Datenschutz -Konzept

Der sichere Umgang mit Xovis Sensoren und dem Vemco Cloudservice

eastek
systems gmbh

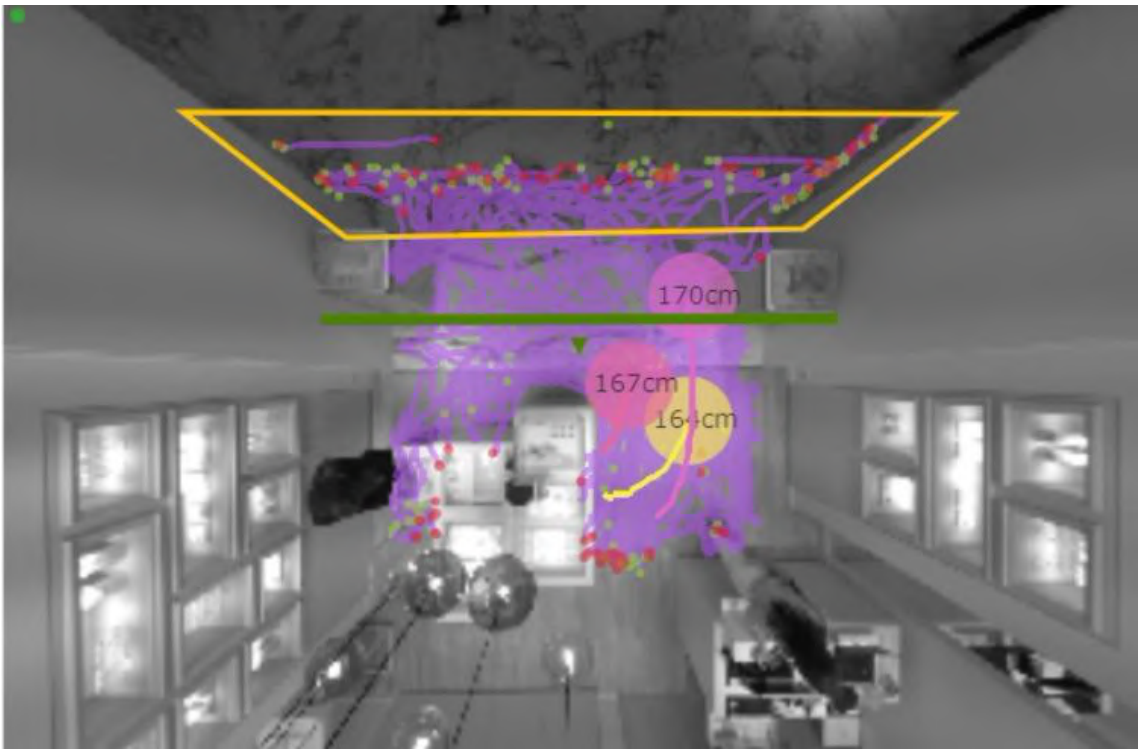
Dieses Konzept dient Behörden, Betriebsräten, Personalorganisationen und anderen Aufsichtsorganisationen als Beleg für die Konformität gemäß EU-DSGVO

Es werden keine personenbezogenen Daten erhoben, dies wird gemäß den folgenden Ausführungen sichergestellt. Grundlage unserer Ausführung sind die Begriffsbestimmungen des Artikel 4 DSGVO, Stand 27.04.2016.

Die gesamte Analyse findet auf dem Sensor statt. Keine Bilder mit personenbezogenen Informationen sind sichtbar. Der Sensor ersetzt Bewegtbilder in ECHTZEIT durch Farbkreise (Privacy Mode 1).

Wenn vor Ort ein Besucher-Tracking eingerichtet, dann wird ein Klarbild für den Zeitraum der Einrichtung benötigt. Nach der Einrichtung wird der Sensor in den Pricacy Mode 1 versetzt.

Bild 1 zeigt die verschiedenen erzeugten Farbkreise. Die angegebenen Größenangaben variieren wenn sich die Personen bewegen, auch so lassen sich keinerlei Rückschlüsse auf Personen ziehen.



eastek systems gmbh

Was bedeuten die Privacy Modes des Sensors ?

