MAKE THE
WORLD SEE

Milestone Systems

DSGVO-Leitfaden zum Schutz der Privatsphäre

milestone

Versionshistorie

Dokumentversion	Release	Anmerkungen
Version 10	2023 R3	In dieser Version enthaltene Aktualisierungen sind u.a.: • Empfehlungen zum Erstellen eines Passworts für die Systemkonfiguration hinzugefügt zu Zusätzliche Sicherungen auf Seite 64. • Empfehlungen in Bezug auf Bilder in Alarmberichten hinzugefügt zu Zusätzliche Sicherungen auf Seite 64.
Version 9	2023 R2	In dieser Version enthaltene Aktualisierungen sind u.a.: • Empfehlungen in Bezug auf Alarmberichte hinzugefügt zu Zusätzliche Sicherungen auf Seite 64.
Version 8	2023 R1	In dieser Version enthaltene Aktualisierungen sind u.a.: • Empfehlungen zur Handhabung von SQL Server Datenbanksicherungen, die zu Sichern Sie die SQL Server Datenbanken auf Seite 61 hinzugefügt wurden. • Verwenden Sie keinen verwalteten SQL Server Dienst, der zu Keinen verwalteten SQL Server Dienst verwenden auf Seite 61 hinzugefügt wurde.
Version 7	2023 R1	In dieser Version enthaltene Aktualisierungen sind u.a.: • Schutzmaßnahmen zum Erstellen von Berichten in XProtect Incident Manager hinzugefügt zu Zusätzliche Sicherungen auf Seite 64.
Version 4	2022 R1	In dieser Version enthaltene Aktualisierungen sind u.a.: • Verschlüsselung für die Kommunikation zwischen allen Servern und Clients wurde zu Wie XProtect die Auswirkungen auf Interessen oder Grundrechte und Freiheiten der betroffenen Person reduziert auf Seite 33 hinzugefügt.

Dokumentversion	Release	Anmerkungen

		• Empfehlungen zur Aktivierung der Verschlüsselung für die gesamte Kommunikation zwischen allen Servern und Clients wurden zu Was sollten Sie tun, um einen standardmäßigen Datenschutz zu gewährleisten? auf Seite 45 hinzugefügt.
		• Empfehlungen zur Aktivierung der Verschlüsselung für die gesamte Kommunikation zwischen allen Servern und Clients wurden zu Schutz der gespeicherten und übertragenen Daten auf Seite 49 hinzugefügt.
		• XProtect Rapid REVIEW wurde zu Komponenten und Geräte, die nicht unter das Europäische Datenschutzsiegel fallen auf Seite 60 hinzugefügt.
		• Die Empfehlungen wurden aus Zusätzliche Sicherungen auf Seite 64entfernt, da Milestone XProtect VMS jetzt die Verschlüsselung der Kommunikation zwischen allen Servern und Clients unterstützt.
		• Angaben zu Datenquellen wurden infolge der externen IDP zu Personenbezogene Daten aus der Umgebung auf Seite 73 hinzugefügt.
		• Zu Personenbezogene Daten aus dem System auf Seite 73 wurden Angaben darüber hinzugefügt, wie der IDP Daten protokolliert und wie personenbezogene Daten aus allen VMS-Debug-Protokollen entfernt werden.
		• Authentifizierung und Authentifizierungsdaten auf Seite 74 aktualisiert:
		  • DSGVO-Unterstützung für Basisnutzer
		  • Empfehlungen zur externen IDP
		  • Verschlüsselung von Tokens, so dass keine weiteren Sicherheitsvorkehrungen erforderlich sind

Version 3	2021 R2	In dieser Version enthaltene Aktualisierungen sind u.a.: • Schutzmaßnahmen gegen die Verwendung eines VPN im Split-Modus hinzugefügt zu Zusätzliche Sicherungen auf Seite 64.
Version 2	2021 R1	In dieser Version enthaltene Aktualisierungen sind u.a.:

Dokumentversion	Release	Anmerkungen
		• Der Grundbenutzertyp fällt jetzt unter das Europäische Datenschutzsiegel (Anhang: Das Milestone XProtect VMS-System und die DSGVO auf Seite 60) und (Anhang: Datenverarbeitung in der Milestone XProtect VMS Umgebung auf Seite 72). • Empfehlungen hinzugefügt zu Verwendung der geographischen Hintergründe in XProtect Smart Client auf Seite 63. • Datensammlung beschrieben in Integrationen von registrierten Partnern. auf Seite 63. • Protokollierung der Authentifizierung beschrieben in Personenbezogene Daten aus dem System auf Seite 73.
Version 1	2020 R3	Dies ist die erste Version dieses Dokumentes.

Inhalt

Copyright, Marken und Verzichtserklärung

Marken

XProtect ist eine eingetragene Marke von Milestone Systems A/S.

Microsoft und Windows sind eingetragene Marken der Microsoft Corporation. App Store ist eine Dienstleistungsmarke von Apple Inc. Android ist eine Handelsmarke von Google Inc.

Alle anderen in diesem Dokument genannten Marken sind Marken ihrer jeweiligen Eigentümer.

Haftungsausschluss

Dieses Dokument dient ausschließlich zur allgemeinen Information und es wurde mit Sorgfalt erstellt.

Der Empfänger ist für jegliche durch die Nutzung dieser Informationen entstehenden Risiken verantwortlich, und kein Teil dieser Informationen darf als Garantie ausgelegt werden.

Milestone Systems A/S behält sich das Recht vor, ohne vorherige Ankündigung Änderungen vorzunehmen.

Alle Personen- und Unternehmensnamen in den Beispielen dieses Dokuments sind fiktiv. Jede Ähnlichkeit mit tatsächlichen Firmen oder Personen, ob lebend oder verstorben, ist rein zufällig und nicht beabsichtigt.

Das Produkt kann Software anderer Hersteller verwenden, für die bestimmte Bedingungen gelten können. In diesem Fall finden Sie weitere Informationen in der Datei `3rd_party_software_terms_and_conditions.txt`, die sich im Installationsordner Ihres Milestone Systems befindet.

Einhaltung der DSGVO und Milestone XProtect VMS

Am 25.05. 2018 trat die Europäische Datenschutzgrundverordnung (DSGVO) in Kraft. Ziel dieser Verordnung ist es, dem Einzelnen mehr Kontrolle darüber zu geben, wie seine persönlichen Daten gesammelt, verarbeitet und weitergegeben werden.

Die DSGVO gibt Unternehmen eine Struktur vor, mit der sie ihre Rollen und Verantwortlichkeiten klären und Einzelpersonen die Möglichkeit geben können, zu kontrollieren, wie ihre personenbezogenen Daten verwendet werden.

Dieses Dokument gibt Ihnen einen Überblick über die Anforderungen und darüber, wie Sie im Einklang mit der DSGVO arbeiten können, wenn Sie das XProtect Video Management System (VMS) nutzen.

Siehe Anhang: Das Milestone XProtect VMS-System und die DSGVO auf Seite 60 für konkrete Informationen dazu, wie ein Milestone XProtect VMS-System am besten DSGVO-gemäß betrieben werden kann.

Haftungsausschluss: Die Informationen in diesem Dokument und alle Empfehlungen werden ohne Gewähr bereitgestellt. Wenn Sie dieses Dokuments befolgen, bedeutet dies noch nicht, dass Ihr System DSGVO-konform ist.

Das Milestone XProtect VMS erfordert eine Konfiguration. Jede Konfiguration oder Änderung von Einstellungen muss dem EU-Datenschutzrecht entsprechen. Während die Anhang: Das Milestone XProtect VMS-System und die DSGVO auf Seite 60 und Zusätzliche Sicherungen auf Seite 64 Informationen dazu enthalten, wie Sie mit einer regelungskonformen Einrichtung beginnen, müssen Sie bei der weiteren Konfiguration des Systems das EU-Datenschutzrecht beachten.

DSGVO - was ist das?

Die Datenschutzgrundverordnung (DSGVO) stellt Regelungen für personenbezogene Daten jeder Art auf, die von einer Organisation gespeichert werden. Die DSGVO gewährleistet das Eigentum jedes Einzelnen an seinen personenbezogenen Daten und führt auf Seiten von Organisationen die Verantwortlichkeit in allen Phasen der Datenverarbeitung und -speicherung ein. Die DSGVO erreicht dies mit einer Reihe von Rechten des Einzelnen und entsprechende Pflichten seitens der Organisationen, die personenbezogene Daten verarbeiten.

Die DSGVO harmonisiert die Datenschutzgesetze EU-weit und ergänzt die bestehenden Vorschriften der Mitgliedsstaaten für CCTV und Videoüberwachung.

Obwohl die DSGVO eine EU-Regelung darstellt, hat sie Auswirkungen in vielen anderen Teilen der Welt.
Sie gilt für die Verarbeitung personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter in der Europäischen Union, unabhängig davon, ob die Verarbeitung innerhalb der Europäischen Union stattfindet oder nicht.
Sie gilt für die Verarbeitung personenbezogener Daten durch einen nicht in der Europäischen Union ansässigen Verantwortlichen oder Auftragsverarbeiter, wenn die Verarbeitungstätigkeiten im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen in der Europäischen Union oder mit der Überwachung ihres Verhaltens stehen, soweit sie dieses Verhalten innerhalb der Europäischen Union zeigen.
Darüber hinaus gelten in vielen anderen Teilen der Welt ähnliche Datenschutzbestimmungen, die auf den Kernprinzipien der DSGVO basieren.

Die DSGVO wird von den Behörden der Mitgliedstaaten durchgesetzt.

Bei Zuwiderhandlung drohen hohe Geldstrafen:

- Bis zu 4% des Jahresumsatzes des betreffenden Unternehmens
- Bis zu €20 Mio. je Vorfall

Wer hat zu gewährleisten, dass ein laufendes XProtect Videoverwaltungssystem die DSGVO einhält?

Der Eigentümer des VMS ist für die Einhaltung der DSGVO verantwortlich, einschließlich:

- Die tatsächliche Installation und Nutzung
- Organisatorische Prozesse und Reifegrad
- Benachrichtigungen bei Datenschutzverletzungen und Meldung an Behörden

Die DSGVO gilt nicht für bestimmte Produkte, jedoch hat die Kombination aus Produkt, davon verarbeiteten Daten und der Nutzung des Produkts und der Daten Auswirkungen auf die Einhaltung der DSGVO.

Die DSGVO hat direkte Auswirkungen für die Installer, Systemintegratoren und Benutzer von Videoüberwachungstechnologie.

Der Eigentümer des VMS ist der für die Verarbeitung Verantwortliche (siehe Die für die Verarbeitung verantwortliche Person auf Seite 16).

Der für die Verarbeitung Verantwortliche mit den Betrieb des VMS ganz oder teilweise einen Datenverarbeiter beauftragen, z. B. ein Sicherheitsunternehmen. In diesem Fall müssen der die Verarbeitung verantwortliche und der Datenverarbeiter eine *Datenverarbeitungsvereinbarung* abschließen. Die *Datenverarbeitungsvereinbarung* gibt an, welche Daten verarbeitet werden, wie sie geschützt werden und wie lange die Daten gespeichert bleiben (siehe Datenverarbeiter auf Seite 25 und Anhang: Vereinbarung mit dem Datenverarbeiter auf Seite 59).

Müssen alle Videoüberwachungsanlagen die DSGVO einhalten?

Die DSGVO gilt für die für die Verarbeitung Verantwortliche und für Auftragsverarbeiter innerhalb der Europäischen Union, unabhängig davon, wo die Videoaufzeichnungen verarbeitet werden.

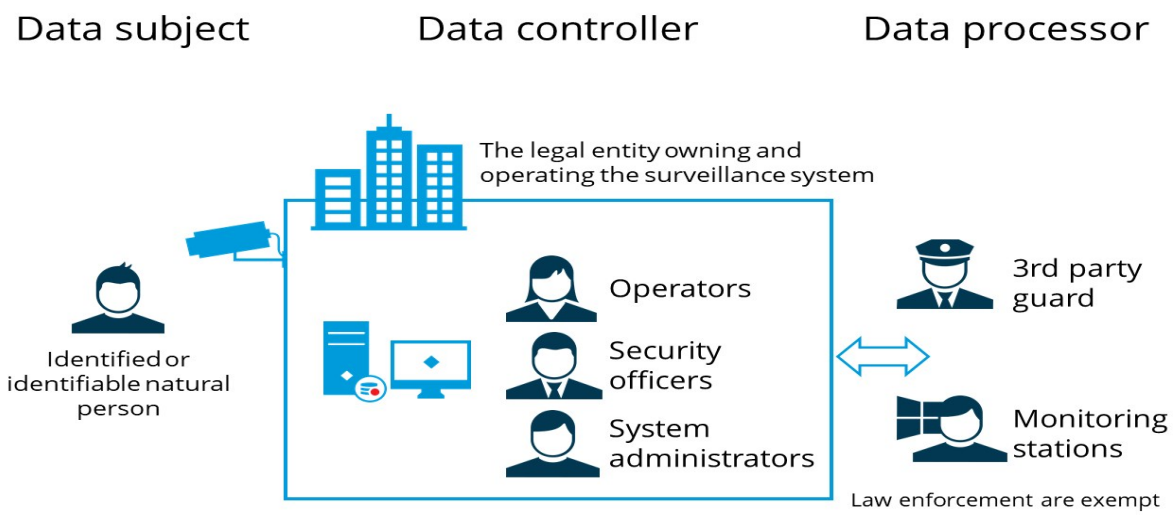
Darüber hinaus schützt die DSGVO die Daten aller Einwohner des geografischen Gebietes der EU, gilt für alle Formen der Videoüberwachung innerhalb der EU und schützt alle EU-Bürger (Paragraph 3 DSGVO).

Weitere Informationen zur DSGVO, insbesondere hinsichtlich Videoüberwachung, siehe Anhang: Einhaltung der DSGVO auf Seite 30.

Wer sind die Hauptanspruchsgruppen in Bezug auf die Videoüberwachung unter den Gesichtspunkten der DSGVO?

Was die DSGVO und Videoüberwachung betrifft, gibt es drei Anspruchsgruppen. In diesem Abschnitt des Dokuments werden die einzelnen Anspruchsgruppen definiert und ihre jeweiligen Verantwortlichkeiten in Bezug auf die DSGVO beschrieben.

- Betroffene Person auf Seite 11
- Die für die Verarbeitung verantwortliche Person auf Seite 16
- Datenverarbeiter auf Seite 25



Betroffene Person

Eine betroffene Person ist jede Person, deren personenbezogene Daten gesammelt, gespeichert oder verarbeitet werden.

Betroffene Personen sind die in den Videoaufzeichnungen Gezeigten, gleichgültig, ob dies vorsätzlich oder zufällig geschieht.

Betroffene Personen sind auch alle registrierten Personen, die am Betrieb des VMS beteiligt sind, z. B. Betreiber oder benanntes Wachpersonal Dritter.

Das Hauptziel der DSGVO ist der Schutz der personenbezogenen Daten dieser betroffenen Personen.

Rechte der betroffenen Personen

Paragraph 12 bis 23 DSGVO behandeln die Rechte der betroffenen Personen.

- Abschnitt 1: Transparenz und Modalitäten
    - Paragraph 12: Transparente Informationen, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person
- Abschnitt 2: Informationen und Zugriff auf personenbezogene Daten
    - Paragraph 13: Informationen, die zur Verfügung gestellt werden müssen, wenn personenbezogene Daten der betroffenen Person erhoben werden
    - Paragraph 14: Informationen, die zur Verfügung gestellt werden müssen, wenn personenbezogene Daten der betroffenen Person erhoben wurden
    - Paragraph 15: Das Recht der betroffenen Person, Zugang zu ihren Daten zu erhalten (siehe Das Zugriffsrecht auf Seite 38)
- Abschnitt 3: Berichtigung und Löschung
    - Paragraph 16: Berichtigungsrecht
    - Paragraph 17: Das Recht, vergessen zu werden (Recht auf Löschung) (siehe Das Recht, vergessen zu werden (Recht auf Löschung) auf Seite 40)
    - Paragraph 18: Das Recht, die Verarbeitung zu beschränken (siehe Das Recht auf die Beschränkung der Verarbeitung auf Seite 42)
    - Paragraph 19: Benachrichtigungspflicht bei Berichtigung oder Löschung personenbezogener Daten oder bei Einschränkung der Verarbeitung
    - Paragraph 20: Recht auf Datenübertragbarkeit
- Abschnitt 4: Widerspruchsrecht und automatisierte individuelle Entscheidung
    - Paragraph 21: Widerspruchsrecht
    - Paragraph 22: Automatisierte individuelle Entscheidung, einschließlich Profilerstellung
- Abschnitt 5: Einschränkungen
    - Paragraph 23: Einschränkungen

Diejenigen davon, die im Hinblick auf die Videoüberwachung am wichtigsten sind, sind folgende:

Das Informationsrecht (Paragraph 12 bis 14 und 34 DSGVO)	Paragraph 12 behandelt die Transparenz und die Modalitäten, während sich Paragraph 13 und 14 mit der Information und dem Zugang zu personenbezogenen Daten befassen. Anhand dieser Paragraphen kann sich die betroffene Person darüber informieren, welche personenbezogenen Daten gesammelt und wie lange sie gespeichert werden. Im Zusammenhang mit einem VMS, siehe Anhang: Ad-hoc-Mitteilung auf Seite 53.

	Aufgrund von Paragraph 34 hat die betroffene Person das Recht, im Fall einer Datenschutzverletzung informiert zu werden, wenn diese mit hoher Wahrscheinlichkeit ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person mit sich bringt.
Das Zugriffsrecht (Paragraph 15 DSGVO)	Dieser Paragraph der DSGVO gibt der betroffenen Person das Recht, Zugang zu den über sie verarbeiteten personenbezogenen Daten zu erhalten, z. B. Videoaufzeichnungen der betroffenen Person. Die betroffene Person hat das Recht, von dem jeweiligen Unternehmen Auskunft darüber zu verlangen, welche ihrer personenbezogenen Daten verarbeitet werden und aus welchem Grund.
Das Löschungsrecht ("Recht, vergessen zu werden") (Paragraph 17 DSGVO)	Dieses Recht gibt der betroffenen Person die Möglichkeit, die Löschung ihrer Daten zu verlangen. Im Zusammenhang mit einem VMS ist die Löschung auf Wunsch der betroffenen Personen aufgrund der Interessen des für die Verarbeitung Verantwortlichen und der kurzen Aufbewahrungszeiten eine Ausnahme. (Siehe Anhang: Richtlinie für die Videoüberwachung auf Seite 54 und *Teilweise Löschung von Videoaufzeichnungen* in Anhang: Das Milestone XProtect VMS-System und die DSGVO auf Seite 60).
Das Widerspruchsrecht (Paragraph 21 DSGVO)	Dieses Recht gibt der betroffenen Person die Möglichkeit, der Verarbeitung ihrer personenbezogenen Daten zu widersprechen. Im Zusammenhang mit einem VMS können andere Interessen die Interessen und Rechte der betroffenen Person überwiegen, z. B. berechtigte Interessen (Betrugsaufdeckung, Gesundheit und Sicherheit), gesetzliche Verpflichtungen (Buchhaltung, Bekämpfung der Geldwäsche) und sogar Vertragserfüllung (z.B. Arbeitsverträge). In allen Fällen muss dies vollkommen transparent sein, damit die betroffene Person informiert ist und Widerspruch einlegen kann. Wenn die betroffene Person Widerspruch einlegt, muss der für die Verarbeitung Verantwortliche den Widerspruch prüfen, andernfalls droht ihm ein Bußgeld.

Anfrage einer betroffenen Person

Ihr Unternehmen muss über ein Verfahren zur Behandlung von Anfragen zu den Rechten betroffener Personen verfügen, z. B. die Ausübung des Rechts auf Datenzugriff. Eine solche Anfrage muss innerhalb eines angemessenen Zeitrahmens bearbeitet werden. Nach Paragraph 12 (3) DSGVO muss dies "unverzüglich, in jedem Fall jedoch innerhalb eines Monats nach Eingang der Anfrage" erfolgen. Es wird empfohlen, eine

Vorlage eine *Anfrage einer betroffenen Person* zu verwenden, um solche Anfragen zu dokumentieren, da dies in einem DSGVO-Fall vor nationalen Datenschutzbehörden entscheidend sein kann. Einen Musterantrag einer betroffenen Person finden Sie unter *Milestone Musterantrag einer betroffenen Person*.

Die *Richtlinie zur Videoüberwachung* beschreibt den Antrag betroffener Personen (siehe Anhang: Richtlinie für die Videoüberwachung auf Seite 54).

Was sind personenbezogene Daten?

Um die DSGVO zu erfüllen, müssen Sie wissen, was personenbezogene Daten sind, und die Erfassung dieser Daten auf das notwendige Maß beschränken.

Nach der Verordnung sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen.

Eine identifizierbare Person ist jemand, der direkt oder indirekt durch Bezugnahme auf eine Kennung identifiziert werden kann, wie z. B.:

- Einen Namen
- Eine Kennnummer
- Standortdaten
- Online-Kennungen wie IP-Adressen oder Cookies
- Benutzerdaten
- Videobilder
- Oder auf einen oder mehrere Faktoren, die eindeutig auf die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität dieser Person hindeuten

Personenbezogene Daten sind alle Informationen, die direkt oder indirekt zur Identifizierung einer natürlichen Person (die betroffene Person) verwendet werden können. Dies sind die Daten, die zur Identifizierung der betrachteten Objekte der Videoüberwachung verwendet werden können, unabhängig davon, ob diese Daten absichtlich oder zufällig gesammelt wurden.

Laut DSGVO geschützte personenbezogene Daten sind:

- Daten, die durch ein IT-Produkt oder den IT-basierten Dienst verarbeitet werden (z. B. Name und Adresse einer Person, Videobild, Zahlungsdaten, Gesundheitsdaten).
- Daten, die bei der Nutzung des Produkts oder Dienstes beiläufig anfallen (z. B. Nutzungsdaten, Protokolldatei, statistische Daten, Daten zur Autorisierung, Konfigurationsdaten). Bei diesen Daten kann es sich um personenbezogene Daten der Nutzer des Dienstes, personenbezogene Daten der Personen, die das Produkt oder den Dienst betreiben (dazu können sowohl Mitarbeiter des Dienstanbieters als auch Mitarbeiter der Nutzer des Produkts oder des Dienstes gehören), oder um datenschutzrelevante Konfigurationsdaten handeln (siehe Die für die Verarbeitung verantwortliche Person auf Seite 16).

