# Vereinbarung zur Auftragsverarbeitung

**iLOQ-Vereinbarung über Auftragsverarbeitung** version 2024-04_DE

Diese Vereinbarung über Auftragsverarbeitung (im Folgenden: AVV) legt die Bestimmungen für die Verarbeitung personenbezogener Daten fest, die iLOQ Oy (im Folgenden: „Anbieter“) verpflichtet ist, bei der Verarbeitung personenbezogener Daten im Auftrag des Endkunden (im Folgenden: „Kunde“) im Zusammenhang mit der Bereitstellung des iLOQ Schließystems, wie im Service- und Wartungsvertrag sowie den allgemeinen Vertragsbedingungen in Anhang 1 (im Folgenden „Vertrag“) vereinbart, einzuhalten.

## Art. 28 Datenschutz-Grundverordnung (DSGVO)

Nachstehend - Auftragsverarbeitungsvertrag oder AVV -

**Zwischen**

**Altenheim Friedrichsburg gGmbH**
Hoppendamm 29
48151 Münster

- Im Folgenden „**Kunde“** genannt –

**Und**

**iLOQ Deutschland GmbH**
Am Seestern 4
40547 Düsseldorf

- Im Folgenden **„Anbieter“** genannt –

schließen nachfolgenden AVV über die Verarbeitung von
Daten des **Kunden** durch den **Anbieter** gemäß
Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO).

**Präambel**

Dieser AVV konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien (nachstehend: „Parteien“).
Sie findet Anwendung auf alle Tätigkeiten, die mit der Durchführung von Aufträgen in Zusammenhang stehen, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Subunternehmer mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

## Inhalt





iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

## 1 Definitionen

**Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, zum Beispiel eine Kennung wie ein Name, eine Kennnummer oder Standortdaten, die vom Anbieter im Zusammenhang mit dem Vertrag verarbeitet werden.

**Betroffene Person** ist eine natürliche Person, die anhand personenbezogener Daten direkt oder indirekt identifiziert werden kann.

**Verarbeitung oder verarbeiten** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

**Verantwortlicher** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

**Auftragsverarbeiter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

**Datenschutzrechtliche Vorschriften** sind die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) der Europäischen Union), alle anderen anwendbaren Bestimmungen zum Datenschutz sowie alle Vorschriften und Anweisungen der Datenschutzbehörden.

Andere Begriffe, die in dieser AVV verwendet werden, haben die in den datenschutzrechtlichen Vorschriften festgelegte Bedeutung.

## 2 Verarbeitung personenbezogener Daten

Der Kunde ist Verantwortlicher der personenbezogenen Daten und allein dafür verantwortlich, dass er personenbezogene Daten auf einer tauglichen Rechtsgrundlage verarbeitet. Der Kunde ist ebenso dafür verantwortlich, alle anderen Verpflichtungen eines Verantwortlichen aus datenschutzrechtlichen Vorschriften zu erfüllen, unter anderem die Informationspflichten gegenüber betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten.



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

Der Anbieter ist Auftragsverarbeiter des Kunden in Bezug auf die Verarbeitung personenbezogener Daten gemäß dem Vertrag. Der Anbieter verarbeitet die personenbezogenen Daten nur im Auftrag und nach den Weisungen des Kunden für und in dem Umfang, der erforderlich ist, um Dienstleistungen in angemessener Weise und wie im Vertrag vereinbart und in Übereinstimmung mit datenschutzrechtlichen Vorschriften zu erbringen; dies gilt nicht, sofern der Anbieter hierzu bereits durch das Recht der Union oder der Mitgliedstaaten, dem der Anbieter unterliegt, verpflichtet ist. In einem solchen Fall teilt der Anbieter dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Bestimmungen des Vertrags einschließlich dieser AVV legen die schriftlichen Weisungen des Kunden an den Anbieter bezüglich der Verarbeitung personenbezogener Daten fest. Ungeachtet dessen kann der Kunde dem Anbieter zusätzliche angemessene schriftliche Weisungen erteilen. Verstoßen die schriftlichen Anweisungen des Kunden gegen datenschutzrechtliche Vorschriften, benachrichtigt der Anbieter den Kunden unverzüglich. Die Ausführung der Anweisungen des Kunden kann Änderungen von Preisen oder anderen Bestimmungen des Vertrags zur Folge haben. Der Anbieter informiert den Kunden über solche Äanderungen, bevor er Weisungen des Kunden umsetzt.

