Allgemeine Geschäftsbedingungen

Inhaltsverzeichnis

Kapitel 1: Nutzungsbedingungen

1. Auftragsgegenstand

1.1. Essentry GmbH (nachfolgend „Auftragnehmer“ genannt) betreibt Systeme zur digitalen Verwaltung von Prozessen im Identitätsverifikations- und Zutrittsmanagement. Mit dem Angebot und diesen Allgemeinen Geschäftsbedingungen (nachfolgend zusammen „Vertrag“ genannt) regeln die Parteien die Benutzung des Systems „essentry“ (nachfolgend „System“ genannt) durch den Auftraggeber.

1.2. Während der Laufzeit des Vertrags stellt der Auftragnehmer dem Auftraggeber das System als „Managed Service“ zur Verfügung. Die von dem Auftraggeber benutzte Systemversion ist auf dem Angebot angegeben. Die Funktionen, Systemumgebung und Verfügbarkeit des Systems sind in **Kapitel 2: Leistungsbeschreibung** beschrieben.

1.3. Der Auftragnehmer kann das System weiterentwickeln und stellt es dem Auftraggeber in der jeweils aktuellen Version zur Verfügung. Weiterentwicklungen des Systems führen nicht dazu, dass der bei Vertragsschluss bestehende Funktionsumfang reduziert wird.

1.4. Der Auftraggeber kann das System nur über das Internet, einen Webbrowser sowie die von dem Auftragnehmer beigestellten Programme, Benutzeroberflächen und Schnittstellen benutzen. Er darf das System nicht verändern, nicht weitergeben und nur für das Zutrittsmanagement in seinen eigenen Geschäftsräumen benutzen.

1.5. Das System ist nicht dafür geeignet und bestimmt, Räume zu sichern, den Zutritt zu kontrollieren und zu verhindern, dass Unbefugte die Räume betreten. Der Auftraggeber ist selbst für die Sicherheit seiner Räume verantwortlich und muss eigene Prozesse einrichten, damit unbefugtes Betreten auch dann verhindert wird, wenn das System nicht verfügbar ist.

1.6. Der Auftraggeber muss eigene Prozesse einrichten, damit seine Räume auch dann betreten werden können, wenn das System nicht verfügbar ist.

1.7. Der Auftraggeber wird die Zugangsdaten zu dem System geheim halten und nicht an unberechtigte Personen weitergeben. Er wird den Auftragnehmer unverzüglich informieren, wenn der Verdacht besteht, dass unberechtigte Personen Zugangsdaten erfahren oder das System benutzen.

2. Subunternehmer

Der Auftragnehmer kann den Betrieb des Systems auf Subunternehmer übertragen. Dabei bleibt er gegenüber dem Auftraggeber zur Leistung verpflichtet und für Handlungen und Versäumnisse der Subunternehmer verantwortlich.

3. Vertragslaufzeit und Vergütung

3.1. Der Vertrag tritt mit Unterzeichnung des Angebots durch beide Parteien in Kraft. Die Laufzeit ist im Angebot geregelt, eine ordentliche Kündigung muss mit einer Frist von einem Monat im Voraus zum Laufzeitende erfolgen. Erfolgt keine Kündigung, verlängert sich der Vertrag automatisch um die initiale Laufzeit, mindestens jedoch um 12 Monate. Ist im Vertrag eine initiale Vertragslaufzeit von mehr als 12 Monaten vereinbart, so verlängert sich der Vertrag um diese initiale Vertragslaufzeit.

3.2. Die Vergütung für die Benutzung des Systems wird jährlich im Voraus in Rechnung gestellt, sofern die Parteien keine abweichende Vereinbarung treffen. Der Auftragnehmer ist berechtigt, die Vergütung jeweils nach 12 Monaten der Vertragslaufzeit in angemessener Höhe an den Prozentsatz anzupassen, um den sich der Verbraucherpreisindex des Statistischen Bundesamtes („VPI“) während der vorangegangenen 12 Monate verändert hat.

3.3. In dem Angebot sind die vereinbarte Systemversion sowie die Höhe der Vergütung bei einer monatlichen oder jährlichen Zahlungsweise angegeben. Die Vergütungssätze sind Nettobeträge zuzüglich der gesetzlichen Umsatzsteuer. Rechnungen sind innerhalb von 14 Tagen fällig.

4. Leistungsmängel

4.1. Mängelansprüche bestehen nicht bei einer unerheblichen Abweichung von der vereinbarten oder vorausgesetzten Beschaffenheit und einer unerheblichen Beeinträchtigung der Benutzung des Systems. Weiterhin steht der Auftragnehmer nicht für Mängel ein, die durch eine unsachgemäße Benutzung oder ungeeignete Betriebsbedingungen und Betriebsmittel auf Seiten des Auftraggebers verursacht werden.

4.2. Verlangt der Auftraggeber wegen eines Mangels Nacherfüllung, kann der Auftragnehmer zwischen Nachbesserung, Ersatzlieferung oder Ersatzleistung wie Bereitstellung eines neuen Release des Systems oder einer Umgehungslösung wählen.

4.3. Wenn der Auftraggeber dem Auftragnehmer nach einer ergebnislos verstrichenen Frist eine weitere angemessene Nachfrist gesetzt hat und auch diese ergebnislos verstrichen ist oder wenn eine angemessene Anzahl an Nachbesserungs-, Ersatzlieferungs- oder Ersatzleistungsversuchen ohne Erfolg geblieben ist, kann der Auftraggeber unter den gesetzlichen Voraussetzungen von dem Vertrag zurücktreten oder die Vergütung mindern und Schadens- oder Aufwendungsersatz verlangen. Eine Selbstvornahme auf Kosten des Auftragnehmers ist ausgeschlossen.

4.4. Mängelansprüche des Auftraggebers bei Unterschreitungen der Verfügbarkeit des essentry Backend-Systems richten sich ausschließlich nach Kapitel 2 Ziff. 5.4.

5. Haftung

5.1. Der Auftragnehmer haftet gegenüber dem Auftraggeber unbeschränkt bei Verletzung von Leben, Körper und Gesundheit, für einen Mangel nach Übernahme einer Garantie für die Beschaffenheit des Systems sowie bei arglistig verschwiegenen Mängeln.

5.2. Der Auftragnehmer haftet gegenüber dem Auftraggeber unbeschränkt, wenn das Schadensereignis auf Vorsatz oder grober Fahrlässigkeit beruht. Ferner haftet der Auftragnehmer für die leicht fahrlässige Verletzung wesentlicher Pflichten, deren Verletzung die Erreichung des Vertragszwecks gefährdet, oder für die Verletzung von Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf. In diesem Fall haftet der Auftragnehmer jedoch nur für den vorhersehbaren, vertragstypischen Schaden. Die Parteien gehen bei Vertragsschluss davon aus, dass sich dieser Schaden maximal auf die Vergütung für die einjährige Benutzung des Systems beläuft. Der Auftragnehmer haftet nicht für die leicht fahrlässige Verletzung anderer Pflichten.

5.3. Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

5.4. Soweit die Haftung des Auftragnehmers ausgeschlossen oder beschränkt ist, gilt dies auch für die persönliche Haftung von Arbeitnehmern, Vertretern und Erfüllungsgehilfen.

5.5. Der Auftragnehmer haftet für den Verlust von Daten nur bis zu dem Betrag, der bei ordnungsgemäßer und regelmäßiger Sicherung der Daten zu deren Wiederherstellung angefallen wäre.

5.6. Eine weitere Haftung des Auftragnehmers ist dem Grunde nach ausgeschlossen.

5.7. Leistungsstörungen und -verzögerungen aufgrund höherer Gewalt (zum Beispiel Unfälle, Unglücksfälle, Pandemien, Katastrophen, Krieg, Blockaden, Embargos, Arbeitskampf, behördliche Anordnungen, allgemeine Störungen der Telekommunikation und des Internets) sowie aufgrund von Umständen im Einflussbereich des Auftraggebers (zum Beispiel nicht rechtzeitige Erbringung von Mitwirkungsleistungen und

Verzögerungen durch dem Auftraggeber zuzurechnende Dritte) hat der Auftragnehmer nicht zu vertreten. Sie berechtigen ihn, die betroffenen Leistungen für die Dauer der Behinderung zuzüglich einer angemessenen Anlaufzeit auszusetzen.

6. Datenschutz

6.1. Die Parteien beachten die geltenden datenschutzrechtlichen Bestimmungen und verpflichten ihre Mitarbeiter auf das Datengeheimnis. Für die Verarbeitung personenbezogener und sonstiger Daten durch den Auftragnehmer im Auftrag des Auftraggebers gilt **Kapitel 3: Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO**.

6.2. Wenn der Auftraggeber das System zur Verarbeitung personenbezogener Daten benutzt, holt er die erforderliche Einwilligung des jeweils Betroffenen ein, soweit kein gesetzlicher Erlaubnistatbestand besteht. Er steht dafür ein, dass er zur Datenverarbeitung berechtigt ist, und stellt im Falle eines Verstoßes den Auftragnehmer von Ansprüchen Dritter frei.

7. Testphase

7.1. Wenn die Parteien einen Vertrag über die Durchführung einer Testphase mit einem „Proof of Concept“ schließen, haben die Regelungen in Ziffer 7 Vorrang vor den sonstigen Nutzungsbedingungen.

7.2. Während der Testphase darf der Auftraggeber das System auf eigene Verantwortung ausschließlich zu Testzwecken und zur Evaluierung benutzen. Der Auftragnehmer ist daher nicht verpflichtet, das System ohne Mängel und Beeinträchtigungen sowie mit bestimmten Funktionen und Verfügbarkeiten zur Verfügung zu stellen. Der Auftragnehmer ist nicht zur Wartung, Pflege und zum Support verpflichtet.

7.3. In dem Vertrag vereinbaren die Parteien die zu testende Systemversion und können „Key Performance Indicators“ („KPIs“) zur Bewertung des Systems festlegen.

7.4. In dem Vertrag vereinbaren die Parteien, ob der Auftragnehmer das System kostenlos oder gegen Vergütung zur Verfügung stellt. Die Vergütung wird zu Beginn der Testphase in Rechnung gestellt und ist innerhalb von 14 Tagen fällig.

7.5. Der Auftraggeber trägt seine Kosten und Aufwände während der Testphase selbst. Er muss Software und Hardware, die der Auftragnehmer ihm während der Testphase leiht, pfleglich behandeln. Er haftet für Beschädigungen und trägt die Kosten der Rückgabe an den Auftragnehmer.

7.6. Wenn der Auftragnehmer dem Auftraggeber das System kostenlos zur Verfügung stellt, haftet er gegenüber dem Auftraggeber nur für Vorsatz und grobe Fahrlässigkeit.

7.7. Die Laufzeit der Testphase ist in dem Vertrag geregelt. Während der Laufzeit können die Parteien die Testphase jederzeit beenden und den Vertrag kündigen. Am Ende der Laufzeit endet die Testphase von selbst, sofern die Parteien in dem Vertrag keine abweichende Regelung treffen.

