Datenschutz-Hinweise zu Video-Sicherheits-Systemen (VSS)

Whitepaper

BeyondHumanVision

MOBOTIX

1 Grundzüge des europäischen Datenschutzrechtes (DS-GVO, Öffnungsklauseln, BDSG, Landesgesetze)

Das europäische Datenschutzrecht wurde durch die am 25.05.2018 in Kraft getretene europäische Datenschutz-Grundverordnung (EU DSGVO 2016/679) für alle Mitgliedsländer der EU neu geregelt. Da es sich hierbei um eine Verordnung und nicht wie vorher um eine Richtlinie handelt, ist diese direkt in allen Ländern der EU rechtswirksam. Mitgliedsländer dürfen nur im Bereich der so genannten Öffnungsklauseln erläuternde bzw. präzisierende Gesetze erlassen. Sollte es hierdurch ggf. zu widersprüchlichen Regelungen kommen, hat die DSGVO als übergeordnete Verordnung primäre Gültigkeit.

In Deutschland greift das gleichzeitig überarbeitete Bundesdatenschutzgesetz (BDSG) die Öffnungsklauseln auf. Hier wird speziell im §4 das Thema Video näher spezifiziert. Zusätzlich gibt es in Deutschland noch verschiedene, weiter ausführende Landesgesetze.

Für den Bereich der Strafverfolgungsbehörden wurde auf europäischer Ebene die Richtlinie 2016/680 und für den Bereich der Fluggastdaten die Richtlinie 2016/681 erlassen. Zur Rechtswirksamkeit erfordern diese auf nationaler Ebene die Verabschiedung zugehöriger nationaler Gesetze. Dies ist in Deutschland z.B. durch länderspezifische Landespolizeigesetze erfolgt.

Unter dem Eindruck der Anschläge in Ansbach und München im Sommer 2016 wurde noch im gleichen Jahr in Deutschland das Videoüberwachungsverbesserungsgesetz erlassen. Dies sollte den Einsatz von Video-Sicherheits-Systemen bei Großveranstaltungen vereinfachen, in dem es die Gewichtung der Schutzinteressen der betroffenen Personen zu Gunsten des berechtigten Interesses der öffentlichen Hand zur Risikominimierung verschob. Wesentliche Teile davon sind bei der Überarbeitung des BDSG in 2018 in den §4 (1) eingeflossen.

2 Datenschutz in MOBOTIX Kameras

MOBOTIX steht dafür, im IT-Bereich Video-Sicherheits-Systeme zu entwickeln und zu vermarkten, die hohen Sicherheitsansprüchen gerecht zu werden. Hierzu hat MOBOTIX das richtungsweisende „Cactus-Konzept“ zur IT-Sicherheit entwickelt.

Die beiden Bereiche IoT-Kameras und MOBOTIX-MOVE Kameras verfolgen dabei aus unterschiedlichen Ansätzen die gleichen Sicherheits-Ziele.

2.1 MOBOTIX IoT-Kameras

Diese Kameras zeichnen sich aus durch das dezentrale Konzept, bei dem die Bildbearbeitung, Analyse und Speicherung in der Kamera durchgeführt bzw. von der Kamera verschlüsselt und gesteuert wird. Dies bietet hierdurch systembedingt einen erhöhten Schutz vor Datenverlust oder fremdem Zugriff beim Bildtransfer.

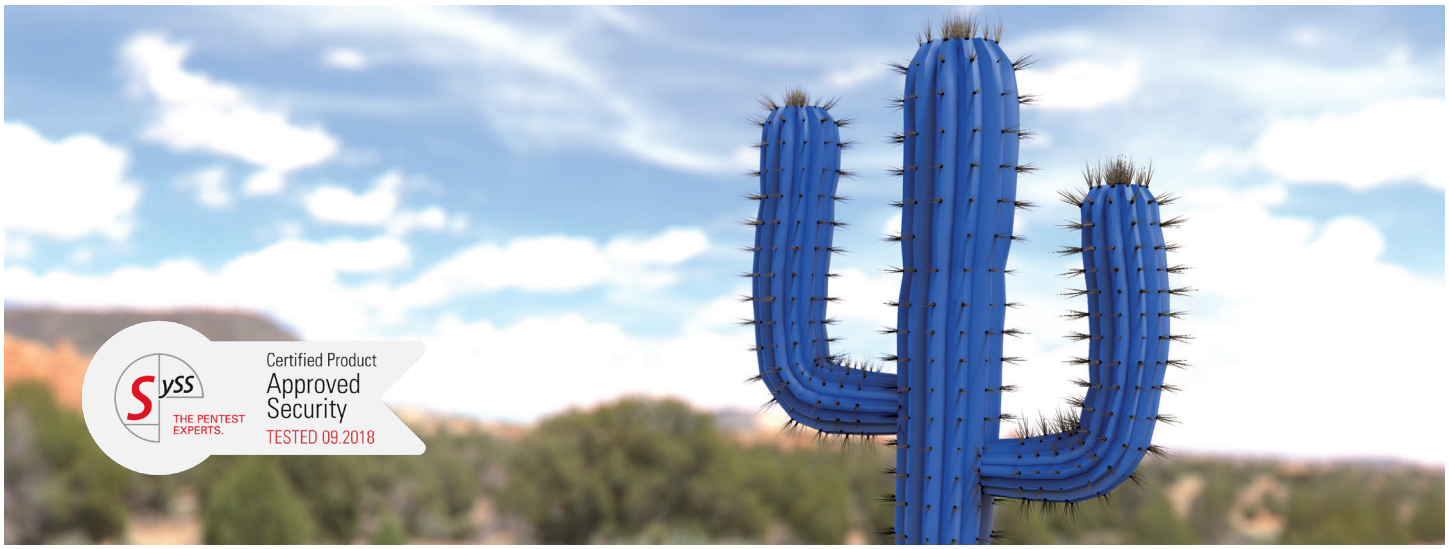
2.1.1 Browser Bedienung

Bei einer Bedienung der IoT-Kameras über einen Browser können bei Bedarf die Softbuttons und drop down Menüs ausgeblendet werden, um unberechtigte Umschaltungen zu verhindern.

Wenn in der Live-Ansicht des Browsers über einen Softbutton der Modus „Privatsphäre“ aktiviert wird, ist der Zugriff auf Livebilder und Bildrecherchen gesperrt. Diese Einstellung ist 24 Stunden oder bis zur manuellen Aufhebung gültig.