Erhält der Anbieter Anfragen von betroffenen Personen oder Datenschutzbehörden betreffend die Verarbeitung personenbezogener Daten im Auftrag des Kunden, informiert der Anbieter den Kunden und leitet solche Anfragen rechtzeitig an den Kunden weiter, es sei denn, er ist durch datenschutzrechtliche Vorschriften daran gehindert. Der Anbieter beantwortet keine Anfragen, ohne den Kunden zuvor hierüber zu informieren, es sei denn, datenschutzrechtliche Vorschriften schreiben etwas anderes vor.

Der Anbieter unterstützt den Kunden darüber hinaus soweit notwendig und angemessen bei der Erfüllung seiner weiteren Verpflichtungen bezüglich der vom Anbieter im Auftrag des Kunden verarbeiteten personenbezogenen Daten. Dies kann beinhalten den Kunden bei der Umsetzung angemessener technischer und organisatorischer Maßnahmen, dem Umgang mit Verletzungen des Schutzes personenbezogener Daten, der Durchführung einer Datenschutz-Folgenabschätzung, der vorherigen Konsultation der zuständigen Datenschutzbehörden sowie der Beantwortung von Anfragen von betroffenen Personen in Bezug auf deren Rechte nach der Datenschutz-Grundverordnung zu unterstützen. Reicht eine betroffene Person eine Anfrage ein, um ihre Rechte gemäß datenschutzrechtlichen Vorschriften auszuüben, nutzt der Kunde zuerst die Funktionen der iLOQ Management Software. Wenn und soweit der Kunde die Anfrage nicht durch Nutzung der Funktionen der iLOQ Management Software beantworten kann, stellt der Anbieter zusätzliche Unterstützung bei der Beantwortung der Anfrage der betroffenen Person zur Verfügung. Der Anbieter hat das Recht, angemessene Kosten, die bei einer solchen zusätzlichen Unterstützung anfallen, in Rechnung zu stellen. Der Kunde zahlt diese zusätzlichen Kosten wie vom Anbieter in Rechnung gestellt.

Der Anbieter legt seinem Personal, das zur Verarbeitung personenbezogener Daten befugt ist, angemessene vertragliche Verpflichtungen hinsichtlich Vertraulichkeit und Sicherheit auf.

## 3 Sicherheit personenbezogener Daten

Der Anbieter stellt unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der unterschiedlichen Wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sicher, dass notwendige, geeignete technische und organisatorische Maßnahmen gemäß den datenschutzrechtlichen Vorschriften getroffen wurden, um eine angemessene Sicherheit der vom Anbieter im Auftrag des Kunden verarbeiteten personenbezogenen Daten zu gewährleisten. Diese Maßnahmen können, soweit geeignet, die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen, die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen sowie die regelmäßige Überprüfung, Bewertung und Evaluierung der Effektivität der getroffenen technischen und organisatorischen Maßnahmen beinhalten.

Der Anbieter hat das Recht, die technischen und organisatorischen Maßnahmen während der Laufzeit des Vertrags zu verändern, sofern sie weiterhin den gesetzlichen Anforderungen entsprechen.

Der Anbieter dokumentiert die von ihm getroffenen technischen und organisatorischen Maßnahmen und verpflichtet sich, dem Kunden eine Kopie der relevanten Dokumentation zur Verfügung zu stellen, sofern die Herausgabe solcher Kopien kein Risiko für die Datensicherheit darstellt.