Level 0: Keine Einschränkungen, Livebild und Trackinginformationen von Personen ist sichtbar

Level 1: Kein Videostream ist sichtbar. Nur das Standbild des Raumes ohne Personen ist sichtbar. Sichtbar sind die Trackingdaten der erfassten Personen, die sich durch das Bild bewegen. Diese Informationen geben keinerlei Aufschluss auf personenbezogene Daten

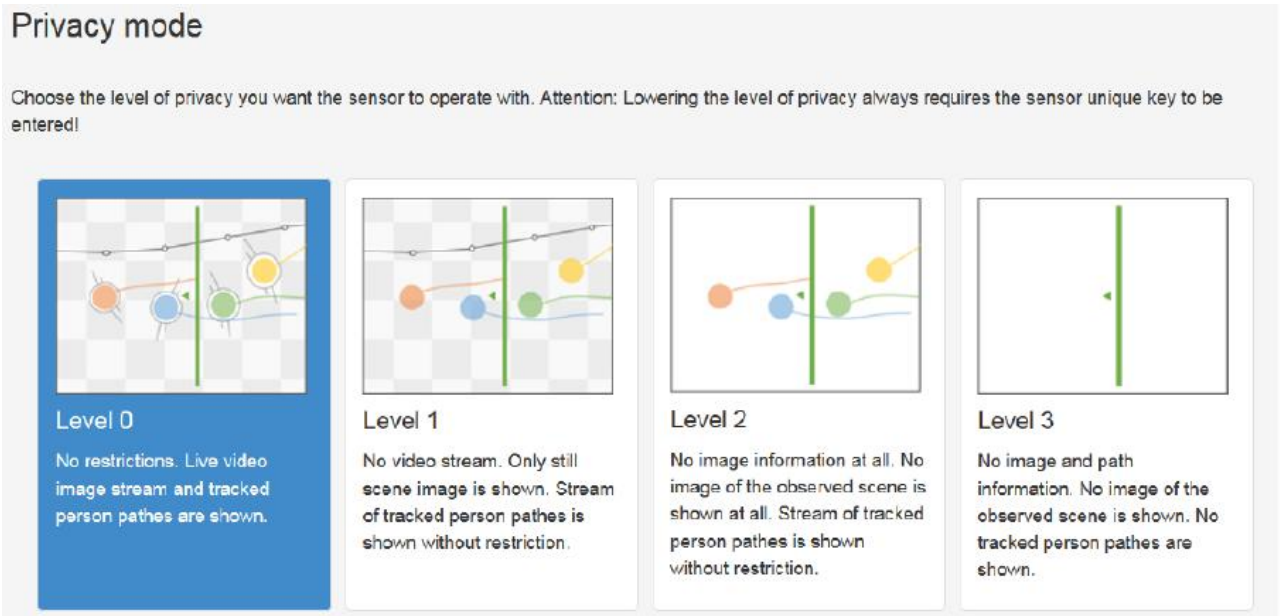
Level 2: Kein Bild ist sichtbar, nur die Trackingdaten der erfassten Personen, die sich durch das Bild bewegen.

Level 3: Kein Bild und keine Trackingdaten sind sichtbar. Nur die Zähllinie und die Zählergebnisse sind sichtbar.

Die Level 1,2 und 3 entsprechen den Anforderungen der EU-DSGVO.
Als Standard gilt bei Eastek der Level 1, bei dem Personen in Echtzeit durch Farbkreise ersetzt werden.

Zur Nutzung der “on Board” Analysefunktionen und Einstellungen kann der Kunde das Passwort des Sensors in einer individuellen Grundauslegung erhalten.
Die Anonymisierungsfunktionen / Privacy Level lassen sich darüber nicht verändern.

Auch über das Administrator Passwort lässt sich der Privacy Mode nicht zurücksetzen.
Der Privacy Mode lässt sich nur über den Sensor Mastser Key zurücksetzen. Dieser bleibt Eigentum der eastek systems gmbh und wird dem Kunden nicht überlassen. Somit ist sichergestellt, dass der Privacy Mode nicht auf ein niedrigeres Niveau eingestellt werden kann.



eastek systems gmbh

Welche Bilddaten bzw. Bilder werden an den Cloudservice übertragen oder gespeichert ?

Es werden keinerlei Bilddaten gespeichert oder übertragen. Die Analyse der Bewegtbilder erfolgt in Echtzeit auf dem Sensor, es gibt keine separate Recheneinheit.

Welche Daten werden vom Sensor an den Cloudservice übertragen ?

Es werden ausschließlich Metadaten übertragen, keinerlei Bilddaten, keine personenbezogenen Daten.