2.1.2 Sichere Verbindungen

Die MOBOTIX IoT-Kameras stellen eine sogenannte Funktion HSTS zur Verfügung. Bei HSTS wird vom Browser eine einwandfreie HTTPS Verbindung erzwungen, was einen maximalen Schutz vor Man-in-the-Middle Angriffen bietet.



MOBOTIX
BeyondHumanVision

2.1.3 Admin-Bereich

Über den Admin-Bereich werden unterschiedliche Sicherheits-Einstellungen der Kameras konfiguriert und verwaltet:

a) Benutzerrechte:

Der Zugriff auf Kamerabilder ist in Werkseinstellung als „öffentlicher Zugriff“ ohne Passwort zu Konfigurationszwecken möglich. Diese Zugriffsmöglichkeit sollte bei der Kamerakonfiguration nach Änderung des admin-Passwortes bzw. Anlegen von individuellen Benutzern deaktiviert werden, damit jeglicher Zugriff auf die Kamera nur noch passwortgeschützt möglich ist. Die Kamera ist durch eine Rechteverwaltung auf **drei Ebenen** abgesichert:

- **Gast:** Mit diesen Nutzerrechten ist nur der Zugriff auf Livebilder mit reduzierter Bildwiderholrate möglich.
- **User:** Auf dieser Benutzerebene können die Funktionen des Setup-Menüs zu den Bildeinstellungen, Ereignissen, Aktionen und Bildspeicherung als auch nicht gesperrte Browserfunktionen ausgeführt werden.
- **Admin:** Benutzer auf diesem Rechtelevel können über das admin-Menü alle sicherheitsrelevanten Einstellungen der Kamera konfigurieren.

b) Admin-Passwort:

Bei erstmaligem Aufruf der Admin-Seite wird man aufgefordert, die werksseitigen Zugangsdaten (Benutzer: „admin“, Passwort: „meinsm“) mit einem individuellen und sicheren Passwort abzuändern. Dieses muss mindesten 8 Stellen haben. Auf Groß-/Kleinschreibung ist genau zu achten. Ohne Änderung des Admin-Standardpasswortes kann keine Änderung im Admin-Menü dauerhaft gespeichert werden.

Sollte das Admin-Passwort einmal vergessen worden sein, ist es notwendig, die betreffende Kamera zu demontieren und an die MOBOTIX Zentrale für einen Hardware Reset zu senden. Gegen Gebühr kann durch einen zertifizierten MOBOTIX Partner eine spezielle, von MOBOTIX individuell programmierte Spezialsoftware mit Einzelfreischaltung zum Passwort-Reset vor Ort (und ohne Kamerademontage) angefordert werden.

c) Mikrofon:

Bei Kameras mit eingebautem Mikrofon ist dieses in der Werkseinstellung der Kamerafirmware ausgeschaltet. Auf Basis der gesetzlichen Vorgaben im Bereich „Privacy by Default“ (Sicherheit auch bei Werkseinstellung), ist hier gewährleistet, dass keine Audioaufnahmen versehentlich erfolgen, solange sie datenschutzrechtlich nicht zulässig sind. Das Mikrofon muss immer erst manuell aktiviert werden, was nur mit Admin-Rechten möglich ist.

d) Netzwerkeinstellungen / Integrationsprotokolle:

Hier werden nicht nur die für eine Integration in Netzwerke oder Drittsysteme notwendigen Eingaben und Profile eingegeben, es werden auch unterschiedliche Profile für Bilder, Mails, Nachrichten und zugehörigen Zertifikaten und Zugangsdaten zu Drittsystemen angelegt und verwaltet. Dies erfolgt generell im Admin-Bereich der Kamerafirmware, um den Datenschutzgrundsatz des Zugriffsschutzes optimal zu gewährleisten.

e) Speicherausfall-Überwachung:

Über diesen Punkt können im Admin-Menü der Kamerafirmware spezielle Tests konfiguriert werden, die im Hintergrund die Verfügbarkeit, erfolgreiche Datenübertragungen zu einem definierten Speicherziel und die erfolgreichen Aufzeichnungen von Ereignissen überprüfen. Diese Tests stellen bereits in der Kamerafirmware getroffene, technisch-organisatorische Maßnahmen (TOMs) im Sinne der DSGVO dar. Die Ergebnisse dieser Tests werden in der Kamera in einer Protokolldatei dokumentiert. Bei evtl. auftauchenden Unstimmigkeiten kann die betreffende Kamera automatisch Benachrichtigungen in unterschiedlicher Form auslösen. Dies kann erfolgen durch Blinken der LEDs, Audiomeldungen, FTP-Bildübertragung, E-Mail-Versand von Fehlermeldungen mit/ohne Bild, Netzwerkmeldungen oder auch durch einen automatischen Telefonanruf durch die Kamera.

2.1.3 Setup-Bereich

a) Bildbereiche verdecken:

Beim Einsatz von Video-Sicherheits-Systemen ist es oft notwendig, aus Gründen des Datenschutzes Bereiche, die nicht erfasst werden dürfen, generell oder temporär auszublenden. Hierzu können im Setup-Bereich der Kameras Bildbereiche definiert werden, die entweder durch eine Verpixelung als Kacheln oder mit vollflächigen Farben verdeckt werden können. Diese Verdeckung wird direkt in der Kamera vor Fertigstellung der Bilder vorgenommen und überschreibt die an diesen Stellen vorhandenen Bildinformationen. Dadurch kann die Verpixelung nicht rückgängig gemacht werden.

b) Scharfschaltung:

Gemäß dem Grundsatz „datenschutzfreundliche Grundeinstellungen“ (Art. 25 DS-GVO) sind bei allen Kameras als Werkseinstellung die Ereignissteuerung und die Analytics-Steuerung deaktiviert. Zur Nutzung dieser Funktionen ist nach der generellen Scharfschaltung die voneinander unabhängige Scharfschaltung der Bereiche Speicherung, Aktionen und/oder Benachrichtigungen möglich. Hierdurch sind individuelle Anpassungen an unterschiedlichste Datenschutzanforderungen möglich.

c) MxAnalytics:

In diesem Bereich können zu Statistikzwecken Zählkorridore oder Heatmaps definiert werden.

1) Zählkorridore:

Durch Zählkorridore erhält man Infos über die Anzahl von Objekten, die sich in zwei Richtungen durch die Zählkorridore bewegen. Während sich bewegende Objekte erkannt wurden werden diese maskiert. Hierdurch sind z.B. im Livebild keine Gesichter erkennbar. Es werden nur die Anzahl und Uhrzeit der erkannten Objekte im Zählkorridor und keine Bilder abgespeichert.