## 4 Verletzungen des Schutzes personenbezogener Daten

Soweit der Anbieter einer gesetzlichen Meldepflicht für den Fall einer Verletzung der Sicherheit personenbezogener Daten unterliegt (insbesondere gemäß Art. 33 und 34 DSGVO) informiert der Anbieter den Kunden rechtzeitig, wenn der Anbieter eine solche Verletzung in Bezug auf diejenigen personenbezogenen Daten feststellt, für welche der Kunde verantwortlich ist. Im Falle einer Verletzung des Schutzes personenbezogener Daten stellt der Anbieter dem Kunden wie in den datenschutzrechtlichen Vorschriften vorgeschrieben Informationen zur Verfügung und gewährt dem Kunden die notwendige und angemessene Unterstützung bei der Lösung der Situation.

## 5 Audit

Der Anbieter wird dem Kunden oder einem unabhängigen, vom Kunden ausgewählten Dritten die Durchführung von Audits gestatten, um sicherzustellen, dass der Anbieter die Bestimmungen dieser AVV sowie datenschutzrechtliche Vorschriften erfüllt. Der Anbieter stellt dem Kunden oder dem vom Kunden ausgewählten unabhängigen Dritten nach angemessener schriftlicher Aufforderung durch den Kunden die erforderlichen Unterlagen zur Verfügung. Soweit diese Unterlagen als nicht ausreichend erachtet werden, um die Einhaltung dieser AVV und der datenschutzrechtlichen Vorschriften zu überprüfen, ermöglicht der Anbieter nach angemessener schriftlicher Aufforderung durch den Kunden den notwendigen Zugang und die Inspektion in den Räumlichkeiten des Anbieters. Der Kunde trägt alle unmittelbaren Kosten im Zusammenhang mit entsprechenden Audits und Inspektionen.

## 6 Unterauftragsverarbeitung

Der Kunde erteilt hiermit seine Zustimmung zum Einsatz von Unterauftragsverarbeitern durch den Anbieter, die in Annex 1 dieser AVV oder auf der Website des Anbieters zum jeweiligen Zeitpunkt aufgeführt sind, zum Zwecke der Verarbeitung personenbezogener Daten im Auftrag des Kunden. Beabsichtigt der Anbieter, Unterauftragsverarbeiter zu ändern oder weitere Unterauftragsverarbeiter einzusetzen, benachrichtigt er den Kunden im Voraus von solchen Änderungen und gibt ihm Gelegenheit, diesen Änderungen aus berechtigten Gründen zu widersprechen. Soweit der Kunde nicht innerhalb von 14 Tagen nach Erhalt der Mitteilung widerspricht, erlischt sein Recht, der entsprechenden Beauftragung zu widersprechen. Widerspricht der Kunde einer solchen Änderung oder Erweiterung der Auftragsverarbeiter des Anbieters, haben beide Parteien das Recht, den Vertrag unter Einhaltung einer Frist von dreißig (30) Tagen schriftlich zu kündigen. Der Anbieter stellt sicher, dass seine Unterauftragsverarbeiter ebenfalls geeignete technische und organisatorische Maßnahmen treffen, wie in datenschutzrechtlichen Vorschriften vorgeschrieben und dass solche Unterauftragsverarbeiter datenschutzrechtlichen Verpflichtungen unterliegen, die mindestens so umfassend sind, wie die hier vereinbarten. Der Anbieter haftet gegenüber dem Kunden in vollem Umfang, wenn ein Unterauftragsverarbeiter seinen datenschutzrechtlichen Verpflichtungen nicht nachkommt.