Personenbezogene Daten werden definiert als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person oder auf eine betroffene Person beziehen, z.B.:

• Der volle Name • Die Hausadresse • Die E-Mail-Adresse • Telefonnummer • Standortdaten • Die digitale Identität	• Das Kennzeichen des Fahrzeugs • Führerscheinnummer • Kreditkartennummern • Identifizierbare Angaben, Bilder usw., wie z.B. Videoaufzeichnungen und Standbilder • Benutzeraktivitäten, wie sie in Protokolldateien finden sind

Solche Daten stehen nicht unbedingt nur in einem direkten Zusammenhang mit dem Objekt. Personenbezogene Daten können auch Quasi-Identifikationen sein. Quasi-Identifikationen sind Informationen, die selbst keine eindeutigen Identifikationen sind, aber ausreichend gut mit etwas korrelieren, so dass sie mit anderen Quasi-Identifikationen kombiniert eine eindeutige Identifikation bilden. Quasi-Identifikationen sind besonders wichtig, wenn es um spezielle Kategorien personenbezogener Daten geht.

Spezielle Kategorien personenbezogener Daten sind u.a. Daten, die die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Daten über Gesundheit oder Daten zum Sexualleben oder zur sexuellen Orientierung abbilden, z. B.:

• Krankengeschichte • Biometrische Daten (einschließlich Fotos, Videos, Fingerabdrücke) • Polizeiliches Führungszeugnis • Rassische oder ethnische Identität	• Genetische Informationen • Politische Meinungen und Engagement • Religiöse oder philosophische Weltanschauung • Sexuelle Orientierung und Vorgeschichte

Die folgenden personenbezogenen Daten können von einem Videoüberwachungssystem erfasst werden:

Was für personenbezogene Datenbeschreibungen, die von XProtect gespeichert werden, fallen unter die DSGVO?

Personenbezogene Daten sind alle Informationen, die direkt oder indirekt zur Identifizierung einer natürlichen Person (der betroffenen Person) verwendet werden können. Dies können Videoüberwachungsstreams, Einzelbilder oder eine Videosequenz in Kombination mit Standortinformationen von Kameras und/oder darüber gelegten Karten, eine Zutrittskontrollintegration, die eine persönliche Zugangskarte erkennt und mit einem bestimmten Standort kombiniert, oder Daten aus der Nummernschilderkennung (LPR) mit oder ohne Standortdaten sein.

Besondere Kategorien personenbezogener Daten liegen vor, wenn die Videoüberwachung in der Nähe von Krankenhäusern (Gesundheitsdaten), Gefängnissen (strafrechtliche Verurteilungen), politischen Aktivitäten (Gewerkschaftsmitgliedschaft), religiösen Aktivitäten oder Bildern erfolgt, die die sexuelle Orientierung offenbaren (z. B. Bars, die von Homosexuellen frequentiert werden).

Personenbezogene Daten sind auch Benutzerdaten (Bediener, Vorgesetzter und Administrator) sowie auf die Protokollierung von Aktivitäten und Audits. Dazu gehören XProtect Smart Client persönliche Benutzerprotokolle, einschließlich Zeitstempel für die An- und Abmeldung und Audit-Protokolle von Videoströmen, auf die zugegriffen wurde, Audio- oder Metadaten sowie die Wiedergabe und der Export von Aufzeichnungen.

Angaben dazu, wie Sie sich vergewissern, dass Sie niemandes Persönlichkeitsrechte verletzen, finden Sie unter Inhärente Risiken bei der Verwendung von VMS auf Seite 58.

Die für die Verarbeitung verantwortliche Person

Im Zusammenhang mit der Videoüberwachung sind die für die Verarbeitung Verantwortlichen Eigentümer und Betreiber der Videoüberwachungssysteme. Für die Verarbeitung verantwortlich ist diejenige juristische Person, die Daten über die betroffene Person sammelt, verarbeitet und weitergibt.

Was ist der für die Verarbeitung Verantwortliche zuständig?

Die für die Verarbeitung Verantwortlichen müssen die Grundsätze des Datenschutzes beachten und haben besondere Verpflichtungen. Der für die Verarbeitung Verantwortliche muss geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen und nachweisen zu können, dass die Verarbeitung in Übereinstimmung mit der DSGVO erfolgt. Hierzu gehört auch:

- Die Anwendung und Pflege von Informationssicherheitsrichtlinien und -verfahren zum Schutz personenbezogener Daten. Solche internen Richtlinien und Prozesse bedürfen der Genehmigung auf höchster Leitungsebene der Organisation und sind somit für alle Mitarbeiter verbindlich.
- Den Überblick über Aufzeichnungen personenbezogener Daten und die Verarbeitung von Video-Streams, z. B. Aufzeichnung zu Verarbeitungstätigkeiten (Paragraph 30 DSGVO) sowie eine Liste der Systeme und Archive, in denen personenbezogene Daten verarbeitet werden (das XProtect VMS-System und sonstige Systeme, in denen personenbezogene Daten gespeichert werden, z. B. Personalakten, Verträge mit Datenverarbeitern usw., einschließlich Angaben dazu, wie und wohin die personenbezogenen Daten fließen). Eine Musteraufzeichnung von Verarbeitungstätigkeiten finden Sie in der Aufzeichnung von Verarbeitungstätigkeiten (Muster).
- Die Einrichtung von Mechanismen, die die Umsetzung der internen Richtlinien und Prozesse unterstützen, einschließlich Beschwerdeverfahren, um diesen Richtlinien zu praktischer Geltung zu verhelfen. Hierzu gehören auch Bewusstmachung für den Datenschutz sowie die Schulung der und Anweisungen an die Mitarbeiter. Eine Schulung zur Bewusstmachung steht unter https://www.milestonesys.com/solutions/services/learning-and-performance/ zur Verfügung.
- Aufstellung einer *Richtlinie für die Videoüberwachung* (siehe Anhang: Richtlinie für die Videoüberwachung auf Seite 54). Eine solche Richtlinie muss auf der nationale Gesetzgebung zur Videoüberwachung beruhen.
- Die Durchführung von Datenschutz-Folgenabschätzungen, insbesondere für bestimmte Datenverarbeitungsvorgänge, von denen angenommen wird, dass sie besondere Risiken für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, z. B. aufgrund ihrer Art, Umfangs oder Zwecks (siehe Anhang: Datenschutz-Folgenabschätzung auf Seite 56).
- Gewährleistung der Transparenz der beschlossenen Maßnahmen gegenüber den betroffenen Personen und der Öffentlichkeit allgemein. Die Anforderungen an die Transparenz tragen zur Rechenschaftspflicht der für die Verarbeitung Verantwortlichen bei (z. B. Veröffentlichung von Datenschutzrichtlinien im Internet, Transparenz bei internen Beschwerdeverfahren und Veröffentlichung in Jahresberichten).
- Veröffentlichung der Mitteilung zum Auskunftsrecht für die Öffentlichkeit (siehe Anhang: Ad-hoc-Mitteilung auf Seite 53). Der Hinweis auf das Auskunftsrecht klärt die betroffenen Personen darüber auf, welchem Zweck die Überwachung dient, wer die erfassten Daten speichert (der für die Verarbeitung Verantwortliche) und die Richtlinie für die Speicherung.
- Die Übertragung der Verantwortung für den Datenschutz an Beauftragte, die direkt für die Einhaltung der Datenschutzgesetze durch ihre Organisation verantwortlich sind. Insbesondere die Ernennung eines Datenschutzbeauftragten (DSB).

Der Datenschutzbeauftragte (DSB)

Jede Organisation muss einen DSB ernennen, oder zumindest eine zuständige Person, die für den Datenschutz verantwortlich ist.

Die Pläne zur Installation oder Aktualisierung eines Videoüberwachungssystems ist von Anfang an dem DSB mitzuteilen.

Der DSB sollte in jedem Fall und zeitnah in allen Fragen konsultiert werden, die den Schutz personenbezogener Daten betreffen, die bei der Bereitstellung oder Nutzung des Dienstes verarbeitet werden.

Der DSB sollte in alle Phasen der Entscheidungsfindung einbezogen werden.

Der DSB ist u. a. zuständig für:

- Die Mitwirkung bei der Festlegung der geschäftlichen Zwecke der Videoüberwachung, z. B. Verbrechensverhütung, Betrugserkennung, Überprüfung der Produktqualität oder öffentliche Gesundheit und Sicherheit usw.
- Kommentare zum Entwurf der *Richtlinie für die Videoüberwachung*der Organisation, einschließlich ihrer Anhänge (siehe Anhang: Richtlinie für die Videoüberwachung auf Seite 54) und die Korrektur von Fehlern sowie Verbesserungsvorschläge
- Unterstützung bei der Kommunikation mit den nationalen oder örtlichen Datenschutzbehörden
- Überprüfung der Vereinbarungen mit Dritten bei der Weitergabe von Daten. D.h. Pflege und Verwaltung der *Vereinbarungen mit Datenverarbeitern* (siehe Anhang: Vereinbarung mit dem Datenverarbeiter auf Seite 59)
- Erstellung von Entwürfen zu Compliance-Berichten und Durchführung von Audits, um Zertifizierungen durch Dritte zu erhalten, die die internen Maßnahmen zur Sicherstellung der Compliance für die wirksame Verwaltung, den Schutz und die Sicherheit personenbezogener Daten bestätigen
- Die Aufzeichnungen zu den Verarbeitungstätigkeiten und die Datenschutz-Folgenabschätzungen (siehe Anhang: Datenschutz-Folgenabschätzung auf Seite 56) aufzubewahren und zu gewährleisten, dass sie stets aktualisiert werden, wenn am VMS datenschutzrelevante Änderungen erfolgen. Eine Musteraufzeichnung von Verarbeitungstätigkeiten finden Sie in der Aufzeichnung von Verarbeitungstätigkeiten (Muster).

Rollen des für die Verarbeitung Verantwortlichen

Die Verantwortung des jeweils für die Verarbeitung Verantwortlichen werden in folgenden Abschnitten beschreiben:

- Sicherheitsbeauftragter (der das VMS überwacht) auf Seite 19
- VMS-Systemadministrator auf Seite 21
- VMS-Bediener auf Seite 22

Sicherheitsbeauftragter (der das VMS überwacht)

Der Sicherheitsbeauftragte ist dafür zuständig, dafür zu sorgen, dass das Umfeld der DSGVO entspricht. Sicherheitsbeauftragte müssen:

- Legen Sie Benutzerberechtigungen fest (siehe Verwaltung von Benutzerberechtigungen auf Seite 19)
- Schulungen zur Bewusstmachung des Personals vorantreiben (siehe Schulungen zum Datenschutz auf Seite 21)
- Sich an den Datenschutzbeauftragten (DSB) wenden, wenn der Verdacht besteht, dass ein Verstoß gegen die DSGVO vorliegt, z. B. wenn Videomaterialien gegen den Datenschutz verstößt (siehe Anhang: Einhaltung der DSGVO auf Seite 30)
- Eine hohes Maß an allgemeiner Sicherheit anwenden und aufrechterhalten. Weitere Informationen dazu, wie Sie Ihre XProtect VMS-Installationen vor Cyber-Angriffen schützen, finden Sie im Schutzleitfaden.

Verwaltung von Benutzerberechtigungen

Wer sollte Zugriff auf Ressourcen des VMS haben?

Die betreffenden Organisationen müssen:

- Den Zugriff auf eine kleine Anzahl klar bezeichneter Benutzer beschränken, die davon Kenntnis haben müssen.
- Audit-Protokolle über Benutzerzugriffe und Aktivitäten führen.

Die Zugriffsberechtigungen sind auf eine kleine Anzahl eindeutig identifizierter Personen und auf streng vertraulicher Basis zu beschränken. Achten Sie darauf, dass autorisierte Benutzer nur auf die Daten zugreifen können, auf die sich ihre Zugriffsberechtigung bezieht. Die Zugangskontrollrichtlinien sollten nach dem Prinzip des "geringsten Privilegs" festgelegt werden: Benutzern sollte nur der Zugang zu den Ressourcen gewährt werden, die für die Ausführung ihrer Aufgaben unbedingt erforderlich sind.

Bei gemeinsamer Nutzung eines Computers empfiehlt Milestone, dass die Bediener des VMS keine gemeinsame Anmeldung für das Windows-Konto verwenden sollten. Jeder Bediener sollte ein eigenes Konto haben.

Außerdem sollten VMS-Anwender nicht die Option auswählen, dass ihr Passwort für die Anmeldung am VMS-System gespeichert wird.

Nur der Sicherheitsbeauftragte, der Systemadministrator oder andere vom Sicherheitsbeauftragten eigens zu diesem Zweck ernannte Mitarbeiter dürfen in der Lage sein, Personen Zugangsberechtigungen zu erteilen, zu

ändern oder sie aufzuheben. Jede Erteilung, Änderung oder Aufhebung von Zugangsberechtigungen muss in Übereinstimmung mit den in der *Richtlinie für die Videoüberwachung* festgelegten Kriterien erfolgen (siehe Anhang: Richtlinie für die Videoüberwachung auf Seite 54).

Personen, die über eine Zugangsberechtigung verfügen, müssen stets eindeutig identifizierbar sein. Zum Beispiel sollten unterbeauftragten Sicherheitsfirman keine generischen oder allgemeinen Benutzernamen und Passwörter gegeben werden, die mehrere Mitarbeiter für das Unternehmen beschäftigt.

In der *Richtlinie für die Videoüberwachung* muss die technische Architektur des Videoüberwachungssystems eindeutig festgelegt und dokumentiert werden, wer zu welchem Zweck Zugriff auf die Aufzeichnungen aus der Videoüberwachung hat und was diese Zugriffsberechtigungen beinhalten. Insbesondere müssen Sie angeben, wer die Berechtigungen hat, um:

• In Echtzeit auf die Videoaufzeichnungen zuzugreifen und diese zu betrachten • Die Schwenk-Neige-Zoom-Kameras (PTZ) zu bedienen • Auf Videoaufzeichnungen zuzugreifen	• Aufzeichnungen und Prüfbelege zu exportieren • Geräte (Kameras) zu löschen oder zu entfernen und Aufzeichnungen zu löschen • Daten nach der Erstkonfiguration zu ändern

Darüber hinaus müssen Sie sicherstellen, dass nur diejenigen, die Zugriff auf folgende Funktionen des VMS benötigen, diese Berechtigungen erhalten:

• Verwaltung des VMS • Lesezeichen erstellen / bearbeiten / anzeigen / löschen • Beweismittelsicherungen erstellen / bearbeiten / anzeigen / löschen • Zum Schutz der Privatsphäre unkenntlich gemachte Bildbereiche freilegen • Export über festgelegte Dateipfade (z. B. nur Export im XProtect Format auf ein freigegebenes Laufwerk mit Verschlüsselung)	• Auditprotokolleinträge lesen • Starten/anhalten der Aufzeichnung • Voreinstellungen der PTZ-Kameras erstellen/bearbeiten/löschen/aktivieren/sperren/freigeben • PTZ-Patrouillenschemata erstellen/bearbeiten/löschen/starten/stoppen • Audio, Metadaten, E/A und Ereignisberechtigungen

Schulungen zum Datenschutz

Alle Mitarbeiter mit Zugangsberechtigung, einschließlich ggf. Fremdpersonal, das mit dem täglichen Betrieb der Videoüberwachung oder der Wartung des Systems betraut ist, sind im Datenschutz zu schulen und müssen mit den Bestimmungen der DSGVO vertraut sein, soweit sie für ihre Aufgaben relevant sind. Bei der Schulung sollte besonders darauf hingewiesen werden, dass Überwachungsvideos ausschließlich an autorisierte Personen weitergegeben werden dürfen.

Die Schulung des Personals ist obligatorisch und muss folgende Inhalte berücksichtigen:

- Cybersicherheit
- Exportieren von VMS-Daten

Solche Schulungen sind durchzuführen, wenn ein neues System installiert wird, wesentliche Änderungen am System erfolgen, eine neue Person in die Organisation eintritt, sowie in regelmäßigen Abständen danach. Für bestehende Systeme sollte die Erstschulung während der Übergangszeit und danach in regelmäßigen Abständen erfolgen.

Weitere Informationen zur DSGVO für den Anwender einer VMS finden Sie in der Milestone DSGVO-Datenschutzrichtlinie für VMS-Anwender und im Milestone E-Learning zur DSGVO für VMS-Anwender.

VMS-Systemadministrator

Systemadministratoren sind für die Einrichtung einer Systemumgebung verantwortlich, die der DSGVO entspricht. Systemadministratoren haben u.a. folgende Zuständigkeiten:

- Eine hohes Maß an allgemeiner Sicherheit anwenden und aufrechterhalten. Weitere Informationen dazu, wie Sie Ihre XProtect VMS-Installationen vor Cyber-Angriffen schützen, finden Sie im Schutzleitfaden.
- Anwendung sicherer Passwortregeln
- Durchführung von Sicherheitsaudits
- Darauf zu achten, dass die Geräte dem festgelegten Zweck entsprechend aufzeichnen - z. B. bei einem Zwischenfall, bei Bewegungen, immer eingeschaltet, usw.
- Darauf zu achten, dass die Dauer der Aufzeichnungen und die Speicherdauer für die Audit-Protokolle den örtlich geltenden Gesetzen und dem definierten Zweck des VMS folgen
- Die Benutzerverwaltung (Benutzer hinzufügen und entfernen)
- Darauf zu achten, dass die Kameras die Gesetze zum Datenschutz einhalten und keine Bereiche aufzeichnen, die nicht aufgezeichnet werden dürfen, und dass Bereiche, die nicht aufgezeichnet werden dürfen, unkenntlich gemacht werden
- Sich an den Datenschutzbeauftragten (DSB) zu wenden, wenn der Verdacht besteht, dass ein Verstoß gegen die DSGVO vorliegt, z. B. wenn Videomaterial gegen den Datenschutz verstößt (siehe Anhang: Einhaltung der DSGVO auf Seite 30)

VMS-Bediener

Die Bediener des VMS müssen Prozesse und Arbeitsanweisungen befolgen, wenn sie auf Daten im System zugreifen, z. B. beim Betrachten oder Exportieren von Videos usw.

Zur Einhaltung der DSGVO haben die Bediener folgende Verantwortung:

- Ein allgemeines Verständnis der DSGVO und der Regeln für den Datenexport
- Eine Schulung im Hinblick auf die DSGVO

  Die Bediener sollten in der Funktion des Videoüberwachungssystems ausreichend geschult sein, damit die Privatsphäre und sonstige Grundrechte der von den Kameras erfassten Personen nicht verletzt werden. Sie müssen darüber unterrichtet werden, was in den *Richtlinien für die Videoüberwachung* festgelegt ist (z. B. Verfahren für die Herausgabe von Videobeweisen), an wen sie sich im Zweifelsfall wenden können (Eskalationsstellen, z. B. der Vorgesetzte oder der Datenschutzbeauftragte) usw. (siehe Sicherheitsbeauftragter (der das VMS überwacht) auf Seite 19).

  Weitere Informationen zur DSGVO für den Anwender einer VMS finden Sie in der Milestone DSGVO-Datenschutzrichtlinie für VMS-Anwender und im Milestone E-Learning zur DSGVO für VMS-Anwender.

Umgang mit exportierten Daten

Der Export erfolgt, wenn es einen Zwischenfall gab, der die Weitergabe von Beweisen an die Behörden erforderlich macht. Wenn Sie als Benutzer die Berechtigung haben, Beweise zu exportieren, tragen Sie die Verantwortung für den Umgang damit. Der Grund für die Sensibilität liegt zum einen im Inhalt, und zum anderen in der Tatsache, dass die Daten das Überwachungssystem verlassen. Mit hoher Wahrscheinlichkeit hat es einen Vorfall gegeben, bei dem kriminelle Handlungen eine Rolle spielen. Die Beweisen können auch sensible private Einzelheiten enthalten. Wenn Sie diese exportieren, werden sie üblicherweise auf irgendeinem Wechseldatenträger (USB-Laufwerk, optischer Datenträger usw.) gespeichert.

Sollten diese Daten in die falschen Hände geraten, wäre die Privatsphäre der betroffenen Personen, die in den Beweismitteln erscheinen, verloren.

Sie sollten ein klares Verfahren für den Export von Beweismitteln haben, zu dem u.a. gehört:

- Wer kann Beweismittel exportieren?
- Wo werden die Beweismittel gespeichert, bis sie den Behörden übergeben werden?
- Wer hat Zugang dazu?
- Welche Formate sind zu verwenden?
- Ob eine Verschlüsselung zur Anwendung kommen sollte (dies wird empfohlen)?
- Wann werden die Beweismittel zerstört?

Die für die Verarbeitung Verantwortlichen müssen technische und organisatorische Maßnahmen ergreifen, um Daten zu schützen, die das Milestone XProtect VMS verlassen. Dies können u.a. folgende Maßnahmen sein:

- Einschränkung der Berechtigung zum Exportieren von Videos und Prüfprotokollen auf bestimmtes Personal
- Erwägen Sie, die Daten vor oder nach dem Exportieren zu verschlüsseln
- Videodaten sind vor dem Exportieren ggf. unkenntlich zu machen
- Physischer Schutz von Wechselmedien mit persönlichen Daten darauf
- Es sind Richtlinien dafür aufzustellen, dass personenbezogene Daten am Ende der Aufbewahrungsfrist von den Medien gelöscht werden
- Es ist ein Register der Wechseldatenträger zu führen - wer hat welche Daten auf die Datenträger exportiert? An wen wurden sie weitergeleitet und zu welchem Zweck? Wird der Empfänger informiert, dass er die Medien nach Erreichen des Zwecks zu vernichten oder zurückzugeben hat? usw.
- Verwenden Sie die Gruppenrichtlinien von Windows, um USB-Anschlüsse oder den Medienzugriff auf den Client-PCs zu deaktivieren
- Überwachen Sie die Audit-Protokolle auf unbefugte Export-Ereignisse
- Mitarbeiter sind auf die Datenschutzpolitik zu verpflichten
- Bereinigen Sie die Medien ordnungsgemäß oder löschen Sie sie physisch, wenn eine Bereinigung nicht möglich ist (z. B. bei DVDs)

Weitere Informationen zum Umgang mit Datenexporten finden Sie im Milestone E-Learning zur DSGVO für VMS-Bediener.

Umgang mit exportierten Daten in Benachrichtigungen und E-Mails

Neben dem Export können die Daten auch in Form von Anhängen an Benachrichtigungen aus dem VMS extrahiert werden. Benachrichtigungen sind E-Mails, die an eine bestimmte E-Mail-Adresse gesendet werden. Beim Erstellen einer Benachrichtigung kann der Administrator wählen, ob er mehrere Schnappschüsse oder eine AVI einer Sequenz mit einschließen möchte. Da die angehängten Momentaufnahmen und AVI-Sequenzen in den Benachrichtigungen das VMS verlassen, befinden sie sich für die Zwecke des Benutzerzugriffs und der Aufbewahrung nicht mehr unter der Kontrolle des VMS. Es wird empfohlen, keine Bilder oder AVI-Sequenzen an E-Mail-Benachrichtigungen anzuhängen. Wenn die Anhänge erforderlich sind, müssen Sie zumindest sicherstellen, dass es organisatorische Verfahren und Kontrollen dafür gibt, wer die E-Mails erhält und wie damit umgegangen wird.