Links sehen Sie ein Beispiel von Datensätzen, die vom Sensor übertragen werden können.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <ns2:count-data-sequence xmlns:ns3="http://www.xovis.com/count-line-sequence"
  xmlns:ns4="http://www.xovis.com/common-types"
  xmlns="http://www.xovis.com/sensor-status"
  xmlns:ns2="http://www.xovis.com/count-data-sequence">
    - <ns2:sensor>
        <serial-number>00:1E:C0:AE:34:BB</serial-number>
        <ip-address>10.10.10.204</ip-address>
        <name>Entrance</name>
        <group>Xovis Office</group>
        <device-type class="COUNTER">PC2</device-type>
      </ns2:sensor>
      <ns2:date-from>2015-06-30T15:45:00+02:00</ns2:date-from>
      <ns2:date-to>2015-06-30T16:00:00+02:00</ns2:date-to>
      <ns2:granularity seconds="900">FIFTEEN_MINUTES</ns2:granularity>
    - <ns2:count-lines>
        - <ns2:count-line line-name="Entrance Xovis" line-id="0">
            - <ns2:count-values>
                - <ns3:value>
                    <ns3:time>2015-06-30T16:00:00+02:00</ns3:time>
                    <ns3:fw-count>3</ns3:fw-count>
                    <ns3:bw-count>3</ns3:bw-count>
                  </ns3:value>
              </ns2:count-values>
          </ns2:count-line>
        - <ns2:count-line line-name="Elevator" line-id="1">
            - <ns2:count-values>
                - <ns3:value>
                    <ns3:time>2015-06-30T16:00:00+02:00</ns3:time>
                    <ns3:fw-count>0</ns3:fw-count>
                    <ns3:bw-count>0</ns3:bw-count>
                  </ns3:value>
              </ns2:count-values>
          </ns2:count-line>
      </ns2:count-lines>
    - <ns2:request-status>
        <ns4:status>OK</ns4:status>
      </ns2:request-status>
</ns2:count-data-sequence>
```

eastek systems gmbh

Technische Daten des Sensors Xovis PC Serie und Informationen für Ihre IT Abteilung:

Installationshöhe:	2.2 – 6.0m
Stromverbrauch:	7W
Größe:	13.0 x 9.4 x 3.0cm
Mindesbeleuchtung:	2 Lux
Spannungsversorgung:	POE IEEE 802.3af
Protokolle:	IPv4, HTTP(S), 802.1x, DNS, TCP, UDP, DHCP, (S)FTP, MQTT
Bandbreite je Sensor:	Ideale Bandbreite: >200 KB/s Bandbreite: 100 KB/s (Konfiguration, Live-Ansicht liefert begrenzte Bilder pro Sekunde)Datenübertragung: <20KB/s (keine Web UI Nutzung)Hinweis: Die tatsächlich benötigte Bandbreite hängt davon ab, wie viele Daten-Push-Agenten, ObjectStreams etc. verwendet werden.
Datenspeicher:	120 Tage, abhängig von der Anzahl der Zonen und Zähllinien
Unterstützte Browser:	Chrome 61 or newer (recommended), Edge 40 / EdgeHTML 15 or newer, Safari 10.1 or newer,Microsoft Internet Explorer 11*
Benötigte Ports:	80 und 443

Die Sensoren können auf feste IP Adressen Ihrer entsprechenden Range eingestellt werden.

Alternativ zur Nutzung in Ihrem Netzwerk, können auch LTE Router eingesetzt werden.

Die Metadaten werden an den Vemco-Cloudservice gesendet, welcher bei AWS in Frankfurt gehostet ist.

Sofern es aus betrieblichen Gründen nicht möglich ist, das vorhandene Netzwerk zu nutzen, so können wir jederzeit einen LTE Router einsetzen über den die Daten übertragen werden.

eastek systems gmbh

Declaration of Product Data Privacy

To whom it may concern,

Data Privacy is a major focus area for Xovis and a reason why our Founders set up the company in 2008.

Since General Data Protection Regulation (GDPR) went into effect we ensured that all our products are compliant with the new framework. In fact, this was primarily paperwork instead of adapting the product. We looked out for a certification which confirms the fact that we are compliant. As there is no governmental body who certifies a product according to GDPR we must rely on private initiatives. We selected a German institute because of Germany's track record of setting a strong focus on data privacy. We submitted our products for the renowned ePrivacy Seal. The certificate is available on our website. As part of the process, a detailed legal assessment has been done. Due to the detailed nature how our products have been scrutinized, we are not able to share the expert report itself.