## 7 Übermittlung personenbezogener Daten an Stellen außerhalb der EU/des EWR

Der Anbieter darf personenbezogene Daten an Stellen außerhalb der EU/des EWR auf Grundlage der hier festgelegten Bedingungen übertragen. Übermittelt der Anbieter als Datenexporteur personenbezogene Daten in ein Land außerhalb der EU/des EWR, dem die Europäische Kommission kein angemessenes Schutzniveau gemäß den datenschutzrechtlichen Vorschriften zuerkennt, stimmt der Anbieter zu, mit dem Datenimporteur einen Zusatzvertrag abzuschließen, der die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer enthält, wie sie in der Entscheidung der Europäischen Kommission vom 4. Juni 2021 (oder sonstige Standardvertragsklauseln, die die Entscheidung der Europäischen Kommission vom 4. Juni 2021 abändern oder ersetzen) festgelegt sind. In einem solchen Fall trifft der Anbieter no3twendige ergänzende Maßnahmen, um sicherzustellen, dass das Schutzniveau für personenbezogene Daten durch die Übermittlung nicht beeinträchtigt wird. Es wird klargestellt, dass der Anbieter nicht für Übermittlungen personenbezogener Daten verantwortlich ist, wenn der Kunde selbst als Datenexporteur personenbezogene Daten übermittelt oder einen Dritten anweist, als Datenexporteur personenbezogene Daten an einen Datenimporteur außerhalb der EU/des EWR zu übermitteln. Der Kunde erklärt seine Bereitschaft, bei der Erfüllung der Anforderungen von Art. 49 DSGVO im erforderlichen Umfang mitzuwirken.

## 8 Freistellung

Verarbeitet eine Partei personenbezogene Daten unter Missachtung datenschutzrechtlicher Vorschriften oder dieser AVV, stellt die Partei, die den Verstoß begangen hat, die andere Partei von allen Schadensersatzansprüchen



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

gegenüber betroffenen Personen frei, die die andere Partei aufgrund datenschutzrechtlicher Vorschriften zu erfüllen verpflichtet ist. Die Haftung der Parteien für von der zuständigen Datenschutzbehörde verhängte Bußgelder richtet sich nach den Bestimmungen der datenschutzrechtlichen Vorschriften. Mit Ausnahme der oben genannten Verluste, Kosten oder Schäden richtet sich die Haftung nach den allgemeinen Bedingungen in Anhang 1.

## 9 Laufzeit

Nach Kündigung oder Ende der Laufzeit des Vertrags gibt der Anbieter alle personenbezogenen Daten, für die der Kunde verantwortlich ist, zurück und löscht diese in Übereinstimmung mit den allgemeinen Bedingungen in Anhang 1, es sei denn, der Anbieter ist gesetzlich verpflichtet, die Daten des Kunden darüber hinaus zu speichern. Der Anbieter kann Unterlagen, welche als Beweis für die ordnungsgemäße und korrekte Verarbeitung der Daten des Kunden dienen, auch nach Beendigung des Vertrages behalten.

Diese AVV gilt ab dem Datum der Unterzeichnung bis alle personenbezogenen Daten, die sich im Besitz des Anbieters befinden, gelöscht sind.

## Anhang 1 Beschreibung der Verarbeitung personenbezogener Daten

Dieser Anhang 1 ergänzt den AVV zwischen dem Kunden und dem Anbieter und bildet einen wesentlichen Teil der AVV. Der Anbieter verpflichtet sich, personenbezogene Daten im Auftrag des Kunden gemäß den Bestimmungen dieses Anhang 1 zu verarbeiten.

| | |
|---|---|
| **Anbieter** | **Name, Adresse und Kontaktdaten**<br><br>iLOQ Oy<br>Yrttipellontie 10, 90230 Oulu, Finland<br>Tel. +358(0)40 3170 200 |
| **Umfang und Zweck der Verarbeitung personenbezogener Daten** | Der Anbieter verarbeitet personenbezogene Daten, um dem Kunden das iLOQ Schließsystem und andere Dienstleistungen wie im Vertrag und den allgemeinen Bedingungen in Anhang 1 vereinbart zur Verfügung zu stellen.<br><br>Die vom Kunden festgelegten Zwecke der Verarbeitung personenbezogener Daten sind die Folgenden:<br><br>☒ Verwaltung und Sicherung der Räumlichkeiten des Kunden<br><br>☒ Untersuchung von Schäden und Sicherheitsvorfällen<br><br>☐ Andere (bitte ausführen) |
| **Kategorien betroffener Personen** | Die betroffenen Personen, deren personenbezogene Daten verarbeitet werden, sind die Endnutzer des iLOQ Schließsystems, die zu den folgenden Kategorien betroffener Personen gehören:<br><br>☒ Nutzer der Räumlichkeiten des Kunden (z.B. Bewohner, Angestellte, etc.)<br><br>☒ Lieferanten oder Dienstleister des Kunden<br><br>☐ Andere (bitte ausführen) |