VMS-Anwender, die ein mobiles Gerät verwenden, müssen sich darüber im Klaren sein, dass Mediengalerien auf ihrem Gerät automatisch auf Google oder Apple-Servern gesichert werden können, wenn dies auf dem Gerät so konfiguriert ist. In diesem Fall könnte es zu einer unrechtmäßigen Datenübermittlung in ein Drittland kommen, wenn es sich um Bilder von identifizierbaren natürlichen Personen handelt.

Um dies in den Griff zu bekommen, sollten Sie Datenschutz- und Sicherheitsrichtlinien mit Software für die Mobilgeräteverwaltung (Mobile Device Management, MDM) durchsetzen und Sicherheitsvorkehrungen wie die in Anhang: Einhaltung der DSGVO auf Seite 30 aufgeführten treffen.

Außerdem sollten Sie ein klares Verfahren haben u.a. für:

- Wo die Daten gespeichert werden

  Achten Sie darauf, dass die E-Mail-Server für den Versand und Empfang unter der Kontrolle der Organisation stehen, die für die Verarbeitung der Daten aus der Videoüberwachung verantwortlich ist / die Daten verarbeitet. Insbesondere sollte es sich bei den Empfängern nicht um Freemail-Konten wie Gmail oder Hotmail usw. handeln.

- Wer hat Zugang dazu?
- Welche Formate sind zu verwenden?
- Ob eine SMTP-Verschlüsselung zur Anwendung kommen sollte

  > ⚠ Beachten Sie bitte: Verwenden Sie einen SMTP/SMTPS-Mailserver. Sie müssen die Verbindung zwischen dem VMS und den Postausgangsservern sowie zwischen dem sendenden und dem empfangenden SMTP-Server verschlüsseln, um unter das Europäische Datenschutzsiegel zu fallen. Eine unverschlüsselte und nicht gesicherte Verbindung würde gegen das EuroPriSe-Siegel verstoßen und zum Verlust der Konformität mit dem EuroPriSe-Datenschutzsiegel führen.

- Wann werden die Daten vernichtet?

  Milestone empfiehlt, die Aufbewahrungszeit von Videodaten in den Ausgangs- und Eingangspostfächern an die Speicherdauer der Mediendatenbank oder an die Speicherdauer für Alarme anzupassen, die durch dieselben Ereignisse ausgelöst worden sein können, die auch die Benachrichtigung verursacht haben.

  Die Speicherdauer in den Mailboxen muss so begrenzt werden, wie es für den Zweck des Benachrichtigungsprozesses angemessen ist.

  Milestone empfiehlt, nur Postfächer des für die Verarbeitung Verantwortlichen / des Datenverarbeiters zu verwenden und die automatische Löschung der E-Mails nach Erreichen der festgelegten Speicherdauer zu konfigurieren.

  Die die Verarbeitung Verantwortlichen / Datenverarbeiter sollten darauf achten, dass diese Postfächer vom E-Mail-System nicht automatisch archiviert werden.

Überlegungen zur Beweissicherung

Mit der Beweissicherungsfunktion können Client-Anwender Videosequenzen, einschließlich Audio und sonstiger Daten, ggf. vor der Löschung schützen, z. B. bei einer Untersuchung oder einem Gerichtsverfahren, die/das noch nicht abgeschlossen ist.

Sofern geschützt, können Daten nicht gelöscht werden, weder automatisch vom System nach der standardmäßigen Speicherzeit oder in anderen Situationen, noch manuell vom Client-Benutzer. Das System oder ein Benutzer kann die Daten erst löschen, wenn ein Benutzer mit ausreichenden Benutzerrechten die Beweismittel freigibt.

Sie müssen die Aufzeichnungen nur so lange unter Verschluss halten, wie es einen triftigen Grund dafür gibt, z. B. eine laufende Untersuchung. Die Aufbewahrung von Aufzeichnungen auf unbestimmte Zeit ist nicht mit der DSGVO vereinbar.

Verletzung des Datenschutzes bei personenbezogenen Daten

Die DSGVO definiert eine "Verletzung des Schutzes personenbezogener Daten" als "eine Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Weitergabe von - oder zum Zugriff auf - personenbezogene Daten führt, die übermittelt, gespeichert oder anderweitig verarbeitet werden."

Im Fall einer Verletzung der Sicherheit muss der DSB entscheiden, ob er die Datenschutzbehörde und die betroffenen Personen gemäß Paragraph 33 und 34 DSGVO benachrichtigt.

Nach Paragraph 33 (1) DSGVO:

> *Im Fall einer Verletzung des Schutzes personenbezogener Daten meldet der für die Verarbeitung Verantwortliche die Verletzung des Schutzes personenbezogener Daten unverzüglich, und möglichst innerhalb von 72 Stunden, nachdem er davon Kenntnis erlangt hat, der gemäß Paragraph 55 zuständigen Aufsichtsbehörde, es sei denn, es ist unwahrscheinlich, dass die Verletzung des Schutzes personenbezogener Daten zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht innerhalb von 72 Stunden, so sind Gründe für die Verzögerung beizufügen.*

Wenn es als notwendig erachtet wird, muss der für die Datenverarbeitung Verantwortliche die Benachrichtigung über die Datenverletzung innerhalb von 72 Stunden nach Bekanntwerden der Verletzung veröffentlichen (siehe Verletzung des Datenschutzes bei personenbezogenen Daten auf Seite 25). Eine Mustervorlage für eine Benachrichtigung über eine Datenschutzverletzung finden Sie unter *Milestone Vorlage für eine Benachrichtigung über eine Datenschutzverletzung*. Auch die betroffenen Personen sind zu benachrichtigen, wenn die Verletzung personenbezogener Daten "wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten von Personen führt."

Datenverarbeiter, die von einer Verletzung des Schutzes personenbezogener Daten betroffen sind, müssen den für die Verarbeitung Verantwortlichen benachrichtigen, haben jedoch nach der DSGVO ansonsten keine weiteren Benachrichtigungs- oder Meldepflichten.

Weitere Informationen zu den Aufgaben des DSB finden Sie unter Die für die Verarbeitung verantwortliche Person auf Seite 16.

Datenverarbeiter

Wenn eine Organisation Dritte (für die Verarbeitung Verantwortliche) mit ihren Videoüberwachungsaktivitäten (oder Teilen davon) beauftragt, bleibt sie als für die Verarbeitung Verantwortlicher für die Einhaltung der DSGVO verantwortlich. Z. B. Sicherheitspersonal, das Live-Überwachungsvideos im Empfangsbereich einer Organisation überwacht und das für ein privates Unternehmen arbeitet, das von der Organisation mit der Live-Überwachung beauftragt wurde. In diesem Fall muss die Organisation gewährleisten, dass das Sicherheitspersonal seine Tätigkeit gem. der DSGVO ausübt.

Um die DSGVO zu erfüllen, müssen Datenverarbeiter als Dritte (mit Ausnahme der Strafverfolgungsbehörden):

- Die gleichen Anforderungen erfüllen wie der Betreiber (siehe VMS-Bediener auf Seite 22)
- Eine *Vereinbarung mit dem Datenverarbeiter* unterzeichnen und erfüllen (siehe Anhang: Vereinbarung mit dem Datenverarbeiter auf Seite 59).

Zusammenfassung

Die DSGVO ist eine Verordnung, die bereits Einfluss darauf hat, wie Organisationen mit Daten umgehen, u.a. auch mit Videodaten.

Jede Organisation, die personenbezogene Daten verarbeitet, muss mindestens eine oder mehrere Personen benennen, die dafür verantwortlich sind, dass die Organisation personenbezogene Daten der DSGVO und ihren eigenen Unternehmensrichtlinien gemäß behandelt (die Anzahl der dafür vorgesehenen Arbeitsstunden hängt von der Größe der Organisation und der Menge der gesammelten und verarbeiteten personenbezogenen Daten ab). Darüber hinaus fordert die DSGVO von manchen Organisationen die Ernennung eines formalen Datenschutzbeauftragten (DSB), der diese Aufgaben wahrnimmt.

Auch in der Verwaltung wird es Veränderungen geben. Nach der DSGVO müssen Organisationen detaillierte und genaue *Aufzeichnungen zur Datenverarbeitung* führen. Eine Musteraufzeichnung von Verarbeitungstätigkeiten finden Sie in der Aufzeichnung von Verarbeitungstätigkeiten (Muster). Es gibt eine Reihe von Einzelheiten, die aufgezeichnet werden müssen, u.a.:

- Auf was für Personengruppen sich die verarbeiteten personenbezogenen Daten beziehen (z.B. Kunden, Mitarbeiter, Ladenbesucher usw.)
- Wofür die personenbezogenen Daten verwendet werden
- Ob die personenbezogenen Daten an andere Unternehmen und/oder außerhalb der EU weitergegeben werden sollen
- Wie lange die personenbezogenen Daten gespeichert werden
- Maßnahmen, die die Organisation hinsichtlich jeder einzelnen Datenverarbeitungstätigkeit ergreift, um die Einhaltung der DSGVO zu gewährleisten

Alle diese Punkte sind relevant, wo gespeicherte Überwachungsvideos betroffen sind, und wird in der *Richtlinie für die Videoüberwachung* festgelegt (siehe Anhang: Richtlinie für die Videoüberwachung auf Seite 54).

Organisationen sind verpflichtet zu erklären, warum eine Videokamera an einem bestimmten Ort angebracht wurde, was gefilmt wird und warum. Im Fall einer Videoüberwachung sollte eine geeignete Beschilderung in und um den videoüberwachten Bereich Informationen dazu geben.

Der für die Verarbeitung Verantwortliche ist ggf. dazu verpflichtet, eine Datenschutz-Folgenabschätzung vorzunehmen (siehe Anhang: Datenschutz-Folgenabschätzung auf Seite 56), wenn an einem öffentlichen Ort eine Kamera angebracht werden soll. Zu der Folgenabschätzung gehört u.a.:

- Eine systematische Beschreibung der vorgesehenen Verarbeitungsvorgänge und deren Zweck
- Eine Bewertung der Notwendigkeit und der Verhältnismäßigkeit der Verarbeitungsvorgänge im Hinblick auf den Zweck (Hierfür kann externe Hilfe erforderlich sein)
- Eine Bewertung der Risiken für die Rechte und Freiheiten einzelner

- Die geplanten Maßnahmen zum Umgang mit diesen Risiken, einschließlich der Maßnahmen zum Schutz und der Mechanismen zur Gewährleistung des Schutzes personenbezogener Daten und der Einhaltung der DSGVO (dabei sollten die Rechte und berechtigten Interessen von Einzelpersonen und sonstigen Betroffenen berücksichtigt werden)

Eine der wichtigsten Funktionen der DSGVO ist, dass die überwachten Personen in vollem Umfang darüber informiert werden müssen, welche Daten über sie gespeichert und wie sie verwendet werden. Der Hinweis auf das Auskunftsrecht klärt die betroffenen Personen darüber auf, welchem Zweck die Überwachung dient, wer die erfassten Daten speichert (der für die Verarbeitung Verantwortliche) und die Richtlinie für die Speicherung. Ein Muster für eine Ad-hoc-Meldung finden Sie unter *Milestone Ad-hoc-Meldung* Muster.

Organisationen, die Videos speichern, haben klare Verantwortlichkeiten, was die Speicherung personenbezogener Daten angeht und müssen robuste Maßnahmen ergreifen, um Unbefugten am Zugriff darauf zu hindern. D. h. es ist wichtig ist, schriftlich festzulegen, wer Zugriff auf die Kameras und Aufzeichnungen hat.

Organisationen sollten auch über ein Verfahren dafür verfügen, wenn jemand von seinem Recht auf Zugang zu personenbezogenen Daten Gebrauch macht oder deren Löschung verlangt. So können sie innerhalb des vorgeschriebenen einmonatigen Zeitfensters bleiben, innerhalb dessen sie laut DSGVO diesen Anfragen nachkommen müssen. Wenn eine solche Anfrage erfolgt, kann vom Antragsteller erwartet werden, dass er entsprechende Angaben macht, mit denen diese Daten gefunden werden können - z.B. einen ungefähren Zeitrahmen und den Ort, wo die Videoaufzeichnung entstanden ist. D. h. der Betreffende sollte zum Nachweis seiner Identität offizielle Ausweispapiere vorlegen, und die Organisation sollte Aufzeichnungen zu den Aufnahmen erstellen, die dieser Person gezeigt oder zur Verfügung gestellt werden. Außerdem sollten andere Personen im Video mit Hilfsmitteln von Drittanbietern unkenntlich gemacht werden.

Organisationen sollten mithilfe strenger Maßnahmen Unbefugte am Zugriff auf die von ihnen gespeicherten personenbezogenen Daten hindern. Die von jeder Organisation angewendete Taktik richtet sich individuell nach den Problemstellungen, mit denen sie sich konfrontiert sieht. In allen Fällen müssen die Unternehmen jedoch robuste Sicherheitskontrollen durchführen, sich über bewährte Verfahren für die Cybersicherheit auf dem Laufenden halten und darauf achten, dass sie mit vertrauenswürdigen Partnern zusammenarbeiten, die sichere Hardware und Software sowie einen gründlichen Kundendienst anbieten.

Umgang mit personenbezogenen Daten

Im Umgang mit personenbezogenen Daten gelten die folgenden Grundsätze:

- Bewertung: Wissen, welche persönlichen Informationen Sie in Ihren Dateien und auf Ihren Computern haben.
- Reduzierung: Behalten Sie nur, was Sie für Ihr Geschäft benötigen.
- Schutz: Schützen Sie die Informationen, die Sie speichern.
- Löschen: Entsorgen Sie auf korrekte Weise, was Sie nicht mehr benötigen.
- Reagieren: Melden Sie sofort alle tatsächlichen oder vermuteten Verletzungen der Sicherheit.

Weitere Informationen finden Sie unter

- Die Volltextversion der *Datenschutz-Grundverordnung* finden Sie hier
- Weitere Informationen zur DSGVO für den Anwender einer VMS finden Sie in der Milestone DSGVO-Datenschutzrichtlinie für VMS-Anwender und im Milestone E-Learning zur DSGVO für VMS-Anwender.
- Wenn Sie sich über neue Entwicklungen bei der DSGVO auf dem Laufenden halten und mehr darüber erfahren wollen, besuchen Sie die Website der Europäischen Kommission zum Datenschutz
- Einen Leitfaden zur DSGVO, der Organisationen bei der Einhaltung ihrer Vorschriften hilft, finden Sie im Leitfaden des Datenschutzbeauftragten zur britischen Datenschutz-Grundverordnung
- Eine Liste mit den wichtigsten Fakten zur DSGVO finden Sie unter *Wichtige Fakten zur Datenschutz-Grundverordnung*
- Empfehlungen für die europäischen Institutionen und Stellen zu Konzeption und Betrieb von Videoüberwachungssystemen finden Sie in den *Richtlinien für Europäische Datenschutzbeauftragte (EDPS)*
- Weitere Informationen dazu, wie Sie Ihre XProtect VMS-Installationen vor Cyber-Angriffen schützen, finden Sie im Schutzleitfaden.
- Weitere Informationen über die Interaktion zwischen den einzelnen Komponenten Milestone XProtect VMS finden Sie im Milestone Dokument zur Beschreibung der Systemarchitektur.

Milestone DSGVO-Vorlagen

- *Milestone Ad-hoc-Mitteilung* (Muster).
- Aufzeichnungen zu Verarbeitungsaktivitäten (Muster).
- *Milestone Videoüberwachungsrichtlinie* (Muster).

> Sie müssen die Vorschriften der DSGVO einhalten, wenn Sie Ihre *Videoüberwachungsrichtlinie* aufstellen und entwickeln. Beachten Sie, dass das Sammeln von Audio- und Metadaten nicht unter das Europäische Datenschutzsiegel (EuroPriSe) fällt.

- *MilestoneMustervereinbarung mit dem Datenverarbeiter*
- *Milestone Musteranfrage einer betroffenen Person*.

> Beachten Sie bitte, dass es sich hierbei nur um ein Beispiel handelt. Für die Anfragen betroffener Personen gibt es keine Vorschriften, was die Form betrifft.

- *Milestone Musterbenachrichtigung bei einem Verstoß gegen den Datenschutz*

Anhänge

Weitere Informationen finden Sie in den folgenden Abschnitten:

Anhang: Einhaltung der DSGVO

Dieser Abschnitt gibt einen Überblick über die für die Videoüberwachung relevanten Vorschriften der DSGVO. In den folgenden Abschnitten wird beschrieben, was die DSGVO ist und wie welche Auswirkungen sie für die Verwendung von Videoüberwachung hat:

- Haben Sie eine Rechtsgrundlage dafür, Daten zu erheben? auf Seite 30
- Individuelle Rechte auf Seite 36
- Eingebauter Datenschutz auf Seite 42
- Rechenschaft auf Seite 50
- Checkliste zur Sicherung von Integrität und Vertraulichkeit auf Seite 52

Haben Sie eine Rechtsgrundlage dafür, Daten zu erheben?

Die DSGVO verlangt, dass alle Organisationen eine gültige, rechtmäßige Grundlage zur Erhebung und Verarbeitung personenbezogener Daten haben.

Eine Videoüberwachung auf der Grundlage einer Einwilligung oder vitaler Interessen kann in Ausnahmefällen möglich sein, z. B. im Gesundheits- und Pflegebereich, wenn eine Person dauerhaft beobachtet werden muss.

Sie sind verpflichtet, die Verarbeitungstätigkeiten in Ihren *Aufzeichnungen zu den Verarbeitungstätigkeiten* zu dokumentieren (Paragraph 30 DSGVO). Eine Musteraufzeichnung von Verarbeitungstätigkeiten finden Sie in der Aufzeichnung von Verarbeitungstätigkeiten (Muster).

Prüfen Sie die Rechtmäßigkeit der Verarbeitung von Video- und Benutzerdaten gemäß den folgenden Regelungsebenen:

1. Datenschutzgrundverordnung (Paragraph 6 DSGVO)

   Insbesondere Paragraph 6 (1)(b) DSGVO:

   > *Die Verarbeitung ist für die Erfüllung eines **Vertrags** erforderlich, dessen Vertragspartei die der für die Verarbeitung Verantwortliche ist, oder für die Durchführung von Maßnahmen im Auftrag der betroffenen Person vor Abschluss eines Vertrags.*

   Und Paragraph 6 (1)(e)(f) DSGVO:

   > *Die Verarbeitung ist rechtmäßig, wenn und soweit die Verarbeitung zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich ist, sofern die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen, **insbesondere dann, wenn die betroffene Person ein Kind ist**.*

2. Richtlinie (EU) 2016/680 Strafverfolgung oder die auf dieser Richtlinie basierenden nationalen Gesetze

   Einhaltung der nationalen Gesetze auf der Grundlage der Richtlinie (EU) 2016/680 Strafverfolgung zur Schaffung einer Rechtsgrundlage zur Überprüfung der Rechtmäßigkeit der Verarbeitung.

3. Nationale Gesetze

   Einhaltung der nationalem Gesetze, z. B. § 4 Bundesdatenschutzgesetz (BDSG), wobei diese Bestimmung nicht für die Videoüberwachung durch Unternehmen gilt.

Vor Umsetzung der Videoüberwachung ist der potenzielle Nutzen sowie die Auswirkungen auf das Recht auf Privatsphäre und sonstige Grundrechte und berechtigte Interessen der Personen im überwachten Bereich zu bewerten.

Wenn Sie sich für den Einsatz von Videoüberwachung entscheiden, dokumentieren Sie den Zweck des Videosystems, welche Informationen gesammelt werden, wofür, von wem und wie lange sie verwendet werden, und legen Sie angemessene Nachweise vor, z. B. statistische Daten über die tatsächliche Anzahl der aufgetretenen Sicherheitsvorfälle sowie Nachweise für die Abschreckungswirkung der Kameras in der Vergangenheit, sowie für ihre Eignung dazu, solche Vorfälle zu verhindern, zu untersuchen oder zu verfolgen.

Der Umfang der Bewertung hängt von der Größe des geplanten Systems und den Auswirkungen auf die Privatsphäre und sonstige legitime Interessen oder Grundrechte der Betroffenen ab.

Verarbeitung aufgrund einer rechtlichen Verpflichtung oder einer öffentlichen Aufgabe

Wann gilt die Rechtsgrundlage für rechtliche Verpflichtungen aller Voraussicht nach? Kurz gesagt, wenn Sie die personenbezogenen Daten zu verarbeiten haben, um dem Gesetz Genüge zu tun. Paragraph 6 (3) DSGVO fordert, dass die rechtliche Verpflichtung in EU-Recht oder in den Gesetzen der Mitgliedstaaten verankert sein muss.

Das heißt nicht, dass es eine rechtliche Verpflichtung geben muss, die die konkrete Verarbeitungstätigkeit ausdrücklich vorschreibt. Der springende Punkt ist dabei, dass der Gesamtzweck der sein muss, einer rechtlichen Verpflichtung nachzukommen, die ausreichend klar entweder im Gewohnheitsrecht oder im Gesetz begründet ist. Zum Beispiel kann ein Gerichtsbeschluss Sie dazu verpflichten, personenbezogene Daten für einen bestimmten Zweck zu verarbeiten, und auch dies gilt als rechtliche Verpflichtung.

Öffentliche Einrichtungen nutzen die Videoüberwachung in der Regel zur Erfüllung einer öffentlichen Aufgabe. Beachten Sie bitte, dass die Interessenabwägung für Behörden keine Rechtsgrundlage bei der Erfüllung dieser Aufgaben ist.

Für öffentliche Einrichtungen ist die Videoüberwachung nur dann legitim, wenn sie zur Erfüllung der öffentlichen Aufgabe erforderlich ist. Wenn Sie eine öffentliche Aufgabe ausführen, müssen Sie eine Verhältnismäßigkeitsprüfung vornehmen (siehe Interessenabwägung/Verhältnismäßigkeitsprüfung auf Seite 32). Der für die Verarbeitung Verantwortliche muss die Grundsätze der Datenminimierung berücksichtigen (z.B. Verdeckung von Bildbereichen zum Schutz der Privatsphäre), Speicherbegrenzung (Speicherdauer) und Zweckbindung (Paragraph 5 (1) DSGVO).