Two points that we would like to highlight regarding data privacy and GDPR on our sensors:

Our approach is based on two image sensors which capture an image of the scenery from an overhead point of view. The images are processed internally on the sensor in a closed hardware environment. On this level an abstract 3D image is generated to track a person as well a Deep Neuronal Network (DNN) analyzes the images and classifies an object based on a trained configuration. After this processing, no image is needed nor further processed and only the configured data points are transferred to the internal system for statistical reasons. No image will be stored during this process. Everything is processed in real time. Based on the fact that attributes (such as gender, view direction, mask detection and any future attribute we may add) cannot be matched back to an individually person, we fully comply with GDPR.

For Wifi based analytics we ensure data privacy by hashing an individual MAC Address with a customized key which makes it impossible to identify a specific person or the according device in a later stage. Only hashed addresses leave the device.

For more information on the ePrivacy Seal please check: https://www.eprivacy.eu/en/privacy-seals/eprivacyseal/

Signed for and on behalf of: **XOVIS AG**

Zollikofen	14.12.2021	Florian Eggenschwiler, CPO	
Place	Date of issue	Name, Function	Signature

XOVIS AG
Industriestrasse 1
CH-3052 Zollikofen

Phone: +41 32 342 04 70 · www.xovis.com · info@xovis.com

CERTIFICATE

no. 355/21

ePrivacyseal GmbH
Große Bleichen 21, 20354 Hamburg, Germany

hereby certifies* that

as determined in the certification decision of 10 June 2021

Xovis AG
Industriestrasse 1, CH-3052 Zollikofen, Switzerland

operates its product or service
„3D Sensor (PC2, PC3, PC4, PC2S, PC3S, PC4S, PCT1, PC2R)“
version 21/05/2021
as defined in annex 1 and to the exclusion of the processing activities in annex 2 to this certificate

in conformity with the criteria catalogue of ePrivacyseal GmbH, version 2.1. of May 2018.

final audit day: 04/06/2021
next planned monitoring by 29/01/2023
period of validity: 30/01/2021 – 29/01/2023

*ePrivacyseal GmbH is not an accredited certification body within the meaning of art. 42(5) GDPR.

Annex 1 to certificate no. 355/21

Definition of processing activities

Xovis AG develops, manufactures and distributes people flow counting technology based on its own portfolio of 3D people tracking sensors. In addition to the sensor system, Xovis develops software solutions tailored to the specific applications of the different markets.

Xovis' customers buy, integrate and/or operate these devices on their premises, to which the general public (e.g. shopping malls, airports, etc.) or other, more narrowly defined groups of persons (e.g. employees in office spaces) have access.

The specific type of end-customer notwithstanding, Xovis does neither own nor operate sensor devices once they have been sold and were mounted in the target environment. In analogy, this applies also to the data captured and transmitted by these sensors to the technical systems of their respective owners.

Annex 2 to certificate no. 355/21

Excluded processing activities

All processing carried out by the controller, Xovis' customer, are out of scope.

Annex 3 to certificate no. 355/21

Validity Conditions

The seal is awarded on the validity condition that optical sensors operate in Privacy Level 2 or 3 and WiFi and/or Bluetooth identifiers are hashed using a strong salt.

*ePrivacyseal GmbH is not an accredited certification body within the meaning of art. 42(5) GDPR.

Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Inhaltsverzeichnis

1.0	**Vertraulichkeit**	**3**
1.1	Zutrittskontrolle	3
1.2	Zugangskontrolle	4
1.3	*Zugriffskontrolle*	5
1.4	*Trennungskontrolle*	5
1.5	*Pseudonymisierung*	6
2.0	**Integrität**	**7**
2.1	Weitergabekontrolle	7