2) Heatmaps:

Bei den Heatmaps werden für erkannte Bewegungen an den betreffenden Stellen farbige Kacheln hinterlegt. Je mehr Kacheln an der gleichen Stelle hinterlegt werden, desto heller ist dort die betreffende Farbe (von dunkelblau bis weiß). Die Kacheln werden bei einer Auswertung in einem vorgespeicherten Referenzbild gespeichert. Eine Speicherung von weiteren Bildern erfolgt nicht.

Die Zählstatistiken und die Heatmap werden in der Kamera, bei Bedarf über ein zusätzliches Passwort verschlüsselt, auf der SD-Karte getrennt von dem Ereignis-Bildspeicher abgelegt.

3) Verhaltensdetektion:

Wenn eine Kamera an der Decke montiert ist, können neben den Funktionen von Zählkorridoren oder einer Heatmap noch Ereignissensoren auf Basis von Verhaltensanalysen aktiviert werden. Hierbei geht es um die Messung von folgenden Aspekten:

- Maximale Verweildauer
- Bewegung in Gegenrichtung einer definierten Hauptrichtung
- Richtungsumkehr
- Abbiegen von der Hauptbewegungsrichtung
- Überschreiten eines definierten Geschwindigkeitswertes
- Betreten eines gesperrten Bereiches.

Bei Erreichen eines dieser Messwerte werden in den Live- oder gespeicherten Bildern zu dem auslösenden Ereignis passende Symbole angezeigt. Die durch die Verhaltensdetektion ausgelösten Ereignisse können als Auslöser für verschiedenste Aktionen wie Bildspeicherung, Benachrichtigungen oder auch Schalten von Warnleuchten, akustischen Signalen etc. verwandt werden.

d) MOBOTIX Certified Apps

Ab den Mobotix7 Modellen können in diesem Bereich die Certified Apps aktiviert werden. Analog zu der Scharfschaltung ist auch hier, gemäß dem Grundsatz „datenschutzfreundliche Grundeinstellungen“ (Art. 25 DS-GVO), bei allen Kameras als Werkseinstellung das Arming des Appservice deaktiviert.

2.1.4 Ende-zu-Ende-Verschlüsselung und Löschfristen

a) Ende-zu-Ende-Verschlüsselung

Grundvoraussetzung für einen effektiven Datenschutz ist eine eingeschaltete Verschlüsselung, denn sie verhindert bei Diebstahl oder Abhandenkommen ein Kompromittieren der Daten. Zur Absicherung von gespeicherten Daten kann man zu jeder Zeit ein Schlüsselwort unter /admin/storageconfig eintragen und ab dem nächsten Reboot werden alle neuen Aufzeichnungen unter Verwendung dieses Worts verschlüsselt.

MxFFS verschlüsselt mittels einem XTEA basierten 128bit Verfahren alle Videoinhalte sowie den Großteil der Meta-Daten innerhalb jeder Kamera und überträgt nur diese verschlüsselten Daten zum NAS- oder Datei-Server-Archiv, wo sie für einen IT-Admin unentschlüsselbar liegen. Die Entschlüsselung erfolgt ebenfalls nur auf dem MxMC Client oder der Playback Kamera und stellt somit eine integrierte End2End-Verschlüsselungslösung dar.

b) Einhaltung der Löschfristen

Nach Ablauf der Löschfrist werden die Daten wie in den meisten Dateisystemen nicht gelöscht oder überschrieben, sondern der Zugriff unmöglich gemacht. Dies ist derzeit "State of the Art". (Ein sicheres Überschreiben würde die Lebensdauer von Flashmedien halbieren.)

Darüber hinaus bietet die neueste Software 7.3.0 aufwärts die Möglichkeit Daten auf dem externen NAS oder Datei-Server wiederum zu löschen, indem alle Dateien mit Video- und Audio-Daten außerhalb der Löschfrist entfernt werden.

2.2 MOBOTIX MOVE Kameras

a) Admin-Passwort:

Wie bei den IoT-Kameras ist auch bei den MOVE-Kameras bei der erstmaligen Einwahl die Änderung des werksseitigen admin-Passwortes „meinsm“ auf ein individuelles Passwort notwendig, um einen Datenschutz konformen „Zugriffsschutz“ zu gewährleisten.

b) Privatzonen:

In den MOBOTIX MOVE-Kameras ist auch direkt in den Kameras eine Funktion zur Verdeckung von Bildbereichen durch Farbflächen integriert. Hierdurch ist es möglich Bereiche zu verdecken, die z.B. aus Datenschutz-Gründen (z.B. während bestimmter Zeiten) nicht aufgenommen werden dürfen. Bei Aktivierung dieser Privatzonen ist darauf zu achten, dass die PTZ-Funktionen deaktiviert werden, da anderenfalls bei einem Schwenken des angezeigten Bildbereiches die Privatzone mit geschwenkt wird und einen falschen Bildbereich maskiert.

3 Datenschutz in MOBOTIX Software

In jeder von der MOBOTIX AG zur Verfügung gestellten Software sind Hinweise zum Datenschutz enthalten. Zusätzlich sind dort unterschiedliche Funktionen zur Gewährleistung von DS-GVO konformen Video-Sicherheits-Lösungen integriert.

3.1 Zertifizierte Kamera-Apps

a) Einhaltung der Datenschutzgrundverordnung

Alle auf der MOBOTIX 7 Plattform verfügbaren zertifizierten Apps folgten den Vorgaben und Grundsätzen des Datenschutzes „by Default“ und „by Design“ gemäß Artikel 25 der Datenschutzgrundverordnung (DSGVO).

