Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO
POS Applikationen

zwischen

Der im Händlervertrag genannte Händler

– Verantwortlicher - nachfolgend „Auftraggeber“ genannt –

und der

Unzer Luxembourg S.A., 18-20 rue Gabriel Lippmann, L-5365 Munsbach

– nachfolgend „Unzer“

– nachfolgend einzeln ggf. “Partei” und/oder zusammen nachfolgend „Parteien“ genannt –

1. Gegenstand und Dauer des Vertrages

1.1 Der Gegenstand des Vertrages ergibt sich aus dem zwischen den Parteien getroffenen Hauptvertrag, auf den hier verwiesen wird (im Folgenden „**Händlervertrag**“).

1.2 Die Dauer dieses Vertrages („**Laufzeit**“) entspricht der Laufzeit des Händlervertrages.

1.3 Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

2. Weisungsgebundene Verarbeitung, Konkretisierung des Vertragsinhalts,

2.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers (Auftragsverarbeitung), sofern er nicht durch das Recht der Union oder deutsches Recht hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Weisungen des Auftraggebers sind grundsätzlich abschließend in den Bestimmungen dieser Vereinbarung zusammen mit dem Händlervertrag festgelegt und dokumentiert.

Weisungen werden vom Auftraggeber grundsätzlich in Textform erteilt; mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.
Die weisungsbefugten Personen sowie die zur Entgegennahme von Weisungen befugten Personen werden die Parteien sich gegenseitig nach Vertragsschluss in Textform nennen.

2.2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen ergeben sich aus **Anlage 1**.

3. Technische und organisatorische Maßnahmen

3.1 Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DSGVO zum Schutz der personenbezogenen Daten. Ein Verzeichnis der derzeitigen technischen und organisatorischen Maßnahmen des Auftragnehmers ergibt sich aus **Anlage 3**.

3.2 Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, sofern sie weiterhin den gesetzlichen Anforderungen genügen und dies nicht zu einer Herabsetzung des initial vereinbarten Schutzniveaus führt.

4. Rechte von betroffenen Personen

Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

5.1 Der Auftragnehmer gewährleistet die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.

g) Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Auftragsverarbeitung bekannt wird, meldet er diese dem Auftraggeber unverzüglich.

h) Soweit der Auftragnehmer mit der Verarbeitung von Daten für den Auftraggeber betraut ist, unterstützt der Auftragnehmer den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang auf Anfrage relevante Informationen zur Verfügung.

i) Soweit der Auftraggeber im Zusammenhang mit der Auftragsverarbeitung zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

6. Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Nimmt der Auftragnehmer im Rahmen eines Unterauftragsverhältnisses die Dienste eines weiteren Auftragsverarbeiters („Unterauftragnehmer“) in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrages, der schriftlich abzufassen ist, was auch in einem elektronischen Format erfolgen kann, dieselben Datenschutzpflichten auferlegt, die in dieser Datenschutzvereinbarung zur Auftragsverarbeitung festgelegt sind; dabei müssen insbesondere hinreichende Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

6.3 Der Auftraggeber erteilt dem Auftragnehmer hiermit seine allgemeine Genehmigung, Unterauftragnehmer in Anspruch zu nehmen. Die zum Zeitpunkt des Vertragsschlusses in Anspruch genommenen Unterauftragnehmer sind in **Anlage 3** aufgeführt.

6.4 Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragnehmers, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Die Parteien vereinbaren, bei jedweden Bedenken des Auftraggebers diese im Geiste einer vertrauensvollen Zusammenarbeit angemessen gemeinsam zu erörtern und möglichst auszuräumen. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund, erhoben werden. Ein wichtiger Grund liegt insbesondere vor, wenn die beabsichtigte Änderung zu einem Verstoß gegen datenschutzrechtliche Anforderungen führen würde. Soweit der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Information. Erhebt der Auftraggeber rechtzeitig Einspruch, so unterbleibt die beabsichtigte Änderung insoweit und der Auftragnehmer ist berechtigt, den zugrundeliegenden Händlervertrag mit einer Frist von drei Monaten zu kündigen.

6.5 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.6 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

7. Internationale Datentransfers

Soweit die Parteien nicht ausdrücklich etwas anderes vereinbaren, findet die Verarbeitung durch den Auftragnehmer grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer nur dann gestattet, die Daten unter Einhaltung der Bestimmungen dieses Vertrages auch außerhalb des EWR zu verarbeiten, wenn die Voraussetzungen der Art. 44 – 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt. In jedem Fall einer Verarbeitung im Drittland gewährleistet der Auftragnehmer die Einhaltung der Voraussetzungen der Art. 44 – 49 DSGVO. Für den Einsatz von Unterauftragsverarbeitern sind zusätzlich die Voraussetzungen und Informationspflichten nach Ziffer 6 zu beachten.

