Technisch-Organisatorische Massnahmen

1. Einleitung

Das vorliegende Dokument beschreibt in generischer Form die technischen und organisatorischen Massnahmen (nachfolgend auch «TOM»), welche der Auftragnehmer in Zusammenhang mit der Erfüllung der vertraglichen Verpflichtungen in Bezug auf personenbezogene Daten des Auftraggebers auf unter der alleinigen vertraglichen und operativen Kontrolle des Auftragnehmers stehenden Informatiksystemen (gemeinsam als «Auftragnehmer-Systeme» bezeichnet) und/oder Räumlichkeiten anwendet.

Die TOM beziehen sich nicht auf Installationen, Instanzen, Servers, Räumlichkeiten etc., welche dem Auftraggeber gehören oder für welche der Auftraggeber direkt mit Drittparteien Verträge abgeschlossen hat. Diesfalls liegt die Verantwortung über die TOM beim Auftraggeber.

2. Beschreibung

2.1. Ausgangslage

Der Auftraggeber überlässt dem Auftragnehmer im Rahmen des Hauptvertrages in seinem eigenen Ermessen und in seinem Auftrag Personendaten zur Bearbeitung von Kundenanfragen, Versand von Benachrichtigungen und Erinnerungen über Aktivitäten in easydoo, Versand von Transaktions-E-Mails wie z.B. Zahlungsaufforderung, temporäre Passwortangaben etc.

Der Gegenstand und die Dauer der Verarbeitung der personenbezogenen Daten des Auftraggebers sind in der Vereinbarung festgelegt.

2.2. Kategorie der betroffenen Daten

Bei der zur Bearbeitung überlassenen Daten kann es sich insbesondere um folgende Arten von Personendaten handeln:

- Persönliche Informationen wie Vorname, Nachname, Kontaktdaten (wie E-Mailadresse, Telefonnummer, Adresse, Rechnungsaderesse etc.) sowie Benutzerinformationen Logindaten, Kundennummer, Nutzerverhalten
- Technische Informationen wie IP-Adresse, Geräteinformationen etc.
- Workspace-Daten: «Workspace-Daten» sind personenbezogene Daten oder andere Informationen, die Nutzer direkt in easydoo eingeben, innerhalb von easydoo erstellen, an easydoo senden oder ihnen easydoo als Services zur Verfügung stellt.

2.3. Kategorie der betroffenen Personen

Bei der zur Bearbeitung überlassenen Personendaten kann es sich insbesondere um folgende betroffene Personen (welche natürliche Personen sind) handeln:

- Mitarbeitende oder andere Vertragspartner des Auftraggebers
- andere speziell zu easydoo eingeladene Nutzer wie Geschäftspartner oder Kunden des Auftraggebers

3. Technische Organisatorische Massnahmen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Auftragsverarbeiter nachfolgend dargelegte technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

3.1. Vertraulichkeit

3.1.1. Zutrittskontrolle

Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

☑ Gesicherter Eingang (z.B. abschliessbare Türen)	☑ Umsetzung einer Schlüsselregelung
☑ Festlegung befugter Personen inkl. Umfang der jeweiligen Befugnisse	☑ Sorgfältige Auswahl von Reinigungspersonal mit entsprechenden Zutrittsberechtigungen
☑ Existenz von Regelungen für Unternehmensexterne	☑ Sorgfältige Auswahl von Reinigungspersonal mit entsprechenden Zutrittsberechtigungen
☑ Begleitung von Besuchern im Unternehmensgebäude	☑ klare Vorschriften und Bestimmungen was Homeoffice Bedingungen anbelangt, Homeoffice-Regelungen in den Allgemeinen Anstellungsbedingungen vorhanden.

3.1.2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme und die unbefugte Systemnutzung sind zu verhindern. Technische und organisatorische Massnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung

☑ Angemessener Passwortschutz (Verhaltensregeln, verschlüsselte Archive)	☑ Verschlüsselung von Datenträgern
☑ Automatische Sperrmechanismen	☑ Konzeption und Implementierung eines - Berechtigungskonzept für Endgeräte (Rechner) - Berechtigungskonzept für Software/Systeme
☑ Zwei-Faktor-Authentifizierung	☑ Identifikation und Berechtigungsprüfung eines Benutzers
☑ Implementierung eines Systems zur Verwaltung von Benutzeridentitäten	☑ Monitoring der Zugangsversuche mit Reaktion auf Sicherheitsvorfälle
☑ Festlegung und Kontrolle der Zugangsbefugnisse	☑ Spezielle Sicherheitssoftware (z. B. Anti-Malware, VPN oder Firewall)
☑ Existenz von Regelungen für Unternehmensexterne	