| | |
|---|---|
| **Kategorien personenbezogener Daten** | Zu den verarbeiteten personenbezogenen Daten gehören die folgenden Kategorien personenbezogener Daten:<br><br>☒ Identifikationsdaten (Kennnummer der betroffenen Person, Name, Schlüsselidentifikations-nummer…)<br><br>☒ Zugangsberechtigungsdaten (einem Schlüssel zugeordnete Zugangsrechte…)<br><br>☒ Ereignis-Logdaten eines Schlosses (Zeitstempel, Logeintrag…)<br><br>☐ Andere (bitte ausführen) |
| **Standort der Verarbeitung personenbezogener Daten** | Der Anbieter verarbeitet personenbezogene Daten in den folgenden Ländern und Regionen:<br><br>☒ Länder innerhalb der EU/des EWR<br><br>☐ Andere Länder (bitte ausführen und Namen des Datenimporteurs hinzufügen): N/a |
| **Technische und organisatorische Maßnahmen** | Der Anbieter trifft geeignete technische und organisatorische Sicherheitsmaßnahmen, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Solche Maßnahmen beinhalten unter anderem Zugriffskontrolle und Authentifizierung, Protokollierung und Überwachung, technische Sicherheitsmaßnahmen bezüglich Software, Backups und Datenwiederherstellung, Verschlüsselung und Pseudonymisierung sowie physische Sicherheitsmaßnahmen.<br><br>Darüber hinaus stellt der Anbieter sicher, dass die Sicherheit der iLOQ Manager Software dem Standard ISO/IEC 27001:2013 „Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme – Anforderungen“ entspricht. |
| **Vorgesehene Fristen für die Löschung verschiedener Kategorien personenbezogener Daten** | Identitätsdaten und Daten über Zugangsrechte werden verarbeitet, solange dies für die Zwecke der Verwaltung und Sicherung der Räumlichkeiten des Kunden notwendig ist. Der Kunde stellt im Wege der Nutzung der Funktionen der iLOQ Manager Software sicher, dass die Identitätsdaten betroffener Personen und Daten über Zugangsrechte gelöscht werden, nachdem es für die betroffene Person nicht mehr notwendig ist, die Räumlichkeiten des Kunden zu betreten.<br><br>Der Kunde kann mit Hilfe der Funktionen der iLOQ Manager Software die geltenden Speicher- und Löschfristen für die Ereignis-Logdaten eines Schlosses auf dem mit dem System verbundenen Server bestimmen. Der Kunde nimmt zur Kenntnis, dass auch das physische Schloss Event-Logdaten sammelt und speichert. Die Daten, die vom Schloss gespeichert werden, sind verschlüsselt, so dass die Daten ohne zusätzliche Informationen keiner bestimmten betroffenen Person zugeordnet werden können. Die Speicherdauer der Event-Logdaten eines Schlosses wird im Einklang mit den Aktivitäten der Türöffnungen bestimmt, wobei ein Schloss in etwa die 500 letzten Ereignis-Logdaten speichert. |
| **Zugriff des Kunden, Löschung und Berichtigung von personenbezogenen Daten und Einschränkung der Verarbeitung** | Der Kunde kann die Funktionen der iLOQ Manager Software nutzen, um auf die verarbeiteten personenbezogenen Daten zuzugreifen, sie zu berichtigten, zu löschen oder die Verarbeitung einzuschränken. |
| **Auftragsverarbeiter des Anbieters** | Die Auftragsverarbeiter, die der Anbieter zur Verarbeitung personenbezogener Daten im Auftrag des Kunden nutzt, sind auf der Website des Anbieters aufgeführt, die hier abgerufen werden kann: [URL Adresse]. |