7.8. Die Parteien können in dem Vertrag vereinbaren, dass der Auftragnehmer dem Auftraggeber am Ende der Testphase mitteilt, ob die vereinbarten KPIs erfüllt wurden. Wenn die KPIs nicht erfüllt wurden, endet die Testphase von selbst. Wenn die KPIs erfüllt wurden, kann der Auftraggeber den Vertrag nach Erhalt der Mitteilung innerhalb der dort angegebenen Frist schriftlich kündigen. Falls der Auftraggeber nicht kündigt, endet die Testphase und der Auftragnehmer stellt dem Auftraggeber das System zum Produktivbetrieb für die in dem Vertrag vereinbarte Laufzeit und Vergütung zur Verfügung.

8. Allgemeine Bestimmungen

8.1. Allgemeine Geschäftsbedingungen des Auftraggebers finden keine Anwendung. Nebenabreden, Änderungen und Ergänzungen des Vertrags bedürfen der Schriftform und müssen als solche ausdrücklich gekennzeichnet sein.

8.2. Die Parteien können den Vertrag nach vorheriger schriftlicher Zustimmung der anderen Partei ganz oder teilweise auf ihre verbundenen Unternehmen (§§ 15 ff. AktG) übertragen. Die Parteien werden ihre Zustimmung nicht unbillig verweigern.

8.3. Die Parteien dürfen die jeweils andere Partei nach vorheriger Freigabe öffentlich als Vertragspartner und Referenz nennen. Allein zu diesem Zweck sind die Parteien berechtigt,

8.3.1. den (Marken-) Namen der anderen Partei samt deren Unternehmensanschrift zu nennen,

8.3.2. die Unternehmenskennzeichnung, das Firmenlogo und die Marke zu nennen,

8.3.3. eine Verlinkung zu der Internetpräsenz zu erstellen und

8.3.4. erkennbar zu machen, in welcher Form die wirtschaftliche Zusammenarbeit besteht.

8.4. Zusätzlich erlaubt der Auftraggeber dem Auftragnehmer, die im Rahmen des Vertrags erbrachten Leistungen unter Nennung des Auftraggebers als Referenz und zu Werbezwecken (Bild, Video, Print, Online und sonstige Medien) zu verwenden.

8.5. Die Einwilligung zur Referenznennung gem. **Ziff. 8.3** und **8.4** kann jederzeit aus wichtigem Grund widerrufen werden.

8.6. Ausschließlicher Gerichtsstand ist Frankfurt am Main. Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts.

Kapitel 2: Leistungsbeschreibung

1. Definitionen

Zutrittsverantwortliche im Sinne dieses Dokuments sind Nutzer, die in essentry oder integrierten Systemen festlegen, wer, wann, wo innerhalb eines Gebäudes bzw. eines geschützten Areales Zutritt erhalten soll. Dies können bspw. Gastgeber, Kunden oder Mieter sein.

Zutrittsberechtigte im Sinne dieses Dokuments sind Nutzer, die über essentry Zutritt zu Gebäuden bzw. geschützten Arealen erhalten. Dies können bspw. Gäste, Dienstleister oder Mitarbeiter sein.

2. Systembeschreibung

essentry ist eine Plattform für die Zutrittsadministration[1]. Mit essentry können die manuellen und semiautomatischen Prozesse des Besucher- und Zutrittsmanagements durch eine durchgehend digitale Plattform ersetzt werden, die alle Prozessschritte integriert. essentry kann Zutrittsanforderungen aus vorgelagerten Systemen (Prä-Prozessoren) übernehmen oder die Initiierung und Genehmigung von Zutrittsanforderungen über die eigene Webapplikation abwickeln. essentry dient als Kontrollinstanz für die Authentifizierung und Autorisierung von Personen vor dem Gebäudezutritt. Hierfür nutzt das System ein Verifizierungsverfahren, bei dem KI-Methoden und Biometrie zum Abgleich des Gesichts einer Person mit einem Ausweisdokument zum Einsatz kommen. Gleichzeitig ermöglicht essentry, diese Personen in die für den Zutritt erforderlichen kundenspezifischen Verfahren, z.B. Arbeitssicherheitsregeln oder Brandschutzvorschriften, einzuweisen. Wiederkehrende Zutritte werden vereinfacht, weil Informationen über durchgeführte Einweisungen gespeichert und wiederverwendet werden können. Verifizierte Zutrittsanforderungen werden an Zutrittskontrollsysteme weitergegeben, die Türen, Schleusen, Drehkreuze usw. steuern.

Der Administrator kann sich mit dem integrierten „Dashboard“ schnell und transparent einen Überblick über den Zutrittsstatus und die abgewickelten Zutrittsvorgänge schaffen.

essentry besteht aus

(1) der essentry SaaS-Plattform zur Verwaltung aller Daten und Steuerung des Gesamtsystems,

(2) einer App für den essentry Self-Service Kiosk,

(3) einem essentry Self-Service Kiosk. Der essentry Self-Service Kiosk wird beim Auftraggeber installiert und ist ein freistehendes Gerät für die Abwicklung der Autorisierungstransaktionen, das mit einem berührungsempfindlichen Bildschirm für die Ein- und Ausgabe von Informationen, Kameras, einem Scanner für Ausweise, einem Kartenausgabegerät und einem Drucker für Zutrittsausweise ausgestattet ist. Der essentry Self-Service Kiosk bleibt im Eigentum des Auftragnehmers und wird dem Auftraggeber während der Vertragslaufzeit zur Benutzung des essentry Systems zur Verfügung gestellt.

3. Mitwirkungsleistungen des Auftraggebers

3.1. Der Auftraggeber wird auf eigene Kosten die folgenden Mitwirkungspflichten erfüllen und Beistellungen leisten. Wenn der Auftraggeber nicht fristgemäß und mangelfrei die Mitwirkungspflichten erfüllt und Beistellungen leistet, ist der Auftragnehmer für dadurch verursachte Verzögerungen und Schäden nicht verantwortlich und hat Anspruch auf Ersatz seiner Kosten. Wenn der Auftraggeber eine fällige Mitwirkungshandlung auch nach Setzen einer angemessenen Nachfrist nicht erbringt, kann der Auftragnehmer als pauschale Kostenerstattung einen Betrag in Höhe einer Monatsvergütung verlangen, sofern der Kunde nicht nachweist, dass die entstandenen Kosten niedriger sind.

3.2. Anforderungen an die Arbeitsplatzrechner Rezeptionist/Administrator/Mitarbeiter:

3.2.1. Für eine optimale Nutzung der Angebote und Funktionen des Systems wird der Auftraggeber die Browsertypen Google Chrome oder Mozilla Firefox in ihrer jeweils aktuellen Version anwenden.

3.2.2. JavaScript muss für app.essentry.com aktiviert sein.

3.3. Der Auftraggeber ist verpflichtet, einen qualifizierten Ansprechpartner nebst Stellvertreter zur Verfügung zu stellen, der berechtigt ist, alle notwendigen Entscheidungen zu treffen oder unverzüglich herbeizuführen, die zur Erbringung der vertraglich vereinbarten Leistung erforderlich sind. Der Auftraggeber ist verpflichtet, Änderungen des Ansprechpartners (nebst Stellvertreter) unverzüglich mitzuteilen.

3.4. Der Auftraggeber ist für die fachliche Einrichtung und Administration des Accounts selbst verantwortlich. Dies gilt unabhängig davon, ob der Auftragnehmer den Auftraggeber bei der Einrichtung des Accounts unterstützt. Hierzu zählen insbesondere: (i) die fachliche Einrichtung des Accounts, insbesondere Migration von Daten, Konfiguration von Prozessen und Produkten; (ii) die fachliche Einrichtung von Integrationen im essentry Account; (iii) die Prüfung der Richtigkeit der Funktion der Integration anhand von Testfällen vor Produktivnutzung; (iv) die Administration des Accounts, insbesondere das Anlegen von Benutzern und Rollen und Zuweisen von Zugängen zum Account.

3.5. Anforderungen zum Betrieb des mit Self-Service Kiosk:

3.5.1. Betriebstemperatur: 15°C - 30°C (59°F - 86°F), innen relativ.

3.5.2. Luftfeuchtigkeit: 30% - 75%, nicht kondensierend.

3.5.3. Stromversorgung: eine 230V-Steckdose je Self-Service Kiosk.

3.5.4. Netzwerkanbindung: Die Versorgung erfolgt durch eine kabelgebundene LAN RJ45 1 Gbit Ethernet Anbindung. Durch Autosensing passt sich die LAN-Schnittstelle an den Switch/Router Port an.

3.5.5. Netzwerkanforderungen: Dem Auftraggeber wird empfohlen, die Self-Service Kioske in einem separaten Netzwerk (VLAN) zu betreiben, das nur einen stabilen Internetzugang und keinen Zugriff von anderen und auf andere Geräte im Netzwerk des Auftraggebers erlaubt. Es ist außerdem ein DHCP-Server erforderlich, der den Self-Service Kiosk mit einer IP-Adresse konfiguriert und so den Internet-Zugang ermöglicht.

Der Self-Service Kiosk kommuniziert über VPN nur zu den essentry Servern und zu Microsofts Update-Servern.

VPN: Die Self-Service Kioske sind über ein VPN mit den essentry Servern verbunden. Hierbei wird ein IPSec mit IKEv2 VPN verwendet. Das VPN ist via kiosk-vpn.essentry.com erreichbar. Es werden die Ports UDP 500 und 4500 für den Authentifizierungsprozess genutzt, sowie IP-Protokoll 50 und 51 für den VPN Tunnel. Eine Internetverbindung über einen Web-Proxy ist daher nicht ausreichend.

Die minimale Path MTU muss 1472 Bytes (1496 Bytes empfohlen) einschließlich des IP-Headers betragen, damit essentrys VPN funktioniert. Diese MTU ist in den meisten regulären Netzwerkkonfigurationen verfügbar. Sollte das Netzwerk jedoch andere VPN-Tunnel verwenden, ist diese MTU möglicherweise nicht verfügbar.

Die minimale Path MTU kann mit dem PING-Kommando ermittelt werden. Die folgenden Beispiele gehen von einem 28-Byte-IP-Header aus:

Linux: ping -s 1444 -M do 1.1.1.1

Windows: ping -f -l 1444 1.1.1.1

3.5.6. Beschaffung von geeigneten Verbrauchsmaterialien (Druckerpapier, RFID Karten) und Befüllung des Self-Service Kiosks gem. **Ziff. 7.2.2.**

3.5.7. Rückgabe des Self-Service Kiosks am Ende der Vertragslaufzeit.

[1] Das System ist nicht dafür bestimmt, Räume zu sichern, den Zutritt zu kontrollieren und zu verhindern, dass Unbefugte die Räume betreten. Die Auftraggeber, Benutzer und Kunden sind selbst für die Sicherheit ihrer Räume verantwortlich. Sie müssen eigene Prozesse einrichten, damit auch dann unbefugtes Betreten verhindert und befugtes Betreten ermöglicht wird, falls das System nicht verfügbar ist.