3.1.3. Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

☑ Zugriffsbeschränkungen (gemäss „Need-to-Know“ und „Least Privilege“)	☑ Standardprozess für Berechtigungsvergabe
☑ Protokollierung von Zugriffen	☑ Sichere Aufbewahrung von Speichermedien
☑ Periodische Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten	☑ Datenschutzgerechte Wiederverwendung von Datenträgern
☑ Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	☑ Clear-Desk/Clear-Screen Policy
☑ Berechtigungs- und Rollenkonzept für Applikationen	☑ Umsetzung von Regelungen zur Zugriffs- und Benutzerberechtigung
☑ Funktionsbegrenzung (funktional/zeitlich	☑ Protokollierung - Protokollierung des lesenden Zugriffs - Protokollierung des schreibenden Zugriffs - Protokollierung von unberechtigten Zugriffsversuchen - Anlassbezogene Auswertung
☑ Umsetzung von Regelungen zur Löschung von Daten	☑ Umsetzung von Regelungen zum Umgang mit elektronischen Speichermedien
☑ Umsetzung von Regelungen zur Entsorgung von Speichermedien	

3.1.4. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind getrennt zu verarbeiten. Massnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

☑ Mandantenfähigkeit: - Physische Trennung - Trennung auf Systemebene - Trennung auf Datenebene	☑ Trennung von Produktiv- und Testsystemen
☑ Dokumentation der Funktionstrennung	☑ Vorhandensein von Richtlinien und Arbeitseinweisungen
☑ Vorhandensein von Verfahrensdokumentationen	

3.1.5. Pseudonymisierung

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

☐ Ja	☑ Nein

3.1.6. Klassifikationsschema für Daten

Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

☑ Ja	☐ Nein

3.2. Datenintegrität

3.2.1. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

☑ Für elektronische Übertragungen: Verschlüsselung der Datenübermittlung

3.2.2. Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

☑ Protokollierung der Eingaben und Überprüfung der Protokolle	☑ organisatorisch festgelegte Zuständigkeiten für die Eingabe
☑ Sonstiges - Protokollierung der Eingabe, Änderung und Löschung von Daten auf Dateiebene (Fileserver) - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen - Rechtevergabe auf Basis eines Berechtigungskonzepts - Erstellung einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert, und gelöscht werden - Eingeschränkte Zugriffsrechte auf erstellte Protokolldaten	

3.3. Verfügbarkeit und Belastbarkeit

3.3.1. Verfügbarkeits-/Belastbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust. Die Verarbeitung der Daten soll tolerant gegenüber Störungen und Fehlern sein.

☑ Backup-Strategie (online/offline; on-site/off-site)	☑ grosszügig vorhandene Netzwerkkapazität
☑ Virenschutz/Anti-Malware/Anti-Ransomware	☑ Firewall
☑ Meldewege und Notfallpläne	☑ Security Checks auf Infrastruktur- und Applikationsebene, teilweise sichergestellt.
☑ Regelmässige Kontrolle des Systemzustands (Monitoring)	☑ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
☑ Funktionsfähige physische Schutzeinrichtungen (Brandschutz, Energie: USV, Klima)	☑ Kurzfristige Wiederherstellbarkeit des normalen Systemzustands
☑ Backup- und Wiederanlaufkonzept (regelmässige Datensicherungen): offline online onsite offsite	☑ Vorhandensein von redundanten IT-Systemen (z. B. Server, Speicher)
☑ Replizierbarkeit virtueller Maschinen	☑ Funktionsfähige physische Schutzeinrichtungen (Brandschutz, Energie: USV, Klima)

3.4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

3.4.1. Datenschutz-Management

☑ Schriftlich fixierte Regelungen der Verantwortlichkeiten für Datenschutz	☑ Existenz eines angemessenen Informationssicherheitsmanagements
☑ Regelmässige Aufklärung und Sensibilisierung der Mitarbeiter und Führungskräfte	☑ Auftragskontrolle, um weisungsgemässe Auftragsverarbeitung zu gewährleisten - Strikte Einhaltung der im vorliegenden Auftragsverarbeitungs-Vertrag festgeschriebenen Vereinbarungen und diesbezügliche Überprüfungen - Konzept dahingehend, wie die regelmässige Kontrolle des Auftragsprozesses erfolgt (z. B. Vorlage von Self-Assessments, Vorlage der Verträge mit Unterauftragnehmern, Durchführung von Kontrollen bei Subunternehmern durch den Auftragnehmer) - Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers, z. B. anhand: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrolle einschliesslich regelmässiger Mitarbeiter-Schulungen.

easydoo AG
Moosholzzelg 9
CH-9322 Egnach