**Anhang 2 Technische und organisatorische Maßnahmen**



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

Der Auftragnehmer hat seine innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird:

1. Maßnahmen zur Pseudonymisierung personenbezogener Daten

   Der Auftragnehmer hat folgende Maßnahmen ergriffen. Kreuzen Sie bitte zutreffendes an und fügen Sie fehlende Maßnahmen hinzu:

   ☒ Trennung von Kundenstammdaten und Kundenumsatzdaten

   ☐ Trennung von Patienten-Kontaktdaten und Behandlungsdaten/Befunden etc.

   ☐ Verwendung von Personal-, Kunden-, Patienten-Kennziffern statt Namen

2. Maßnahmen zur Verschlüsselung personenbezogener Daten (z.B. in stationären und mobilen Speicher-/Verarbeitungsmedien, beim elektronischen Transport).

   Der Auftragnehmer hat folgende Maßnahmen ergriffen. Kreuzen Sie bitte die zutreffenden Felder an und fügen Sie fehlende Maßnahmen hinzu:

   ☒ Verschlüsselung von E-Mails und aller anderen physischen oder digitalen Datenträger

   ☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops (z.B. über Betriebssysteme, True Crypt, Safe Guard Easy, WinZip, PGP)

   ☒ getunnelter Fernzugriff (z.B. über VPN = Virtual Private Network)

   ☐ sicherer Transport des physikalischen Datenträgers (z.B. über einen verschlossenen Transportbehälter)

   ☐ gesichertes WLAN

   ☒ SSL-Verschlüsselung für den Web-Zugang

3. Maßnahmen zur Gewährleistung der Vertraulichkeit der Systeme und Dienste, die einen unautorisierten Zugang oder Zugriff auf personenbezogene Daten verhindern sollen, beim Verantwortlichen selbst oder auf dem Transportweg zum Auftragsverarbeiter oder zu Dritten. Hierzu zählen u.a.: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle und Trennungskontrolle.

   Der Auftragnehmer hat folgende Maßnahmen ergriffen. Kreuzen Sie bitte die zutreffenden Felder an und fügen Sie fehlende Maßnahmen hinzu:

3.1 Zutrittskontrolle



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

☐ Sicherheitsschlösser mit Schlüsselregelung

☒ verschlossene Türen bei Abwesenheit

☒ Fenstersicherung (insbesondere im Erdgeschoss)

☐ Festlegung von Sicherheitsbereichen

☒ Zutrittskontrollsystem (z. B. Ausweisleser, Magnetkarte, Chipkarte, kontrollierte Schlüsselvergabe)

☒ Codeschloss

☒ Protokollierung der Zu- und Abgänge

☒ Zutrittsregelungen für betriebsfremde Personen

☒ Empfang, Werkschutz, Pförtner

☒ Schlüsselmanagement / Dokumentation der Schlüsselverteilung

☒ Türschutz (elektronischer Türöffner; Zahlenschloss etc.)

☐ Zaunanlagen

☒ Alarmanlage

☒ Videoüberwachung

☒ Einrichtung von Sicherheitsbereichen

☒ spezieller Schutz des Serverraums

☐ Überwachungseinrichtung

☐ _____

☐ _____

3.2 Zugangskontrolle

☒ Tastatursicherung durch Schloss

☒ Identifizierung und Authentifizierung einschließlich Verfahrensregelungen zur Kennwortvergabe (Mindest-länge, Sonderzeichen, regelmäßiger Wechsel des Kennworts)

☒ Begrenzung der Fehlversuche

☒ Protokollierung



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

☒ Systemverwalterbefugnisse /-protokollierung

☒ Dunkelschaltung des Bildschirms mit Passwortschutz

☒ Firewall

☒ Einbruchmelde-/Schutzsysteme

☒ Verschlüsselungsverfahren entsprechend dem Stand der Technik

☒ persönliche und individuelle Benutzeranmeldung im System bzw. Netzwerk

☐ Keyword-Richtlinien (Beschreibung der Keyword-Parameter bezüglich Komplexität und Aktualisierungsintervall)