8. Kontrollrechte des Auftraggebers

8.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig (d.h. mindestens zwei Wochen vorher) anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers zu überzeugen.

8.2 Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen nachzuweisen.

8.3 Der Auftragnehmer ist unbeschadet der Rechte des Auftraggebers nach den Ziffern 8.1 und 8.2 nicht verpflichtet, rechtswidrig Informationen zu offenbaren oder Geschäftsgeheimnisse offenzulegen. Der Auftraggeber ist insbesondere nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten, zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die Überprüfungszwecke sind, zu erhalten.

8.4 Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

8.5 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen.

8.6 Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Überprüfung, hat der Auftraggeber den Dritten schriftlich auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber ihm die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

9. Löschung und Rückgabe von personenbezogenen Daten

9.1 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung des Händlervertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

9.2 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Eine Unterzeichnung dieses Auftragsverarbeitungsvertrages ist nicht notwendig.

Dieser Vertrag wird mit Unterzeichnung des Händlervertrages Anhang zum Händlervertrag.

Anlagen

Anlage 1	Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen
Anlage 2	Liste der Unterauftragsverarbeiter
Anlage 3	Technische und organisatorische Maßnahmen

Anlage 1 –

Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen

1. Gegenstand des Auftrags und Zweck der Datenverarbeitung

Gegenstand des Auftrags ist die Bereitstellung von cloudbasierten Softwareapplikationen des Auftragnehmers und die damit einhergehende Verarbeitung personenbezogener Daten zu den im Händlervertrag beschriebenen Zwecken (**Zweck der Datenverarbeitung**).

Bei Nutzung einiger Funktionen durch den Auftraggeber bzw. dessen Mitarbeiter und/oder Endkunden sowie im Rahmen des damit verbundenen Hostings werden abhängig von der jeweiligen Nutzungshandlung personenbezogene Daten erhoben, erfasst, organisiert, geordnet, gespeichert, abgefragt, übermittelt und verändert bzw. ggf. gelöscht (**Art der Datenverarbeitung**).

2. Art der personenbezogenen Daten (Datenarten)

Folgende Datenarten sind Gegenstand dieses Auftrags:

- Kontaktdaten- und Bestandsdaten wie Name, Vorname, Anschrift, E-Mail und Telefonnummer;
- Geburtsdatum;
- Daten zu Dienstleistungs- und Produktnutzung (nur Endkunde);
- IP-Adresse (nur Endkunde);
- Transaktionszeitpunkt (nur Endkunde);
- Reservierungszeitpunkt / Terminart (nur Endkunde);
- Technische Merkmale wie Geräteinformationen (nur Endkunde);
- Mitarbeiterverwaltung (nur Mitarbeiter);
  - Notfallkontaktdaten (nur Mitarbeiter);
  - Anwesenheitszeiten (nur Mitarbeiter);
  - Profilbilder (nur Mitarbeiter);
  - Berufliche Stellung (nur Mitarbeiter)

3. Kategorien betroffener Personen

Folgende Kategorien betroffener Personen sind Gegenstand des Auftrags:

- Händler des Auftragnehmers,
- Mitarbeiter (z.B. Angestellte, Auszubildende, Freelancer) von Händlern des Auftragnehmers,
- Endkunden der Händler

Anlage 2 – Unterauftragsverarbeiter

Unterauftragnehmer	Anschrift / Land	Leistung
Tillhub GmbH	Schöneberger Straße 21A 10963 Berlin, Deutschland	Bereitstellung der cloudbasierten POS-Applikationen (einschließlich Fiskalisierung) sowie des Tillhub-Dashboards (einschließlich CRM, Staff-Management und Terminreservierung) jeweils unter Einbindung der • fiskaly GmbH (Stutterheimstr. 16-18, 20e, 1150 Wien, Österreich) für die Fiskalisierungsleistungen; • Google Cloud EMEA limited (70 SIR JOHN ROGERSON'S QUAY Dublin D02 R296 CO DUBLIN) zum Hosting (Datenbank, POS Go-Kassensoftware und POS Go-Dashboard); sowie der • Unzer Group GmbH (Schöneberger Straße 21A 10963 Berlin) zur Bereitstellung des zur Reservierungsbestätigung genutzten SMS-Services (erbracht von der Link Mobility Austria GmbH als Unterauftragsverarbeiter der Unzer Group GmbH)

