
- Schließsystem
- Tragepflicht von Ausweisen / Ausweissystem

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

- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Two-Factor Authentication wird eingesetzt
- Automatische Sperrung (z.B. Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes pro User
- Verschlüsselung von Datenträgern und Datensätzen
- Software Firewall
- Hardware Firewall
- Einsatz von zentraler Administrations-Software für mobile Endgeräte (z.B. zum externen Sperren und Löschen von Daten)

- Anti-Viren Software
- Gehäuseschutz
- Schutzmaßnahmen zur Sicherung bei Nutzung von eigenen Geräten durch Mitarbeiter (z.B. Fernlöschung oder -sperrung)

Es findet eine Zugriffskontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems) statt. Dies umfasst folgende Maßnahmen:

- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte (Profile, Rollen, Transaktionen und Objekte)
- Benutzerkennung mit Passwort
- Ausgabe von Zertifikaten zur Authentifizierung
- Virenschutz / Firewall
- Einschränkung der Nutzung von mobilen Datenträgern / sonstigen Geräten
- Regelmäßige Updates der Systeme
- Klassische Rollen(Auswertungen, Kenntnisnahme, Veränderung, Löschung)
- Protokollierung von Zugriffen in Logs

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

- Kontrolle der Zweckbindung
- Separierung von Datenbanken
- Separierung von Tables in Datenbanken
- Funktionstrennung: Produktion, Test & Sandboxing

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

- Umwandeln von Identifiaktionsmerkmalen in zufällige Zeichenfolgen (Z.B. Namen und Geburtsdaten)
- Identifizierung von Datensätzen mit IDs anstatt Klarnamen und anderen persönlichen Daten
- Keine Eingabemöglichkeiten von nicht psedonymen Daten (z.B. Angabe von Nicknames statt Klarnamen)
- Kontrolle der Bestimmbarkeit bei Kumulation von Datensätzen
- Automatische Pseudonymisierungsverfahren bei neuen 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:

- Verschlüsselung / Tunnelverbindung
- Prüfung der Rechtmäßigkeit der Weitergabe von Daten
- Regelungen zum datenschutzkonformen Vernichten von Datenträgern
- Elektronische Signatur
- Protokollierung
- Transportsicherung
- Sorgfältige Auswahl von Transportpersonal und –fahrzeugen beim physischen Transport von Daten

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:

- Dokumentenmanagement, Dokumentenlenkung
- Protokollierungs- und Protokollauswertungssysteme
- Protokollierungs- und Protokollauswertungssysteme (3 Monate Revisionssicher)
- Plausibilitätskontrollen
- 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 (offline)
- 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
- Incident Management
- 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)
- Implementierung von Fernlöschung, z.B. auf mobilen Endgeräten
- Zerstörung von Datenträgern vor der Entsorgung
- Schreddern / mechanische Deformierung von Datensätzen auf Papier / DVD / CD oder sonstigen Datenträgern
- Entmagnetisierung von physischen Datenträgern (Festplatten / Datenbändern)
- Automatische Löschung von Datensätzen nach einem festgelegten Ablaufdatum
- Sorgfältige Auswahl von Entsorgungsdienstleistern
- Umsetzung der DIN-EN 15713 “Sichere Vernichtung von vertraulichen Unterlagen - Verfahrensregeln”

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:

16.08.2019

Die dokumentierten Maßnahmen sind unter Berücksichtigung des aktuellen Standes der Technik, angemessener Implementierungs- und Wartungskosten, der Art, des Umfangs und der Zwecke der Verarbeitung, sowie unter Abwägung der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen wie folgt geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:

Sie sind geeignet.

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
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle für Drittstaaten (BCR)
- Auftragskontrolle für Auftagsverarbeiter (AV)
- Eindeutige Vertragsgestaltung
- Vorabüberzeugungspflicht

Es liegen folgende Anweisungen, Regeln oder Analysen schriftlich vor:

- Interne Verhaltensregeln
- Risikoanalyse
- Allgemeine Datensicherheitsbeschreibung
- Datensicherheitskonzept
- Auftragskontrolle für Drittstaaten (BCR)
- Auftragskontrolle für Auftagsverarbeiter (AV)
- Wiederanlaufkonzept / Wiederherstellungskonzept

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.

....

Verantwortlicher	Datum	Unterschrift

Rechtliche Hinweise und Bedingungen der Nutzung

Die Generatoren der DeinData GmbH stellen keine rechtliche Beratung dar und können diese auch nicht ersetzen, Ihre Angaben werden lediglich automatisiert mittels Software umgesetzt.

Wir weisen Sie darauf hin, dass eine rechtliche Beratung oder Prüfung nicht Bestandteil unserer Leistung ist und Sie hierfür einen Fachmann beauftragen müssen. Wir stellen Ihnen lediglich unsere Software bzw. unsere Vorlage zu Informationszwecken zur Verfügung, überprüfen jedoch nicht, ob alle für Ihr Unternehmen relevanten Angaben in unserer Software/Vorlage zur Genüge berücksichtigt oder angegeben werden. Sie haben sich vor der Nutzung unseres Dienstes selbst darüber zu informieren, welche Angaben Sie für Ihr Unternehmen benötigen bzw. welche Angaben notwendig sind. Eine Überprüfung Ihrer generierten Dokumente auf Vollständigkeit und Richtigkeit erfolgt nicht. Wir stellen Ihnen lediglich unsere Software bzw. die Vorlage als technische Hilfeleistung zur Verfügung. Ein aus der Durchführung des Vertrages bzw. der Verwertung unserer Informationen resultierender Erfolg z.B. im Sinne einer rechtlichen Absicherung ist ausdrücklich nicht geschuldet und kann auch nicht garantiert werden, da Sie allein für die von Ihnen erstellten Dokumente verantwortlich sind. Es wird ausdrücklich auf die Beratung bzw. Prüfung durch einen Fachmann verwiesen, der eine individuelle Anpassung für Sie vornehmen kann.

Der Inhalt unserer Software und der Vorlage dient ausschließlich zu Informationszwecken. Die Daten stammen aus Quellen, die wir für vertrauenswürdig halten und zum jeweiligen Zeitpunkt in den öffentlich zugänglichen Medien oder anderen Informationsquellen von jedermann zu erlangen wären. Es kann und wird insoweit aber keine Gewähr für die Richtigkeit, Zuverlässigkeit, Genauigkeit und Vollständigkeit der Informationen übernommen. Insbesondere für eine rechtliche Prüfung bzw. Beratung haben Sie einen Fachmann zu beauftragen.

Datum: 16/08/2019

- Ich habe die Hinweise gelesen und stimme den Bedingungen zu.