☐ BIOS-Passwörter

☒ zusätzliches System-Login für bestimmte Anwendungen

☒ automatisches Blockieren von Clients nach einer bestimmten Zeitspanne ohne Benutzeraktivität (passwortgeschützter Bildschirmschoner oder automatische Abmeldung)

☒ Verschlüsselung von elektronisch gespeicherten Passwörtern

☐ Aufbewahrung von Datenträgern in abschließbaren Schränken - Datensafes

☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops (z.B. über Betriebssysteme, True Cript, Safe Guard Easy, WinZip, PGP)

☐ _____

☐ _____

3.3 Zugriffskontrolle

☒ Berechtigungskonzept mit differenzierten Berechtigungen

☒ Identifizierung und Authentifizierung

☒ Verschlüsselungsverfahren entsprechend dem Stand der Technik

☒ Aufbewahrung von Datenträgern in verschließbaren Schränken - Data Safes

☒ Verwaltung von Zugriffs- und/oder Berechtigungsrechten sowie von Systemrollen

☒ Dokumentation der Zugriffsrechte

☒ Autorisierungsroutine

☒ Auswertung / Protokollierung



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

☒ Überprüfung / Auditierung (z.B. im Rahmen der ISO-Zertifizierung oder SOX Compliance)

☐ _____

☐ _____

3.4 Weitergabekontrolle

☐ Kennzeichnung der Datenträger

☒ Verschlüsselung von Daten auf Datenträgern bzw. bei der elektronischen Übertragung entsprechend dem Stand der Technik

☐ Bestandsverzeichnis und Bestandskontrolle der Datenträger

☐ Festlegung der zur Abgabe von Datenträgern bzw. zur elektronischen Übertragung berechtigten Personen

☒ Verwendung einer elektronischen Signatur

☐ Festlegung des Empfängerkreises von Daten

☐ Regelungen für den Transport von Datenträgern (z. B. Kurier, verschlossener Behälter)

☒ Einrichtung eines VPN (Virtual Private Network)

☒ Kryptographische Verschlüsselung der übertragenen Daten

☒ Fernwartungskonzept

☒ Protokollierung von Weitergaben und Auswertung der Protokolle

☒ Verschlüsselung von E-Mails

☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops (z.B. über Betriebssysteme, True Cript, Safe Guard Easy, WinZip, PGP)

☒ getunnelter Fernzugriff (z.B. über VPN = Virtual Private Network)

☐ sicherer Transport des physikalischen Datenträgers (z.B. über einen verschlossenen Transportbehälter)

☐ gesichertes WLAN

☒ SSL-Verschlüsselung für den Web-Zugang



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

☐ _____

3.5 Trennungskontrolle

☒ Physikalische Trennung

☒ Logische Trennung

☒ Interne Mandantenfähigkeit

☒ Trennung von Test und Produktion

☒ getrennte Datenbanken

☐ _____

☐ _____

4. Maßnahmen zur Gewährleistung der Integrität der Systeme und Dienste, die gewährleisten, dass personenbezogene Daten nicht (unbemerkt) geändert werden können

Der Auftragnehmer hat folgende Maßnahmen ergriffen. Kreuzen Sie bitte die zutreffenden Felder an und fügen Sie fehlende Maßnahmen hinzu:

4.1 Eingabekontrolle

☒ Protokollierungs- und Protokollauswertungssysteme bezüglich sämtlicher Systemaktivitäten; datenschutz-gerechte Aufbewahrung der Protokolle durch den Auftragnehmer für definierten Zeitraum

☒ organisatorische und technische Absicherung von Berechtigungen, Protokollierungsmaßnahmen, Protokollauswertungen/-revision etc

☐ _____

☐ _____

5. Maßnahmen zur Gewährleistung der Verfügbarkeit der Systeme u. Dienste, die sicherstellen, dass personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn sie gebraucht werden