Anlage 3 – Technische und organisatorische Maßnahmen

1. Zielsetzung

- Gegenstand dieses Dokuments sind die technischen und organisatorischen Maßnahmen, die zum Schutz personenbezogener Daten gemäß der DSGVO getroffen werden
- Die Schutzziele sind gemäß Art. 32 DSGVO definiert. Die in diesem Dokument beschriebenen Maßnahmen zielen insbesondere darauf ab, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten zu gewährleisten
- Zur Ermittlung eines angemessenen Schutzniveaus wird ein risikobasierter Ansatz verwendet, der Ursache, Art, Eintrittswahrscheinlichkeit und Auswirkungen potenzieller Bedrohungen berücksichtigt

2. Physische Zutrittskontrolle

Die im Folgenden beschriebenen Maßnahmen dienen dazu, Unbefugten den Zugang zu Bereichen, Geräten und Anlagen, in denen personenbezogene Daten verarbeitet, aufbewahrt oder gespeichert werden, zu verwehren.

Büroräume

- Schlüssel werden nur an befugte Personen ausgegeben und nach deren Ausscheiden aus dem Unternehmen wieder eingezogen
- Es existiert ein System zur Verwaltung der Schlüssel/Zugangsmittel
- Alle Fenster sind außerhalb der Geschäftszeiten stets geschlossen
- Eine “clean desk policy” ist vorhanden

IT Räume (Serveräume, Datenzentralen)

- Es existieren dokumentierte und kommunizierte Regeln für die physische Zugangskontrolle und für Sicherheitsbereiche
- Für die Zugangskontrolle gilt der Grundsatz „least privilege“: Zugang nur bei Bedarf und mit Genehmigung
- Schlüssel werden nur an berechtigte Personen ausgegeben
- Zutrittsrechte können je nach Standort individuell zeitlich begrenzt werden
- Bei Verlust eines Zugangstokens wird dieser individuell gesperrt
- Es existiert ein System zur Verwaltung der Schlüssel bzw. der Zugangstoken
- Um den Zugang und das Verlassen von externen Personen zu protokollieren werden Besucherlisten verwendet
- Die Türen zu den IT-Räumen sind bei Abwesenheit immer geschlossen
- In den von außen zugänglichen Räumen im Erdgeschoss und im Untergeschoss sind die Fenster gesondert gesichert (vergitterte Fenster, Alarmanlage usw.)
- Eine Schließanlage für den Serverraum ist vorhanden
- Das Rechenzentrum ist kameraüberwacht

3. Zugangskontrolle und Verschlüsselung

Die im Folgenden beschriebenen Maßnahmen sollen die nicht autorisierte Nutzung von Datenverarbeitungssystemen durch den Einsatz von Zugangskontrollen verhindern.

- Das Authentifizierungsverfahren basiert auf dem Erfordernis des Schutzes der Informationen
- Der Zugang zu den Datenverarbeitungssystemen ist mindestens durch einen Benutzernamen und ein Passwort geschützt
- Angemessene Richtlinien für die Passwortnutzung sind implementiert
- Wenn möglich, werden für Datenverarbeitungssysteme Nutzerkonten eingerichtet (keine Gruppenkonten)
- Systeme mit sehr hohem Schutzbedarf werden durch Multifaktor-Authentifizierung geschützt

4. Logische Zugangskontrolle

Die im Folgenden beschriebenen Maßnahmen dienen dazu, den Zugriff auf die Daten zu regeln und einzuschränken (z.B. auf der Grundlage eines Rollen- und Rechtekonzepts).

- Es existiert eine Richtlinie, die die Vergabe von Berechtigungen für Benutzer und Administratoren regelt
- Geeignete Datenschutzcontainer zur Verhinderung unbefugter Entnahmen sind im Einsatz
- Papierausdrucke werden mit einem Aktenvernichter entsorgt

5. Trennungskontrolle

Die im Folgenden beschriebenen Maßnahmen sollen sicherstellen, dass unvereinbare Rollen getrennt und dass Daten oder Systeme entsprechend den jeweiligen Sicherheitsanforderungen getrennt verarbeitet oder betrieben werden.