Interessenabwägung/Verhältnismäßigkeitsprüfung

Private Organisationen betreiben ein VMS in der Regel, um die berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten zu verfolgen (Paragraph 6 (1)(f) DSGVO). Daher ist eine Interessenabwägung erforderlich, um die Rechtmäßigkeit der Verarbeitung zu prüfen. Der für die Verarbeitung Verantwortliche muss seine Interessen angeben und sie gegen die Interessen oder Grundrechte und -freiheiten der betroffenen Personen abwägen, die den Schutz personenbezogener Daten fordern.

Die Verarbeitung von Audit- und Alarmverlaufsdaten kann in der Regel auf dem berechtigten Interesse des für die Verarbeitung Verantwortlichen beruhen (Paragraph 6 (1)(f) DSGVO. Das Gleiche gilt für die Daten zur Benutzerverwaltung (Kontodaten, Authentifizierungsdaten, Autorisierungsdaten, Konfigurationsdaten), wenn der Benutzer Mitarbeiter eines Sicherheitsunternehmens ist.

Sie müssen zu den Betroffenen von Anfang an klar, offen und ehrlich darüber sein, wie Sie deren persönlichen Daten nutzen wollen. Gehen Sie bei Ihrer Beurteilung auf die folgenden Fragen ein:

- Was sind die Vorteile der Videoüberwachung? Überwiegen die Vorteile ggf. die nachteiligen Auswirkungen?
- Wurde der Zweck des Systems klar angegeben, und ist er eindeutig und legitim? Gibt es eine

rechtmäßigen Begründung für die Videoüberwachung?

- Wurde die Notwendigkeit für den Einsatz der Videoüberwachung eindeutig nachgewiesen? Ist dies ein wirksames Werkzeug für den beabsichtigten Zweck? Gibt es weniger einschneidende Alternativen?

Darüber hinaus darf der für die Verarbeitung Verantwortliche die personenbezogenen Daten nur dann für einen neuen Zweck nutzen, wenn dieser mit dem ursprünglichen Zweck vereinbar ist oder der für die Verarbeitung Verantwortliche die Einwilligung dazu einholt oder eine eindeutige Rechtsgrundlage hat.

Typische Interessen des für die Verarbeitung Verantwortlichen

Üblicherweise obliegt es dem für die Verarbeitung Verantwortlichen:

- Zu bestimmen, wer Zugang zu den Daten erhält und wer nicht
- Die rechtmäßigen Interessen für konkret angegebene Zwecke zu gewährleisten

Im Zusammenhang mit einer Beschäftigung sollte sich der für die Verarbeitung Verantwortliche darüber im klaren sein, dass die Verarbeitung personenbezogener Daten von Mitarbeitern - sowohl Videodaten als auch Benutzerdaten - in Verbindung mit einer Beschäftigung durch die Gesetze der Mitgliedsstaaten u. U. genauer geregelt sein kann (Paragraph 88 DSGVO), z.B. Abschnitt 26 BDSG (Deutschland).

Typische Interessen und Rechte der betroffenen Personen

Die betroffenen Personen haben das Recht:

- Nicht dauerhaft überwacht zu werden
- Nicht in intimen Situationen beobachtet zu werden
- Kurze Speicherzeiten
- Angemessene Sicherungen, wenn besondere Kategorien personenbezogener Daten (Paragraph 9 DSGVO) verarbeitet werden

Wie XProtect die Auswirkungen auf Interessen oder Grundrechte und Freiheiten der betroffenen Person reduziert

Milestone XProtect reduziert die Auswirkungen auf Interessen oder Grundrechte der betroffenen Person, indem:

- Schutz personenbezogener Daten durch:
    - Zugriffskontrolle auf Rollenbasis
        - Aus Datenschutzgründen verdeckte Bildbereiche können nur vom Vorgesetzten offengelegt werden
        - Zugriffsprotokollierung
    - Verschlüsselung der Aufzeichnungen
    - Verschlüsselung der gesamten Kommunikation zwischen XProtect VMS Servern und Clients
    - Automatisierte Speicherung von Videoaufzeichnungen (automatisierte Löschung)
    - Privatsphärenausblendung
    - Sicherer und überprüfbarer Export von Videoaufzeichnungen
- Cybersicherheit
    - Verstärkter Schutz des Systems. Weitere Informationen dazu, wie Sie Ihre XProtect VMS-Installationen vor Cyber-Angriffen schützen, finden Sie im Schutzleitfaden.
    - Meldung und Behebung bekannter Schwachstellen. Weitere Informationen finden Sie unter Meldung und Behebung bekannter Schwachstellen.
- Ausbildung und Bewusstmachung
    - Programm zur Zertifizierung der Ausbildung unserer Partner
    - Programm zur Zertifizierung der Produkte unserer Partner (siehe Milestone Technologiepartnerprogramm und Milestone Marketplace)
    - Milestone E-learning für VMS-Betreiber zur DSGVO

Übertragene und offengelegte Daten

In der DSGVO gibt es drei wichtige Regeln für die Weitergabe von Daten, die sich danach richten, ob die Aufnahmen weitergegeben werden:

- An einen Empfänger innerhalb der Organisation oder an einen in einer anderen Organisation

  In diesem Fall sieht die DSGVO vor, dass die Aufzeichnungen an andere innerhalb derselben Organisation oder in einer anderen Organisation übertragen werden können, wenn dies für die rechtmäßige Erfüllung von Aufgaben erforderlich ist, die in die Zuständigkeit des Empfängers fallen.

- An Dritte innerhalb der Europäischen Union

  In diesem Fall kann die Weitergabe an Dritte außerhalb der Organisation, jedoch innerhalb der Europäischen Union, erfolgen, wenn dies für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder durch eine öffentliche Behörde erfolgt, oder wenn der Empfänger in sonstiger Weise nachweist, dass die Weitergabe erforderlich ist und kein Grund zu der Annahme besteht, dass die berechtigten Interessen der Personen, deren Bilder weitergegeben werden, beeinträchtigt werden könnten.

- Oder außerhalb der Europäischen Union

  In diesem Fall kann die Weitergabe an Dritte außerhalb der Europäischen Union erfolgen: (i) wenn dies nur geschieht, damit die Organisation ihre Aufgaben erfüllen kann und (ii) nur unter Beachtung weiterer Anforderungen, vo allem um sicherzustellen, dass die Daten im Ausland angemessen geschützt sind.

Zusammengefasst

Achten Sie darauf, dass Sie mit den Daten nichts tun, was gegen Gesetze verstößt.

Sie müssen personenbezogene Daten fair verwenden. Das heißt Sie dürfen die Daten in keiner Weise verarbeiten, die für die betroffenen Personen nachteilig, unerwartet oder irreführend ist.

Sie dürfen die personenbezogenen Daten nur dann für einen neuen Zweck nutzen, wenn dieser mit dem ursprünglichen Zweck vereinbar ist oder wenn Sie die Einwilligung dafür erhalten oder eine eindeutige Rechtsgrundlage haben.

In manchen Fällen, bei denen ein hohes Risiko dafür gesehen wird, dass Eingriffe in die Privatsphäre erfolgen, müssen Sie eine formale Folgenabschätzung vornehmen (siehe Anhang: Datenschutz-Folgenabschätzung auf Seite 56).

Durchführung einer Folgenabschätzung

Bevor Sie Videoüberwachungssysteme installieren und implementieren, sollten Sie eine *Datenschutz-Folgenabschätzung* vornehmen.

Der Zweck der Datenschutz-Folgenabschätzung besteht darin, die Auswirkungen des geplanten Systems auf die Privatsphäre von Einzelpersonen sowie auf sonstige Grundrechte zu ermitteln und Möglichkeiten zur Minderung oder Vermeidung negativer Auswirkungen zu suchen.

Wie viel Aufwand sollte für die Folgenabschätzung betrieben werden? Das hängt von den Umständen ab. Ein Videoüberwachungssystem mit einem hohen Risiko der Verletzung der Privatsphäre rechtfertigt eine höhere Investition als ein Videoüberwachungssystem mit begrenzten Auswirkungen auf die Privatsphäre, z. B. ein herkömmliches statisches CCTV-System.

Nach Paragraph 35 (7) DSGVO muss die Bewertung mindestens enthalten:

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich des vom für die Verarbeitung Verantwortlichen verfolgten berechtigten Interesses
- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge im Hinblick auf deren Zweck
- Eine Bewertung der Risiken für die Rechte und Freiheiten der in Paragraph 35 (1) DSGVO genannten betroffenen Personen:

  Kann eine Verarbeitungsweise, insbesondere mit neuen Technologien und unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, so nimmt der Verantwortliche vor der Verarbeitung eine Abschätzung der Folgen der geplanten Verarbeitungsvorgänge für den Schutz personenbezogener Daten vor. Eine Einzelbewertung kann eine Reihe ähnlicher Verarbeitungsvorgänge betreffen, die ähnliche Risiken mit sich bringen.
- Die geplanten Maßnahmen zum Umgang mit den Risiken, einschließlich der Maßnahmen zum Schutz und zur Sicherheit und der Mechanismen, die den Schutz personenbezogener Daten gewährleisten und die Einhaltung der DSGVO unter Berücksichtigung der Rechte und berechtigten Interessen der betroffenen und sonstiger Personen nachweisen sollen

In jedem Fall müssen Sie bewerten und begründen, ob Sie auf Videoüberwachung zurückgreifen wollen, wo Sie Ihre Systeme aufstellen, auswählen und konfigurieren und wie Sie den Datenschutz umsetzen wollen. Weitere Informationen dazu, wie Sie Ihre XProtect VMS-Installationen schützen können, finden Sie im Schutzleitfaden und im Zertifikate-Leitfaden.

Individuelle Rechte

Einer der Hauptzwecke der DSGVO ist es, Einzelpersonen mehr Schutz und eine Reihe von Rechten hinsichtlich ihrer persönlichen Daten zu geben.

Die Verordnung sieht einige sehr konkrete Anforderungen vor, die alle bedeuten, dass die Partei, die persönliche Daten verarbeitet oder speichert, eine Verantwortung hat, diese Daten zu schützen.

Die DSGVO gibt Einzelpersonen das Recht auf Information darüber, wann ihre personenbezogenen Daten erfasst werden (im Erfassungspunkt) und wie sie verwendet werden. Bei einer Videoüberwachung bedeutet dies z.B. eine angemessene Kennzeichnung in und um den Bereich, in dem die Videoüberwachung eingesetzt wird.

Paragraph 12 bis 23 DSGVO behandeln die Rechte der betroffenen Personen.

- Abschnitt 1: Transparenz und Modalitäten
  - Paragraph 12: Transparente Informationen, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

- Abschnitt 2: Informationen und Zugriff auf personenbezogene Daten
    - Paragraph 13: Informationen, die zur Verfügung gestellt werden müssen, wenn personenbezogene Daten der betroffenen Person erhoben werden
    - Paragraph 14: Informationen, die zur Verfügung gestellt werden müssen, wenn personenbezogene Daten der betroffenen Person erhoben wurden
    - Paragraph 15: Das Recht der betroffenen Person, Zugang zu ihren Daten zu erhalten (siehe Das Zugriffsrecht auf Seite 38)
- Abschnitt 3: Berichtigung und Löschung
    - Paragraph 16: Berichtigungsrecht
    - Paragraph 17: Das Recht, vergessen zu werden (Recht auf Löschung) (siehe Das Recht, vergessen zu werden (Recht auf Löschung) auf Seite 40)
    - Paragraph 18: Das Recht, die Verarbeitung zu beschränken (siehe Das Recht auf die Beschränkung der Verarbeitung auf Seite 42)
    - Paragraph 19: Benachrichtigungspflicht bei Berichtigung oder Löschung personenbezogener Daten oder bei Einschränkung der Verarbeitung
    - Paragraph 20: Recht auf Datenübertragbarkeit
- Abschnitt 4: Widerspruchsrecht und automatisierte individuelle Entscheidung
    - Paragraph 21: Widerspruchsrecht
    - Paragraph 22: Automatisierte individuelle Entscheidung, einschließlich Profilerstellung
- Abschnitt 5: Einschränkungen
    - Paragraph 23: Einschränkungen

Diejenigen davon, die im Hinblick auf die Videoüberwachung am wichtigsten sind, sind folgende:

Das Informationsrecht (Paragraph 12 bis 14 und 34 DSGVO)	Paragraph 12 behandelt die Transparenz und die Modalitäten, während sich Paragraph 13 und 14 mit der Information und dem Zugang zu personenbezogenen Daten befassen. Anhand dieser Paragraphen kann sich die betroffene Person darüber informieren, welche personenbezogenen Daten gesammelt und wie lange sie gespeichert werden. Im Zusammenhang mit einem VMS, siehe Anhang: Ad-hoc-Mitteilung auf Seite 53. Aufgrund von Paragraph 34 hat die betroffene Person das Recht, im Fall einer Datenschutzverletzung informiert zu werden, wenn diese mit hoher Wahrscheinlichkeit ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person mit sich bringt.

Das Zugriffsrecht (Paragraph 15 DSGVO)	Dieser Paragraph der DSGVO gibt der betroffenen Person das Recht, Zugang zu den über sie verarbeiteten personenbezogenen Daten zu erhalten, z. B. Videoaufzeichnungen der betroffenen Person. Die betroffene Person hat das Recht, von dem jeweiligen Unternehmen Auskunft darüber zu verlangen, welche ihrer personenbezogenen Daten verarbeitet werden und aus welchem Grund.
Das Löschungsrecht ("Recht, vergessen zu werden") (Paragraph 17 DSGVO)	Dieses Recht gibt der betroffenen Person die Möglichkeit, die Löschung ihrer Daten zu verlangen. Im Zusammenhang mit einem VMS ist die Löschung auf Wunsch der betroffenen Personen aufgrund der Interessen des für die Verarbeitung Verantwortlichen und der kurzen Aufbewahrungszeiten eine Ausnahme. (Siehe Anhang: Richtlinie für die Videoüberwachung auf Seite 54 und *Teilweise Löschung von Videoaufzeichnungen* in Anhang: Das Milestone XProtect VMS-System und die DSGVO auf Seite 60).
Das Widerspruchsrecht (Paragraph 21 DSGVO)	Dieses Recht gibt der betroffenen Person die Möglichkeit, der Verarbeitung ihrer personenbezogenen Daten zu widersprechen. Im Zusammenhang mit einem VMS können andere Interessen die Interessen und Rechte der betroffenen Person überwiegen, z. B. berechtigte Interessen (Betrugsaufdeckung, Gesundheit und Sicherheit), gesetzliche Verpflichtungen (Buchhaltung, Bekämpfung der Geldwäsche) und sogar Vertragserfüllung (z.B. Arbeitsverträge). In allen Fällen muss dies vollkommen transparent sein, damit die betroffene Person informiert ist und Widerspruch einlegen kann. Wenn die betroffene Person Widerspruch einlegt, muss der für die Verarbeitung Verantwortliche den Widerspruch prüfen, andernfalls droht ihm ein Bußgeld.

Für die Einhaltung der DSGVO durch VMS-Systeme sind drei Rechte besonders wichtig: das Informationsrecht, das Zugriffsrecht und das Recht auf Löschung.

Das Zugriffsrecht

Laut Paragraph 15 gibt die DSGVO Einzelpersonen die Kontrolle über Ihre personenbezogenen Daten, einschließlich des Rechts auf Einsichtnahme in diese Daten. Besonders wichtig ist das Recht, dass die betroffenen Personen eine Kopie ihrer Daten erhalten können und dass unbeteiligte Dritte unkenntlich gemacht werden (und zwar mit Hilfsmitteln von Drittanbietern).

Auf Anfrage muss die betreffende Organisation einer betroffenen Person alle über sie gesammelten personenbezogenen Daten zur Verfügung stellen, einschließlich der von Videoüberwachungssystemen aufgezeichneten Videos.

Achten Sie darauf, dass Sie formale Verfahren und Richtlinien für den Umgang mit Anfragen zum Auskunftsrecht einrichten, wie unter *Register der übertragenen und offengelegten Daten* beschrieben.

Übertragene und offengelegte Daten

In der DSGVO gibt es drei wichtige Regeln für die Weitergabe von Daten, die sich danach richten, ob die Aufnahmen weitergegeben werden:

- An einen Empfänger innerhalb der Organisation oder an einen in einer anderen Organisation

  In diesem Fall sieht die DSGVO vor, dass die Aufzeichnungen an andere innerhalb derselben Organisation oder in einer anderen Organisation übertragen werden können, wenn dies für die rechtmäßige Erfüllung von Aufgaben erforderlich ist, die in die Zuständigkeit des Empfängers fallen.

- An Dritte innerhalb der Europäischen Union

  In diesem Fall kann die Weitergabe an Dritte außerhalb der Organisation, jedoch innerhalb der Europäischen Union, erfolgen, wenn dies für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder durch eine öffentliche Behörde erfolgt, oder wenn der Empfänger in sonstiger Weise nachweist, dass die Weitergabe erforderlich ist und kein Grund zu der Annahme besteht, dass die berechtigten Interessen der Personen, deren Bilder weitergegeben werden, beeinträchtigt werden könnten.

- Oder außerhalb der Europäischen Union

  In diesem Fall kann die Weitergabe an Dritte außerhalb der Europäischen Union erfolgen: (i) wenn dies nur geschieht, damit die Organisation ihre Aufgaben erfüllen kann und (ii) nur unter Beachtung weiterer Anforderungen, vo allem um sicherzustellen, dass die Daten im Ausland angemessen geschützt sind.

Register der übertragenen und offengelegten Daten

Die betreffende Organisation sollte ein Register der übertragenen und offengelegten Daten führen - möglichst in elektronischer Form. Darin sollten alle an Dritte übertragende Daten aufgezeichnet werden. (solche Dritte sind u.a. alle Personen innerhalb der Organisation, an die durch diejenigen Daten übertragen werden, die zunächst Zugang zu den Aufzeichnungen haben. Hierzu gehört typischerweise jede Übertragung außerhalb der Sicherheitseinheit). Das Register sollte außerdem alle Fälle enthalten, in denen Dritten die Aufzeichnungen gezeigt wurden oder der Inhalt der Aufzeichnungen in sonstiger Weise an Dritte weitergegeben wurde, auch wenn keine Kopie der Aufzeichnung durch die Videoüberwachung nicht übertragen wurde.

Das Register sollte mindestens Folgendes enthalten:

- Das Datum der Aufzeichnungen
- Die anfordernde Partei (Name, Titel und Organisation)
- Name und Titel der Person, die Übertragung autorisiert hat
- Eine Kurzbeschreibung des Inhalts der Aufzeichnung
- Eine Begründung für die Anfrage und der Grund für ihre Genehmigung
- Ob eine Kopie der Aufzeichnung übertragen wurde, die Aufzeichnung gezeigt oder mündliche Informationen gegeben wurden

Das Recht, vergessen zu werden (Recht auf Löschung)

Laut Paragraph 17 gibt die DSGVO Einzelpersonen die Kontrolle über ihre personenbezogenen Daten, einschließlich des Rechts auf Löschung dieser Daten, wenn Sie für den beabsichtigten Zweck des Systems nicht mehr benötigt werden.

Laut Paragraph 17 (1)(c) DSGVO muss der für die Verarbeitung Verantwortliche Widersprüche der betroffenen Personen behandeln. Da es praktisch nicht möglich ist, eine bestimmte Person aus einem Video zu löschen, sollten die Datenverarbeiter die Aufbewahrungsdauer des Videos entsprechend dem dokumentierten Zweck des Systems streng begrenzen.

Was sollten Sie tun?

Überprüfen Sie die Aufbewahrungsdauer für alle Kameras und achten Sie darauf, dass sie entsprechend dem dokumentierten Zweck des Systems eingestellt ist.

Das Recht, vergessen zu werden, gilt häufig nicht für die Videoüberwachung, da die Aufbewahrungsdauer in der Regel kurz ist und andere Rechtsgrundlagen die "zumutbaren" technischen und rechtlichen Interessen überwiegen, z. B. gesetzliche Verpflichtungen (Arbeitsgesetz), öffentliches Interesse (Verbrechensverhütung, öffentliche Gesundheit und Sicherheit), vitale Interessen (lebens- und gesundheitsrelevante Daten, gefährliche Umgebungen), berechtigte Interessen (Betrugserkennung, Beschäftigung, Produktentwicklung) oder sogar Vertragserfüllung (Beschäftigung, Abonnements und Lizenzierung). Ein Beispiel für ein berechtigtes Interesse ist, dass die Aufzeichnungen aus der Videoüberwachung zum betreffenden Zeitpunkt eine vertrauenswürdige Beweisquelle sein müssen. Daher schützt das VMS in erster Linie Videobeweise vor der Manipulation und gewährleistet ihre Authentizität, so dass das Recht, vergessen zu werden, nachrangig ist.

Es gibt in der Regel zwei Gründe für die betroffenen Personen, der Speicherung von Videoaufzeichnungen zu widersprechen:

- Die Interessen des für die Verarbeitung Verantwortlichen an der Speicherung der Daten sind hinter den Interessen oder Grundrechte und Freiheiten der betroffenen Person, die den Schutz der personenbezogenen Daten erfordern, nachrangig (Paragraph 17 (1)(c) DSGVO)
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet, z. B. die ein Kindergarten oder eine Umkleidekabine wurde überwacht (Paragraph 17 (1)(d) DSGVO)

Daher muss jede Anfrage gründlich geprüft werden.

Wie lange sollten die Aufzeichnungen aufbewahrt werden?

Generell gilt der Grundsatz, dass Aufzeichnungen nicht länger aufbewahrt werden dürfen, als es für die konkreten Zwecke erforderlich ist, für die sie gemacht wurden. Es muss auch überlegt werden, ob die Aufzeichnung überhaupt notwendig ist und ob eine Live-Überwachung ohne Aufzeichnung ausreichen würde.

Wenn sich eine Organisation für die Aufzeichnung entscheidet, muss sie den Zeitraum angeben, für den die Aufzeichnungen aufbewahrt werden sollen. Nach Ablauf dieser Frist müssen die Aufzeichnungen gelöscht werden. Milestone XProtect VMS automatisiert den Löschvorgang, indem Aufzeichnungen automatisch gelöscht werden, die älter sind als die eingestellte Aufbewahrungsdauer.

Wenn Dateien, die die aufgezeichneten Videodaten enthalten, vom VMS gelöscht werden, werden die Dateien und ihr Inhalt tatsächlich nicht von den Datenblöcken auf dem Speichersystem gelöscht, sondern lediglich im Dateisystem als frei markiert, so dass andere Dateien an diese Stelle des Speichersystems geschrieben werden können. Bis die Datenblöcke tatsächlich mit neuen Daten überschrieben werden, können die alten Videodaten, die gelöscht wurden, ggf. wiederhergestellt werden, was den Zugriff auf Aufnahmen ermöglicht, die älter sind als die eingestellte Aufbewahrungsdauer.

Daher wird empfohlen, das Speichersystem nicht zu groß zu machen, da das Risiko mit der Größe des ungenutzten Speicherplatzes steigt.