Der Auftragnehmer hat folgende Maßnahmen ergriffen. Kreuzen Sie bitte die zutreffenden Felder an und fügen Sie fehlende Maßnahmen hinzu:

5.1 Verfügbarkeitskontrolle

☒ Backup-Verfahren (mit Festlegung von Rhythmus, Medium, Aufbewahrungszeit und -ort)



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

☒ Spiegelung von Festplatten

☒ Unterbrechungsfreie Stromversorgung (USV)

☒ Betriebsbereitschaft

☒ Notfallkonzept

☒ Brandmelder

☒ Virenschutz

☒ Firewall

☒ Intrusion Detection Systeme

☐ Zusätzliche Sicherungskopien mit Lagerung an besonders geschützten Orten

☒ Speicherverfahren für Backups (Safe, separater Bereich usw.)

☒ Notfallplan

☒ Klimatisierung des Serverraums

☒ Brand- und Wasserschutz

☒ entsprechende Archivierungseinrichtung

☐ _____

☐ _____

5.2 Auftragskontrolle

☒ Schriftliche Festlegung der Weisungen

☒ Festlegung von turnusgemäßen Kontrolle des Auftragnehmers durch den Auftraggeber

☒ Regelmäßige interne Kontrolle und Dokumentation des Auftragnehmers, dass Weisungen und Regelungen zur Auftragsdurchführung beachtet werden

☒ Berichte über Sicherheitsvorfälle an den Kunden

☒ Regelmäßige Schulung der Mitarbeiter mit Zugriffsrechten

☒ Festlegung von Ansprechpartnern und Verantwortlichkeiten

☐ _____



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

☐ _____

6. Maßnahmen zur Gewährleistung der Belastbarkeit der Systeme u. Dienste, die sicherstellen, dass die Systeme und Dienste so ausgelegt sind, dass auch punktuell hohe Belastungen oder hohe Dauerbelastungen von Verarbeitungen leistbar bleiben

   Der Auftragnehmer hat folgende Maßnahmen ergriffen. Kreuzen Sie bitte die zutreffenden Felder an und fügen Sie fehlende Maßnahmen hinzu:

   ☒ Maßnahmen hins. Speicher-, Zugriffs- und Leitungskapazitäten

   ☐ _____

   ☐ _____

7. Maßnahmen, um nach einem physischen oder technischen Zwischenfall die Verfügbarkeit personenbezogenen Daten und den Zugang zu ihnen rasch wiederherzustellen.

   Der Auftragnehmer hat folgende Maßnahmen ergriffen. Kreuzen Sie bitte die zutreffenden Felder an und fügen Sie fehlende Maßnahmen hinzu:

   ☒ Backup-Konzept (unter Angabe von Häufigkeit, Medium, Verweildauer und Standort)

   ☒ Redundante Datenspeicherung

   ☒ Cloud-Services

   ☐ Doppelte IT-Infrastruktur

   ☒ Schatten-Rechenzentrum

   ☐ _____

   ☐ _____

8. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen.

   Der Auftragnehmer hat folgende Maßnahmen ergriffen. Kreuzen Sie bitte die zutreffenden Felder an und fügen Sie fehlende Maßnahmen hinzu:

   ☒ Entwicklung eines Sicherheitskonzepts

   ☐ Prüfungen des DSB, der IT-Revision

   ☒ Externe Prüfungen, Audits, Zertifizierungen



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com

☐ _____

☐ _____

| | |
|---|---|
| 22.05.2024 Münster | 15.05.2024 Düsseldorf |
| Datum, Ort | Datum, Ort |
| Unterschrift (Kunde) | Unterschrift (Anbieter) |
| Runde, Martin, Geschäftsführer | Hilgers Sascha, Country Manager |
| Name, Vorname, Funktion | Name, Vorname, Funktion |



iLOQ Oy

Yrttipellontie 10
90230 Oulu, Finland
VAT-Nr.: FI18428216

Tel +358 40 3170 200

www.iLOQ.com