- Alle App-Funktionen, einschließlich des übergeordneten zugehörigen Kamerasoftware-Dienstes, sind standardmäßig deaktiviert.
- Auch nach Aktivierung der App-Funktionen gibt keine der Apps ohne ausdrückliche Zustimmung des Nutzers Daten an den Kameraherstel-ler oder den App-Hersteller weiter. Dies kann zwar z. B. zum Zweck der kundenspezifischen Erweiterung/Verbesserung einer App notwendig sein, erfordert aber in jedem Fall eine durch den Anwender bewusst ausgeführte Spezialkonfiguration der App.
- Eine Weiterverarbeitung oder Weitergabe der von einer App generierten Daten, beispielsweise zum Zwecke der zentralen Zusammenführung (Server oder Cloud), bedarf eines Eingriffs des Nutzers und damit dessen ausdrücklicher Zustimmung. Entsprechende Reporting-Schnittstellen müssen vom Nutzer ordnungsgemäß konfiguriert sein.

b) Übersicht der Apps

MOBOTIX Object Recognition

Einsatzzweck: Erkennung und Klassifizierung von bekannten Objekttypen (z.B. Personen, Autos, etc.) im Sichtfeld der Kamera. Die Analyse auf Basis von Einzelbildern dient der Erzeugung von Metadaten, auf deren Grundlage zugeordnete Apps (z.B. MOBOTIX Analytics oder ActivitySensor) ihre Funktionen ausführen können. Außer der Information über den erkannten Objekttyp (z.B. Person), dem Zeitstempel des Einzelbildes und der Position des Objekts im Bild werden keine personenbezogenen Daten verarbeitet. Es ist nicht möglich, ein personenbezogenes Muster zu erstellen.

MOBOTIX ActivitySensor

Einsatzzweck: Der ActivitySensor dient der Bewegungserkennung auf Basis von Pixeländerungen im Bild (reguläre Anwendung) oder speziell trainierter Objekterkennung (basierend auf künstlicher Intelligenz). In beiden Fällen werden weder personenbezogene Daten noch Bewegungsmuster erstellt, um die Funktion der Anwendung zu erfüllen.

MOBOTIX Analytics

Einsatzzweck: Definition von Zählkorridoren und Heatmaps für statistische Zwecke und die Generierung von Ereignissen aufgrund der Erkennung von auffälligem Verhalten von Objekten (z.B. Personen)

- Zählkorridore

Zählkorridore liefern Informationen über die Anzahl der Objekte, die sich in zwei Richtungen durch die Zählkorridore bewegen. die sich in zwei Richtungen durch die Zählkorridore bewegen. Während sich bewegende Objekte erkannt werden, werden sie maskiert. Das bedeutet, dass z.B. Gesichter im Livebild nicht sichtbar sind. Es werden nur die Anzahl und der Zeitpunkt der erkannten Objekte im Zählkorridor und keine Bilder gespeichert.

- Heatmaps

In den Heatmaps werden an den relevanten Punkten für erkannte Bewegungen farbige Kacheln hinterlegt. Je mehr Kacheln an der gleichen Position abgelegt sind, desto heller ist die Farbe (von dunkelblau bis weiß). Die Kacheln werden während einer Auswertung in einem vorgespeicherten Referenzbild abgelegt. Es werden keine zusätzlichen Bilder gespeichert. Die Zählstatistik und die Heatmap werden in der Kamera auf der SD-Karte getrennt vom Ereignisbildspeicher abgelegt (optional verschlüsselt durch ein zusätzliches Passwort).

- Erkennung von bestimmtem Verhalten

Bei der Montage einer Kamera an der Decke können neben den Funktionen Zählkorridore oder Heatmaps auch Ereignissensoren auf Basis einer Verhaltensanalyse aktiviert werden. Dabei sind folgende Verhaltensweisen erfassbar:

- Maximale Verweildauer
- Bewegung in die entgegengesetzte Richtung zu einer definierten Hauptrichtung
- Richtungsumkehr
- Abweichenvon der Hauptbewegungsrichtung
- Überschreiten einer festgelegten Geschwindigkeitsgrenze
- Betreten eines Sperrbereichs

Bei Erfassung einer dieser Verhaltensweisen werden, in den Livebildern und in der Aufzeichnung, Symbole angezeigt, die dem auslösenden Ereignis entsprechen. Die durch die Verhaltenserkennung erfassten Ereignisse können als Auslöser für verschiedene Aktionen wie Bildspeicherung, Benachrichtigung oder Schalten von Warnleuchten, akustischen Signalen usw. verwendet werden.

MOBOTIX Color Recognition

Einsatzzweck: Die Anwendung erkennt, wenn eine bestimmte Anzahl von Pixeln in einem zuvor definierten Bildbereich einem vom Benutzer ausgewählten Farbwert zugeordnet werden kann. So kann z.B. das plötzliche Auftreten von Signalfarben jeglicher Art erkannt und als Ereignis (Aufnahmestart, Benachrichtigung einer Leitstelle, etc.) verarbeitet werden. Die App erfordert keine weitere Verarbeitung oder Speicherung von personenbezogenen Daten.

MOBOTIX Thermal Heat Radiometry (CNPP) & MOBOTIX Advanced Radiometry App

Einsatzzweck: Als Erweiterung der Radiometrie-Funktionen von MOBOTIX Wärmebildkameras bietet diese App die Überwachung von Oberflächentemperaturen auf der Grundlage individuell angepasster Kalibrierungsparameter gemäß den CNPP-Anforderungen für Brandschutzsysteme. Damit kann der Anwender die Parameter wie Emissionsgrad, Transmissionsgrad und Reflexionsgrad für jedes Temperaturmessfenster und damit für jedes Zielobjekt individuell, in Abhängigkeit von den Eigenschaften der Objektoberfläche, anpassen. Als Datenquelle für die vorgesehenen Funktionen der App werden nur thermische Rohdaten verarbeitet oder gespeichert, und damit keinerlei personenbezogene Daten.

Zertifizierte A.I. Tech Apps inkl. integriertem Dashboard

MOBOTIX Videoanalyselösungen erfordern Datenerfassung, Datenverarbeitung, Datennutzung und Datenweitergabe und müssen folgende Punkte berücksichtigen:

- Grundsatz der Transparenz

Mit der Ausführung geeigneter technischer und organisatorischer Sicherheitsmaßnahmen ist ein angemessenes Sicherheitsniveau für die Risiken zu gewährleisten. Die Daten müssen, wenn möglich, auf ein Minimum reduziert, anonymisiert oder pseudonymisiert werden.

Es ist notwendig, eine Beschränkung der Datennutzung festzulegen: Die Verwendung der Daten ist nur erlaubt, wenn sie mit den zu verfolgenden Zwecken vereinbar sind. Die Rechte der betroffenen Parteien müssen geschützt werden. Bei der Konfiguration der technischen Verfahren im Rahmen der Videoanalyse muss gewährleistet sein, dass die Kriterien, die von der Anfangsphase eines Projekts an zu berücksichtien sind, klar eingehalten werden und die Datensicherheit dem „Privacy by Design“-Ansatz entspricht.