4. Funktions- und Leistungsumfang

Die nachfolgend aufgeführten Funktionen sind auch auf https://essentry.com/produkt/essentry-plattform/ weiter erläutert. Für den Funktionsumfang sind jeweils die Angaben auf dieser Webseite maßgeblich.

(1) **Visitor Manager**: Der essentry Visitor Manager hilft, jedes Event rund um den Zutritt (z.B. dem Besuch) zu planen und zu steuern – von der Einladung bis hin zum Check-out.

- E-Mail-Einladungen
- Gruppen-Import
- Multi-Tenant
- Adressbuch
- Sammel-Aktionen (Bulk)
- Antwort-Button für Zutrittsverantwortliche
- Mitarbeiter-Modus
- Veranstaltungsmodus
- Unbegrenzte Zutrittsberechtigte
- Unbegrenzte Berechtigte
- Prozess- & Workflow-Designer
- Benutzerdefinierte Konfiguration
- Verwaltung einer unbegrenzten Anzahl von Self-Service Kiosken
- Ausweise aus dem Dashboard drucken
- Self-Service Kiosk-Branding
- Benutzerdefinierte Ausweise
- Mehrere Sprachen
- Unbegrenzte Anzahl an benutzerdefinierten Feldern

(2) **Compliance Manager**: Der essentry Compliance Manager hilft, DSGVO- und industrie-spezifische Regulatorik umzusetzen. Rechte- und Rollenkonzepte sind dabei individuell anpassbar und erhöhen Compliance-Standards.

- Individuelle Richtlinien zur Datenspeicherung und -löschung
- Granulare Benutzerrechte
- Erweiterte Datenschutzrechte
- Check-in-Benachrichtigungen
- Check-out-Erinnerungen
- Privates Adressbuch
- Mehrere Admin-Konten
- Hinzufügen von Mitarbeitern aus einem existierenden Mitarbeiterverzeichnis
- Standortverwaltung
- Analytics (Zutrittsstatistiken)
- Self-Service Kiosk-Status
- Assistenten-Benachrichtigungen
- Benachrichtigungen über abwesende Zutrittsverantwortliche
- Zutrittsexporte
- Freigabe von Zutrittsverantwortlichen
- Sicherheitsanweisungen am Self-Service Kiosk
- Unterzeichnung von Vereinbarungen (z.B. NDA)
- Vorlagen für Vereinbarungen
- Gültigkeit von Vereinbarungen
- Echtheitsprüfung des Ausweisdokuments
- Biometrischer Gesichtsabgleich (1:1)

(3) **Integration Manager**: Der Integration Manager unterstützt dabei, essentry in bestehende Prozesse und IT-Systeme zu integrieren - von Zutrittskontrollsystemen und Verzeichnisdiensten bis hin zu Kommunikationssystemen. Integrationen sind nur dann Vertragsbestandteil, wenn sie im Angebot explizit angegeben sind.

- Tyco C-Cure 9000
- AMAG Symmetry
- Paxton Net2
- dormakaba Kaba Exos 9300
- Honeywell ProWatch
- Microsoft Entra ID (ehem. Azure AD)
- Microsoft Outlook / Teams
- Google Calendar
- Salesforce
- Slack
- RFID/NFC Kartenausgabe

(4) **Support**

- Online Help Center und Knowledgebase
- Online-Einrichtungssitzung für die Verwaltung
- Persönliches Onboarding-Programm
- Zugewiesener Customer Success Manager

(5) **Managed Service**

- Hardware Installations-Service
- Hardware Support vor Ort (24 x 7 x 4) - DACH und BENELUX
- Workshop zur Definition der Anforderungen
- 24/7 Kundensupport
- Online Training
- Self-Service Kiosk Releases (Windows Sicherheitsupdates, Funktionsverbesserungen etc.)
- Regelmäßige Updates der Ausweisdokumentendatenbank

5. Service Level Agreement und Wartungsfenster für das essentry Backend-System

5.1. Das essentry Backend-System ist zu mindestens 99,5%, gemessen über einen Kalendermonat, verfügbar. Zusätzlich zu der ungeplanten Nicht-Verfügbarkeit kann es zu kurzzeitigen Ausfällen, vorübergehenden Unterbrechungen oder Beeinträchtigungen des essentry Backend-Systems durch Wartung, Updates oder die Behebung von Funktionsstörungen kommen. Solche Ausfälle, Unterbrechungen und Beeinträchtigungen werden bei der Messung der Verfügbarkeit nicht berücksichtigt.

Die Verfügbarkeit des essentry Backend-Systems kann unter https://status.essentry.com eingesehen werden.

5.2. Geplante Wartungsarbeiten oder Updates werden nur in einem Wartungsfenster von 23:00 Uhr bis 02:00 Uhr (MEZ/MESZ) durchgeführt. Hierüber wird der Auftraggeber rechtzeitig informiert. Betriebsunterbrechungen für geplante Wartungsarbeiten in diesem Wartungsfenster werden bei der Messung der Verfügbarkeit nicht berücksichtigt.

5.3. Die Parteien werden sich gegenseitig über Ausfälle und Funktionsstörungen des essentry-Systems informieren. Der Auftragnehmer beginnt mit der Behebung unverzüglich und teilt dem Auftraggeber mit, wie lange ein Ausfall oder eine Funktionsstörung voraussichtlich bestehen wird. Der Auftraggeber wird den Auftragnehmer dabei unterstützen, insbesondere die erforderlichen Informationen geben und den Zugang zu den essentry Self-Service Kiosken ermöglichen. Bei Unterschreitung der Verfügbarkeit kann der Auftraggeber die Vergütung für die Benutzung des essentry-Systems gemäß der folgenden Tabelle mindern:

Verfügbarkeit im Mittel über den Monat (X)	Minderung der Vergütung für einen Monat
> 99,5%	0%
99,5% > (X) > 98,0%	5%
98,0% > (X) > 96,0%	10%
96,0% > (X) > 94,0%	15%
94,0% > (X)	20%

5.4. Der Auftraggeber hat berechtigte Ansprüche auf Minderung der Vergütung innerhalb von drei Monaten, nachdem er Kenntnis von der Unterschreitung der Verfügbarkeit hat, schriftlich geltend zu machen. Maßgeblich ist der Zugang der Geltendmachung. Macht der Auftraggeber Ansprüche nicht oder verspätet geltend, verfallen seine Ansprüche ersatzlos. Bei berechtigten Ansprüchen erstellt der Auftragnehmer eine Gutschrift. Dem Auftraggeber ist es nicht gestattet, seine Rechnung eigenmächtig und ohne Vorliegen einer Gutschrift zu kürzen oder aufzurechnen. Neben der Minderung der Vergütung hat der Auftraggeber keine weitergehenden Schadensersatz- und Aufwendungsersatzansprüche wegen einer Unterschreitung der Verfügbarkeit.

5.5. Für Probleme mit der beim Auftraggeber installierten Hardware (essentry Self-Service Kioske) gelten die in **Ziff. 7.1.7** vereinbarten Reaktionszeiten. Ausfallzeiten der Self-Service Kioske werden bei der Messung der Verfügbarkeit des essentry-Systems nicht berücksichtigt

6. Daten Löschkonzept

Die Daten von Zutrittsberechtigten und Kunden werden nur für die nötige Dauer gespeichert und es wird ein entsprechendes einheitliches Löschkonzept umgesetzt. Es wird zwischen den nachfolgenden Datenarten unterschieden. Durch den Auftraggeber kann je Datenart eine Löschfrist festgelegt werden, die von der Standard-Löschfrist abweicht.

Datenart	**Beschreibung**	**Löschfrist** (sofern vom Kunden keine Löschfrist festgelegt wird)	**Durch den Kunden festgelegte Löschfrist**
Zutrittsdaten	Bei jedem Check-In über den essentry Self-Service Kiosk wird der Zutritt (Zeitpunkt vom Betreten bis zum Verlassen des Gebäudes) zusammen mit den persönlichen Daten des Zutrittsberechtigten gespeichert. Check-Ins, die älter als die Löschfrist sind, werden automatisch gelöscht. Hierbei entscheidet der Zeitpunkt des Verlassens des Gebäudes. Die Stammdaten des Zutrittsberechtigten (siehe nächste Datenart) bleiben in dieser Löschklasse bestehen, können aber keinem Zutritt mehr zugeordnet werden.	1 Jahr	Abweichende Löschfristen können über den Support (gem. Ziff. **7**) angefordert werden.
Stammdaten der Zutrittsberechtigten	Die Stammdaten der Zutrittsberechtigten (Name, Firma, E-Mail-Adresse und unterschriebene Dokumente, ggf. weitere durch den Zutrittsberechtigten während des Check-in Prozesses gemachte Angaben) werden nach Ablauf der Löschfrist nach dem letzten Zutritt gelöscht.	1 Jahr	
Ausgeschnittenes Lichtbild aus dem Ausweisdokument	Das Foto des Zutrittsberechtigten, das aus dem Ausweisdokument ausgeschnitten wird, wird nach Ablauf der Löschfrist nach dem letzten Zutritt gelöscht.	1 Monat	
Vom Self-Service Kiosk aufgenommenes Foto des Zutrittsberechtigten	Das Foto des Zutrittsberechtigten, das vom essentry Self-Service Kiosk aufgenommen wird, wird nach Ablauf der Löschfirst nach dem letzten Zutritt gelöscht.	1 Monat	
Aggregierte Zutrittsdaten	Keine automatische Löschung, da aggregierte Bewegungsdaten keinen Personen zugeordnet werden können. Bei jedem Check-In über den essentry Self-Service Kiosk wird der Zutritt zusätzlich pseudonymisiert für Statistiken und Auswertungen gespeichert. Dieser Datensatz enthält keine persönlichen Informationen und kann auch keiner Person zugeordnet werden. Er enthält lediglich einen Zeitstempel für das Betreten und einen Zeitstempel für das Verlassen des Gebäudes, den Eingang, durch den die Person gekommen ist, und welchen Self-Service Kiosk die Person benutzt hat.	nicht anwendbar	
Mitarbeiterdaten	Administratoren (oder eine Mitarbeiterdatenbank-Integration) können Mitarbeiterdaten jederzeit manuell (oder über eine Schnittstelle) löschen. Eine automatische Löschung findet nicht statt. Bei Löschung eines Mitarbeiteraccounts werden die Mitarbeiterdaten unmittelbar gelöscht.	nicht anwendbar	

Anmerkung:

Da essentry über einen Zeitraum von 30 Tagen Backups anfertigt, werden die Daten noch für 30 weitere Tage nach dem Löschen in den Backups vorhanden sein. Vollständig gelöscht sind die Daten nach Ablauf dieser zusätzlichen 30 Tage.

7. Vereinbarung zum Kundenservice

7.1. Technischer Support

7.1.1. essentry stellt den technischen Support für technische Fragen und die Meldung von Störungen (nachfolgend Tickets). Tickets können via E-Mail (support@essentry.com) und Telefon (+49 30 2555 5346) eröffnet werden.