Ist das zugewiesene Speichersystem z. B. doppelt so groß wie die Menge der für die eingestellte Aufbewahrungsdauer gespeicherten Videodaten - z. B. sieben Tage - können die gelöschten Datenblöcke, die gelöschte Altvideodaten enthalten, statistisch gesehen noch weitere sieben Tage auf dem Speichersystem herumliegen, bevor sie überschrieben werden.

Um das Risiko des Zugriffs auf gelöschte Altvideodaten weiter zu senken sowie aus allgemeinen Sicherheitsüberlegungen heraus wird empfohlen, die Verschlüsselung der Mediendatenbanken zu aktivieren, da dies neben der Wiederherstellung der gelöschten Dateien dann außerdem erfordert, dass die Verschlüsselung überwunden wird.

Unabhängig davon, ob die Videodaten verschlüsselt sind oder nicht, ist es wichtig, dass Sie die zum Speichern von Mediendatenbanken verwendeten Festplatten desinfizieren oder physisch zerstören, bevor sie entsorgt werden (z. B. durch Schreddern oder in ähnlicher Weise), sobald sie im Speichersystem nicht mehr verwendbar sind.

Informationen darüber, wie Sie dies in Milestone XProtect einrichten können, finden Sie im Abschnitt Speicherung und Archivierung (Erklärung) im Administratorhandbuch für das XProtect VMS.

Wenn die Videoüberwachung Sicherheitzwecken dient und ein Sicherheitsvorfall eintritt und festgestellt wird, dass die Aufzeichnungen zur weiteren Untersuchung des Vorfalls oder zur Verwendung als Beweismittel erforderlich sind, kann die betreffende Aufzeichnung über die üblichen Aufbewahrungsfristen hinaus so lange aufbewahrt werden, wie sie für diese Zwecke benötigt wird. Danach müssen jedoch auch sie gelöscht werden.

Aufbewahrungsfrist für typische Sicherheitszwecke: eine Woche bis ein Monat

Wenn aus Sicherheitsgründen Kameras installiert werden, sollte eine Woche bis zu einem Monat ausreichen, damit das Sicherheitspersonal eine begründete Entscheidung treffen kann, ob die betreffende Aufzeichnung für einen längeren Zeitraum aufbewahrt werden soll, um den Sicherheitsvorfall weiter zu untersuchen oder um sie als Beweismittel zu verwenden.

Ein Beispiel für örtlich geltende Gesetze: Laut einigen deutschen Datenschutzbehörden, sowie einem Großteil der Literatur zum Thema Datenschutz, beträgt diese Aufbewahrungsfrist als Richtwert für die Zugriffskontrolle und die Untersuchung von Straftaten 48 bis 72 Stunden.

Auf dem Gebiet der Mitgliedstaaten oder von Drittländern: 48 Stunden

Falls sich die Überwachung auf Bereiche außerhalb der Gebäude auf dem Gebiet eines Mitgliedstaates (oder eines Drittlandes) erstreckt (typischerweise Bereiche in der Nähe von Ein- und Ausfahrten) und es

unvermeidbar ist, dass Passanten oder vorbeifahrende Fahrzeuge von den Kameras erfasst werden, wird empfohlen, die Aufbewahrungsdauer auf 48 Stunden zu reduzieren oder den örtlichen Belangen möglichst in sonstiger Weise Rechnung zu tragen.

Das Recht auf die Beschränkung der Verarbeitung

Die betroffene Person kann nach Paragraph 18 (1) DSGVO das Recht beanspruchen, die Verarbeitung zu beschränken. In einem VMS-Basisszenario kann die betroffene Person geltend machen, dass die Verarbeitung durch das VMS rechtswidrig ist, z. B. wenn die betroffene Person nicht weiß, dass die Videoüberwachung im öffentlichen Raum so durchgeführt wird, dass Bildbereiche aus Datenschutzgründen verdeckt werden. Es wird empfohlen, dies unter Verwendung einer Vorlage für eine *Anfrage der betroffenen Person* geltend zu machen (siehe Anfrage einer betroffenen Person auf Seite 13). Einen Musterantrag einer betroffenen Person finden Sie unter *Milestone Musterantrag einer betroffenen Person*.

Der Anspruch ist innerhalb eines angemessenen Zeit zu bearbeiten, insbesondere vor Ablauf der Aufbewahrungsfrist, um eine automatische Aufbewahrung oder Löschung der beanspruchten Beweise aus dem VMS zu vermeiden. Es ist allgemein ratsam, sich hinsichtlich der Einschränkung der Verarbeitung rechtlich beraten zu lassen. Eine Art des Umgangs mit einer solchen Anfrage ist, dass der Administrator des VMS die Zugriffsrechte der Bediener des VMS oder ihrer Vorgesetzten durch Zuweisung entsprechender Rollen so einschränkt, dass sie Aufnahmen nur innerhalb einer kurzen Zeitdauer nach ihrer Aufzeichnung abspielen können - z.B. für vier Stunden oder einen Tag (siehe Was sollten Sie tun? auf Seite 43: "Ziehen Sie die Einschränkung des Zugriffs auf Videoaufzeichnungen für die Bediener in Betracht, entweder vollständig, nur auf in den letzten Stunden aufgezeichneten Videos oder nur mit zweifacher Genehmigung"). Einschränkungen der Wiedergabe gelten auch für Beweissicherungen. Wenn weitere Einschränkungen der Verarbeitung erforderlich sind, wird empfohlen, sowohl eine Geschäftsfolgenabschätzung als auch eine Datenschutzfolgenabschätzung (siehe Durchführung einer Folgenabschätzung auf Seite 35) als Teil der Bearbeitung des Anspruchs durchzuführen.

Eingebauter Datenschutz

Die DSGVO verlangt, dass der Datenschutz von der Konzeption des Systems bis zu dessen Inbetriebnahme Priorität hat. Der im Hinblick auf den Datenschutz verfolgte Ansatz muss proaktiv sein, nicht reaktiv. Risiken sind vorwegzunehmen, und das Ziel muss sein, Zwischenfälle zu vermeiden, bevor sie eintreten.

Organisationen müssen sorgfältig prüfen und dokumentieren, wie ihre Systeme konzipiert sind, um die angegebenen Ziele zu erreichen.

Es ist darauf zu achten, dass keine personenbezogenen Daten von Personen zu erfassen, die außerhalb des Geltungsbereichs des Systems liegen (z. B. angrenzende öffentliche Bereiche).

Es ist sorgfältig zu überlegen, wer welche Informationen sehen muss (z. B. live/aufgezeichnet, Zeitrahmen, Auflösung) und wer auf welche Funktionen Zugriff hat (z. B. Suche).

Was sollten Sie tun?

- Die Auflösung verschiedener Punkte im Kamerabild dokumentieren
- Die beabsichtigte Speicherdauer dokumentieren
- Erwägen Sie die Verwendung verdeckter Bildbereiche aus Datenschutzgründen - permanent oder so, dass sie entfernt werden können
- Erwägen Sie, Berechtigungen zum Betrachten von Live-Videos, Aufzeichnungen einzurichten
- Erwägen Sie, den Zugriff zum Exportieren von Aufzeichnungen und zum Freilegen von aus Datenschutzgründen verdeckten Bildbereichen zu beschränken
- Überprüfen Sie regelmäßig die Rollen und Verantwortlichkeiten der Bediener, Ermittler, Systemadministratoren und sonstiger Personen, die Zugriff auf das System haben
- Erwägen Sie, den Zugriff auf Gruppen zu beschränken, die mit Ermittlungen befasst sind, für Kameras, die eigens zur Identitätserfassung positioniert sind (z. B. Gesichter von Personen, die ein Geschäft betreten)
- Ziehen Sie die Einschränkung des Zugriffs auf Videoaufzeichnungen für die Bediener in Betracht, entweder vollständig, nur auf in den letzten Stunden aufgezeichneten Videos oder nur mit zweifacher Genehmigung
- Begrenzen Sie die Anzahl der Benutzer mit Administratorrollen

Anforderungen für den eingebauten Datenschutz

Beschränkung der Daten auf ein Mindestmaß	Sie müssen sicherstellen, dass die von Ihnen verarbeiteten personenbezogenen Daten: • angemessen sind – ausreichend für den angegebenen Zweck • relevant sind – zu diesem Zweck in einem vernünftigen Verhältnis stehen • auf das notwendige Maß beschränkt sind – Sie also nicht mehr speichern, als Sie für diesen Zweck benötigen.
Korrektheit	Für personenbezogene Daten gilt allgemein: • Sie sollten alles Zumutbare tun, damit die von Ihnen gespeicherten personenbezogenen Daten nicht falsch oder in Bezug auf einen bestimmten Sachverhalt irreführend sind.

	• Sie müssen die persönlichen Daten ggf. auf dem aktuellen Stand halten, obwohl dies davon abhängt, wofür Sie diese verwenden. • Wenn Sie feststellen, dass personenbezogene Daten falsch oder irreführend sind, müssen Sie das Zumutbare tun, um diese Daten schnellstmöglich zu berichtigen, oder sie löschen. • Sie müssen alle Zweifel an der Richtigkeit der personenbezogenen Daten sorgfältig prüfen.
Begrenzung der Speicherdauer	• Sie dürfen personenbezogene Daten nicht länger aufbewahren, als Sie sie benötigen. • Sie müssen darüber nachdenken - und auch begründen können - wie lange Sie die personenbezogenen Daten aufbewahren. Dies hängt von den Zwecken ab, für die Sie die Daten speichern. • Sie benötigen eine Richtlinie, die möglichst Standardfristen für die Aufbewahrung festlegt, um die dokumentierten Anforderungen zu erfüllen. • Sie sollten die von Ihnen gespeicherten Daten auch regelmäßig überprüfen und sie löschen oder anonymisieren, wenn Sie sie nicht mehr benötigen. • Sie müssen alle Zweifel an Ihrer Datenspeicherung sorgfältig prüfen. Einzelpersonen haben ein Recht auf die Löschung ihrer Daten, wenn Sie diese nicht mehr benötigen. • Sie können personenbezogene Daten länger aufbewahren, wenn Sie sie lediglich für Zwecke archivieren, die im öffentlichen Interesse liegen, für wissenschaftliche oder historische Recherchen oder für statistische Zwecke.

Eingebauter Datenschutz und standardmäßiger Datenschutz

Nach der DSGVO muss der für die Verarbeitung Verantwortliche bei der Verarbeitung personenbezogener Daten technische oder organisatorische Maßnahmen ergreifen, die darauf ausgelegt sind, die in der DSGVO dargelegten Datenschutzgrundsätze umzusetzen. Die DSGVO bezeichnet dies als eingebauten Datenschutz.

Im Zusammenhang mit einer Kamera wäre ein Beispiel für "eingebauten Datenschutz" eine digitale Funktion, mit der der Benutzer die Bilderfassung auf einen bestimmten Umkreis beschränken kann, wodurch die Kamera daran gehindert wird, Bilder außerhalb dieses Umkreises zu erfassen, die ansonsten erfasst würden.

Im XProtect VMS gibt es Unterstützung zur Privatsphärenausblendung aus Datenschutzgründen in zwei Formen: dauerhaft verdeckte Bildbereiche, die nicht aufgedeckt werden können, und reversibel verdeckte Bildbereiche, die (mit den entsprechenden Berechtigungen) aufgedeckt werden können, um das verdeckte Bild freizulegen.

Der für die Verarbeitung Verantwortliche muss außerdem technische oder organisatorische Maßnahmen ergreifen, die standardmäßig die am wenigsten in die Privatsphäre eingreifende Verarbeitung der betreffenden personenbezogenen Daten gewährleisten. Die DSGVO nennt dies den standardmäßigen Datenschutz. Im Zusammenhang mit Kameras wäre ein Beispiel für den standardmäßigen Datenschutz die Abdeckung von Bildbereichen aus Datenschutzgründen, um sensible Bereiche im Sichtfeld der Kamera privat zu halten.

Was wäre ein Beispiel für eine XProtect Funktion, die den Ansatz des standardmäßigen Datenschutzes unterstützt?

Milestone entwickelt sein Produktportfolio kontinuierlich weiter, und der standardmäßige Datenschutz ist ein wichtiges Bewertungskriterium dafür, dass XProtect die DSGVO erfüllt. Weitere Informationen finden Sie im Leitfaden zum sicheren Entwicklungslebenszyklus unter Milestone. Dieser Leitfaden ist integraler Bestandteil des standardmäßigen Datenschutzes, und wendet Prinzipien an wie "Defense-in-Depth", "Least Privileges" sowie die Vermeidung weniger sicherer Standardeinstellungen und die standardmäßige Abschaltung selten verwendeter Funktionen.

Was sollten Sie tun, um einen standardmäßigen Datenschutz zu gewährleisten?

- Denken Sie über die Auflösung verschiedener Punkte im Kamerabild nach und dokumentieren Sie diese

  Unterschiedliche Zwecke erfordern unterschiedliche Bildqualitäten. Wenn keine Identifizierung erforderlich ist, sollten die Kameraauflösung und andere einstellbare Faktoren so gewählt werden, dass keine Bilder aufgenommen werden, in denen Gesichter erkennbar sind.

- Verschlüsseln Sie Ihre Aufzeichnungen

  Milestone empfiehlt, dass Sie Ihre Aufzeichnungen sichern, indem Sie im Speicher und in den Archiven Ihres Aufzeichnungsservers die Verschlüsselung aktivieren. Milestone verwendet zur Verschlüsselung den Algorithmus AES-256. Bei der Auswahl der Schwachen Verschlüsselung wird nur ein Teil der Aufzeichnung verschlüsselt. Bei der Auswahl der Starken Verschlüsselung wird die gesamte Aufzeichnung verschlüsselt.

- Sichern des Netzwerkes

  Milestone empfiehlt, dass Sie Kameras auswählen, die HTTPS unterstützen. Es wird empfohlen, die Kameras auf separate VLANs einzustellen und für die Kommunikation zwischen Kamera und Aufzeichnungsserver sowie zwischen Clients und Aufzeichnungsserver HTTPS zu verwenden.

  Es wird empfohlen, die Verschlüsselung für die gesamte Kommunikation zwischen allen Servern und Clients zu aktivieren. Weitere Informationen dazu, wie Sie Ihre XProtect VMS-Installationen schützen können, finden Sie im Schutzleitfaden und im Zertifikate-Leitfaden.

  Es wird empfohlen, dass sich XProtect Smart Client und XProtect Smart Wall im selben VLAN befinden wie die Server.

  Verwenden Sie ein VPN-verschlüsseltes Netzwerk oder ähnliches, wenn Sie Smart Client oder Smart Wall von einem entfernten Standort aus verwenden.

- Aktivieren und dokumentieren Sie die beabsichtigte Speicherdauer

  Nach Paragraph 17 (1) (a) DSGVO dürfen Aufzeichnungen nicht länger aufbewahrt werden, als es für die konkreten Zwecke erforderlich ist, für die sie gemacht wurden. Milestone empfiehlt, die Verweilzeit entsprechend einzustellen. Somit wird dann die Löschung von Videoaufzeichnungen automatisiert.

- Sicherer Export

  Milestone empfiehlt, dass Sie den Zugriff auf die Exportfunktion nur einer ausgewählten Gruppe von Benutzern erlauben, die diese Berechtigung benötigen.

  Milestone empfiehlt außerdem, das Smart Client Profil so zu ändern, dass der Export nur im XProtect Format mit aktivierter Verschlüsselung möglich ist. Der Export als AVI und JPEG sollte nicht erlaubt sein, da diese Formate nicht sicher gemacht werden können. Dadurch wird der Export von Beweismaterial passwortgeschützt, verschlüsselt und digital signiert, so dass gewährleistet ist, dass das forensische Material echt ist, nicht manipuliert wurde und nur von einem befugten Empfänger betrachtet werden kann.

- Aktivieren Sie aus Datenschutzgründen verdeckte Bildbereiche - permanent oder so, dass sie wieder sichtbar gemacht werden können

  Verwenden Sie aus Datenschutzgründen verdeckte Bildbereiche, um die Überwachung von Bereichen auszuschließen, die für Ihr Überwachungsziel irrelevant sind.

- Zugriffsberechtigungen mit Rollen einschränken

  Wenden Sie das Prinzip des geringsten Privilegs (PoLP) an.

  Milestone empfiehlt, dass Sie den Zugriff auf die Exportfunktion nur einer ausgewählten Gruppe von Benutzern erlauben, die diese Berechtigung benötigen. Standardmäßig kann nur der Systemadministrator auf das System zugreifen und Aufgaben ausführen. Alle Rollen und Benutzer, die neu angelegt werden, haben keinen Zugriff auf Funktionen, bis sie von einem Administrator absichtlich konfiguriert werden.

  Richten Sie Berechtigungen für alle Funktionen ein, einschließlich des Abspielens von Live-Video und Aufzeichnungen, des Anhörens von Audio, des Zugriffs auf Metadaten, der Steuerung von PTZ-Kameras, des Zugriffs und der Konfiguration von Smart Wall, des Freilegen von Bildbereichen, die zum Schutz der Privatsphäre unkenntlich gemacht wurden, der Arbeit mit Exporten, des Speicherns von Schnappschüssen usw.

  Schränken Sie den Zugriff auf Video- und Audioaufzeichnungen und Metadaten für die Bediener entweder vollständig ein, oder beschränken Sie den Zugriff auf ausschließlich Video- und Audioaufzeichnungen oder Metadaten, die erst in den vorangegangenen Stunden aufgezeichnet wurden.

  Überprüfen Sie regelmäßig die Rollen und Zuständigkeiten der Bediener, Ermittler, Systemadministratoren und sonstiger Personen, die Zugriff auf das System haben. Gilt Prinzip des geringsten Privilegs weiterhin?

- Schränken Sie die Berechtigungen der Administratoren ein

  Milestone empfiehlt Ihnen, die Anzahl der Benutzer mit Administratorrolle zu begrenzen.

Einrichtung und Konfiguration des Videoüberwachungssystems

Das Leitprinzip bei allen in diesem Abschnitt behandelten Punkten sollte sein, negative Auswirkungen für die Privatsphäre und sonstige Grundrechte und legitime Interessen der überwachten Personen auf ein Mindestmaß zu begrenzen.

Standorte und Blickwinkel der Kameras

Die Standorte der Kameras sollten so gewählt werden, dass sichtbare Bereiche, die für die beabsichtigten Zwecke irrelevant sind, auf ein Mindestmaß begrenzt werden.

Wenn ein Videoüberwachungssystem zum Schutz der Vermögenswerte (Eigentum oder Informationen) der Organisation oder der Sicherheit der Mitarbeiter und Besucher installiert wird, sollte die Organisation die Überwachung in der Regel beschränken auf

- sorgfältig ausgewählte Bereiche, die sensible Informationen, wertvolles Eigentum oder sonstige Werte enthalten, für die aus bestimmten Gründen ein erhöhter Schutz erforderlich ist,
- Zu- und Ausgänge zu Gebäuden (einschließlich Notausgänge und Fluchtwege sowie Umgebungsmauern oder -zäune um das Gebäude oder Grundstück), und

- Ein- und Ausgänge innerhalb des Gebäudes, die verschiedene Bereiche verbinden, die unterschiedlichen Zugangsberechtigungen unterliegen und durch verschlossene Türen oder andere Zugangskontrollmechanismen getrennt sind.

Anzahl Kameras

Die Anzahl der zu installierenden Kameras hängt von der Größe der Gebäude und von den Sicherheitsanforderungen auf ab, die ihrerseits von einer Vielzahl von Faktoren abhängen. Dieselbe Anzahl und derselbe Kameratyp kann für die eine Organisation geeignet und für die andere vollkommen unverhältnismäßig sein. Bei ansonsten gleichen Voraussetzungen ist die Anzahl der Kameras jedoch ein guter Indikator für die Komplexität und Größe eines Überwachungssystems und kann ein Hinweis auf erhöhte Risiken für die Privatsphäre und sonstige Grundrechte sein. Mit zunehmender Anzahl Kameras steigt auch die Wahrscheinlichkeit, dass diese nicht effizient eingesetzt werden und Informationen im Übermaß gesammelt werden. Daher empfiehlt der Europäische Datenschutzbeauftragte (EDSB), die Anzahl der Kameras auf das unbedingt erforderliche Maß zu begrenzen, mit dem die Zwecke des Systems erreicht werden können. Die Anzahl Kameras muss in der *Videoüberwachungsrichtlinie*angegeben sein.

Überwachungszeiten

Die eingestellten Zeit, zu denen die Kameras aufzeichnen, sollten so gewählt werden, dass die Überwachung zu Zeiten auf ein Mindestmaß begrenzt wird, die für die beabsichtigten Zwecke irrelevant sind. Wenn die Videoüberwachung Sicherheitszwecken dient, sollte das System möglichst eingestellt werden, dass es nur zu Zeiten aufzeichnet, zu denen die Wahrscheinlichkeit höher ist, dass mögliche Sicherheitsprobleme auftreten.

Auflösung und Bildqualität

Es sollte eine angemessene Auflösung und Bildqualität gewählt werden. Unterschiedliche Zwecke erfordern unterschiedliche Bildqualitäten. Ist es z.B. entscheidend, dass Personen erkannt werden, sollten die Auflösung der Kameras, die Komprimierungseinstellungen in einem digitalen System, der Standort, die Ausleuchtung und sonstige Faktoren berücksichtigt und so gewählt oder verändert werden, dass die erhaltene Bildqualität ausreichen würde, um Bilder zu erhalten, auf denen Gesichter erkannt werden können. Wenn keine Erkennung erforderlich ist, sollten die Kameraauflösung und sonstige einstellbare Faktoren so gewählt werden, dass keine Bilder aufgenommen werden, in denen Gesichter erkennbar sind.

Wer sollte Zugriff auf das VMS haben?

Die Zugriffsberechtigungen müssen auf eine kleine Anzahl eindeutig angegebener Personen beschränkt werden, die nur bei Bedarf Zugang erhalten. Die VMS-Zugriffsrichtlinien sollten nach dem Prinzip des "geringsten Privilegs" festgelegt werden: Benutzern wird der Zutritt nur zu denjenigen Ressourcen gestattet, die für die Ausführung ihrer Aufgaben unbedingt erforderlich sind.

Nur der für die Verarbeitung Verantwortliche, der Systemadministrator oder andere von dem für die Verarbeitung Verantwortlichen eigens zu diesem Zweck benannte Mitarbeiter sollten in der Lage sein, Personen Zugangsberechtigungen zu erteilen, diese zu ändern oder sie aufzuheben. Jede Erteilung, Änderung oder Aufhebung von Zugangsberechtigungen muss in Übereinstimmung mit den in der *Videoüberwachungsrichtlinie* der Organisation festgelegten Kriterien erfolgen.