2.2	Eingangskontrolle	7
3.0	**Verfügbarkeit und Belastbarkeit**	**9**
3.1	Verfügbarkeitskontrolle	9
4.0	**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**	**10**
4.1	Datenschutz-Maßnahmen	10
4.2	Incident-Response-Management	11
4.3	Datenschutzfreundliche Voreinstellungen	11
4.4	Auftragskontrolle (Outsourcing an Dritte)	12

1.0 Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
■ Alarmanlage	■ Schlüsselregelung / Liste
■ Automatisches Zugangskontrollsystem	☐ Empfang / Rezeption / Pförtner
☐ Biometrische Zugangssperren	☐ Besucherbuch / Protokoll der Besucher
■ Chipkarten / Transpondersysteme	☐ Mitarbeiter- / Besucherausweise
■ Manuelles Schließsystem	■ Besucher in Begleitung durch Mitarbeiter
■ Sicherheitsschlösser	☐ Sorgfalt bei Auswahl des Wachpersonals
☐ Schließsystem mit Codesperre	■ Sorgfalt bei Auswahl Reinigungsdienste
☐ Absicherung der Gebäudeschächte	☐
■ Türen mit Knauf Außenseite	☐
■ Klingelanlage mit Kamera	☐
■ Videoüberwachung der Eingänge	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen bitte hier beschreiben:

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).

Technische Maßnahmen	**Organisatorische Maßnahmen**
■ Login mit Benutzername + Passwort	■ Verwalten von Benutzerberechtigungen
☐ Login mit biometrischen Daten	☐ Erstellen von Benutzerprofilen
■ Anti-Viren-Software Server	☐ Zentrale Passwortvergabe
■ Anti-Virus-Software Clients	■ Richtlinie „Sicheres Passwort"
■ Anti-Virus-Software mobile Geräte	■ Richtlinie „Löschen / Vernichten"
■ Firewall	☐ Richtlinie „Clean desk"
■ Intrusion Detection Systeme	☐ Allg. Richtlinie Datenschutz und / oder Sicherheit
☐ Mobile Device Management	☐ Mobile Device Policy
☐ Einsatz VPN bei Remote-Zugriffen	☐ Anleitung „Manuelle Desktopsperre"
☐ Verschlüsselung von Datenträgern	☐
☐ Verschlüsselung Smartphones	☐
☐ Gehäuseverriegelung	☐
■ BIOS Schutz (separates Passwort)	☐
☐ Sperre externer Schnittstellen (USB)	☐
■ Automatische Desktopsperre	☐
■ Verschlüsselung von Notebooks / Tablet	☐
☐	☐
☐	☐
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen:

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐ Aktenschredder (mind. Stufe 3, cross cut)	■ Einsatz Berechtigungskonzepte
■ Externer Aktenvernichter (DIN 32757)	■ Minimale Anzahl an Administratoren
■ Physische Löschung von Datenträgern	☐ Datenschutztresor
■ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☐ Verwaltung Benutzerrechte durch Administratoren
☐	☐
☐	☐

Weitere Maßnahmen:

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐ Trennung von Produktiv- und Test-umgebung	☐ Steuerung über Berechtigungskonzept
☐ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☐ Festlegung von Datenbankrechten
☐ Mandantenfähigkeit relevanter Anwendungen	☐ Datensätze sind mit Zweckattributen versehen
☐	☐
☐	☐

Weitere Maßnahmen:

1.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technichen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	☐ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
☐	☐
☐	☐

Weitere Maßnahmen:

eastek verarbeitet keine personenbezogenen Daten

2.0 Integrität

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	**Organisatorische Maßnahmen**
■ Email-Verschlüsselung	☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☐ Einsatz von VPN	☐ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☐ Protokollierung der Zugriffe und Abrufe	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☐ Sichere Transportbehälter	☐ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☐ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☐ Persönliche Übergabe mit Protokoll
☐ Nutzung von Signaturverfahren	☐
☐	☐
☐	☐

Weitere Maßnahmen: eastek verarbeitet keine personenbezogenen Daten

2.2 Eingangskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
■ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☐ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☐ Manuelle oder automatisierte Kontrolle der Protokolle	■ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☐	■ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐	☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verar-beitungen übernommen wurden