Anhand folgender Grundsätze steht A.I. Tech steht für die Datensicherheit seiner Apps ein:
- Rechtmäßigkeit, Fairness und Transparenz.

Personenbezogene Daten werden nur zu einem bestimmten Zweck oder zu den erklärten Zwecken und mit einem Aufbewahrungskriterium unter Beachtung der gesetzlichen Vorschriften erhoben. Die Daten können nach dem Grundsatz „Privacy by Design und Privacy by Default“ auf ein Minimum reduziert werden. Standardmäßig werden nur die personenbezogenen Daten verarbeitet, die zur Erreichung des Zwecks, für den sie verarbeitet werden, erforderlich sind. Die Bilder werden weder lokal auf dem Gerät gespeichert noch an andere Systeme übertragen, es sei denn, der Nutzer entscheidet sich durch ausdrückliche Zustimmung und durch eine spezifische Konfiguration des Systems dafür, die Bilder zu den vom System erzeugten Ereignissen mit den dazugehörigen Metadaten zu speichern, indem er beispielsweise die Speicherung von Bildern auf AI-DASH-EMBEDDED aktiviert. Bei der Klassifizierung der Bilder (z. B. für die Gesichtsanalyse) wird kein Bild gespeichert, das mit den Gesichtern von Personen in Verbindung steht (außer im Falle einer ausdrücklichen Zustimmung des Betreibers, wie oben erwähnt). Das Gesicht wird in einem Vektor hervorstechender Merkmale kodiert (die in keiner Weise dem Gesicht selbst und somit der Identität der Person zuzuordnen sind) und in Echtzeit mit Hilfe von Klassifikatoren verarbeitet, d. h. komplexen mathematischen Modellen, die anhand dieses Vektors beispielsweise das Geschlecht oder das Alter der betreffenden Person ableiten können.

Irisity Core AI Analytics

Einsatzzweck: Basierend auf speziell trainierten KI-Modellen erkennt die Anwendung wichtige Verhaltensweisen von Objektklassen (z. B. von Personen, Fahrzeugen, Tieren) oder signifikante Veränderungen im Sichtfeld der Kamera.

Intrusion Detection:

- Ein Alarmereignis wird ausgelöst, wenn ein als Person oder Fahrzeug (je nach Konfiguration des Benutzers) klassifiziertes Objekt in eine oder mehrere vom Benutzer konfigurierte Region(en) von Interesse eindringt.
- Die erzeugten Ereignisdaten enthalten nur die Informationen über die erkannte Objektklasse, den Zeitstempel des Ereignisses und den Namen der Region von Interesse.
- Personenbezogene Daten werden nicht erzeugt.

Erkennung von Manipulationen:

- Ein Alarmereignis wird ausgelöst, wenn sich ein signifikanter Teil des Kamerabildes abrupt ändert.
- Dies kann z. B. passieren, wenn ein Eindringling die Kamera verdeckt oder mit einem Gegenstand angreift.
- Personenbezogene Daten werden nicht erzeugt.

Erkennung von Herumlungern:

- Ein Alarmereignis wird ausgelöst, wenn sich ein als Person oder Fahrzeug (je nach Konfiguration des Benutzers) klassifiziertes Objekt länger als gewöhnlich an einem Ort in einem benutzerdefinierten Bereich aufhält.
- Die erzeugten Ereignisdaten enthalten nur die Informationen über die erkannte Objektklasse, den Zeitstempel des Ereignisses und den Namen der Region von Interesse.
- Personenbezogene Daten werden nicht erzeugt.

Vaxtor Technologies: VaxALPR, VaxALPR ADR, VaxOCR Cargo Container, VaxOCR USDOT, VaxOCR Railway

Die Vaxtor Zeichenerkennungs-Apps lesen aus dem Kameravideo über eine OCR-Funktion die Werte von Kennzeichen, Gefahrgut-, Güterzugzeichen, Luftfahrzeug-Identifikationsnummern, Frachtcontainer-Codes in verschiedenen Sprachen und Länderspezifikationen – je nach verwendeter App.

Bilddaten werden in der App analysiert, dann übermittelt die App Eventtrigger und Ergebnisse an die Kamera und ggf. das VMS weiter. Gespeichert werden die Daten auf der Kamera oder einem VMS (z.B. MxMC). Die Daten sind ohne die App nicht verwendbar und werden auf der Kamera verschlüsselt abgelegt. Die Löschfristen werden über die Kamera konfiguriert.

Vaxtor Technologies: VaxALPR MMC

Diese App erkennt Kennzeichen und zusätzlich die Marke, das Modell und die Farbe des Fahrzeugs. Die Daten sind ohne die App nicht verwendbar und werden auf der Kamera verschlüsselt abgelegt. Die Löschfristen werden über die Kamera konfiguriert.

Visage Technologies - Face Recognition

Einssatzzweck: Der Funktionsumfang der (seit Ende 2023 nicht mehr von MOBOTIX angebotenen) App umfasst die identitätsunabhängige Detektion von Gesichtern im Sichtfeld der Kamera sowie die Erkennung von Gesichtern, die in einem vom Administrator gesteuerten Prozess erfasst werden. Die Erkennung von Personen ist als ein möglicher Faktor zur Authentifizierung in Zutrittskontrollszenarien vorgesehen (z.B. Erkennung von Mitarbeitern, gesuchten Personen, etc.)

- Gesichtsdetektionsmodus:

Die Detektion von Gesichtern erfolgt unabhängig von der Identität und detektiert Gesichter im Sichtfeld der Kamera auf der Grundlage bekannter Muster. Bei diesem Prozess werden keine personenbezogenen Daten erzeugt oder verarbeitet.

- Einlernmodus:

Wird im Einlernmodus ein Gesicht im Livebild der Kamera detektiert, wird der entsprechende Bildausschnitt als temporäres Bild-Overlay angezeigt, um dem Administrator als visuelle Bestätigung zu dienen. Die entsprechenden Daten werden verworfen, sobald die zugehörigen Gesichtsdeskriptoren erfasst oder überschrieben sind.

- Gesichtserkennungsmodus:

Die Gesichtserkennung basiert auf Gesichtsdeskriptoren. Das System berechnet die Ähnlichkeit zwischen den Gesichtsdeskriptoren der aktuell detektierten Gesichter im Sichtfeld der Kamera und allen zuvor in der dezentralen Datenbank registrierten Gesichtsdeskriptoren. Ziel ist es, das Gesicht bzw. die Gesichter aus der Datenbank zu finden, die dem aktuell detektierten Gesicht am ähnlichsten sind.