7.1.2. Die Nutzer des Auftraggebers, die den technischen Support in Anspruch nehmen dürfen, werden im Rahmen des Onboardings definiert und geschult.

7.1.3. Bei Störungen des essentry Self-Service Kiosks steht der essentry Hardwaresupport zur Verfügung.

7.1.4. Falls für die Mängelbeseitigung der Austausch einzelner Hardwarekomponenten notwendig ist, werden diese durch einen Techniker am Einsatzort des Self-Service Kiosks ausgetauscht. Hierfür führt der Techniker die notwendigen Ersatzteile mit oder die Ersatzteile werden separat an den Einsatzort geliefert.

7.1.5. Die Reaktionszeit (von Eingang des Tickets bis zur ersten Reaktion durch den technischen Support) und die Bearbeitungszeiten ergeben sich aus der nachfolgenden Severity Tabelle.

7.1.6. Die Severity-Einstufung des Tickets erfolgt durch den technischen Support aufgrund der Angaben der support-berechtigten Nutzer des Auftraggebers. Die Bearbeitung von Anfragen und Problemen erfolgt gemäß der folgenden Tabelle:

Severity	Erläuterung	Reaktionszeit	Bearbeitungszeit
1	Das gesamte essentry-System ist an allen Standorten nicht mehr verfügbar	1h	7/24
2	Ein gesamter Standort mit mind. 2 Self-Service Kiosken ist nicht mehr verfügbar	2h im Fall von Softwareproblemen, 4h bei Hardware-Problemen bis zum Erscheinen des Service-Technikers am Standort innerhalb DACH und BeNeLux, sonst nächster Arbeitstag	
3	Ein Self-Service Kiosk ist ausgefallen, weitere Self-Service Kioske am Standort sind weiterhin funktionsfähig		8:00-18:00 Uhr (MEZ/MESZ) an allen Arbeitstagen
4	Fehler, die den Betrieb nicht gefährden	Nächster Arbeitstag	
5	Service-Anfrage	Nach Verfügbarkeit	

7.1.8. Es gelten die bundeseinheitlichen Feiertagsregelungen. Bei nicht bundeseinheitlichen Feiertagen gelten die Feiertagsregelungen des Landes Berlin.

7.2. Mitwirkungsleistungen des Auftraggebers bei der Erbringung des Kundenservice.

7.2.1. Anfragen von Nutzern sind durch den Helpdesk des Auftraggebers zu beantworten. Falls der Helpdesk des Auftraggebers eine Anfrage erhält, die das essentry-System direkt betreffen und die der Helpdesk des Auftraggebers mithilfe des essentry Online Help Centers (support.essentry.com) nicht beantworten kann, kann der Helpdesk eine Anfrage an den technischen Support richten.

7.2.2. Ein Support-Manager/Administrator vor Ort („Lokaler Support“) nebst Stellvertreter muss vom Auftraggeber während der Servicezeit gem. **Ziff. 7.1.6** zur Verfügung gestellt werden. Er ist die erste Kontaktperson für alle Probleme (Neustart, Netzwerk-Check, Kommunikation mit dem essentry-Support bei Problemen, die er/sie nicht lösen kann, Nachfüllen von Verbrauchsmaterial). Der Auftraggeber ist verpflichtet, Änderungen des als Lokaler Support definierten Mitarbeiters (nebst Stellvertreter) unverzüglich mitzuteilen.

7.2.3. Der Auftraggeber stellt sicher, dass die als Lokaler Support definierten Mitarbeiter für

7.2.4. Anfragen des Auftragnehmers zur Verfügung stehen. Verzögerungen im Support und etwaige Einschränkungen der Systemverfügbarkeit, die durch eine Nichterreichbarkeit des Lokalen Supports verursacht werden, werden von der Berechnung der Systemverfügbarkeit ausgeschlossen.

7.2.5. Der Auftraggeber stellt sicher, dass ein Backup Check-in Prozess vorhanden ist, der eingeleitet werden kann, falls das System nicht verfügbar ist.

7.2.6. Der Auftraggeber stellt sicher, dass Techniker, die Leistungen gemäß Ziff. 7.1.4 erbringen, Zutritt zum Einsatzort des Self-Service Kiosks erhalten.

Kapitel 3: Auftragsverarbeitungs-vereinbarung nach Art. 28 Abs. 3 DSGVO

1. Generelles

1.1. Die Essentry GmbH, Düsseldorfer Str. 15, 65760 Eschborn (nachfolgend „Auftragnehmer“ genannt) betreibt Systeme zur digitalen Verwaltung von Prozessen im Zutrittsmanagement und schließt mit Auftraggebern Verträge über die Benutzung des Systems „essentry“ (nachfolgend „Systemverträge“ oder „Systemvertrag“).

1.2. Die vorliegende Vereinbarung (nebst ihrer unten näher bezeichneten Anlagen) zur Auftragsverarbeitung nach Art. 28 DSGVO (nachfolgend auch „Vereinbarung“) konkretisiert gesetzliche Rechte und Pflichten, die sich für den Auftragnehmer und den Auftraggeber aus der Datenschutzgrundverordnung (VO (EU) 2016/679, nachfolgend auch „DSGVO“) ergeben, wenn der Auftragnehmer für den Auftraggeber im Rahmen der Systemverträge personenbezogene Daten verarbeitet oder Auftragswartung betreibt (nachfolgend auch „Auftragsverarbeitung“).

1.3. Der Auftragnehmer erkennt an, dass die DSGVO die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten schützt und diese Prinzipien auch für den Auftragnehmer gelten.

2. Begriffsbestimmungen

2.1. Es gelten die Begriffsbestimmungen aus Art. 4 und Art. 9 DSGVO sowie folgende zusätzlichen Begriffsbestimmungen:

2.2. „Auftragswartung“ meint Leistungen des Auftragnehmers (z.B. Pflege-, Wartungs- oder sonstige Leistungen an Computerprogrammen oder technischen Gegenständen zur Informationsverarbeitung), bei deren Ausführung nicht auszuschließen ist, dass der Auftragnehmer Zugriff auf personenbezogene Daten erhält, die der Auftraggeber verantwortet.

2.3. „Systemvertrag“ meint das jeweilige Rechtsverhältnis zwischen dem Auftraggeber und dem Auftragnehmer, aufgrund dessen der Auftragnehmer für den Auftraggeber bestimmungsgemäß Auftragsverarbeitung oder Auftragswartung betreibt.

2.4. „Unterauftragnehmer“ meint Dritte i.S.d. Art. 4 Nr. 10 DSGVO, die der Auftragnehmer mit schriftlicher Gestattung des Auftraggebers zur Leistungserbringung im Rahmen des Systemvertrags einsetzt.

2.5. Weitere Begriffsbestimmung können kontextbezogen in der jeweiligen Ziffer dieser Vereinbarung getroffen werden.

3. Bestandteile der Vereinbarung

3.1. Die Auftragsverarbeitung oder -wartung durch den Auftragnehmer erfolgt stets auf der Grundlage eines Systemvertrags zwischen dem Auftragnehmer und dem Auftraggeber. Der Systemvertrag ist maßgeblich für den Gegenstand, die Dauer, die Art und den Zweck der Auftragsverarbeitung, sowie für die Festlegung der Art der personenbezogenen Daten und der Kategorien der betroffenen Personen (nachfolgend auch „Auftragsgegenstand“). Zur Bestimmung des Auftragsgegenstands verwenden Auftragnehmer und Auftraggeber die **Anlage 3-1: Gegenstand der Auftragsverarbeitung** und fügen diese dem entsprechenden Systemvertrag rechtsverbindlich hinzu.

3.2. Die vorliegende Vereinbarung beinhaltet Regelungen zur Auftragsverarbeitung bzw. -wartung, die auf alle zwischen Auftraggeber und Auftragnehmer geschlossenen Systemverträge anzuwenden sind. Verbindliche Bestandteile dieser Vereinbarung sind:

Anlage 3-1: Gegenstand der Auftragsverarbeitung
Anlage 3-2: Sicherheit der Verarbeitung
Anlage 3-3: Ansprechpartner
Anlage 3-4: Unterauftragnehmer
Anlage 3-5: Meldeformular für Datenschutzverstöße

3.3. Die Bestimmungen dieser Vereinbarung einschließlich ihrer Anlagen gehen etwaigen widersprüchlichen Regelungen eines Systemvertrags vor.

4. Grundsätze zur Auftragsverarbeitung

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach Maßgabe des Systemvertrags, nach Maßgabe dieser Vereinbarung sowie im Rahmen von Weisungen des Auftraggebers.

5. Dauer der Auftragsverarbeitung

5.1. Die Laufzeit dieser Vereinbarung richtet sich nach der Dauer der Systemverträge.

5.2. Die Vereinbarung endet automatisch und ohne, dass es einer Kündigung bedarf, wenn der Auftragnehmer für den Auftraggeber insgesamt keine Auftragsverarbeitung oder -wartung mehr betreibt.

5.3. Das Recht zur ordentlichen Kündigung ist—vorbehaltlich der Kündigungsmöglichkeit nach **Ziff. 5.4**—ausgeschlossen. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund nach Maßgabe des § 314 BGB bleibt unberührt.

5.4. Der Auftraggeber kann einen Systemvertrag, ungeachtet etwaiger entgegenstehender Regelungen im Systemvertrag, kündigen, wenn der Auftragnehmer gegen eine gesetzliche Datenschutzbestimmung oder gegen eine Verpflichtung aus dieser Vereinbarung verstößt, oder eine Garantie verletzt. Die Kündigungsfrist beträgt in diesem Fall drei (3) Monate zum Monatsende. Ansprüche des Auftragnehmers wegen einer vorzeitigen Vertragsbeendigung, insbesondere Schadensersatz, sind ausgeschlossen.

6. Ort der Auftragsverarbeitung

6.1. Die Auftragsverarbeitung darf ausschließlich—vorbehaltlich der nachfolgenden Bestimmungen—in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erfolgen.

6.2. Jede Auftragsverarbeitung außerhalb eines Mitgliedsstaates der Europäischen Union oder außerhalb eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum (im Folgenden „Drittland“) bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers.

6.3. Die Zustimmung zur Auftragsverarbeitung in einem Drittland wird insbesondere dann nicht erteilt, soweit die besonderen Voraussetzungen der Art. 44 f. DSGVODSGVO nicht dauerhaft erfüllt sind, insbesondere ein angemessenes Schutzniveau im Drittland nicht besteht, oder keine geeigneten Garantien bestehen, die ein angemessenes Schutzniveau sicherstellen.