Personen, die über eine Zugangsberechtigung verfügen, müssen stets eindeutig identifizierbar sein.

In der *Videoüberwachungsrichtlinie* muss eindeutig festgelegt und dokumentiert werden, wer zu welchem Zweck Zugriff auf die Aufzeichnungen aus der Videoüberwachung und/oder die technische Architektur, z. B. den VMS-Server, das Videoüberwachungssystem, hat und was diese Zugriffsberechtigungen beinhalten. Insbesondere müssen Sie angeben, wer die Berechtigungen hat, um

- Die Video-/Audioaufzeichnungen in Echtzeit zu betrachten
- Die Schwenk-Neige-Zoom-Kameras (PTZ) zu bedienen
- Die Aufzeichnungen anzusehen
- Aufzeichnungen zu Exportieren oder
- zu löschen

Darüber hinaus müssen Sie den Zugriff auf die folgenden Funktionen des VMS konfigurieren:

- Lesezeichen
- Beweissicherungen
- Privatzonenmasken aufheben
- Exportieren
- Auslösende Ereignisse
- Starten/anhalten der Aufzeichnung
- Voreinstellungen der PTZ-Kameras erstellen/bearbeiten/löschen/aktivieren/sperren/freigeben
- PTZ-Patrouillenschemata erstellen/bearbeiten/löschen/starten/stoppen
- intelligente Suche
- Audio, Metadaten, E/A und Ereignisberechtigungen

Schutz der gespeicherten und übertragenen Daten

Zuallererst muss eine interne Analyse der Sicherheitsrisiken durchgeführt werden, um ermitteln, welche Sicherheitsmaßnahmen zum Schutz des Videoüberwachungssystems, einschließlich der darin verarbeiteten personenbezogenen Daten, erforderlich sind.

In jedem Fall müssen Maßnahmen getroffen werden, um die Sicherheit zu gewährleisten hinsichtlich

- Weitergabe
- Speicherung (z.B. in Computerdatenbanken)
- Zugriff (z.B. Zugriff auf Server, Speichersysteme, das Netzwerk und die Räumlichkeiten)

Die Übermittlung muss über sichere Kommunikationskanäle erfolgen und abhörgeschützt sein, z.B. durch folgende Maßnahmen:

- Verschlüsselung der Mediendatenbank im Recording Server und Verschlüsselung der gesamten Kommunikation zwischen Servern und Clients. Weitere Informationen dazu, wie Sie Ihre XProtect VMS-Installationen schützen können, finden Sie im Schutzleitfaden und im Zertifikate-Leitfaden.
- Anschließen der HTTPS-Kamera an das Recording Server
- VPN für Smart Client oder Management Client mit Verbindung über das Internet verwenden

Der Abhörschutz ist besonders wichtig, wenn ein drahtloses Übertragungssystem verwendet wird oder wenn Daten über das Internet übertragen werden. In solchen Fällen müssen die Daten bei der Übertragung verschlüsselt werden, oder es muss ein gleichwertiger Schutz vorhanden sein.

Verschlüsselung oder sonstige technische Mittel, die einen gleichwertigen Schutz gewährleisten, müssen auch in anderen Fällen, während der Speicherung, in Betracht gezogen werden, wenn die interne Analyse der Sicherheitsrisiken dies rechtfertigt. Dies kann z. B. dann der Fall sein, wenn es sich um besonders sensible Daten handelt. Dies geschieht durch die Aktivierung der Verschlüsselung der Mediendatenbank.

Alle Räumlichkeiten, in denen die Videoüberwachungsdaten gespeichert werden und in denen sie gesichtet werden, müssen gesichert sein. Der physische Zugang zum Kontrollraum und zum Serverraum, in dem die VMS-Server untergebracht sind, muss geschützt werden. Dritte (z. B. Reinigungs- oder Wartungspersonal) dürfen keinen unbeaufsichtigten Zugang zu diesen Räumlichkeiten haben.

Der Standort der Monitore muss so gewählt werden, dass sie nicht von Unbefugten eingesehen werden können. Wenn sie sich in der Nähe öffentlicher Bereiche befinden müssen, müssen die Monitore so aufgestellt werden, dass nur das Sicherheitspersonal sie einsehen kann.

Der XProtect VMS protokolliert standardmäßig Basisinformationen. Wir empfehlen jedoch, dass Sie die Protokollierung der Benutzerzugriffe im Management Client für das Auditprotokoll aktivieren.

Dieses digitale Protokollierungssystem soll sicherstellen, dass bei einer Prüfung jederzeit festgestellt werden kann, wer wann und wo Zugriff auf das System hatte. Das Protokollierungssystem kann feststellen, wer die Videoüberwachungsdaten angesehen, gelöscht oder exportiert hat (hierzu müssen Sie die Protokollierung der Benutzerzugriffe aktivieren).

Diesbezüglichh, und auch an anderer Stelle, ist auf die Schlüsselfunktionen und -befugnisse der Systemadministratoren zu achten, sowie auf die Notwendigkeit, diese gegen angemessene Überwachungs- und Schutzmaßnahmen abzuwägen.

Rechenschaft

Paragraph 5 (2) DSGVO besagt:

der für die Verarbeitung Verantwortliche ist für die Einhaltung von Paragraph 1 ("Rechenschaft") verantwortlich und muss dies auch nachweisen können.

Wo die Prinzipien hinsichtlich der Verarbeitung personenbezogener Daten Gesetzlichkeit, Fairness und Transparenz, Zweckbindung, Begrenzung der gesammelten Daten auf ein Mindestmaß, Richtigkeit, Begrenzung des Speicherplatzes, Integrität und Vertraulichkeit sind.

Das Prinzip der Rechenschaftspflicht verlangt, dass Sie die Verantwortung dafür übernehmen, was Sie mit den personenbezogenen Daten tun.

Paragraph 30 DSGVO besagt insbesondere:

Jeder für die Verarbeitung Verantwortliche sowie ggf. dessen Vertreter, muss Aufzeichnungen über die Verarbeitungstätigkeiten unter seiner Verantwortung führen.

Das Protokoll muss folgende Informationen enthalten:

a. *den Namen und die Kontaktdaten des für die Verarbeitung Verantwortlichen sowie ggf. des gemeinsamen für die Verarbeitung Verantwortlichen, seines Vertreters und des Datenschutzbeauftragten*

b. *die Zwecke der Verarbeitung*

c. *eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten*

d. *die Kategorien der Empfänger, an die die personenbezogenen Daten weitergegeben wurden oder werden, einschließlich der Empfänger in Drittländern oder internationale Organisationen*

e. *ggf. an ein Drittland oder eine internationale Organisation weitergegebene personenbezogene Daten, einschließlich der Angabe des Drittlandes oder der internationalen Organisation und - bei der Weitergabe nach dem zweiten Unterabsatz in Paragraph 49 (1), der Dokumentation geeigneter Sicherungen*

f. *wenn möglich, die vorgesehenen Fristen für die Löschung der Daten der verschiedenen Kategorien*

g. *wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen gemäß Paragraph 32 (1).*

Rechenschaftspflicht ist einer der Datenschutzgrundsätze - danach sind Sie für die Einhaltung der DSGVO verantwortlich und müssen die Einhaltung nachweisen können.

Sie müssen geeignete technische und organisatorische Maßnahmen ergreifen, um Ihre Rechenschaftspflicht zu erfüllen.

Es gibt mehrere Maßnahmen, die Sie ergreifen können und in einigen Fällen auch müssen, darunter:

- Einführung und Umsetzung von Datenschutzrichtlinien
- Verfolgung des Ansatzes "Eingebauter Datenschutz als Standard" (weitere Informationen finden Sie unter Eingebauter Datenschutz auf Seite 42)
- Abschluss schriftlicher Verträge mit Organisationen, die in Ihrem Auftrag personenbezogene Daten verarbeiten
- Dokumentation Ihrer Verarbeitungstätigkeiten
- Umsetzung geeigneter Sicherheitsmaßnahmen

- Aufzeichnung und ggf. Meldung von Verstößen gegen den Datenschutz
- Durchführung von Datenschutz-Folgenabschätzungen für Verwendungen personenbezogener Daten, die mit hoher Wahrscheinlichkeit ein hohes Risiko für die Interessen Einzelner mit sich bringen
- Ernennung eines Datenschutzbeauftragten
- Einhaltung entsprechender Verhaltensnormen und Übernahme von Zertifizierungsprogrammen

Verwendung einer Vorlage für die Aufzeichnung von Verarbeitungsaktivitäten, um Probleme der Verantwortlichkeit zu ermitteln und zu verfolgen. Eine Musteraufzeichnung von Verarbeitungstätigkeiten finden Sie in der Aufzeichnung von Verarbeitungstätigkeiten (Muster).

Rechenschaftspflichten bestehen fortlaufend. Sie müssen die von Ihnen ergriffenen Maßnahmen überprüfen und ggf. aktualisieren.

Wenn Sie ein Privacy Management Framework implementieren, kann dies Ihnen dabei helfen, Ihre Maßnahmen im Sinne der Rechenschaft einzubetten und eine Kultur des Datenschutzes in Ihrer gesamten Organisation zu schaffen.

Ihre Rechenschaftspflicht kann Ihnen dabei helfen, bei Einzelpersonen Vertrauen aufzubauen und Maßnahmen zur Durchsetzung der DSGVO abzumildern.

Checkliste zur Sicherung von Integrität und Vertraulichkeit

Die DSGVO schreibt vor, dass Organisationen über umfassende Richtlinien und Verfahren verfügen, die gewährleisten, dass die personenbezogenen Daten stets unter der Kontrolle der Organisation bleiben. Darüber hinaus müssen Verstöße gegen den Datenschutz innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde gemeldet werden, die von der Regierung ihres Landes ernannt wurde.

Ergreifen Sie alle geeigneten organisatorischen und technischen Maßnahmen zum Schutz vor Datenschutzverletzungen.

Was sollten Sie tun?

- Überprüfen Sie die Sicherheitsrichtlinien für die Passwortsteuerung und Kontonutzung.
- Erwägen Sie, Mindestanforderungen für die Stärke der Passwörter für alle Domänengruppen festzulegen. Erwägen Sie, strengere Anforderungen für Administratorkonten auf Domänenebene festzulegen.
- Richten Sie Verfahren zur Überprüfung des Schutzstatus und zur Erkennung von Verstößen ein.
- Achten Sie darauf, dass die Benutzer ihre Konten nicht gemeinsam nutzen, sei es durch Weitergabe von Kennwörtern oder dadurch, dass sie sich am Ende/Anfang ihrer Schicht nicht an-/abmelden.
- Geben Sie Ihrer Organisation eine dokumentierte Richtlinie und ein Verfahren für geeignete Maßnahmen im Falle einer Datenschutzverletzung.

- Sie müssen darauf achten, dass Sie über geeignete Sicherheitsmaßnahmen verfügen, um die von Ihnen gespeicherten personenbezogene Daten zu schützen.
- Ein zentrales Prinzip der DSGVO ist, dass Sie personenbezogene Daten mit "geeigneten technischen und organisatorischen Maßnahmen" sicher verarbeiten – dies ist das "Sicherheitsprinzip".
- Dazu müssen Sie Dinge berücksichtigen wie Risikoanalyse, Organisationsrichtlinien und physische und technische Maßnahmen.
- Zudem müssen Sie weitere Anforderungen an die Sicherheit Ihrer Datenverarbeitung berücksichtigen – und diese gelten auch für Datenverarbeiter.
- Sie können den Stand der Technik und die Kosten der Umsetzung bei der Entscheidung berücksichtigen, welche Maßnahmen Sie ergreifen wollen – diese müssen jedoch sowohl Ihren Umständen als auch dem Risiko angepasst sein, das Ihre Datenverarbeitung darstellt.
- Sie sollten ggf. Maßnahmen wie Pseudonymisierung (z. B. Schutz der Privatsphäre durch Unkenntlichmachung) und Verschlüsselung verwenden.
- Ihre Maßnahmen müssen die "Vertraulichkeit, Integrität und Verfügbarkeit" Ihrer Systeme und Dienste und der personenbezogenen Daten gewährleisten, die Sie in diesen Systemen und Diensten verarbeiten.
- Mit diesen Maßnahmen müssen Sie bei einem physischen oder technischen Zwischenfall außerdem den Zugriff und die Verfügbarkeit personenbezogener Daten zeitnah wieder herstellen können.
- Sie müssen außerdem sicherstellen, dass Sie über geeignete Prozesse verfügen, mit denen Sie die Wirksamkeit Ihrer Maßnahmen testen und ggf. erforderliche Verbesserungen vornehmen können.

Anhang: Ad-hoc-Mitteilung

Ad-hoc-Mitteilungen sollten ein Piktogramm enthalten (z. B. das ISO-Piktogramm oder das Piktogramm, das üblicherweise da verwendet wird, wo sich das Gebäude befindet). Das Piktogramm muss auch für Kinder verständlich sein. Dieses finden Sie z.B. auf der Seite mit den grafischen ISO-Symbolen (https://www.iso.org/obp/ui/#search/grs/). Die Mitteilung muss:

- Den für die Verarbeitung Verantwortlichen bezeichnen
- Den Zweck der Überwachung angeben:
    - Damit die Behörden ihre Aufgaben erfüllen können
    - Das Recht auszuüben, zu bestimmen, wer Zugang zu den Daten erhält und wer nicht
    - Die legitimen Interessen für konkret angegebene Zwecke zu gewährleisten
- Deutlich anzugeben, ob die Bilder aufgezeichnet werden
- Stellen Sie Kontaktinformationen und einen Link zur *Online-Richtlinie zur Videoüberwachung zur Verfügung*
- Wenn ein Bereich außerhalb von Gebäuden überwacht wird, sollte dies klar angegeben werden

Das Sicherheitspersonal und der Empfang müssen in den Datenschutzaspekten der Videoüberwachung geschult sein und Kopien der detaillierten Datenschutzerklärung machen können (siehe Anhang: Richtlinie für die Videoüberwachung auf Seite 54), die auf Anfrage zur Verfügung gestellt wird. Sie müssen außerdem die Öffentlichkeit darüber informieren können, an wen man sich mit weiteren Fragen wenden oder wo man auf seine Daten zugreifen kann.

Die Schilder müssen an solchen Stellen angebracht werden und groß genug sein, dass betroffene Personen sie vor dem Betreten der überwachten Zone bemerken und problemlos lesen können. Dies bedeutet nicht, dass neben jeder einzelnen Kamera ein Hinweis platziert werden muss.

Die Schilder in Gebäuden müssen in der (den) Sprache(n) verfasst sein, die von den Mitarbeitern und den häufigsten Besuchern allgemein verstanden wird. Auch Schilder außerhalb von Gebäuden (falls Außenbereiche überwacht werden) müssen in der Landessprache (oder den Landessprachen) angebracht werden.

Ein Muster für eine Ad-hoc-Meldung finden Sie unter *Milestone Ad-hoc-Meldung* Muster.

Anhang: Richtlinie für die Videoüberwachung

Die *Richtlinie für die Videoüberwachung* verfolgt mehrere Zwecke und dient dazu, den folgenden Anforderungen gerecht zu werden:

- Die Annahme dieses Dokumentes ist oft notwendig, um die Rechtsgrundlage zu vervollständigen und genau anzugeben und damit eine gesetzliche Grundlage für die Videoüberwachung zu schaffen (siehe Paragraph 5 DSGVO).
- Die Niederschrift der Methoden und die Überlegung, welche sonstigen Maßnahmen ergriffen werden müssen, verbessern mit hoher Wahrscheinlichkeit die Verfahren und gewährleisten eine bessere Compliance.
- Durch Einführung und Veröffentlichung einer Richtlinie kann der Verantwortliche für die Verarbeitung seine Verpflichtung lt. DSGVO erfüllen und der Öffentlichkeit die erforderlichen Informationen zur Verfügung zu stellen, um eine faire Verarbeitung zu gewährleisten.
- Die Richtlinie legt eine Reihe von Regeln fest, an denen die Compliance gemessen werden kann (z. B. bei einem Audit).
- Durch erhöhte Transparenz und den Nachweis ihrer Bemühungen im Sinne der Compliance schaffen Unternehmen Vertrauen bei ihren Mitarbeitern und Dritten und erleichtern die Abstimmung mit ihren Anspruchsgruppen.

Die *Richtlinie für die Videoüberwachung* sollte:

- Einen Überblick über das Videoüberwachungssystem geben und dessen Zwecke beschreiben
- Beschreiben, wie das System betrieben wird, wie personenbezogene Daten verwendet werden und welche Vorkehrungen für den Datenschutz getroffen werden
- Die Einhaltung der DSGVO ausdrücklich bestätigen
- Alle notwendigen Maßnahmen zur Umsetzung skizzieren

Organisationen sollten ihre *Richtlinien für die Videoüberwachung* auf ihren Intranet- und Internetseiten öffentlich zugänglich machen. Wenn dieses Dokument vertrauliche Informationen enthält, so sollte eine nicht vertrauliche Version veröffentlicht werden.

Um als Datenschutzhinweis geeignet zu sein, müssen Sie die folgenden Informationen in benutzerfreundlicher Sprache und entsprechendem Format in Ihre *Richtlinie für die Videoüberwachung* aufnehmen:

- Die Identität des für die Verarbeitung Verantwortlichen (z. B. der Organisation, der Generaldirektion, Direktion und Referat)
- Eine Kurzbeschreibung der durch das Videoüberwachungssystem beobachteten Bereiche (z. B. Ein- und Ausgänge, Computerräume, Archivräume)
- Die gesetzliche Grundlage für die Videoüberwachung, z.B. Paragraph 6 (1)(f) DSGVO
- Die gesammelten Daten und der Zweck der Videoüberwachung (auch Einschränkungen der zulässigen Verwendungszwecke sind ggf. klar anzugeben)
- Wer Zugriff auf das Überwachungsmaterial hat und an wen die Aufnahmen weitergegeben werden dürfen
- Wie die Informationen geschützt und gesichert werden
- Für wie lange die Daten aufbewahrt werden
- Wie die betroffenen Personen ihre Daten überprüfen, ändern oder löschen können (einschließlich der Ansprechpartner, die weitere Fragen beantworten und Informationen darüber geben können, wie intern Rechtsmittel eingelegt werden können)

Darüber hinaus sollte die *Richtlinie für die Videoüberwachung* Bezug nehmen auf:

- Die Audit-Berichte der Organisation
- Die Berichte der Organisation zur Folgenabschätzung

Eine Musterrichtlinie zur Videoüberwachung finden Sie in der *Milestone Richtlinie zur Videoüberwachung* Muster.

Haftungsausschluss: Die *Musterrichtlinie zur Videoüberwachung* ist von dem für die Verarbeitung Verantwortlichen zu überprüfen. Er ist für die Einhaltung der DSGVO durch diese Mustervereinbarung verantwortlich.

Beachten Sie bitte: Das Sammeln von Audio- und Metadaten wird im Europäischen Datenschutzsiegel nicht berücksichtigt. Das EuroPriSe-zertifizierte Produktprofil darf für eine VMS-Konfiguration mit der Sammlung von Audio- und Metadaten nicht verwendet werden. Ein für die Verarbeitung Verantwortlicher, er dies tut, kann sich nicht darauf berufen, dass er ein Produkt verwendet, das den Datenschutz und die Einhaltung der DSGVO besonders fördert.

Anhang: Datenschutz-Folgenabschätzung

Nach Paragraph 35 der DSGVO ist eine *Datenschutz-Folgenabschätzung* erforderlich, wenn die Überwachung

mit großer Wahrscheinlichkeit ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben kann. In diesem Fall nimmt der für die Verarbeitung Verantwortliche vor der Datenverarbeitung eine Abschätzung der Folgen der geplanten Verarbeitungsvorgänge für den Schutz der personenbezogenen Daten vor.

Der für die Verarbeitung Verantwortliche muss vor der Verarbeitung die Aufsichtsbehörde konsultieren, wenn eine *Datenschutz-Folgenabschätzung* nach Paragraph 35 darauf hinweist, dass die Verarbeitung zu einem hohen Risiko führen würde, wenn der für die Verarbeitung Verantwortliche keine Maßnahmen zur Risikominderung ergreift (Vorherige Konsultation, Paragraph 36 DSGVO).

Erstellen und pflegen Sie eine *Datenschutz-Folgenabschätzung*, eine Mitteilung an betroffene Personen. Dieses Dokument:

- Beschreibt den Zweck der Überwachung
- Wird von dem für die Verarbeitung Verantwortlichen oder vom Datenverarbeiter aufbewahrt
- Legt die Aufbewahrungsrichtlinie fest

Eine *Datenschutz-Folgenabschätzung* ist vor der Installation und Implementierung von Videoüberwachungssystemen immer dann vorzunehmen, wenn dies einen Mehrwert für die Bemühungen der Organisation zur Einhaltung der gesetzlichen Vorschriften darstellt. Der Zweck der *Datenschutz-Folgenabschätzung* besteht darin, die Auswirkungen des geplanten Systems für die Privatsphäre von Einzelpersonen sowie auf sonstige Grundrechte zu ermitteln und Möglichkeiten zur Minderung oder Vermeidung negativer Auswirkungen zu suchen.

Nach Paragraph 35 (7) DSGVO muss die Bewertung mindestens enthalten:

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich des vom für die Verarbeitung Verantwortlichen verfolgten berechtigten Interesses
- Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge im Hinblick auf deren Zweck
- Eine Bewertung der Risiken für die Rechte und Freiheiten der in Paragraph 35 (1) DSGVO genannten betroffenen Personen:

  Kann eine Verarbeitungsweise, insbesondere mit neuen Technologien und unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, so nimmt der Verantwortliche vor der Verarbeitung eine Abschätzung der Folgen der geplanten Verarbeitungsvorgänge für den Schutz personenbezogener Daten vor. Eine Einzelbewertung kann eine Reihe ähnlicher Verarbeitungsvorgänge betreffen, die ähnliche Risiken mit sich bringen.

- Die geplanten Maßnahmen zum Umgang mit den Risiken, einschließlich der Maßnahmen zum Schutz und zur Sicherheit und der Mechanismen, die den Schutz personenbezogener Daten gewährleisten und die Einhaltung der DSGVO unter Berücksichtigung der Rechte und berechtigten Interessen der betroffenen und sonstiger Personen nachweisen sollen

Welcher Aufwand für eine *Datenschutz-Folgenabschätzung* angemessen ist, hängt von den Umständen ab. Ein Videoüberwachungssystem mit großen inhärenten Risiken oder eines, das komplexe oder neuartige Fragen aufwirft, rechtfertigt einen wesentlich größeren Aufwand als eines mit vergleichsweise geringen Auswirkungen auf die Privatsphäre und sonstige Grundrechte, wie z. B. ein herkömmliches statisches CCTV-System, das zu typischen Sicherheitszwecken betrieben wird.