- Keine Gesichtsbilder werden gespeichert oder verarbeitet
- Die Datenbank enthält nur die Gesichtsdeskriptoren und die entsprechenden Namen / IDs, aber keine Bilder

Da es sich bei allen biometrischen Vorlagen ausschließlich um mathematische Darstellungen der Gesichter der Nutzer handelt, werden biometrische und persönliche Informationen strikt voneinander getrennt. Diese Art des Umgangs mit Daten gewährleistet ein Höchstmaß an Datenschutz, selbst wenn es sich um äußerst sensible Daten handelt.

- Visage entwickelt seine Software zu 100% selbst.
- Biometrische Vorlagen können nicht exportiert oder in ihr ursprüngliches Format zurückverwandelt werden.

Da es sich bei den erstellten Gesichtsdeskriptoren um rein mathematische Modelle der eingelernten Gesichter handelt, berücksichtigt die Software nur die Form, Textur und andere spezielle mathematische Merkmale eines Gesichts. Zu keinem Zeitpunkt wird eine Bewertung anhand von Hautfarbe, Herkunft oder anderen möglicherweise typischen Gesichtsmerkmalen von Personen vorgenommen.

3.2 MxManagementCenter

a) Online Verbindung:

Das MxManagementCenter kann komplett ohne Internet-Verbindung betrieben werden. Eine Online Verbindung wäre bei Bedarf nur zu zwei Zeitpunkten erforderlich:

1) Software Update:

In den Einstellungen des MOBOTIX ManagementCenter gibt es im Bereich „Software-Update“ die Möglichkeit eine Funktion zu aktivieren, die beim Programmstart oder zu definieren Zeitintervallen die MOBOTIX Homepage anwählt, um zu überprüfen, ob dort eine neue Software-Version vorhanden ist. Diese Funktion ist in den Werkseinstellungen aus Datenschutz-Gründen deaktiviert. Die Suche kann auch über dieses Menü manuell ausgelöst werden.

2) Nutzung von Lizenzpflichtigen Komponenten:

Wenn ein MOBOTIX ManagementCenter mit Lizenzpflichtigen Komponenten genutzt werden soll, ist für die Aktivierung des Lizenzcodes eine Online-Verbindung oder eine Datei, die sie von uns erhalten, notwendig, um die Gültigkeit des Lizenzcodes bei dem Lizensierungs-Server in den USA überprüfen zu können. Da Lizenzcodes bei MOBOTIX nach Aktivierung dauerhaft gültig sind ist nach erfolgter Aktivierung keine Online-Verbindung mehr notwendig.

c) Benutzerverwaltung:

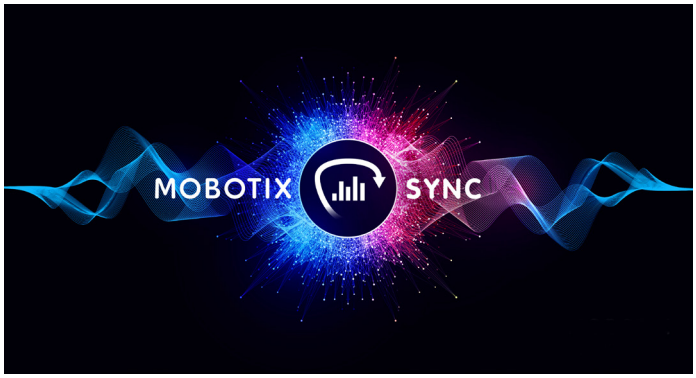
Das MOBOTIX ManagementCenter greift auf die zugewiesenen Videoquellen (Kameras, NAS etc.) auf Admin-Ebene zu, um möglichst alle Funktionen der angeschlossenen Geräte steuern zu können. Zur Gewährleistung von evtl. unterschiedlichen Datenschutz-Anforderungen verfügt das MxMC über eine differenzierte Benutzerverwaltung. Dies betrifft u.a. die Möglichkeit der Zugriffsbeschränkung nur auf definierte Kameras oder tätigkeitsbezogene Nutzung von Funktionen. Unterstützt wird in der aktuellen Version der sog. Supervisor Mode, der maximal eine 6-Augenkontrolle unterstützt.

Das Kaktus Konzept gilt auch im MxMC für die Kameras (Secure System im Bereich der Komponenten des MxMC). Es wird geprüft, ob alle IoT-Kameras in der Gruppe sind und ob das Standardpasswort für den Admin Bereich und den ONVIF-Bereich geändert wurde. Geprüft wird ebenfalls, ob HTTPS aktiviert und Public Access deaktiviert ist. Das MxMC passt automatisch die Einstellungen in den Kameras gegebenenfalls an.

Eine Zertifikate-Manager in MxMC ermöglicht das Erstellen von eigenen Zertifikaten für die SSL Kommunikation und verwaltet auch das Verteilen der offiziellen oder eigenen Zertifikate auf die einzelnen IoT-Kameras.

Jede datenschutzrelevante Benutzer-Aktion im MxMC wird in dem Action Log des Systems mitprotokolliert.

3.3 MOBOTIX SYNC Server



a) Einleitung:

Die Software MOBOTIX SYNC ist ein Back-Office-Integrationstool, das die Effizienz verschiedener Prozesse wie Parkraumbewirtschaftung, Zutrittskontrolle und Verkehrsüberwachung erhöht.

b) Speicherung personenbezogener Daten

Die MOBOTIX SYNC Software kann personenbezogene Daten speichern, dies ist jedoch standardmäßig nicht erforderlich. Die Benutzer haben die Möglichkeit, das System so zu konfigurieren, dass nur die für den beabsichtigten Zweck erforderlichen Informationen erfasst werden.

c) Zweck der Speicherung personenbezogener Daten

Wenn personenbezogene Daten gespeichert werden, dient das nur dem Zweck, die Funktionalität und Effizienz der Software zu verbessern – einschließlich Kennzeichenerkennung, Fahrzeugidentifizierung und Bereitstellung statistischer Daten zur Unterstützung von Managemententscheidungen.

d) Speicherort der Daten

Die von der MOBOTIX SYNC Software erhobenen personenbezogenen Daten werden auf sicheren Servern innerhalb der Europäischen Union gespeichert, in Übereinstimmung mit den Anforderungen der Datenschutz-Grundverordnung (DSGVO).