6.4. Der Auftragnehmer trägt auf seine Kosten dafür Sorge, dass ein angemessenes Schutzniveau im Drittland sichergestellt ist und weist dies dem Auftraggeber im Rahmen der Zustimmungseinholung nach, insbesondere durch:

- einen Angemessenheitsbeschluss der EU-Kommission (Art. 45 Abs. 3 DSGVO);
- verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b. i.V.m. Art. 47 DSGVO);
- Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und lit. d DSGVO);
- genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. Art. 40 DSGVO);
- genehmigte Zertifizierungsmechanismen (Art. 46 Abs. 2 lit. f. i.V.m. Art. 42 DSGVO); oder
- sonstige Maßnahmen (Art. 46 Abs. 2 lit. a., Abs. 3 lit. a und lit. b DSGVO).

7. Weisungen des Auftraggebers

7.1. Unbeschadet bindender Festlegungen i.S.d. **Ziff. 3.1** dieser Vereinbarung erkennt der Auftragnehmer an, dass allein der Auftraggeber die Zwecke der Auftragsverarbeitung bestimmt und diese auch durch einzelfallbezogene Weisungen anordnen darf, und dass jede Verarbeitung durch den Auftragnehmer außerhalb der Zweckbestimmung oder einer Weisung rechtswidrig ist. Für Ausnahmen hiervon ist Art. 28 Abs. 3 lit. a DSGVO maßgeblich.

7.2. Jede Weisung des Auftraggebers verpflichtet den Auftragnehmer dazu, jeden in der Weisung bezeichneten Vorgang (z.B. Erheben, Speichern, Übermitteln, Löschen oder Vernichten von personenbezogenen Daten) weisungsgemäß vorzunehmen, zu dulden oder zu unterlassen („Handlungen“). Das Weisungsrecht des Auftraggebers beinhaltet insbesondere, dass der Auftraggeber gegenüber dem Auftragnehmer bestimmen darf, wie der Systemvertrag in datenschutzrechtlicher Hinsicht durchzuführen ist, sowie auftragskontrollbezogene Informationen verlangen zu dürfen, als auch Handlungen zu verlangen, die zur Erfüllung einer gesetzlichen, hoheitlichen oder behördlichen Anforderung, welcher der Auftraggeber unterliegt, dienen kann.

7.3. Weisungen bedürfen grundsätzlich der Schrift- (§ 126 BGB) oder Textform (§ 126b BGB). Mündliche Weisungen sind nur in Ausnahmefällen zulässig; sie sind vom Auftragnehmer in Schrift- (§ 126 BGB) oder Textform (§ 126b BGB) zu dokumentieren. 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

8. Anpassungen und Fortentwicklung

8.1. Bei der Verarbeitung personenbezogener Daten, der Auslegung der Anforderungen der DSGVO sowie der Auslegung dieser Vereinbarung sind die jeweils geltenden Empfehlungen der Art. 29 Datenschutzgruppe oder deren Nachfolgeorganisation (Europäischer Datenschutzausschuss) angemessen zu berücksichtigen.

8.2. Auftraggeber und Auftragnehmer sind sich einig, die vorliegende Vereinbarung einschließlich Anlagen im Fall von Änderungen, Anpassungen und/oder Ergänzungen datenschutzrechtlicher Bestimmungen—insbesondere der DSGVO und/oder der jeweils anwendbaren nationalen Umsetzungsgesetze—einvernehmlich und für den Auftraggeber unentgeltlich anzupassen und zu ändern.

9. Verschwiegenheitspflicht

9.1. Der Auftragnehmer garantiert, dass er die bei ihm mit der Verarbeitung beschäftigten Personen zur Vertraulichkeit verpflichtet hat, und er diese Verpflichtung durch organisatorische Vorkehrungen auch nachhält, insbesondere dass personenbezogene Daten nicht unbefugt, nur auftragsgemäß bzw. nach Weisungen verarbeitet werden, und dass diese Verpflichtung auch nach Beendigung ihrer Tätigkeit fortbesteht (Art. 28 Abs. 3 lit. b); Art. 29; Art. 32 Abs. 4 DSGVO). Entsprechendes gilt für weitere datenschutzrechtliche Vertraulichkeits- und/oder Schutzbestimmungen, soweit diese für die Verarbeitung einschlägig sind.

9.2. Dem Auftraggeber sind auf Verlangen entsprechende Nachweise unentgeltlich zur Verfügung zu stellen. Dem Auftragnehmer bleibt es nachgelassen, den Nachweis durch die Einhaltung genehmigter Verhaltensregeln (Art. 40 DSGVO) oder die Einhaltung eines genehmigten Zertifizierungsverfahrens (Art. 42 DSGVO) zu erbringen, soweit hieraus hervorgeht, dass die bei der Verarbeitung eingesetzten Personen nach **Ziff. 9.1** zur Vertraulichkeit verpflichtet sind.

10. Sicherheit der Verarbeitung

10.1. Der Auftragnehmer bestätigt, die in seinem Verantwortungsbereich nach Art. 32 DSGVO erforderlichen Maßnahmen ergriffen zu haben. Der Auftragnehmer verpflichtet sich, seine innerbetriebliche Organisation unter Berücksichtigung des jeweiligen Stands der Technik, der Implementierungskosten und der Art, des Umfangs sowie der Umstände und Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen entsprechend auszugestalten und zu aktualisieren, sodass diese den besonderen Anforderungen des Datenschutzes nach der DSGVO entsprechen und den Schutz der Rechte der betroffenen Personen gewährleisten. Generell umfassen die zu ergreifenden technisch-organisatorischen Maßnahmen (TOM) insbesondere

10.1.1. die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Daten;

10.1.2. die Verschlüsselung personenbezogener Daten und—nach Möglichkeit—deren Pseudonymisierung;

10.1.3. die Möglichkeit zur raschen Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen im Fall eines physischen oder technischen Zwischenfalls;

10.1.4. die Einführung und das Vorhalten von Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung in einem Turnus von nicht länger als vierundzwanzig (24) Kalendermonaten.

10.2. Der Auftragnehmer wird die Maßnahmen, auf die er sich verpflichtet, bereits im Vorfeld der Auftragsvergabe korrekt, vollständig und übersichtlich gegenüber dem Auftraggeber darlegen, diese hinsichtlich der konkreten Auftragsdurchführung dokumentieren, und dem Auftraggeber zur Prüfung vorlegen. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage der jeweiligen Auftragsverarbeitung und als **Anlage 3-2: Sicherheit der Verarbeitung** zu dieser Vereinbarung genommen.

10.3. Dem Auftragnehmer bleibt es nachgelassen, die Geeignetheit der – insbesondere nach Art. 32 DSGVO zu treffenden – technisch-organisatorischen Maßnahmen durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO oder die Einhaltung eines genehmigten Zertifizierungsverfahrens nach Art. 42 DSGVO nachzuweisen. Der Nachweis kann nur (und nur solange) dadurch erfolgen, dass der Auftragnehmer dem Auftraggeber ein gültiges Zertifikat vorweist, welches von einer akkreditierten Zertifizierungsstelle nach Art. 43 DSGVO für diejenigen Verarbeitungsverfahren und -orte erteilt ist, die für die Verarbeitungen unter dieser Vereinbarung beziehungsweise den entsprechenden Systemvertrag relevant sind. Veränderungen am Zertifikat oder dessen Ablauf hat der Auftragnehmer dem Auftraggeber unverzüglich mitzuteilen.

10.4. Die Vorlage vorgenannter Zertifizierung mindert nicht die Verantwortlichkeit des Auftragnehmers und ersetzt nicht die Verpflichtung des Auftragnehmers zu garantieren, dass die unter dieser **Ziff. 10** und der **Anlage 3-2: Sicherheit der Verarbeitung** beschriebenen technisch-organisatorischen Maßnahmen i.S.d. Art. 32 DSGVO sowohl vorhanden sind als auch aufrechterhalten und aktualisiert werden.

10.5. Zur Erhöhung der Sicherheit und zur Weiterentwicklung der essentry-App wertet der Auftragnehmer anonymisierte Nutzungsdaten aus. Diese Informationen können keiner Person zugeordnet werden, und der Auftragnehmer führt diese Daten nicht mit anderen Datenquellen zusammen. Zu diesem Zweck nimmt der Auftragnehmer die Anonymisierung im Auftrag des Auftraggebers vor.

10.6. Es ist dem Auftragnehmer gestattet, eine andere als eine ausdrückliche beschriebene technische Maßnahme zu ergreifen und umzusetzen, wenn das Sicherheitsniveau der Verarbeitung dadurch erhöht, die Maßnahme dokumentiert und dem Auftraggeber mitgeteilt wird.

10.7. Der Auftraggeber ist jederzeit berechtigt, die Einhaltung der in dieser Ziffer eingegangenen Verpflichtungen und Garantien nach Maßgabe der **Ziff. 16** zu überprüfen. Etwaige festgestellte Pflichtverletzungen sind vom Auftragnehmer unverzüglich abzustellen.

11. Unterauftragnehmer

11.1. Die Unterbeauftragung der Verarbeitung durch den Auftragnehmer an einen Unterauftragnehmer ist unzulässig, es sei denn folgende Voraussetzungen sind erfüllt:

11.1.1. Der Auftraggeber hat der Unterbeauftragung schriftlich (in dieser Vereinbarung, oder in einem Systemvertrag) ausdrücklich zugestimmt.

11.1.2. Der Auftragnehmer hat den Unterauftragnehmer sorgfältig ausgewählt und gegenüber dem Auftraggeber die Garantie abgegeben, dass der Unterauftragnehmer alle an diesen unterbeauftragten Leistungen in Übereinstimmung mit allen dafür relevanten Bestimmungen dieser Vereinbarung und der einschlägigen gesetzlichen Bestimmungen, insbesondere der DSGVO, ausführt.

11.1.3. Der Auftragnehmer hat durch entsprechende Vereinbarungen mit dem Unterauftragnehmer sichergestellt und gegenüber dem Auftraggeber nachgewiesen, dass der Auftraggeber während der Laufzeit der Unterbeauftragung alle Rechte, die ihm gegenüber dem Auftragnehmer zustehen, auch gegenüber dem Unterauftragnehmer ausüben kann; dies beinhaltet auch Einsichtsrechte in datenschutzrelevante Unterlagen und Verträge und Auskunft über datenschutzrechtlich relevante Vorgänge.

11.2. Die Verarbeitung, insbesondere auch die Übermittlung von personenbezogenen Daten an bzw. durch den Unterauftragnehmer sind nur (und nur solange) zulässig, als die in **Ziff. 11.1** genannten Voraussetzungen nachweislich erfüllt sind und der Auftraggeber seine Zustimmung nicht nach Maßgabe von **Ziff. 11.4** widerrufen hat.

11.3. Bei Abschluss dieser Vereinbarung zwischen Auftraggeber und Auftragnehmer genehmigte Unterauftragnehmer sind in der

11.4. **Anlage 3-4:** Unterauftragnehmer abschließend aufgezählt; etwaige Nachträge dazu sind schriftlich auszufertigen. Es bleibt unbenommen, Unterauftragnehmer im Systemvertrag zu gestatten.

11.5. Der Auftraggeber kann die Zustimmung zum Einsatz eines Unterauftragnehmers in begründeten Fällen—insbesondere im Falle einer Gesetzes- oder sonstigen Pflichtverletzung—widerrufen. Der Auftragnehmer hat unverzüglich die Unterbeauftragung einzustellen.