In jedem Fall müssen Organisationen, sei es in einer förmlichen *Datenschutz-Folgenabschätzung* oder in anderer Weise, bewerten und begründen, ob sie auf Videoüberwachung zurückgreifen, wie sie ihre Systeme aufstellen, auswählen und konfigurieren und wie sie den Datenschutz umsetzen will.

Darüber hinaus kann es Fälle geben, in denen eine Organisation ein nicht-standardmäßiges System plant. In diesem Fall sollte die Organisation die geplanten Abweichungen von der Praxis und den Empfehlungen sorgfältig bewerten, diese mit ihrem Datenschutzbeauftragten und mit sonstigen Anspruchsgruppen besprechen und ihre Bewertung schriftlich dokumentieren, sei es in einer förmlichen *Datenschutz-Folgenabschätzung* oder in sonstiger Weise. Die Prüfung des Systems durch die Organisation sollte sich auch auf die Gesetzlichkeit der Anpassungen des Systems erstrecken.

Schließlich wird aufgrund ihrer Komplexität, Neuartigkeit, Spezifität oder der inhärenten Risiken dringend empfohlen, eine *Datenschutz-Folgenabschätzung* vorzunehmen, und zwar in den folgenden Fällen:

- Videoüberwachung zu anderen als zu Sicherheitszwecken (einschließlich zu Ermittlungszwecken)
- Videoüberwachung in der Öffentlichkeit
- Mitarbeiterüberwachung
- Überwachung im Hoheitsgebiet von Mitgliedstaaten sowie in Drittländern
- Besondere Datenkategorien
- Bereiche mit erhöhten Erwartungen an die Privatsphäre
- High-Tech und/oder intelligente Videoüberwachung
- Untereinander verbundene Systeme
- Audioaufzeichnungen

Die *Datenschutz-Folgenabschätzung* kann intern oder durch einen unabhängigen Auftragnehmer erfolgen. Die Bewertung sollte in einer frühen Phase des Projekts erfolgen. Je nachdem, wie die Ergebnisse der *Datenschutz-Folgenabschätzung* ausfallen, kann sich die Organisation dazu entscheiden:

- Die geplante Überwachung zu unterlassen oder sie zu modifizieren und/oder
- Zusätzliche Sicherungen umzusetzen

Inhärente Risiken bei der Verwendung von VMS

Bei der Pflege der *Datenschutz-Folgenabschätzung* sollten Sie sich der Risiken bewusst sein, die mit dem Einsatz eines VMS einhergehen.

Die *Datenschutz-Folgenabschätzung* ist angemessen zu dokumentieren. Grundsätzlich sollte ein Bericht zur *Datenschutz-Folgenabschätzung* die von der Organisation ermittelten Risiken für die Privatsphäre bzw. sonstige Grundrechte klar benennen, sowie auch zusätzliche Schutzmaßnahmen, die sie vorschlägt. Seien Sie sich der folgenden Risiken der Verletzung von Persönlichkeitsrechten bewusst:

- Unternehmen/Arbeitgeber, unter Verwendung der Video-Feeds, Alarme oder Auditprotokolle, um:
    - Die Arbeitszeiten der Mitarbeiter am untersuchten Standort zu überwachen - z. B. die Zeiten von Dienstbeginn Dienstschluss
    - Die Arbeitsleistung der Mitarbeiter zu überwachen, indem überwacht wird, wo diese ihre Zeit verbringen, wie viel Zeit sie an der Kaffeemaschine verbringen, wie viel Zeit sie auf der Toilette verbringen, solange sie effektiv an ihrer jeweiligen Aufgabe arbeiten
    - Zu überwachen, was der jeweilige Mitarbeiter auf seinem Computerbildschirm ansieht
    - Zu überwachen, ob die Mitarbeiter die Arbeits- oder Sicherheitsanforderungen einhalten - z. A. auf Baustellen
    - Videoaufnahmen von Mitarbeitern anderen Mitarbeitern oder ihren Vorgesetzten zeigen, um Mitarbeiter zu schikanieren oder anderen Mitarbeitern damit zu drohen, dies zu tun
    - Zu prüfen, ob das Sicherheitspersonal/Bedienpersonal seine Aufgaben wirksam ausführt - z. B. ob es die Clients aktiv benutzt, Kameras auswählt, Aufzeichnungen abspielt usw.
- Unternehmen/Eigentümer/Betreiber/Sicherheitspersonal, die die Videoübertragungen dafür verwenden:
    - Videoaufnahmen von Personen (Mitarbeiter des Unternehmens oder Personen in der Öffentlichkeit) in peinlichen oder heiklen Situationen auf sozialen Medien zu veröffentlichen
    - PTZ-Kameras dazu zu verwenden, Personen heranzuzoomen, um ohne ihr Wissen intime/unangemessene Nahaufnahmen von ihnen zu erhalten
- Unternehmen/Eigentümer/Betreiber/Sicherheitspersonal
    - Auf Nachfrage Videoaufzeichnungen zu exportieren oder unkritisch den Zugang dazu zu gewähren

Weitere Quellen zur Erkennung möglicher Risiken sind:

- Der *Milestone Hardening Guide*, der das Cyber Risk Management Framework vorgibt, in dem die empfohlenen sechs Schritte der Kategorisierung, Auswahl, Umsetzung, Beurteilung, Autorisierung und Überwachung von Risiken angegeben werden. Im *Milestone Hardening Guide* werden eine Reihe technischer Risiken angegeben und Implementierungen empfohlen, mit denen sich diese Risiken abmildern lassen. Hierzu gehören u. a. der Schutz der Privatsphäre im VMS im Hinblick auf eine Reihe von Datenschutzverletzungen und Risiken des unbefugten Zugriffs aufgrund einer mangelhaften technischen Konfiguration, Konstruktion und Wartung. Weitere Informationen dazu, wie Sie Ihre XProtect VMS-Installationen vor Cyber-Angriffen schützen, finden Sie im Schutzleitfaden.
- Die *Milestone Anleitung zum Schutz der Privatsphäre* (diese) gibt Empfehlungen zum Umgang mit den nicht-technischen Betriebsrisiken, einschließlich des Umgangs mit den Rechten und Anfragen der betroffenen Personen, der Rollen und Verantwortlichkeiten eines VMS, Vorlagen für Sofortmeldungen, *Videoüberwachungsrichtlinien*und *Vereinbarungen mit den für die Verarbeitung Verantwortlichen*.
- Das Milestone E-Learning zum Datenschutz für Endbenutzer soll beim VMS-Betreiber und Vorgesetzte ein Bewusstsein dafür bilden, wie im Tagesbetrieb mit VMS-bezogenen Datenschutzrisiken umgegangen werden sollte. Weitere Informationen finden Sie auf der Milestone Internetseite zur Zertifizierung nach DSGVO.

Anhang: Vereinbarung mit dem Datenverarbeiter

Der für die Verarbeitung Verantwortliche muss mit Dritten, mit denen er Videoüberwachungsmedien gemeinsam nutzt, eine *Datenverarbeitungsvereinbarung* abschließen, außer bei der gemeinsamen Nutzung von Videoüberwachungsmedien mit den Strafverfolgungsbehörden.

Wenn eine Organisation Dritte (für die Verarbeitung Verantwortliche) mit ihren Videoüberwachungsaktivitäten (oder Teilen davon) beauftragt, bleibt sie als für die Verarbeitung Verantwortlicher für die Einhaltung der DSGVO verantwortlich. Z. B. Sicherheitspersonal, das Live-Überwachungsvideos im Empfangsbereich einer Organisation überwacht und das für ein privates Unternehmen arbeitet, das von der Organisation mit der Live-Überwachung beauftragt wurde. In diesem Fall muss die Organisation gewährleisten, dass das Sicherheitspersonal seine Tätigkeit in Übereinstimmung mit den Bestimmungen der DSGVO ausübt.

Eine Mustervereinbarung mit dem Datenverarbeiter finden Sie unter *Milestone Mustervereinbarung mit dem Datenverarbeiter*.

Haftungsausschluss: Die Beispiel-*Datenverarbeitungsvereinbarung* ist von dem für die Verarbeitung Verantwortlichen zu prüfen. Er ist für die Einhaltung der DSGVO durch diese Mustervereinbarung verantwortlich.

Anhang: Das Milestone XProtect VMS-System und die DSGVO

> Beachten Sie bitte: In diesem Abschnitt werden die Anforderungen und Einschränkungen für ein nach dem europäischen Datenschutzsiegel (EuroPriSe) zertifiziertes Produkt beschrieben. Ein von diesen Anforderungen abweichender für die Verarbeitung Verantwortlicher/Datenverarbeiter kann sich nicht darauf berufen, dass er ein Produkt verwendet, das den Datenschutz und die Einhaltung der DSGVO besonders erleichtert.

Komponenten und Geräte, die nicht unter das Europäische Datenschutzsiegel fallen

Die folgenden Komponenten und Geräte fallen nicht unter das Europäische Datenschutzsiegel:

- Auf dem Milestone Marketplace erhältliche Plug-ins
- XProtect Mobile-Server (standardmäßig deaktiviert)
- XProtect Mobile Client
- XProtect Web Client
- XProtect Access (standardmäßig deaktiviert)
- XProtect LPR (standardmäßig deaktiviert)
- XProtect Transact (standardmäßig deaktiviert)
- Milestone Interconnect
- XProtect DLNA Server
- Milestone Open Network Bridge (sichere Videointegration privat-zu-öffentlich)
- XProtect Rapid REVIEW
- XProtect Event Server-Plug-ins
- Verarbeitung von Audiodaten (standardmäßig deaktiviert)
- Verarbeitung von Metadaten (standardmäßig deaktiviert)
- Verarbeitung von Daten von Ein- und Ausgabegeräten (standardmäßig deaktiviert)
- XProtect BYOL wie zur Verfügung gestellt über https://aws.amazon.com/marketplace/pp/prodview-ryozifnbg4kas

Diese Komponenten dürfen nicht installiert werden, wenn die Milestone XProtect VMS Installation unter das Europäische Datenschutzsiegel fallen soll.

Darüber hinaus verfügt das Standardprodukt nicht über Funktionen zur Gesichtserkennung, Verhaltensanalyse, automatische Verfolgung oder Erkennung von Personen im Live-Feed oder in aufgezeichneten Medien. Diese Funktionen entsprechen auch nicht dem Europäischen Datenschutzsiegel.

Dies bedeutet, dass Sie bei der Installation der XProtect VMS die Option **Einzelcomputer** im Installationsprogramm nicht verwenden dürfen, da diese das Mobile Server automatisch installiert.

Installieren Sie stattdessen das XProtect VMS-System, entweder mit den Optionen **Verteilt** oder **Benutzerdefiniert**. Hiermit werden die Mobile Server nicht installiert.

Nach der Installation der XProtect VMS werden auf der Downloadseite auf der Management Server die zusätzlichen DLNA Server und Mobile Server Komponenten aufgeführt. Installieren Sie diese Server nicht.

Upgradeanleitung

Wenn Sie eine Milestone XProtect VMS-Installation der Version 2018 R2 oder früher erweitern, müssen die alten Protokolldateien von Hand gelöscht werden, damit die Installation der DSGVO entspricht.

Sobald Sie die XProtect VMS erweitert haben, können die alten Protokolldateien mithilfe der in diesem Knowledge-Base-Artikel beschriebenen Informationen und dem in diesem Knowledge-Base-Artikel beschriebenen Tool gelöscht werden.

Sichern Sie die SQL Server Datenbanken

Es wird empfohlen, eine Sicherungskopie der SQL Server Datenbank zu erstellen, insbesondere bevor Sie ein Upgrade starten, damit Sie die vorherige funktionierende Installation wiederherstellen können, falls das Upgrade fehlschlägt. Unabhängig davon, ob das Upgrade über das XProtect Installationsprogramm oder Management Client oder über die systemeigenen SQL Server Funktionen durchgeführt wird, müssen Sie die Sicherungsdaten an einem sicheren Ort aufbewahren und dürfen sie nicht auf einem Cloud-Laufwerk speichern, wenn der Cloud-Anbieter außerhalb der EU liegt, wie z. B. Microsoft.

Keinen verwalteten SQL Server Dienst verwenden

Zwar unterstützt XProtect die Verwendung von extern verwalteten Datenbanken wie Azure SQL, doch dadurch werden möglicherweise personenbezogene Daten außerhalb der EU offengelegt. Um die DSGVO-Vorschriften einzuhalten, sollten Sie keinen verwalteten SQL Server Dienst verwenden.

> ⚠ Beachten Sie bitte: Die Nutzung eines verwalteten SQL Server Dienstes fällt nicht unter das Europäische Datenschutzgütesiegel und würde gegen das EuroPriSe Siegel verstoßen.

Sicheres Netzwerk für Authentifizierung und Datenübertragung

Entwerfen Sie eine Netzwerkinfrastruktur, die so weit wie möglich die physische Netzwerk- oder VLAN-Segmentierung nutzt.

Milestone empfiehlt, dass Sie Kameras auswählen, die HTTPS unterstützen. Es wird empfohlen, die Kameras auf separate VLANs einzustellen und für die Kommunikation zwischen Kamera und Aufzeichnungsserver sowie zwischen Clients und Aufzeichnungsserver HTTPS zu verwenden.

Es wird empfohlen, dass sich XProtect Smart Client und XProtect Smart Wall im selben VLAN befinden wie die Server.

Verwenden Sie ein VPN-verschlüsseltes Netzwerk oder ähnliches, wenn Sie Smart Client oder Smart Wall von einem entfernten Standort aus verwenden.

Aktivieren Sie die Verschlüsselung für die gesamte Kommunikation. Weitere Informationen dazu, wie Sie Ihre XProtect VMS-Installationen schützen können, finden Sie im Schutzleitfaden und im Zertifikate-Leitfaden.

> ⚠ Beachten Sie bitte: Ein unverschlüsselter und nicht gesicherter Transport von Videodaten würde gegen das EuroPriSe-Siegel verstoßen und zum Verlust der Konformität mit dem EuroPriSe-Datenschutzsiegel führen.

Personen bei Zugang unkenntlich machen

Nach Paragraph 15 DSGVO hat die betroffene Person das Recht, Zugang zu ihren verarbeiteten personenbezogenen Daten zu erhalten, z. B. Videoaufzeichnungen der betroffenen Person.

Die betroffene Person hat das Recht, von dem jeweiligen Unternehmen Auskunft darüber zu verlangen, welche ihrer personenbezogenen Daten verarbeitet werden und aus welchem Grund.

Da XProtect VMS die automatische Erkennung von Personen nicht unterstützt, müssen Sie zusätzliche Maßnahmen zum Schutz der Rechte des Einzelnen ergreifen. Im Zusammenhang mit einem VMS, siehe Anhang: Ad-hoc-Mitteilung auf Seite 53.

Mehr noch, XProtect VMS unterstützt nicht die Unkenntlichmachung sonstiger beweglicher Personen, die zusammen mit dem Antragsteller für das Recht auf Zugang aufgezeichnet werden.

Mehrere Milestone technische Lösungen unserer Partner zur dynamischen Unkenntlichmachung aller oder anderer Personen vor dem Export finden Sie auf dem Milestone Marketplace. Alternativ kann die Unkenntlichmachung zu einzelnen Bildern oder Videostreams manuell oder, nach dem Export, unterstützt hinzugefügt werden. Es gibt Firmen, die die Unkenntlichmachung als Dienstleistung anbieten (z.B. FACIT Data Systems).

Teilweise Löschung von Videoaufzeichnungen

Nach Paragraph 17 DSGVO hat die betroffene Person das Recht, die Löschung ihrer Daten zu verlangen. Im Zusammenhang mit einem VMS wird dies aufgrund überwiegender berechtigter Interessen (Betrugserkennung, Gesundheit und Sicherheit) oder anderer in der *Richtlinie für die Videoüberwachung* festgelegter geschäftlicher Zwecke oft nicht erfüllt (siehe Das Recht, vergessen zu werden (Recht auf Löschung) auf Seite 40 und Anhang: Richtlinie für die Videoüberwachung auf Seite 54). Die *Richtlinie für die Videoüberwachung* legt die automatische Aufbewahrungsfrist fest (standardmäßig 7 Tage), die gewährleistet, dass das Filmmaterial automatisch gelöscht wird; dabei müssen die Rechte der betroffenen Personen gegen angemessene Geschäftszwecke abgewogen werden.

Wenn die betroffene Person die Löschung ihrer Daten verlangt, wird empfohlen, dass der für die Verarbeitung Verantwortliche den Anspruch in einer *Anfrage der betroffenen Person* dokumentiert (siehe Anfrage einer betroffenen Person auf Seite 13). Einen Musterantrag einer betroffenen Person finden Sie unter *Milestone Musterantrag einer betroffenen Person*.

Sie müssen alle Aufzeichnungen von den betreffenden Kameras löschen.

Um alle anderen Aufzeichnungen zu behalten, die nicht gelöscht werden sollen, exportieren Sie alle Daten und bewahren sie sicher auf. Sie können diese Daten auf dem VMS nicht wiederherstellen.

Jeder Export muss verschlüsselt und digital signiert sein und die angegebenen Zeitintervalle von den konkret angegebenen Kameras ausschließen. Das heißt, Export bis zum Zeitpunkt/Datum und Export nach dem Zeitpunkt/Datum. Dies kann dazu führen, dass Sicherungen über mehrere Zeiträume erfolgen müssen.

Der Smart Client – Player kann dann dazu verwendet werden, die Daten einzusehen.

Es wird empfohlen, dass sich der für die Verarbeitung Verantwortliche rechtlich beraten lässt und sowohl eine Geschäftsfolgenabschätzung als auch eine Datenschutzfolgenabschätzung durchführt (siehe Durchführung einer Folgenabschätzung auf Seite 35), bevor die betroffene Person ihr Recht ausgeübt, vergessen zu werden, da die Löschung neue geschäftliche Risiken mit sich bringen kann, die die Interessenabwägung umkehren und Risiken mit sich bringen kann, die sich auf den Schutz der Privatsphäre anderer betroffener Personen negativ auswirken.

Verwendung der geographischen Hintergründe in XProtect Smart Client

XProtect Smart Client unterstützt die Verwendung geographischer Hintergründe. Diese Hintergründe zeigen Kartenhintergründe.

Sie riskieren einen Verstoß gegen die DSGVO, wenn Sie einen der folgenden Kartendienste nutzen, und Sie erfüllen dann nicht die DSGVO im Rahmen der EuroPriSe-Zertifizierung:

- Bing Maps
- Google Maps
- Milestone Map Service

Diese Dienste bieten keinen angemessenen Schutz vor der Verarbeitung personenbezogener Daten in den USA. Der Kunde wird (Mit-)Verantwortlicher für die Verarbeitung der Nutzerdaten.

Siehe ggf. Aktualisierungen des Urteils Schrems II der EU-Kommission auf der offiziellen Website.

Als Alternative wird empfohlen, den privaten Dienst **OpenStreetMap** für den geografischen Hintergrund einzurichten.

Integrationen von registrierten Partnern.

Wenn eine Lizenz aktiviert wird, sammelt Milestone Daten auf der Basis "je Integration". Der XProtect VMS sammelt Daten über Plugins und Plugin-Hersteller sowie über die vom Kunden verwendeten Plugins und Integrationen.

Die von jeder Installation gesammelten Daten sind:

- Name der Integration
- Hersteller der Integration
- Integrationsversion
- Integrationstyp (eigenständig, Smart Client, Management Client, Event Server) und Anzahl der Instanzen jedes Typs (d. h. auf wie vielen Clients das Plugin läuft)

Die Entwickler von Plugins dürfen bei der Registrierung ihres Produktes niemals ihre persönlichen Namen verwenden. Verwenden Sie nur den Firmennamen.

Die Daten werden von Milestone nur verarbeitet, wenn der Hersteller des Plugins im Marketplace gelistet ist und der Verarbeitung der Daten zum Zweck der Verbesserung von Milestone XProtect Corporate (und nicht für Marketing und Marktforschung) zugestimmt hat. Wenn das Plugin nicht registriert ist, werden die Daten sofort gelöscht. Die Rechtsgrundlage der Verarbeitung ist Paragraph 6 (1)(f) DSGVO, der die berechtigten Interessen von Milestone und die Nutzer des VMS zeigt.

Zusätzliche Sicherungen

Um besser zu gewährleisten, dass die Konfiguration des Milestone XProtect VMS der DSGVO entspricht, finden Sie in dieser Liste einige zusätzliche Sicherheitsvorkehrungen, die Sie bei der Konfiguration des Systems beachten sollten.

Problem	Negative Auswirkungen auf den Datenschutz	Hinweise für den für die Verarbeitung Verantwortlichen
Die PTZ-Kameras und Privatsphärenausblendung arbeiten nicht zusammen. Die unkenntlich gemachten Bildbereiche folgen nicht den PTZ-Bewegungen.	Die Wirkung der unkenntlich gemachten Bildbereiche zugunsten der Privatsphäre kann umgangen werden.	Milestone empfiehlt Ihnen eine der folgenden Maßnahmen:

Problem	Negative Auswirkungen auf den Datenschutz	Hinweise für den für die Verarbeitung Verantwortlichen
		• Sie sollten die XProtect eingebaute Funktion zur Unkenntlichmachung von Bildbereichen zum Schutz der Privatsphäre bei PTZ-Kameras nicht verwenden, da sich die Maske im Verhältnis zu den dekodierten Pixeln des Bildes statisch ist, nicht auf die tatsächliche Richtung / Position der PTZ-Kamera. • Deaktivieren Sie die PTZ-Funktion, wenn Sie Bildbereiche unkenntlich machen. • Erwerben Sie PTZ-Kameras, die eine dynamische Unkenntlichmachung von Bildbereichen zum Schutz der Privatsphäre unterstützen (damit die ausgewählten Bereiche immer unkenntlich gemacht werden, unabhängig von der Position und dem Zoomfaktor der Kamera).
Die Verwendung von Mikrofonen oder Metadatengeräten kann	Die Art der Verwendung von Mikrofonen kann leicht gegen die DSGVO verstoßen.	Bevor Sie Mikrofone oder Metadatengeräte in Betrieb nehmen, müssen muss

Problem	Negative Auswirkungen auf den Datenschutz	Hinweise für den für die Verarbeitung Verantwortlichen
die persönliche Privatsphäre beeinträchtigen. (In XProtect Corporate sind diese standardmäßig deaktiviert.)	Beachten Sie bitte: Die Verwendung von Mikrofonen und Metadatengeräten wird nicht durch das Europäische Datenschutzgütesiegel abgedeckt. Ihre Aktivierung würde gegen das EuroPriSe-Siegel verstoßen.	gewährleistet sein, dass Sie für die Datenerfassung einen klar begründeten Zweck haben. Siehe Haben Sie eine Rechtsgrundlage dafür, Daten zu erheben? auf Seite 30
Bediener und Administratoren können Videodaten, Videoarchive, Konfigurationssicherungen und Prüfprotokolle auf lokale Festplatten oder Wechselmedien wie CDs, DVDs, USB-Sticks usw. exportieren oder kopieren.	Personenbezogene Daten verlassen die Grenzen von XProtect VMS. Die Daten sind nicht mehr durch die Zugriffskontrollmechanismen von XProtect VMS geschützt und können von XProtect VMS nicht mehr gelöscht werden, wenn die Aufbewahrungsfrist verstrichen ist. Dies bringt das Risiko mit sich, dass die Daten länger gespeichert werden als erlaubt, dass sie für andere Zwecke verwendet werden und dass die Vertraulichkeit der Daten verletzt wird.	Die für die Verarbeitung Verantwortlichen müssen technische und organisatorische Maßnahmen ergreifen, um Daten zu schützen, die die Grenzen von XProtect VMS verlassen. Mögliche Maßnahmen, die Sie ergreifen können, finden Sie unter Umgang mit exportierten Daten auf Seite 22.
Audit-Protokolldaten und sonstige personenbezogene Daten werden vom Produkt erst verschlüsselt, wenn sie in den SQL Server-Datenbanken gespeichert werden. Datenbankadministratore	Insbesondere können die sensiblen Audit-Protokolldaten unbefugten Benutzern zugänglich gemacht werden. Siehe Schutz der gespeicherten und übertragenen Daten auf Seite 49. Weitere Informationen dazu, wie Sie Ihre XProtect VMS-Installationen vor Cyber-Angriffen schützen, finden Sie im Schutzleitfaden.	Führen Sie folgende Schritte aus: • Führen Sie für die Datenbankverwaltung ein adäquates Rollenkonzept ein.