☐	☐ Klare Zuständigkeiten für Löschungen

Weitere Maßnahmen: eastek verarbeitet keine personenbezogenen Daten

3.0 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
■ Feuer- und Rauchmeldeanlagen	☐ Backup & Recovery-Konzept (ausformuliert)
☐ Feuerlöscher Serverraum	☐ Kontrolle des Sicherungsvorgangs
■ Serverraumüberwachung Temperatur und Feuchtigkeit	☐ Regelmäßige Tests zur Datenwiederherherstellung und Protokollierung der Ergebnisse
☐ Serverraum klimatisiert	☐ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
■ USV	☐ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
■ Schutzsteckdosenleisten Serverraum	☐ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☐ Datenschutztresor (S60DIS, S120DIS andere geeignete Normen mit Quelldichtung etc.)	☐ Getrennte Partitionen für Betriebs-systeme und Daten
☐ RAID System / Festplattenspiegelung	☐
■ Videoüberwachung Serverraum	☐
☐ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☐
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen: eastek verarbeitet keine personenbezogenen Daten und betreibt keinen Server, daher ist nicht eastek sondern der Serverhoster AWS nach ISO27001 zertifiziert.

4.0 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Software-Lösungen für Datenschutz-Management im Einsatz	☐ Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten
■ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	■ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
☐ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	■ Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
☐ Anderweitiges dokumentiertes Sicherheitskonzept	☐ Interner / externer Informationssicherheitsbaauftragter Name / Firma Kontakt
☐ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	■ Die Datenschutz-Folgenabschätzung (DSFA wird bei Bedarf durchgeführt)
☐	■ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
☐	☐ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
☐	☐
☐	☐

Weitere Maßnahmen: eastek verarbeitet keine personenbezogenen Daten und betreibt keinen Server, daher ist nicht eastek sondern der Serverhoster AWS nach ISO27001 zertifiziert.

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
■ Einsatz von Firewall und regelmäßige Aktualisierung	☐ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
■ Einsatz von Spamfilter und regelmäßige Aktualisierung	☐ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
■ Einsatz von Virenscanner und regelmäßige Aktualisierung	☐ Einbindung von ☐ DSB und ☐ ISB in Sicherheitsvorfälle und Datenpannen
☐ Intrusion Detection System (IDS)	■ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☐ Intrusion Prevention System (IPS)	☐ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvor-fällen und Datenpannen
☐	☐
☐	☐

Weitere Maßnahmen:

4.3 Datenschutzfreundliche Voreinstellungen

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
■ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☐
■ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	☐
☐	☐
☐	☐

Weitere Maßnahmen: eastek verarbeitet keine personenbezogenen Daten

4.4 Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
☐	☐ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
☐	■ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
☐	☐ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standardvertragsklauseln
☐	☐ Schriftliche Weisungen an den Auftragnehmer
☐	☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☐	☐ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
☐	☐ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
☐	☐ Regelung zum Einsatz weiterer Subunternehmer
☐	☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐	☐ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Weitere Maßnahmen: Nicht zutreffend

alternativ:

☒ *Hiermit versichern wir, keine Subunternehmer im Sinne einer Auftragsverarbeitung einzusetzen.*

Ausgefüllt für die Organisation durch

Name	Andreas Hahnhausen
Funktion	CEO
Rufnummer	01724494084 / 040 68 28 20 11