11.6. Stimmt der Auftraggeber dem Einsatz eines neuen Unterauftragnehmers nicht zu, oder widerruft er seine Zustimmung eines bereits genehmigten Unterauftragnehmers, so besteht ein beiderseitiges Sonderkündigungsrecht des Vertrages und dieser Auftragsverarbeitungsvereinbarung mit einer Frist von einem Monat.

12. Rechte der betroffenen Personen

12.1. Der Auftraggeber ist für die Wahrung der Rechte der betroffenen Personen nach dem 3. Kapitel der DSGVO verantwortlich. Dem Auftragnehmer ist eine Umsetzung der Rechte betroffener Personen nur nach Weisung des Auftraggebers gestattet. Der Auftragnehmer ist jedoch verpflichtet, den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen nach dem 3. Kapitel der DSGVO vollumfänglich zu unterstützen.

12.2. Werden Betroffenenrechte unmittelbar gegenüber dem Auftragnehmer geltend gemacht, hat der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterzuleiten. Ist dem Auftragnehmer eine Zuordnung des Ersuchens zu einer Person nicht möglich, weist er die fehlende Identifizierbarkeit gegenüber dem Auftraggeber entsprechend Art. 11 Abs. 2 DSGVO nach. Werden Ersuchen nicht unverzüglich weitergeleitet, haftet der Auftragnehmer dem Auftraggeber für etwaige Verzögerungen bei der Bearbeitung von Anfragen von betroffenen Personen unter Berücksichtigung der in Art. 12 Abs. 3 DSGVO genannten Bearbeitungsfristen, es sei denn, er hat die Verzögerung nicht zu vertreten.

13. Meldung von Datenschutzvorfällen

13.1. Der Auftragnehmer erstattet in jedem Fall dem Auftraggeber Meldung, in dem er (i) von einer Verletzung des Schutzes personenbezogener Daten durch ihn oder die bei ihm beschäftigten Personen, (ii) von einem Verstoß gegen Vorschriften zum Schutz personenbezogener Daten oder (iii) von einem Verstoß gegen die in dieser Vereinbarung getroffenen Festlegungen Kenntnis erlangt (im folgenden „Datenschutzvorfall“).

13.2. Die Meldung hat unverzüglich, spätestens innerhalb von achtundvierzig (48) Stunden ab Kenntniserlangung zu erfolgen.

13.3. Nach Kenntniserlangung eines Datenschutzvorfalls trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Abmilderung nachteiliger Auswirkungen für die betroffenen Personen und den Auftraggeber.

13.4. Die Meldung eines Datenschutzvorfalls hat—soweit möglich-sämtliche Informationen zu enthalten, die der Auftraggeber zur Erfüllung seiner Pflichten nach Art. 33 und Art. 34 DSGVO benötigt; insbesondere

13.4.1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

13.4.2. den Namen und die Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers oder einer in der Sache auskunftsfähigen Person des Auftragnehmers;

13.4.3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

13.4.4. eine Beschreibung der vom Auftragnehmer bereits ergriffenen und der vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

13.5. Für Meldungen ist das in der Anlage 3-5: Meldeformular für Datenschutzverstöße beigefügte Formular zu verwenden.

13.6. Der Auftragnehmer ist verpflichtet, Datenschutzvorfälle einschließlich deren Auswirkungen und der ergriffenen Abhilfemaßnahmen ausführlich zu dokumentieren. Die Dokumentation ist dem Auftraggeber unverzüglich zur Verfügung zu stellen.

14. Mitwirkungspflichten des Auftragnehmers

14.1. Bezogen auf seinen Verantwortungsbereich ist der Auftragnehmer verpflichtet, eine ausführliche Dokumentation über die Verarbeitung personenbezogener Daten zu führen und diese dem Auftraggeber auf erstes Anfordern unverzüglich zur Verfügung zu stellen. Anhand der Dokumentation muss der Auftraggeber in die Lage versetzt werden, jederzeit die Ordnungsmäßigkeit der Datenverarbeitung entsprechend Art. 24 Abs. 1 DSGVO in geeigneter Weise nachzuweisen.

14.2. Bezogen auf seinen Verantwortungsbereich ist der Auftragnehmer verpflichtet, die für das Verfahrensregister des Auftraggebers nach Art. 30 Abs. 1 DSGVO erforderlichen Angaben und Informationen bereitzustellen.

14.3. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten. Insbesondere denen zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu wird der Auftragnehmer dem Auftraggeber sämtliche für Art. 32 - 36 DSGVO erforderlichen Unterlagen, Dokumente und Nachweise zur Verfügung stellen.

14.4. Der Auftraggeber ist über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, insbesondere nach Art. 58 DSGVO, unverzüglich zu informieren. Dies gilt auch, soweit eine zuständige Behörde beim Auftragnehmer ermittelt.

14.5. Der Auftragnehmer ist verpflichtet, die Durchführung der Verarbeitung regelmäßig auf ihre Konformität mit dieser Vereinbarung hin selbst zu überprüfen. Werden im Rahmen der Prüfung Fehler oder Unregelmäßigkeiten bekannt, ist der Auftraggeber unverzüglich zu informieren.

14.6. Der Auftragnehmer ist verpflichtet, soweit gesetzlich vorgeschrieben, einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37, 38 DSGVO ausüben kann, zu bestellen. Die Kontaktdaten des Datenschutzbeauftragten oder eines anderen Ansprechpartners für Datenschutzfragen—soweit ein Datenschutzbeauftragter nicht zu bestellen ist—werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

15. Herausgabe von personenbezogenen Daten

15.1. Der Auftragnehmer erkennt an, dass der Auftraggeber infolge seiner Rolle als Verantwortlicher jederzeit dazu berechtigt sein muss, vom Auftragnehmer die Herausgabe von personenbezogenen Daten zu verlangen. Der Auftragnehmer garantiert dem Auftraggeber daher, technische und organisatorische Maßnahmen getroffen zu haben, um den Herausgabeanspruch unverzüglich erfüllen zu können, und verzichtet darauf, etwaige Einwendungen und Einreden gegen den Herausgabeanspruch zu erheben.

15.2. Der Herausgabeanspruch umfasst sämtliche personenbezogenen Daten, die der Auftragnehmer unter der Verantwortung des Auftraggebers verarbeitet, insbesondere vom Auftraggeber übermittelte personenbezogene Daten sowie personenbezogene Daten, die im Rahmen der Durchführung eines Systemvertrages verändert, entstanden oder geschaffen worden sind.

15.3. Nach vom Auftraggeber in Schrift- oder Textform bestätigter erfolgreicher Herausgabe der personenbezogenen Daten sind diese unverzüglich von den Speichermedien des Auftragnehmers derart zu löschen, sodass diese nicht mehr reproduziert werden können. Der Auftragnehmer übernimmt die Garantie für eine entsprechende Löschung dieser personenbezogenen Daten auf Speichermedien seiner etwaigen Unterauftragnehmer. Der Auftragnehmer hat dem Auftraggeber auf Verlangen die Durchführung dieser Löschung durch geeignete Dokumente oder eine entsprechende Versicherung nachzuweisen. Vorstehendes gilt entsprechend, wenn die Verarbeitung personenbezogener Daten durch den Auftragnehmer endet, der Auftraggeber gegenüber dem Auftragnehmer jedoch ausdrücklich auf die Herausgabe verzichtet, und keine einer Löschung entgegenstehende Vereinbarung getroffen wurde.

15.4. Der Auftragnehmer darf bestimmte personenbezogene Daten anstelle ihrer Löschung in gesperrter Form speichern, solange und soweit der Auftragnehmer zwingenden gesetzlichen Bestimmungen unterliegt, die ihn zu einer Aufbewahrung verpflichten. Die Rechtmäßigkeit eines Zugriffs auf gesperrte Daten beurteilt sich nach der gesetzlichen Bestimmung, aufgrund derer die personenbezogenen Daten gesperrt werden mussten.

15.5. Im Fall der Wegnahme oder der Pfändung eines Speichermediums durch einen Dritten, auf dem personenbezogene Daten des Auftraggebers gespeichert sind, oder bei Betreibung der Zwangsvollstreckung in ein solches Speichermedium durch einen Dritten, hat der Auftragnehmer sowohl den Dritten über den Umstand, dass sich personenbezogene Daten des Auftraggebers auf dem betroffenen Datenträger befinden, als auch den Auftraggeber über die entsprechende Maßnahme, unverzüglich

zu informieren. Etwaige Rechtsmittel des Auftraggebers gegen die Maßnahmen des Dritten bleiben unberührt.

16. Kontrollrechte des Auftraggebers

16.1. Der Auftraggeber hat während der Laufzeit dieser Vereinbarung bis zum Eintritt der allgemeinen Verjährung von Ansprüchen aus dieser Vereinbarung das Recht, Überprüfungen durchzuführen, oder im Einzelfall durch zur Verschwiegenheit verpflichtete Dritte bzw. Prüfer durchführen zu lassen. Der Auftraggeber hat insbesondere das Recht, sich durch Stichprobenkontrollen von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in seinem Geschäftsbetrieb zu den üblichen Geschäftszeiten zu überzeugen. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

16.2. In Abweichung von **Ziff. 16.1** bestehen die in dieser Ziffer genannten Kontrollrechte über die Laufzeit dieser Vereinbarung als auch die allgemeine Verjährung hinaus insoweit fort, als dass und solange der Auftragnehmer personenbezogene Daten entsprechend **Ziff. 15.4** speichert.

16.3. Dies umfasst das Recht, das Grundstück, die Geschäftsräume und die Standorte der informationstechnischen Anlagen des Auftragnehmers zu betreten und dort Besichtigungen und Prüfungen vorzunehmen oder vornehmen zu lassen, sowie geschäftliche Unterlagen und gespeicherte Daten und Datenverarbeitungsprogramme einzusehen, soweit dies zur Auftragskontrolle erforderlich ist.

16.4. Kontrollen sind in der Regel mit einer Vorlaufzeit von vierzehn (14) Tagen anzukündigen. In dringenden Fällen kann der Auftraggeber die Ankündigungsfrist auf 24 Stunden verkürzen. Ein dringender Fall liegt insbesondere bei Inspektionen durch Datenschutzaufsichtsbehörden, sonstige hoheitlichen Aufsichtsbehörden, oder bei eventuell meldepflichtigen Vorfällen vor.

16.5. Der Auftragnehmer stellt sicher, dass der Auftraggeber oder die von ihm beauftragten Prüfer sich von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen können.

17. Pflichten des Auftraggebers

17.1. Der Auftraggeber ist für die Einhaltung der auf ihn anwendbaren gesetzlichen Bestimmungen zum Schutz personenbezogener Daten verantwortlich.

17.2. Der Auftraggeber wird den Auftragnehmer unverzüglich und vollständig informieren, wenn er bei Prüfung der Verarbeitungsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

17.3. Dem Auftraggeber obliegt die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DSGVO. Die Verpflichtung des Auftragnehmers zur Führung eines eigenen Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO bleibt hiervon unberührt.