e) Dauer der Datenspeicherung

Die von der MOBOTIX SYNC Software erhobenen personenbezogenen Daten werden gemäß den Richtlinien der Datenschutz-Grundverordnung (DSGVO) nur so lange aufbewahrt, wie es für den jeweiligen Zweck erforderlich ist. Die Aufbewahrungsfrist kann vom Nutzer je nach Bedarf und gesetzlichen Vorgaben konfiguriert werden.

f) Zugang zu personenbezogenen Daten

Der Zugriff auf personenbezogene Daten, die in der MOBOTIX SYNC Software gespeichert sind, ist auf autorisierte Personen beschränkt, denen entsprechende Benutzerrechte erteilt wurden. Die Software verwendet ein rollenbasiertes Zugriffskontrollsystem, um sicherzustellen, dass nur autorisierte Benutzer auf personenbezogene Daten zugreifen und diese bearbeiten können. Eine detaillierte Beschreibung der Benutzerrechte, der Zugriffsebenen und des Verfahrens zur Gewährung und zum Entzug des Zugriffs findet sich in der Benutzerdokumentation der Software.

g) Maßnahmen zum Schutz der Daten

Die MOBOTIX SYNC Software verfügt über mehrere Sicherheitsebenen, um personenbezogene Daten vor unberechtigtem Zugriff zu schützen, darunter Datenverschlüsselung, eine sichere Serverinfrastruktur und regelmäßige Sicherheitsaudits. Die Software entspricht außerdem den branchenüblichen Best Practices für den Datenschutz. Um die Datensicherheit bei der Übertragung zwischen der MOBOTIX SYNC Software und externen Systemen oder Geräten weiter zu erhöhen, kann eine Ende-zu-Ende-Verschlüsselung konfiguriert werden.

h) Pseudonymisierung durch Design

Die MOBOTIX SYNC Software wurde mit Pseudonymisierungs-Funktionen entwickelt, die es den Nutzern ermöglichen, personenbezogene Daten zu verarbeiten, ohne Personen direkt zu identifizieren. Diese Funktionen tragen dazu bei, die Einhaltung der DSGVO-Grundsätze „Privacy by Design“ und „Privacy by Default“ zu gewährleisten.

i) REST API und Sicherheit

Die MOBOTIX SYNC Software bietet eine REST API, die es Anwendungen und Systemen von Drittanbietern ermöglicht, mit den Daten und Funktionen der Software zu interagieren. Die API verwendet API-Schlüssel für die Sicherheit, um sicherzustellen, dass nur autorisierte Benutzer und Anwendungen auf die Daten zugreifen können. Um einen API-Schlüssel zu erhalten, ist eine Benutzerauthentifizierung erforderlich, und der Schlüssel sollte vertraulich behandelt werden, um unbefugten Zugriff zu verhindern. Die API ist für Entwickler und Integratoren gedacht, die die Funktionen der MOBOTIX SYNC-Software in ihre Anwendungen einbinden möchten, sowie für Anwender, die eigene Datenanalysen oder Berichte benötigen.

j) Gemeinsame Nutzung und Verbreitung von Daten

Personenbezogene Daten, die von der MOBOTIX SYNC Software erfasst werden, werden standardmäßig nicht an Externe weitergegeben oder verteilt. Wenn eine Weitergabe von Daten erforderlich ist, müssen die Nutzer das System entsprechend konfigurieren und die Einhaltung der DSGVO-Anforderungen für Datenübertragungen sicherstellen.

k) Automatische Datensicherung und RAID-Levels

Die MOBOTIX SYNC Software unterstützt die automatische Datensicherung und verwendet RAID-Levels, um Datenredundanz und Zuverlässigkeit zu gewährleisten. Welcher RAID-Level verwendet wird, hängt von der Systemkonfiguration und den Präferenzen des Benutzers ab.

l) Allgemeiner Zweck

Die MOBOTIX SYNC Software zielt darauf ab, ein leistungsstarkes und flexibles Back-Office-Integrationstool zu bieten und gleichzeitig die Einhaltung der DSGVO zu gewährleisten. Durch die Integration von Funktionen zum Schutz der Privatsphäre und des Datenschutzes hilft die Software den Nutzern, ihre personenbezogenen Daten verantwortungsvoll und transparent zu verwalten.

Zusammenfassend lässt sich sagen, dass die MOBOTIX SYNC Software mit Blick auf die Einhaltung der DSGVO entwickelt wurde und den Nutzern die notwendigen Werkzeuge und Optionen zur Verfügung stellt, um den Schutz personenbezogener Daten zu gewährleisten. Obwohl die Speicherung personenbezogener Daten nicht standardmäßig erforderlich ist, müssen Anwender, die sich für die Speicherung solcher Informationen entscheiden, die in diesem Dokument dargelegten Richtlinien und Empfehlungen befolgen, um Transparenz und die Einhaltung der DSGVO-Anforderungen sicherzustellen.

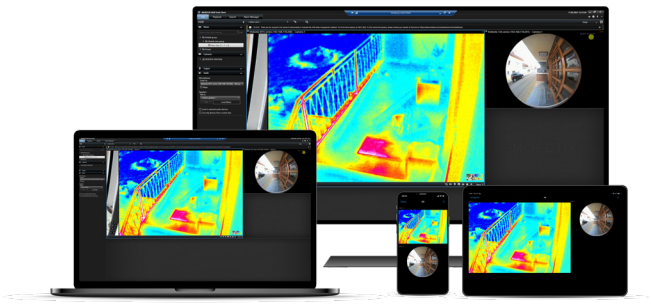
3.4 MOBOTIX HUB

a) Online-Verbindung:

Eine sichere Verschlüsselung und HTTPS-Verbindungen sind im MOBOTIX HUB vorgesehen und wir empfehlen unbedingt die Installation von SSL-Zertifikaten zu diesem Zweck.

Desweiteren können Zugriffe ebenso über einzelne IP-Adressen oder IP-Adressbereiche reglementiert werden.

Wir empfehlen auf jeden Fall den MOBOTIX HUB Hardening Guide, um das System sowohl sicherer als auch datenschutzkonform zu konfigurieren. Sie finden ihn unter: https://www.mobotix.com/sites/default/files/2021-07/Mx_GL_MOBOTIX_HUB_Hardening_V1-00_EN_210701.pdf



b) Benutzerverwaltung:

Zur Installation von MOBOTIX HUB ist ein Windows Admin-Zugang erforderlich. Damit wird sichergestellt, dass keine Standardbenutzer eine Installation oder Erstellung eines Admin-Accounts auf MOBOTIX HUB durchführen können. Für eine sichere Benutzerverwaltung empfehlen wir die Anbindung an das Active Directory von Windows.