Email	hahnhausen@eastek.de

Ort, Datum Stapelfeld, 2022

Vom Auftraggeber auszufüllen:

Geprüft am *durch* *. Ergebnis(se):*

☐ *Es besteht noch Klärungsbedarf zu*

☒ *TOM sind für den angestrebten Schutzzweck ausreichend*

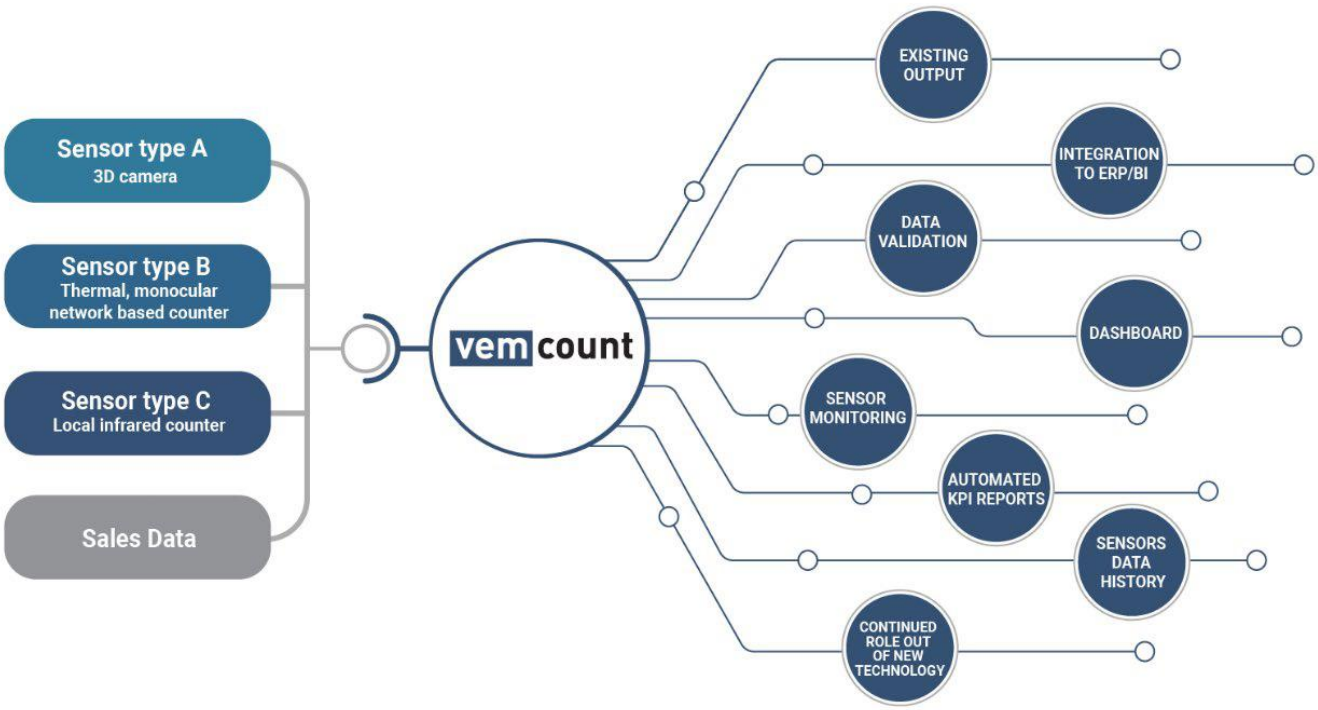
☒ *Vereinbarung Auftragsverarbeitung kann geschlossen werden*

Hinweis: *Diese Vorlage verwendet noch Begrifflichkeiten des BDSG a.F. Inhaltlich unterscheiden sich die technischen und organisatorischen Maßnahmen nicht von denen, die in der DSGVO gefordert werden!*

Vemco Cloudservice

Mit dem Vemco Cloudservice können wir eine Vielzahl von Sensoren miteinander kombinieren.

Sollte der Xovis Sensor z.B. auf Stockwerksebene Besucherzahlen ermitteln, so können zusätzliche Sensoren die Temperatur in einzelnen Bereichen ermitteln oder Desk Sensoren, freie Schreibtische in Coworking Spaces ausweisen.



eastek systems gmbh

Vemco Cloudservice

Mit dem Vemco Cloudservice können wir eine Vielzahl von Sensoren miteinander kombinieren.

Sollte der Xovis Sensor z.B. auf Stockwerksebene Besucherzahlen ermitteln, so können zusätzliche Sensoren die Temperatur in einzelnen Bereichen ermitteln oder Desk Sensoren, freie Schreibtische in Coworking Spaces ausweisen.

Den Cloudservice Nutzern werden Rollen zugewiesen, um sicherzugehen, dass jeder Nutzer nur die Daten sieht, die für ihn bestimmt sind.

Der Cloudservice ist gehostet bei Amazon AWS in Frankfurt und die Daten verbleiben innerhalb Deutschlands.

AWS ist zertifiziert nach ISO 27001, der anerkanntesten internationalen Norm für Informationssicherheits-Managementsysteme. Sie legt die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems (ISMS) fest.

Der Login in den Cloudservice ist mit Benutzername und Passwort, sowie der optionalen 2 Faktor Authentifizierung geschützt.

Eastek Systems

Alle Mitarbeiter sind unterwiesen in den sicheren und verantwortungsvollen Umgang mit der Informationstechnologie. Dies ersehen Sie auch in den technischen- und organisatorischen Maßnahmen.

Jährlich werden gemeinsam, die getroffenen Verpflichtungen geprüft, besprochen und weiter entwickelt.

eastek
systems gmbh

Certificate

Certificate number: 2013-009

Certified by EY CertifyPoint since: November 18, 2010

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/A1:2020, the Information Security Management System as defined and implemented by

Amazon Web Services, Inc.*

and its affiliates (collectively referred to as Amazon Web Services (AWS)) are compliant with the requirements as stated in the standard:

ISO/IEC 27001:2013

Issue date of certificate: November 5, 2019
Re-issue date of certificate: March 22, 2022
Expiration date of certificate: November 7, 2022
Last certification cycle expiration date: November 7, 2019

EY CertifyPoint will, according to the certification agreement dated October 25, 2019, perform surveillance audits and acknowledge the certificate until the expiration date noted above.

**With regard to the specific requirements for information security as stated in the Statement of Applicability, version 2021.01 dated September 30, 2021, this certification is applicable to (a) the services and their associated assets and locations as described in the scoping section of this certificate, and (b) any affiliates that are responsible for, or that contribute to, the provision of such services and their associated assets and locations.*

DocuSigned by: 30 March 2022 | 1:23:58 PM CEST
Jatin Sehgal
6E3A0F2A5EBF4C7...

J. Sehgal | Director, EY CertifyPoint

Amazon Web Services, Inc.

Scope for certificate 2013-009

The scope of this ISO/IEC 27001:2013 certification is bounded by specified services of Amazon Web Services, Inc. and specified facilities. The Information Security Management System (ISMS) is centrally managed out of Amazon Web Services, Inc. headquarters in Seattle, Washington, United States of America.