17.4. Der Auftraggeber benennt einen für die im Rahmen des Vertrages anfallenden Datenschutzfragen zuständigen Ansprechpartner und teilt dessen Kontaktdaten zum Zweck der direkten Kontaktaufnahme mit.

18. Sonstige Pflichten und Bestimmungen

18.1. Der Auftragnehmer informiert den Auftraggeber, sobald bei ihm ein Eigentümerwechsel, wie nachstehend definiert, aller Voraussicht nach bevorsteht. Soweit der Eigentümerwechsel nach dem auf den Auftraggeber anwendbaren Recht der Europäischen Union oder der Bundesrepublik Deutschland eine Anpassung dieser Vereinbarung erfordert, wird der Auftragnehmer mit dem Auftraggeber die Anpassung im erforderlichen Umfang vereinbaren. Wird die Anpassung vom Auftragnehmer verweigert oder deren Abschluss verzögert, kann der Auftraggeber außerordentlich kündigen, oder Zahlungen an den Auftragnehmer, gleich aus welchem Rechtsverhältnis, bis zum Abschluss der erforderlichen Anpassungsvereinbarung zurückbehalten. „Eigentümerwechsel“ bedeutet jede Veränderung der Herrschaftsverhältnisse über den Auftragnehmer, gleich ob infolge von Stimmrechtserwerben, Umwandlungen oder Vereinbarungen. Das Vorstehende gilt für Unterauftragnehmer des Auftragnehmers entsprechend.

18.2. Die teilweise oder vollständige Abtretung oder Übertragung von Forderungen, Rechten und Pflichten aus dieser Vereinbarung durch den Auftragnehmer ist unzulässig, es sei denn der Auftraggeber hat zuvor schriftlich zugestimmt. § 354a HGB bleibt unberührt.

18.3. Jede Änderung dieser Vereinbarung bedarf zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für einen Verzicht auf das Schriftformerfordernis selbst.

18.4. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

18.5. Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung und datenschutzrelevanter Streitigkeiten aus Systemverträgen ist Frankfurt am Main. Dabei steht es dem Auftraggeber frei, etwaige Ansprüche aus dieser Vereinbarung auch bei dem für den Sitz des Auftragnehmers sachlich und örtlich zuständigen Gericht geltend zu machen. Gesetzliche Regelungen über ausschließliche Zuständigkeiten bleiben unberührt.

Anlage 3-1: Gegenstand der Auftragsverarbeitung

1. Gegenstand der Auftragsverarbeitung

1.1. **Digitales Zutrittsmanagement:** Programmierung, Anpassung, Bereitstellen und Betrieb der Software für das digitale Zutrittsmanagement. Hosting, Betreuung und Wartung der Software. Projektmanagement und Training.

2. Art und Zweck der Verarbeitung

2.1. Zweck der Verarbeitung: Digitales Zutrittsmanagement inkl. Identitätsverifikation von Zutrittsberechtigten und anderen Personen mit temporärer Zutrittsberechtigung.

2.2. Art der Verarbeitung:

- Erfassen von Namen und Identifikationsmerkmalen von Einzelpersonen, die ein vom Auftraggeber zu schützendes Gelände, Gebäude oder Gebäudeteil betreten wollen
- Verifizieren von amtlichen Lichtbildausweisdokumenten
- Erfassen einer Fotografie der Person zum Abgleich mit dem Ausweisdokument
- Erfassen von Informationen über die Ausgabe von Zutrittsmedien, die an diese Personen ausgegeben werden, sowie von zugeordneten Zutrittsprofilen
- Speichern dieser Daten für eine vom Auftraggeber festgelegte Dauer

2.3. Der Auftragnehmer wird zum Zwecke der Zurverfügungstellung von statistischen Übersichten an den Auftraggeber Daten aus der essentry Plattform anonymisieren und auswerten.

Dabei werden folgende Daten aus der essentry Plattform anonymisiert und ausgewertet:

- Gästevolumen
- Automationsgrad
- Anteil der Nutzer, die einen Online Check-in durchgeführt haben
- Häufigkeit von Ausweisdokumententypen
- Anteil der Check-ins mit fehlgeschlagener Identitätsverifikation
- Anteil der Check-ins, die manuell freigegeben wurden

Die Anonymisierung dieser Daten erfolgt entsprechend der Anonymisierungsmethode der k-Anonymität. Es kommt die k=7 Anonymisierung zur Anwendung. Somit sind jeweils 7 verschiedene Datensätze einer Kategorie von Daten notwendig, damit sie Teil der statistischen Auswertung werden dürfen.

3. Art der personenbezogenen Daten

3.1. Kreis der Betroffenen

Folgende Personengruppen sind von der Auftragsverarbeitung betroffen:

- Beschäftigte des Auftraggebers
- Zutrittsberechtigte, Interessenten, Kunden, Lieferanten und Dienstleister des Auftraggebers

3.2. Datenkategorien

Folgende Datenarten oder -kategorien sind Gegenstand der Erhebung, Verarbeitung und/oder Nutzung durch den Auftragnehmer:

Nr.	Datenfeldbezeichnung	Personengruppe	Datenart gemäß Löschkonzept
001	Vorname	Zutrittsberechtigte	Stammdaten der Zutrittsberechtigten
002	Nachname	Zutrittsberechtigte	Stammdaten der Zutrittsberechtigten
003	Firma	Zutrittsberechtigte	Stammdaten der Zutrittsberechtigten
004	Emailadresse	Zutrittsberechtigte	Stammdaten der Zutrittsberechtigten
005	Geburtsdatum (optional, kann deaktiviert werden)	Zutrittsberechtigte	Stammdaten der Zutrittsberechtigten
006	Ausweisnummer (optional, kann deaktiviert werden)	Zutrittsberechtigte	Stammdaten der Zutrittsberechtigten
007	Ausgeschnittenes Lichtbild des Zutrittsberechtigten aus dem Ausweisdokument	Zutrittsberechtigte	Ausgeschnittenes Lichtbild des Zutrittsberechtigten aus dem Ausweisdokument
008	Vom Self-Service Kiosk aufgenommenes Foto des Zutrittsberechtigten	Zutrittsberechtigte	Vom Self-Service Kiosk aufgenommenes Foto des Zutrittsberechtigten
009	Vorname	User / Mitarbeiter / Zutrittsverantwortliche	Mitarbeiterdaten
010	Nachname	User / Mitarbeiter / Zutrittsverantwortliche	Mitarbeiterdaten
011	Emailadresse	User / Mitarbeiter / Zutrittsverantwortliche	Mitarbeiterdaten
012	Passwort	User / Mitarbeiter / Zutrittsverantwortliche	Mitarbeiterdaten
013	Startzeitpunkt des Termins	Zutrittsberechtigte / Zutrittsverantwortliche	Zutrittsdaten
014	Endzeitpunkt des Termins	Zutrittsberechtigte / Zutrittsverantwortliche	Zutrittsdaten
015	Check-in Zeitpunkt	Zutrittsberechtigte / Zutrittsverantwortliche	Zutrittsdaten
016	Check-out Zeitpunkt	Zutrittsberechtigte / Zutrittsverantwortliche	Zutrittsdaten

Nr.	Datenfeldbezeichnung	Personengruppe	Datenart gemäß Löschkonzept
017	Name des Zutrittsverantwortlichen	Zutrittsberechtigte / Zutrittsverantwortliche	Zutrittsdaten
018	Ort des Termins	Zutrittsberechtigte / Zutrittsverantwortliche	Zutrittsdaten

Gegebenenfalls können weitere benutzerdefinierte Datenfelder als Teil der „Stammdaten der Zutrittsberechtigten“ erhoben, verarbeitet und gespeichert werden, falls der Administrator des Kunden weitere Daten in der essentry SaaS Plattform zur Abfrage am Self-Service Kiosk oder dem Rezeptions-Dashboard aktiviert.

Anlage 3-2: Sicherheit der Verarbeitung

1. Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)

1.1. **Pseudonymisierung:** Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen.

Beschreibung der getroffenen Maßnahmen:

- Zur Erfüllung des Auftragszwecks kann keine direkte Pseudonymisierung der personenbezogenen Daten erfolgen.
- Auswertungen und Abfragen für statistische Zwecke erfolgen anonymisiert.
- Im Rahmen der Anwendung werden serverseitig pseudonymisierte Nutzungs- und Verkehrsdaten erfasst. Diese Informationen werden nicht mit dem Träger (Anwender) des Pseudonyms zusammengeführt, es sei denn dies ist für die Bereitstellung von Funktionen nötig.

1.2. **Verschlüsselung:** Einsatz von Verfahren und Algorithmen, die personenbezogene Daten mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich in eine nicht lesbare Form umwandeln. Es kommen symmetrische und asymmetrische Verschlüsselungstechniken in Betracht:

Beschreibung der getroffenen Maßnahmen:

- Verschlüsselung aller Daten „in transit“ (während der Übertragung) und „at rest“ (auf der Festplatte gespeichert). Es werden ausschließlich starke kryptographische Verfahren angewendet.
- Um die Schlüssel der verschlüsselten Datenbanken zu speichern, wird der Cloud KMS (Key Management Service) verwendet. Dieser schützt die Schlüssel auf sogenannten Hardware Security Modules (HSMs). Die Schlüssel verlassen diese Hardware Module nicht, und die Zugriffe hierauf werden protokolliert.
- TLS Verschlüsselungen
- cloud.google.com/se
- images.apple.com/de/business/docs/iOS_Security_Guide.pdf
- android.com/intl/de_de/security-center/
- Für die Verbindung vom Browser des Nutzers zu den essentry-Servern wird HTTPS eingesetzt. Die konkrete Version des Protokolls und die Art der Verschlüsselung sind abhängig vom genutzten Browser. Die essentry-Server akzeptieren nur sichere Protokolle.

2. Maßnahmen zur Sicherstellung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1. **Zutrittskontrolle:** Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere zur Legitimation der Berechtigten:

Beschreibung der getroffenen Maßnahmen:

- Sicherung des Zutritts zu Rechenzentren durch bauliche Maßnahmen und eine Schließanlage
- Persönlicher Empfang von Kunden und Zutrittsberechtigten
- Zutrittsberechtigte werden begleitet oder beaufsichtigt
- Sensible Unternehmensbereiche und Räume, in denen keine eigenen Mitarbeiter tätig sind, werden verschlossen

Organisatorische Maßnahmen:

- interne Dokumentation und Vorgaben zur Vertragserfüllung, z.B. interne Richtlinien und Anweisungen zur Datensicherheit und zum Datenschutz
- interne Dokumentationen und Richtlinien zum Datenschutz und zur Datensicherheit

2.2. **Zugangskontrolle:** Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammdatensatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Beschreibung der getroffenen Maßnahmen:

- Die Datenverarbeitungssysteme sind durch Log-in und Autorisierungsprozeduren vor unbefugter Nutzung geschützt.
- Maßnahmen für die Passwortsicherheit umfassen personifizierte und automatisierte Anmeldeprozeduren.
- Definition von Anforderungen an Länge und Komplexität von Passwörtern in einer Passwortrichtlinie.
- Der Zugang auf die SaaS-Plattform über mobile Systeme und Endgeräte erfolgt über verschlüsselte Leitungen und Verbindungen.