Passwörter für den HUB-Account müssen generell mindestens 8 Stellen lang sein, Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen enthalten.

c) Erweiterte Zugriffsrechte-Verwaltung:

MOBOTIX HUB unterstützt den DSGVO-konformen Zugriff nach dem 4-Augen-Prinzip. Des Weiteren können Verpixelungen von Kamerabildbereichen so eingerichtet werden, dass nur berechtigte User diese in den Playbacks aufheben können.

Zugriffe auf Playbacks oder Livebilder können für bestimmte User-Rollen eingeschränkt werden. Dies kann z.B. die Abspieldauer sein, als auch die Zeit bis wann in der Vergangenheit auf Aufnahmen zuggegriffen werden darf.

d) Logs und Auditprotokolle:

Zugriffe werden geloggt, so dass nachträglich festgestellt werden kann, welcher Benutzer Einstellungen geändert hat und welche, ob er/sie Alarme bearbeitet hat oder was angeklickt wurde. So können Manipulationen leicht nachverfolgt werden.

3.5 MOBOTIX Cloud

a) Sicherheit und Datenschutz

Die gesamte Kommunikation zwischen Kameras, der Bridge bis zu den Devices ist verschlüsselt. Optional kann die 2-Faktor-Authentifizierung für mehr Sicherheit genutzt werden. Über eine feingranulare Rechtevergabe und Benutzerverwaltung können Sie die Rechte optimal an ihre Bedürfnisse und den Datenschutz anpassen.

Alle Daten unserer deutschen Kunden werden in Datencentern in Frankfurt a.M. gehostet. Die unserer EU-Kunden auf Datencentern in der EU. Die Datencenter sind zertifiziert (SOC 1+2, ISO 27001), legen die Daten in 3-Fach-Backups ab und garantieren damit die Verfügbarkeit nach DSGVO. Für Endkunden-Subaccounts steht ein Privacy Mode zur Verfügung, um Bilder- und Audio-Zugriffe des Resellers einzuschränken (verpixeln oder ausblenden). In den Action- und Audit-Logs werden Benutzeraktivitäten gespeichert, so dass Änderungen nachvollzogen werden können.

b) Bridge

Die Bridge hat keinen Inbound-Port, so dass kein Direktzugriff möglich ist. Sicherheitsupdates auf der Bridge erfolgen automatisch über die Cloud.

3.6 MOBOTIX Live Türstations- und Kamera-App

Bei der IOS- und Android-App MOBOTIX Live werden auf dem mobilen Gerät (Smartphone, Tablet) keine personenbezogenen Daten erfasst bzw. gespeichert. Bei Einräumung von Nutzerrechten auf den Kameras ist bereits darauf zu achten, ob der betreffende Nutzer z.B. Rechte für eine Recherche erhalten soll. Diese in der Kamera definierten Rechte greifen auch bzgl. des Zugriffs über die MOBOTIX Live-App auf die Kamera.

Über die MOBOTIX LIVE APP können auch die Verpixelung der IoT Kameras gesteuert werden. Hierzu gibt es vordefinierte API Kommandos die als Softbuttons in der App aktiviert werden können.

3.7 Ältere MOBOTIX Türstations-App

Die Nutzung der MOBOTIX App für IOS-Geräte kann mit einem PIN-Code gesichert werden, damit nur berechtigte Personen Zugriff auf die MxApp erhalten. Zusätzlich kann definiert werden, welche Bereiche / Funktionen der App nur mit Eingabe dieses PIN Codes genutzt werden können. Dies ist z.B. dann sehr hilfreich, wenn ein Nutzer für seine Tätigkeit zwar auf Livebilder einer Türsprechstelle zugreifen darf, aber z.B. über die APP aus Datenschutzgründen keine Berechtigung zur Recherche in gespeicherten Bildern erhalten soll.

3.8 MOBOTIX Partner Toolbox

Bei der MOBOTIX Partner Toolbox handelt es sich um eine App für IOs und Android Endgeräte, die MOBOTIX Partnern in kompakter und thematisch strukturierter Form Zugriff auf von MOBOTIX zur Verfügung gestellte Unterlagen gewährt. Der Zugriff auf diese Informationen ist durch Benutzername/ Passwort geschützt. Eine weitergehende Speicherung personenbezogener Daten erfolgt nicht.

4 Datenschutz auf der MOBOTIX Homepage

a) Unterlagen zum Download:

MOBOTIX stellt über ihre Homepage umfangreiche Unterlagen zum freien Download zur Verfügung. Dies betreffen neben vielfältigen technischen Daten und Konfigurationshilfen auch Unterlagen zu den unterschiedlichen Aspekten des Datenschutzes.

Die letztgenannten Unterlagen sind über den Link <Haftung und Datenschutz> im unteren Bereich jeder Internet-Seite, oder direkt über https://www.mobotix.com/de/haftung-und-datenschutz erreichbar.

b) Auch bei der Kommunikation mit unseren Kunden berücksichtigen wir auf vielfältige Weise die Belange des Datenschutzes. Möchte sich z.B. ein Kunde über unsere Homepage für einen Newsletter registrieren, wird er auf die Datenschutzbestimmungen und sein gesetzliches Widerrufsrecht hingewiesen und muss durch Anklicken seine Kenntnisnahme bzw. sein Einverständnis bestätigen. In Anlehnung an den Datenschutz-Grundsatz der Daten-Sparsamkeit hat jeder Kunde auch die Möglichkeit, Themen für die gewünschten Newsletter zu definieren (und auch jederzeit zu ändern), damit eine unnötige Zusendung von Newslettern vermieden wird.

DE_10/23

MOBOTIX AG
Kaiserstraße
D-67722 Langmeil
Tel.: +49 6302 9816-0
Fax: +49 6302 9816-190
vertrieb@mobotix.com
www.mobotix.de

© MOBOTIX AG 2023
MOBOTIX ist ein eingetragenes Markenzeichen der MOBOTIX AG in der Europäischen Union, den USA und anderen Ländern. Änderungen vorbehalten. MOBOTIX übernimmt keine Verantwortung für technische Fehler, Tippfehler oder Auslassungen. Alle Rechte vorbehalten.

MOBOTIX
BeyondHumanVision