The in-scope applications, systems, people, and processes are globally implemented and operated by teams out of an explicit set of facilities that comprise Amazon Web Services, Inc. and are specifically defined in the scope and bounds.

The Amazon Web Services, Inc. ISMS scope includes the services as mentioned on https://aws.amazon.com/compliance/iso-certified/, the locations and AWS Service and Supporting Resources are stated in the following section of this certificate.

The Information Security Management System mentioned in the above scope is restricted as defined in "PISMS Manual" version 2022.02, dated March 2, 2022.

Amazon Web Services, Inc.

Scope for certificate 2013-009

Locations in scope:

AWS Services are offered and available across multiple geographic regions around the world. The scope of AWS infrastructure includes corporate headquarters, data center facilities, network and server hardware, and resources which support the datacenter operations.

AWS data centers, which house the hardware supporting the AWS Services listed above. AWS Data centers are located in US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-East), AWS GovCloud (US-West), Canada (Montréal), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), EU (Stockholm), EU (Milan), Asia Pacific (Hong Kong), Asia Pacific (Singapore), Asia Pacific (Mumbai), Asia Pacific (Osaka), Asia Pacific (Seoul), Asia Pacific (Sydney), Asia Pacific (Tokyo), South America (São Paulo) Regions, Middle East (Bahrain), Asia Pacific (Jakarta), South Africa (Cape Town), as well as the following:

AWS Edge Locations in:

- Buenos Aires, Argentina
- Canberra, Australia
- Melbourne, Australia
- Alexandria, Australia
- Perth, Australia
- Sydney, Australia
- Ultimo, Australia
- Vienna, Austria
- Manama, Bahrain
- Brussels, Belgium
- Rio de Janeiro, Brazil
- São Paulo, Brazil
- Montréal, Canada
- Toronto, Canada
- Vancouver, Canada
- Santiago, Chile
- Bogota, Colombia
- Prague, Czech Republic
- Hong Kong, China
- Copenhagen, Denmark
- London, England
- Manchester, England
- Slough, England
- Stretford, England
- Tallinn, Estonia
- Helsinki, Finland
- Marseille, France
- Paris, France
- Berlin, Germany
- Frankfurt, Germany
- Munich, Germany
- Athens, Greece
- Budapest, Hungary
- Bengaluru, India
- Chennai, India
- Hyderabad, India
- Kolkata, India
- Mumbai, India
- New Delhi, India
- Jakarta, Indonesia
- Dublin, Ireland
- Parkwest, Ireland
- Tel Aviv, Israel
- Milan, Italy
- Palermo, Italy
- Rome, Italy
- Osaka, Japan
- Tokyo, Japan

Amazon Web Services, Inc.

Scope for certificate 2013-009

- Nairobi, Kenya
- Seoul, Korea
- Kuala Lumpur, Malaysia
- Amsterdam, Netherlands
- Noord Holland, Netherlands
- Oslo, Norway
- Manila, Philippines
- Warsaw, Poland
- Singapore
- Cape Town, South Africa
- Johannesburg, South Africa
- Madrid, Spain
- Stockholm, Sweden
- Zurich, Switzerland
- Taipei, Taiwan
- Dubai, United Arab Emirates
- Fujairah, United Arab Emirates
- Arizona, United States
- California, United States
- Colorado, United States
- Florida, United States
- Georgia, United States
- Illinois, United States
- Massachusetts, United States
- Minnesota, United States
- Missouri, United States
- Nevada, United States
- New Jersey, United States
- New York, United States
- Ohio, United States
- Oregon, United States
- Pennsylvania, United States
- Texas, United States
- Virginia, United States
- Washington, United States
- Hanoi, Vietnam
- Ho Chi Minh, Vietnam

Wavelength locations in:

- Osaka, Japan
- Tokyo, Japan
- Daejeon, Korea
- California, United States
- Colorado, United States
- Florida, United States
- Georgia, United States
- Maryland, United States
- Massachusetts, United States
- Nevada, United States
- New Jersey, United States
- Texas, United States
- Washington, United States

Local zone locations in:

- Arizona, United States
- California, United States
- Colorado, United States
- Florida, United States
- Massachusetts, United States
- Missouri, United States [1]
- Texas, United States

[1] This is a Local Zone location. This Local Zone may not be available to all customers.