2.3. **Zugriffskontrolle:** Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Beschreibung der getroffenen Maßnahmen:

- Die Zugriffsberechtigungen für Mitarbeiter zu den IT-Systemen werden restriktiv vergeben.
- Mitarbeiter erhalten nur die Berechtigungen, die sie für Ihre Tätigkeit auch tatsächlich benötigen.
- Zugriffsberechtigungen auf Server mit Kundendaten werden auf das zwingend erforderliche Maß gemäß den Prinzipien Need-to-Know bzw. Least-Priviledge eingeschränkt. Entwickler haben lediglich Zugriff auf Testsysteme, auf denen sie neue Features testen können. Erst getestete neue Features werden von einem Admin auf die Server übertragen, auf denen essentry läuft.
- essentry Server sind durch mehrere Abwehrmechanismen vor Hacking-Attacken geschützt, unter anderem durch eine Firewall.

2.4. **Trennungskontrolle:** Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Beschreibung der getroffenen Maßnahmen:

- Die Datenhaltung erfolgt auf IT-Systemen der Google Cloud, die logisch von anderen Kunden der Google Cloud getrennt sind. cloud.google.com/security/

3. Maßnahmen zur Sicherstellung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1. **Weitergabekontrolle:** Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Beschreibung der getroffenen Maßnahmen:

- Für die Übertragung der personenbezogenen Daten vom jeweiligen Endgerät auf die Server ist eine Transportverschlüsselung (TLS) implementiert.
- Eine nachträgliche Überprüfung der Weitergabekontrolle kann auch durch die Sichtung der Log-Files erfolgen.

3.2. **Eingabekontrolle:** Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Beschreibung der getroffenen Maßnahmen:

- Eine nachträgliche Überprüfung der Eingabekontrolle kann auch durch die Sichtung der Log-Files erfolgen.

4. Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 lit. b DSGVO)

4.1. Verfügbarkeitskontrolle

Beschreibung der getroffenen Maßnahmen:

- Die Datensicherungen unserer IT-Systeme erfolgen nach einem verbindlichen Datensicherungskonzept. Es wird täglich zwischen 1:00 und 3:00 Uhr ein Backup der Datenbanken angefertigt. Es wird für 30 Tage gespeichert und ist mit AES256 verschlüsselt.
- Kundendaten des Auftraggebers werden in der Google Cloud verarbeitet. Hier wird auf die Maßnahmen zur Verfügbarkeit und Belastbarkeit von Google verwiesen. cloud.google.com/compute/ cloud.google.com/storage/
- Die Dateien, für die eine Speicherung nötig ist, sind redundant an verschiedenen Standorten gespeichert, um den Verlust zu verhindern. Außerdem werden bestimmte kritische Objekte versioniert, was bedeutet, dass das Ersetzen oder Löschen einer Datei protokolliert wird und die jeweils alte Datei nicht verloren geht, sondern weiter gespeichert bleibt. Alle Dateien sind mit AES256 verschlüsselt.
- In der Google Cloud wird die Rechenkapazität im Falle eines starken Anstiegs von Anfragen oder Benutzern automatisch erhöht.

- Jede Änderung in der Konfiguration wird zuerst auf den Testsystemen getestet und Änderungen werden in Logdateien zur Nachvollziehbarkeit gespeichert. Es werden regelmäßige Sicherheitsscans der Server durchgeführt. Grundlegende Konfigurationen der Kommunikationswege zwischen Instanzen werden von definierten Administratoren vorgenommen.

4.2. Verfügbarkeit der eingesetzten IT-Systeme

Beschreibung der getroffenen Maßnahmen:

- Für unsere IT-Systeme sind im Rahmen eines Notfallkonzepts angemessene Maßnahmen zum Brandschutz, Stromversorgung, Klimatisierung, Datensicherung, Disaster-Recovery etc. getroffen.
- Der Cluster Scheduler Kubernetes verteilt die Instanzen der Software jeweils so, dass die verschiedenen Instanzen immer auf unterschiedlichen Server laufen. Ein Hardware-Defekt führt somit in der Regel zu keiner Unerreichbarkeit des essentry-Systems.
- Die Kundendaten des Auftraggebers werden in der Google Cloud verarbeitet. Hier wird auf die Maßnahmen zur Verfügbarkeit und Belastbarkeit von Google verwiesen. cloud.google.com/compute/ cloud.google.com/storage/

5. Maßnahmen zur Wiederherstellung der Verfügbarkeit und dem Zugang zu personenbezogenen Daten bei einem technischen Zwischenfall (Art. 32 lit. c DSGVO)

5.1. Recovery / Backup-Systeme

Beschreibung der getroffenen Maßnahmen:

- Für unsere IT-Systeme sind im Rahmen eines Notfallkonzepts angemessene Maßnahmen zum Brandschutz, Stromversorgung, Klimatisierung, Datensicherung, Disaster-Recovery etc. getroffen. Eine Wiederanlaufzeit binnen 24 Stunden ist gewährleistet.
- Die Kundendaten des Auftraggebers werden in der Google Cloud verarbeitet. Google garantiert eine Verfügbarkeit von über 99,99%. Im Übrigen wird auf die Maßnahmen zur Widerherstellung der Verfügbarkeit von Google verwiesen. cloud.google.com/compute/ cloud.google.com/storage/

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der technisch-organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO; Art 25. Abs. 1 DSGVO)

6.1. Datenschutzmanagement

Beschreibung der getroffenen Maßnahmen:

- Es ist ein Datenschutz Management System (DPMS) im Einsatz. Das DPMS wird vom Datenschutzbeauftragten des Auftragnehmers bereitgestellt und zusammen mit dem Auftragnehmer betrieben. Im Rahmen von Wiedervorlagen und regelmäßigen Meetings werden unsere Verfahren regelmäßig überprüft, bewertet und evaluiert. Je nach Art der Verarbeitung erfolgen diese Maßnahmen nach 3, 6 oder höchstens 12 Monaten.

6.2. Datenschutzfreundliche Voreinstellungen (Privacy by Default)

Beschreibung der getroffenen Maßnahmen:

- Das System wird in einer datenschutzfreundlichen Voreinstellung ausgeliefert. Etwaige kundenspezifische Entwicklung erfolgt auf Weisung des Auftraggebers.
- Die Betroffenen können sich bei der Verwendung der Software/App jederzeit mit Hilfe der Datenschutzerklärung über die Verwendung ihrer Daten Informieren.
- Der Auftraggeber gibt die zu erhebenden Datenkategorien vor.

6.3. **Auftragskontrolle:** Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

Beschreibung der getroffenen Maßnahmen:

- Bei der Verarbeitung personenbezogener Daten werden mit Subunternehmern Verträge gemäß Art. 28 DSGVO / EU Model Clauses geschlossen.

Anlage 3-3: Ansprechpartner

Verantwortliche und weisungsberechtigte Personen des Auftraggebers und Auftragnehmers.

Auftragnehmer: Essentry GmbH

Weisungsempfänger	**Name**	**E-Mail**	**Tel.**
Geschäftsführer	Dr. Dennis Lips	dennis.lips@essentry.com	wird separat bekannt gegeben
IT-Leiter	Christian Böhlke	christian.boehlke@essentry.com	wird separat bekannt gegeben

Sonstige Funktionen	**Name**	**E-Mail**	**Tel.**
Ext. Datenschutzbeauftragter	AGOR AG	datenschutz@essentry.com	wird separat bekannt gegeben
Informationssicherheitsbeauftragter	AGOR AG	informationssicherheit@essentry.com	wird separat bekannt gegeben

Der Auftraggeber teilt dem Auftragnehmer seine verantwortlichen und weisungsberechtigten Personen entsprechend mit.

Anlage 3-4: Unterauftragnehmer

Übersicht über alle für den Auftragnehmer tätigen Unterauftragnehmer, die unmittelbar die Daten des Auftraggebers erheben, verarbeiten und/oder nutzen.

Folgende Unterauftragnehmer sind mit Zustimmung des Auftraggebers tätig:

Unterauftragnehmer	Anschrift	Aufgabenfeld
Google Ireland Limited	Gordon House, Barrow Street Dublin, D04 E5W5, Ireland	Hosting der Datenbanken und Server in Deutschland.
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy 1855, Luxembourg	Versenden von E-Mails und der Generierung der Namensschilder für den Drucker; Lichtbildabgleich; die Datenverarbeitung findet innerhalb der EU statt.
Cubefinity GmbH Produkt NinjaOne	Stanisla-Kist-Str. 14A 94330 Aiterhofen Deutschland	Verwaltung von Kiosk-Geräten einschließlich der Installation von App- und Systemupdates, Zuweisung von kunden- und standortspezifischen Profilen und Fernüberwachung bei Problemen und anderen Supportfällen. Die Datenverarbeitung und -speicherung findet in der EU statt.
Twilio Inc.	375 Beale Street Suite 300 San Francisco CA 94105, USA	Versand von SMS und (Video-)telefonie Service. Der Subunternehmer kann ausschließlich bei expliziter Bestellung der Funktionalität zum Einsatz kommen.

Anlage 3-5: Meldeformular für Datenschutzverstöße

Name (Auftragnehmer/in)	Adresse (Auftragnehmer/in)
Name (Auftraggeber/in)	Adresse (Auftraggeber/in)

	Nähere Bezeichnung des betroffenen Auftragsverhältnisses:
Zeitraum des Vorfalles (Datum, Uhrzeit):	
Beschreibung des Datenschutzvorfalls: (Verletzung des Schutzes personenbezogener Daten)	
Betroffene personenbezogene Daten: (nach Datenkategorien)	
Zahl der betroffenen Personen (ungefähr):	
Zahl der betroffenen Datensätze (ungefähr):	
Betroffene IT-Systeme:	
Zuständiger Fachbereich / ggf. zuständige IT-Abteilung:	
Name und Kontaktdaten des Datenschutzbeauftragten oder sonstiger Anlaufstelle:	
Verfasser und Datum der Meldung:	
Wer wurde bereits durch wen informiert: (z.B. Datenschutzbeauftragter, Datenschutz-Aufsichtsbehörde etc.)	
Davon erfahren durch (Quelle):	
Beschreibung der wahrscheinlichen Folgen des Datenschutzvorfalls:	
Beschreibung der vom Auftragnehmer ergriffenen Sofortmaßnahmen zur Behebung:	
Vorschlag für zu ergreifende Maßnahmen:	
Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen:	
Gesamtrisiko:	

Rechtsverbindliche Bestätigung der Richtig- und Vollständigkeit vorstehender Angaben:

Ort, Datum	Unterschrift	Unterschrift (Datenschutzbeauftragte/r)