Problem	Negative Auswirkungen auf den Datenschutz	Hinweise für den für die Verarbeitung Verantwortlichen
n können über Datenbank-Clients auf Auditprotokolldaten zugreifen. XProtect Corporate kann diesen Zugriff weder kontrollieren noch protokollieren.		• Beschränken Sie den Zugriff auf die Datenbank ausschließlich auf befugtes Personal. • Aktivieren Sie möglichst die Verschlüsselung der Datenbank mithilfe von Datenbankmechanisme n.
Die Sicherungen der SQL Server Konfigurationsdatenbank sind nicht verschlüsselt.	Legen Sie ein Passwort für die Systemkonfiguration zum Schutz sensibler Kontoinformationen in einer Erweiterung zur Verschlüsselung der SQL Server Datenbank fest. Sicherungen der SQL Server Konfigurationsdatenbank werden automatisch verschlüsselt, wenn die Konfigurationsdatenbank passwortgeschützt ist.	Schützen Sie die Gesamtsystemkonfiguration, indem Sie ein Passwort für die Systemkonfiguration festlegen. Sobald Sie ein Passwort für die Systemkonfiguration festgelegt haben, werden alle Backups mit diesem Passwort geschützt. Die Passworteinstellungen werden auf demjenigen Computer gespeichert, auf dem der Management Server in einem sicheren Ordner läuft. Sie benötigen dieses Passwort für: • Die Wiederherstellung der Konfiguration aus einem Backup, das mit anderen Passworteinstellungen erstellt wurde als den aktuellen

Problem	Negative Auswirkungen auf den Datenschutz	Hinweise für den für die Verarbeitung Verantwortlichen
		• Umzug oder Installation des Management Servers auf einem anderen Computer aufgrund eines Hardwarefehlers (Wiederherstellung) • Die Konfiguration eines zusätzlichen Management Servers in einem System mit Clustering Weitere Informationen finden Sie im Administratorhandbuch für XProtect VMS.
Das Produkt richtet eine Sicherungsfunktion ein. Diese Funktion sorgt für die Sicherung der Konfiguration des VMS, jedoch nicht der Audit-Log-Datenbank.	Die physische Zerstörung des Datenträgers, auf dem sich die Auditprotokolldatenbank befindet, kann den für die Verarbeitung Verantwortlichen daran hindern, seinen Rechenschaftspflichten nachzukommen, wenn keine Sicherungskopien der Auditprotokolle existieren.	Erwägen Sie die Erstellung von Sicherungskopien der Auditprotokolldatenbank. Wenn der Verantwortliche für die Verarbeitung beschließt, Sicherungskopie der Auditprotokolldatenbank zu erstellen, sollte auch ein Prozess eingerichtet werden, um die Sicherungskopien nach Ablauf der Aufbewahrungsfrist zu löschen und sie vor unberechtigtem Zugriff zu schützen (z. B. indem die Sicherungskopien verschlüsselt oder die Sicherungsmedien eingeschlossen werden usw.). Weitere Informationen finden Sie im Administratorhandbuch für XProtect VMS.

Problem	Negative Auswirkungen auf den Datenschutz	Hinweise für den für die Verarbeitung Verantwortlichen
Der Betrieb eines VPN im Split-Modus kann möglicherweise die IP-Adresse von XProtect VMS-Benutzern offenlegen.	Wenn Split-Tunneling aktiviert ist, umgehen Benutzer Sicherheitsmaßnahmen auf Gateway-Ebene, die innerhalb der Netzwerk-Infrastruktur vorhanden sein können.	Führen Sie folgende Schritte aus: • Verwenden Sie eine sichere VPN-Verbindung (ein VPN ist grundsätzlich sicher, aber einige alte VPN-Protokolle verschlüsseln die zwischen Server und Client ausgetauschten Daten nicht) • Verwenden Sie stets vollständiges Tunneling • Verwenden Sie die höchsten unterstützten Authentifizierungs-Protokolle (falls vorhanden) • Verwenden Sie Active Directory, um VPN-Benutzer zu authentifizieren Weitere Informationen dazu, wie Sie Ihre XProtect VMS-Installationen vor Cyber-Angriffen schützen, finden Sie im Schutzleitfaden.
Das Produkt ermöglicht die Einstellung von Aufbewahrungszeiten für Audit-Protokolle, Videodaten, Alarme und sonstige personenbezogene Daten.	Wenn Sie die Aufbewahrungszeit auf zu lange Zeiträume einstellen, kann dies gegen die Anforderungen für die Speicherbegrenzung laut DSGVO verstoßen (Paragraph 5 (1)(e) und Paragraph 17 DSGVO).	Die Aufbewahrungszeiten müssen sich nach den Verarbeitungszwecken richten (siehe Das Recht, vergessen zu werden (Recht auf Löschung) auf Seite 40).

Problem	Negative Auswirkungen auf den Datenschutz	Hinweise für den für die Verarbeitung Verantwortlichen
Der Administrator kann E-Mail-Empfänger konfigurieren, die bei bestimmten Ereignissen vom VMS Ausschnitte oder Standbilder aus Videoaufzeichnungen erhalten können. Für solche E-Mail-Empfänger kann keine Whitelist mit erlaubten Domänen konfiguriert werden.	Ein Tippfehler könnte zu einem Verstoß gegen den Datenschutz führen, wenn Dritte E-Mails mit Videodaten und Systemalarmen erhalten.	Der für die Verarbeitung Verantwortliche ist über diese Gefahr aufzuklären. Milestone empfiehlt, einen organisatorisches Verfahren einzurichten, z. B. das Vier-Augen-Prinzip, der das Risiko von Fehlern bei der Eingabe von E-Mail-Adressen senkt.
Benachrichtigungen sind E-Mails, die an eine bestimmte E-Mail-Adresse gesendet werden. Beim Erstellen einer Benachrichtigung kann der Administrator wählen, ob er mehrere Schnappschüsse oder eine AVI einer Sequenz mit einschließen möchte.	Da die angehängten Momentaufnahmen und AVI-Sequenzen in den Benachrichtigungen das VMS verlassen, befinden sie sich für die Zwecke des Benutzerzugriffs und der Aufbewahrung nicht mehr unter der Kontrolle des VMS.	Da E-Mails und deren Inhalte hinsichtlich Zugriff und Aufbewahrung der Kontrolle durch das VMS entzogen sind, wird empfohlen, keine Bilder oder AVI-Sequenzen an E-Mail-Benachrichtigungen anzuhängen. Wenn der Kunde diese Funktion benötigt, muss er zumindest sicherstellen, dass es organisatorische Verfahren und Kontrollen dafür gibt, wer die E-Mails erhält und wie damit umgegangen wird. Siehe Umgang mit exportierten Daten in Benachrichtigungen und E-Mails auf Seite 23.
Wenn Push-Benachrichtigungen aktiviert sind, verarbeitet der Anbieter des mobilen Betriebssystems (d. h.	Obwohl die Daten anonymisiert werden sollen, kann Milestone nicht garantieren, dass Google und Apple aus den von ihnen verarbeiteten Daten keine personenbezogenen Daten ableiten	Gemäß Artikel 49 (1)(a) der DSGVO ist eine Zustimmung des VMS-Anwenders erforderlich, wenn die Push-Benachrichtigung aktiviert ist.

Problem	Negative Auswirkungen auf den Datenschutz	Hinweise für den für die Verarbeitung Verantwortlichen
Google oder Apple) Daten, um die Push-Benachrichtigungen an die Smartphones zu senden.	können. Die Anbieter des mobilen Betriebssystems (d. h. Google oder Apple) verwenden ein Schema zur Adressierung von Nachrichten. Dieses Schema umfasst Registrierungs-Tokens und Installations-IDs der mobilen Client-App. Damit können Anbieter die Nachrichten an die entsprechenden Apps auf den Geräten zustellen. Für Google und Apple sind das Token und die Installations-ID pseudonymisiert.	Es wird empfohlen, die Einwilligung einzuholen oder andernfalls Push-Nachrichten zu deaktivieren.
Mit XProtect Incident Manager können Organisationen Vorfälle dokumentieren und sie mit Sequenzbeweisen (Video und ggf. Audio) aus ihrem XProtect VMS VMS kombinieren. Verantwortliche oder Anwender können Vorfallberichte erstellen, die Informationen in Textform enthalten, die einem Vorfallprojekt hinzugefügt wurden. Diese Berichte können die personenbezogenen Daten des Verantwortlichen oder Anwenders enthalten, d. h. ihren Namen.	Wenn Vorfallberichte außerhalb des Umfelds des Verantwortlichen oder des Anwenders verfügbar gemacht werden, könnten personenbezogene Daten offengelegt werden. Verantwortliche oder Anwender sollten nur dann Berichte mit eindeutigen, identifizierbaren Namen des Verantwortlichen oder Anwenders erstellen, wenn je nach Zweck und Empfänger des Berichts ein eindeutiger Bedarf dafür besteht.	Geben Sie die Namen des Verantwortlichen oder des Anwenders nur dann in den Vorfallberichten an, wenn es einen bestimmten und angemessenen Zweck für die Angabe der Namen gibt. Verantwortliche oder Anwender sollten das Kontrollkästchen **Benutzernamen anzeigen** nur dann aktivieren, wenn es einen bestimmten und angemessenen Zweck gibt, die Namen in den Bericht aufzunehmen.
Verantwortliche oder Anwender können Alarmberichte mit	Wenn Alarme außerhalb des Umfelds des Verantwortlichen oder des Anwenders verfügbar gemacht werden, könnten personenbezogene Daten offengelegt	Geben Sie die Namen des Verantwortlichen oder des Anwenders nur dann in den Alarmberichten an, wenn es

Problem	Negative Auswirkungen auf den Datenschutz	Hinweise für den für die Verarbeitung Verantwortlichen
Informationen zum Alarm ausdrucken, einschließlich des Alarmverlaufs und eines Standbilds vom Zeitpunkt, an dem der Alarm ausgelöst wurde, sofern verfügbar. Diese Berichte können die personenbezogenen Daten des Verantwortlichen oder Anwenders enthalten, d. h. ihren Namen.	werden. Verantwortliche oder Anwender sollten nur dann Berichte mit eindeutigen, identifizierbaren Namen des Verantwortlichen oder Anwenders erstellen, wenn je nach Zweck und Empfänger des Berichts ein eindeutiger Bedarf dafür besteht.	einen bestimmten und angemessenen Zweck für die Angabe der Namen gibt. Verantwortliche oder Anwender sollten das Kontrollkästchen **Namen anzeigen** nur dann aktivieren, wenn es einen bestimmten und angemessenen Zweck gibt, die Namen in den Bericht aufzunehmen.
Alarmberichte können Bilder mit Passanten enthalten.	Falls die Berichte an Dritte weitergegeben werden, verletzt dies unter Umständen die Rechte unbeteiligter Passanten.	Erwägen Sie, die Bilder auf den PDF-Berichten oder Ausdrucken manuell zu schwärzen oder zu maskieren.

Anhang: Datenverarbeitung in der Milestone XProtect VMS Umgebung

Das *Milestone Dokument zur Systemarchitektur* beschreibt die Systemkomponenten und die Art und Weise, wie diese miteinander und mit den Systemkomponenten in der Umgebung zusammenarbeiten. Für jeden der relevanten Anwendungsfälle für das Produkt finden Sie ein Diagramm, das den Kommunikationsfluss zwischen den Komponenten illustriert, die an den Anwendungsfällen beteiligt sind. Diese Diagramme geben eine allgemeine Übersicht über die übertragenen Daten. Weitere Informationen über die Interaktion zwischen den einzelnen Komponenten Milestone XProtect VMS finden Sie im Milestone Dokument zur Beschreibung der Systemarchitektur.

In diesem Abschnitt sind die Standardinstallationsverfahren für XProtect für persönliche Daten, Authentifizierungs- und Konfigurationsdaten aufgeführt, die für Datenschutz- und Sicherheitseinstellungen relevant sind.

Personenbezogene Daten aus dem VMS

Der Hauptdatentyp sind die Videodaten von den Videokameras. Diese Daten werden vom Recording Server Dienst gespeichert. Videodaten können entweder live oder im Wiedergabemodus an den XProtect Smart Client gestreamt werden. Die übrigen Daten sind die Stammdaten der VMS-Benutzer, die in der SQL Server-Datenbank gespeichert werden.

Personenbezogene Daten aus der Umgebung

Personenbezogene Daten zu den VMS-Benutzern stammen unter zwei Umständen aus der Umgebung:

- In einer Windows-Umgebung, in der Active Direct (AD) für die Benutzerauthentifizierung und als Quelle für Gruppenmitgliedschaften verwendet wird. Der Dienst Milestone XProtect Management Server fragt über das LDAP-Protokoll das AD ab, um Informationen über die Benutzer zu erhalten, die sich am System anmelden.
- Von externen Third-Party IDP-Diensten, bei denen Basisnutzer in diesem Dienst verwaltet werden.

Personenbezogene Daten aus dem System

Diese personenbezogenen Daten beinhalten Daten jeder Art, die dafür benötigt werden, das System zu sichern, zu konfigurieren, zu betreiben, zu warten oder in sonstiger Weise zu unterstützen. Arten personenbezogener Daten sind u.a.:

- Protokolldaten

  IT-Systeme protokollieren in der Regel Benutzer- und Systemdaten in Audit- und Debug-Protokolldateien, um beim Betrieb und bei der Wartung der Systeme zu helfen. XProtect Corporate tut dies ebenfalls. Das VMS protokolliert Informationen über Benutzeraktionen und speichert sie in Log Server (SQL Server). Dieses Audit-Protokoll dient dazu, die Verantwortlichkeit für vergangene Maßnahmen und das Systemverhalten nachzuvollziehen, sowie um ggf. Missbrauch des Systems zu verfolgen. Debug-Protokolle dienen dazu, Defekte und Fehler im System zu erkennen. Die Debug-Daten enthalten keine personenbezogenen Daten.

  Die Protokolleinträge können detaillierte Informationen über die Nutzung des Systems durch die Bediener und Administratoren enthalten und eignen sich ggf. zur Überwachung des Verhaltens und der Leistung von Mitarbeitern.

- Protokollierung der Authentifizierung

  Der Authorization Server Duende OAuth und Identity Provider (IDP) erstellen Auditprotokoll-Dateien. Diese Dateien werden im Log Server (SQL Server), gespeichert, und aus allen Debug-Protokollen wurden personenbezogene Daten und Identitätskennzeichen entfernt. Diese Auditprotokolle können über den XProtect Management Client eingesehen werden.

Authentifizierung und Authentifizierungsdaten

- Authentifizierung des Benutzers im VMS

  Es gibt drei Optionen zur Authentifizierung von VMS-Benutzern von XProtect Management Client und XProtect Smart Client. Sie können entweder die Anmeldemechanismen von Windows, die VMS-eigene Authentifizierung oder einen externen IDP verwenden.

  Eine Windows Active Directory-Umgebung können Sie so konfigurieren, dass die eingebauten Anmeldemechanismen von Windows verwendet werden. Die Authentifizierung mit der Windows-Anmeldung basiert standardmäßig auf dem Kerberos-Protokoll. Dies ist die sicherste Option. In älteren Umgebungen unterstützen die Domain Controller Kerberos u.U. nicht. In diesem Fall greift die Windows-Anmeldung automatisch auf das LAN-Manager-Protokoll (NTLMv2) zurück, das als weniger sicher gilt als Kerberos.

  In Umgebungen ohne Windows-Domänencontroller können Sie die systemeigene Authentifizierungsmethode XProtect verwenden. Dies ist die Basis-Authentifizierung mit Benutzer-ID und Kennwort gegenüber der lokalen Identity Provider Authentifizierung oder die Authentifizierung von Windows für Arbeitsgruppen, sofern diese zur Verfügung steht.

  Alternativ können Sie einen externen IDP verwenden. Ein externer IDP ist eine externe Anwendung und ein Dienst, in dem Sie Angaben zur Identität der Benutzer speichern und verwalten und Dienste zur Benutzerauthentifizierung für andere Systeme bereitstellen können. Sie können einen externen IDP mit dem XProtect VMS verknüpfen.

  > Um den Datenschutz zu gewährleisten, sollten Sie keine IDPs von Drittanbietern aus dem Internet verwenden. Wenn Sie einen externen IDP verwenden, muss er lokal installiert sein und von derselben Organisation oder Firma verwaltet werden, die auch das VMS betreibt.

  Es gibt drei Arten von Authentifizierungsnachweisen:

  - Windows-Anmeldungstokens (entweder Kerberos- oder NTLM-Tokens)
  - Basis-Authentifizierungsdaten
  - Die Authentifizierung von Windows für Arbeitsgruppen

  Nach erfolgreicher Authentifizierung wird der Benutzer am VMS angemeldet, und von dem Dienst Management Server wird eine Benutzersitzung erstellt, in der die Anmeldung erfolgt. Der Client hat nun im Kontext dieser Benutzersitzung Zugriff auf die Funktionen des Management Server Dienstes. Wenn der Benutzer auf Funktionen im Recording Server Dienstes zugreifen möchte, braucht auch der XProtect Smart Client eine Benutzersitzung bei diesem Serverdienst.

- Benutzerberechtigung in dem Recording Server Dienst

  Da die Sitzung eines Benutzers zwischen dem XProtect Smart Client / XProtect Management Client und dem Dienst Management Server nicht wiederverwendet werden kann, um auf Recording Serverzuzugreifen, muss der Recording Server auch den Benutzer autorisieren. Um sich bei dem Dienst Recording Server zu autorisieren, stellt der Dienst Management Server dem Kunden ein Autorisierungs-Token zur Verfügung, das der Kunde dem Dienst Recording Server gegenüber vorweisen muss. Gleichzeitig sendet der Dienst Management Server das Autorisierungs-Token an alle Recording Server-Dienste in der VMS-Installation. Diese können wiederum zur späteren Autorisierung von Benutzern verwendet werden.

  XProtect VMS verwendet eine einfache GUID als so ein Autorisierungs-Token, das der Client an den Recording Server-Dienst sendet. Die GUIDs werden dann von dem Management Server Dienst erstellt und verwaltet, der diese Tokens nach einer gewissen Zeit erneuert. Die GUID ist schlicht eine Kennung für den Benutzer in der SQL Server Datenbank.

- Authentifizierungsdaten

  Die Authentifizierungsdaten für VMS-Benutzer werden in der SQL Server-Datenbank auf SQL Server gespeichert. Zum Startzeitpunkt ziehen die Dienste Management Server und Recording Server die entsprechenden Autorisierungsdaten, einschließlich der Authentifizierungstokens, für alle Benutzer aus der SQL Server-Datenbank, um spätere Zugriffe auf die Server durch Benutzer vorbereitet zu sein. Wenn ein Administrator Berechtigungen oder Rollen oder irgendetwas anderes ändert, das Auswirkungen auf die Benutzerberechtigungen hat, wird diese Aktualisierung vom Dienst Management Server in der SQL Server-Datenbank auf SQL Server gespeichert und außerdem aktiv an alle Recording Server Dienste weitergegeben. Die Recording Server Dienste speichern Benutzerautorisierungsdaten und alle Authentifizierungstoken lokal und können so Client-Benutzer sofort authentifizieren, die ihre Authentifizierungstokens vorweisen können.

- Konfigurationsdaten

  Abgesehen von den Ansichtsdaten, die über den XProtect Smart Client eingestellt werden, werden alle Konfigurationsdaten für das VMS-System über den XProtect Management Client des VMS konfiguriert und in der SQL Server-Datenbank gespeichert. Es gibt verschiedene Arten von Konfigurationsdaten:

  - Benutzereinstellungen und Präferenzen
  - Benutzerrechte
  - Serverkonfiguration
  - Systemeinstellungen
  - Kamera- und Gerätekonfiguration

  Wenn die Konfigurationsdaten auch keine personenbezogenen Daten enthalten mögen, können sie Einfluss auf die Art und Weise haben, wie das VMS personenbezogene Daten verarbeitet. Nur für die Auswertung sind die Autorisierungsangaben und die Sicherheits- und Datenschutzeinstellungen unter den oben aufgeführten Konfigurationsdaten relevant.

Index

G

I

L

M

N

O

P

U

V

X

helpfeedback@milestone.dk

Info über Milestone

Milestone Systems ist ein weltweit führender Anbieter von Open-Platform-Videomanagementsoftware – Technologie, die Unternehmen hilft für Sicherheit zu sorgen, Ressourcen zu schützen und die Wirtschaftlichkeit zu erhöhen. Milestone Systems ist die Basis einer Open Platform Community, die die Zusammenarbeit und Innovation bei der Entwicklung und dem Einsatz von Netzwerkvideotechnologie vorantreibt und für zuverlässige, individuell anpassbare Lösungen sorgt, die sich an über 150.000 Standorten auf der ganzen Welt bewährt haben. Milestone Systems wurde 1998 gegründet und ist ein eigenständiges Unternehmen der Canon Group. Weitere Informationen erhalten Sie unter https://www.milestonesys.com/.