- Rollen und Verantwortlichkeiten sind definiert, festgelegt und kommuniziert
- Wenn möglich, wird die Speicherung von personenbezogenen Daten vermieden
- Referenzdaten und Originaldaten (z.B. bei anonymisierten oder pseudonymisierten Daten) werden getrennt gespeichert. Wenn dies nicht möglich ist, werden technische oder organisatorische Ersatzmaßnahmen mit gleichem Schutzniveau eingesetzt
- Es erfolgt eine Trennung von Test- und Produktionssystemen

6. Weitergabekontrolle

Die im Folgenden beschriebenen Maßnahmen sollen das unbefugte Lesen, Kopieren, Verändern oder Entfernen personenbezogener Daten während der Übermittlung (elektronisch, analog oder auf Datenträgern) verhindern und die Rückverfolgbarkeit von Datenübertragungen sicherstellen.

- Interne Netze werden gegen Zugriffe von außen durch Firewalls abgeschottet
- Die Kommunikation zu Diensten im internen Netzwerk und im Internet erfolgt gemäß Art. 32 Abs. 1 lit. a) DSGVO über verschlüsselte Verbindungen
- Personenbezogene Daten werden, soweit möglich, pseudonymisiert, bevor sie übertragen und verarbeitet werden
- Kreditkartendaten werden gemäß den PCI-DSS-Anforderungen unkenntlich gemacht
- Personenbezogene Daten werden nur nach Unterzeichnung einer Geheimhaltungsvereinbarung an externe Parteien weitergegeben
- Es bestehen Vereinbarungen und Dokumentationen für die Datenübermittlung zwischen der Organisation und externen Parteien

7. Eingabekontrolle

Die im Folgenden beschriebenen Maßnahmen dienen der Absicherung von Eingaben sowie der nachträglichen Überprüfbarkeit, ob und von wem (personenbezogene) Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Eingaben, Änderungen und Löschungen in Datenverarbeitungssystemen werden protokolliert
- Protokolldaten werden für einen festgelegten Zeitraum aufbewahrt

8. Verfügbarkeits- und Belastbarkeitskontrolle

Die im Folgenden beschriebenen Maßnahmen dienen dazu die Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicherzustellen (Art. 32 Abs. 1 lit. b) DSGVO). Des Weiteren dienen sie dazu, die Verfügbarkeit der personenbezogenen Daten nach einem Sicherheitsvorfall oder einem Notfall rasch wieder gewährleisten zu können (Art. 32 Abs 1 lit. c) DSGVO).

- Spezielle Schutzsoftware (Antivirensoftware usw.) wird verwendet.
- Die Daten werden entsprechend ihres Schutzbedarfes gesichert
- Sensible Daten werden besonders gesichert aufbewahrt
- Sicherungs- und Wiederherstellungskonzepte sind vorhanden

9. Verarbeitungskontrollen

Es wird sichergestellt, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur gemäß den Anweisungen des Auftraggebers verarbeitet werden können.

- Die Datenverarbeitung erfolgt auf der Grundlage von Auftragsverarbeitungsverträgen (AVV) gemäß Art. 28 Abs. 3 S. 1 DSGVO
- Unterauftragsverarbeiter werden sorgfältig unter Berücksichtigung der Anforderungen an Informationssicherheit und Datenschutz ausgewählt
- AVV mit Unterauftragsverarbeitern unterschreiten nicht das Schutzniveau der Verträge zwischen der Unzer POS GmbH und dem verantwortlichen Auftraggeber

10. Überprüfung, Bewertung und Evaluierung

Die im Folgenden beschriebenen Maßnahmen dienen dazu, die Wirksamkeit der technischen, organisatorischen und administrativen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d) DSGVO) regelmäßig zu überprüfen, zu bewerten und zu evaluieren, um Verbesserungen und Anpassungen zu initiieren.

- Alle Mitarbeiter (auch Externe) sind zur Wahrung des Datengeheimnisses bzw. zur Vertraulichkeit verpflichtet und werden regelmäßig im Bereich des Datenschutzes geschult.
- Es gibt klare Verantwortlichkeiten für die Bearbeitung von Sicherheitsvorfällen.
- Sicherheitsvorfälle werden dokumentiert und ausgewertet.
- Ein qualifizierter und zertifizierter Datenschutzbeauftragter ist benannt.
- Es erfolgen interne Audits durch abteilungsexterne, qualifizierte Mitarbeiter.
- Es erfolgen externe Audits durch akkreditierte Prüfer
- Es werden regelmäßig Penetrationstests durch Dritte durchgeführt.
- Für alle IT-Anwendungen sind Applikationseigner festgelegt, die für die Behebung von Schwachstellen in ihrer Anwendung zuständig sind.
- Es existiert eine IT-Nutzungsrichtlinie, über die alle Mitarbeiter Kenntnis haben.