MAKE THE
WORLD SEE

Milestone Systems

Guida alla privacy in base al GDPR (Regolamento generale sulla protezione dei dati)

milestone

Cronologia del documento

Versione del documento	Release	Commenti
Versione 3	2021 R2	Gli aggiornamenti a questa release includono: • Misure di salvaguardia contro l'utilizzo di una VPN in modalità suddivisione aggiunte a Misure di salvaguardia aggiuntive a pagina 56.
Versione 2	2021 R1	Gli aggiornamenti a questa release includono: • Il tipo di utente di base è ora coperto dal marchio di certificazione europeo della tutela della privacy (Appendice: Il sistema Milestone XProtect VMS e il GDPR a pagina 53) e (Appendice: Trattamento dei dati nell'ambiente Milestone XProtect VMS a pagina 62). • Consigli aggiunti in Uso di sfondi geografici in XProtect Smart Client a pagina 55. • Raccolta dei dati descritta in Integrazioni di partner registrati a pagina 56. • Registrazione dell'autenticazione descritta in Dati personali del sistema a pagina 63.
Versione 1	2020 R3	Questa è la prima release del presente documento.

Sommario

Copyright, marchi e declinazione di responsabilità

Marchi

XProtect è un marchio registrato di Milestone Systems A/S.

Microsoft e Windows sono marchi registrati di Microsoft Corporation. App Store è un marchio di servizi Apple Inc. Android è un marchio registrato di Google Inc.

Tutti gli altri marchi citati in questo documento sono marchi di proprietà dei rispettivi titolari.

Declinazione di responsabilità

Questo documento ha un puro scopo informativo ed è stato preparato con la dovuta attenzione.

Qualunque rischio derivante dall'uso di queste informazioni è a carico dell'utente e nulla di quanto contenuto in questo documento può essere considerato una forma di garanzia.

Milestone Systems A/S si riserva il diritto di modificarlo senza notifica.

Tutti i nomi di persone e di organizzazioni utilizzati negli esempi del documento sono di fantasia. Qualunque somiglianza con organizzazioni o persone viventi o decedute è puramente casuale e non intenzionale.

Questo prodotto può fare uso di software di terze parti a cui possono applicarsi clausole e condizioni specifiche. In tal caso è possibile trovare ulteriori informazioni nel file 3rd_party_software_terms_and_conditions.txt disponibile nella cartella di installazione del sistema Milestone.

Conformità al GDPR e Milestone XProtect VMS

Il 25 maggio 2018, è entrato in vigore il Regolamento generale sulla protezione dei dati (General Data Protection Regulation, GDPR) europeo. L'obiettivo di questo regolamento è fornire agli individui maggiore controllo della modalità con cui i loro dati personali vengono raccolti, trattati e condivisi.

Il GDPR fornisce una struttura per le aziende che chiarisce i loro ruoli e responsabilità e offre agli individui l'opportunità di controllare la modalità di uso dei loro dati personali.

Il presente documento rappresenta una panoramica dei requisiti e di come è possibile lavorare con la conformità al GDPR durante l'uso del sistema di gestione video (Video Management System, VMS) XProtect.

Per informazioni specifiche su come migliorare la conformità di un sistema Milestone XProtect VMS al GDPR, vedere Appendice: Il sistema Milestone XProtect VMS e il GDPR a pagina 53.

Declinazione di responsabilità: Le informazioni contenute nel presente documento ed eventuali consigli sono forniti così come sono. Seguire il presente documento non significa in modo implicito che il sistema sarà conforme al GDPR.

Milestone XProtect VMS richiede la configurazione. Qualsiasi configurazione o modifica delle impostazioni deve essere conforme alla legge sulla protezione dei dati dell'UE. Sebbene Appendice: Il sistema Milestone XProtect VMS e il GDPR a pagina 53 e Misure di salvaguardia aggiuntive a pagina 56 forniscano informazioni su come avviare una configurazione conforme, è necessario rispettare le leggi sulla protezione dei dati dell'UE nel configurare ulteriormente il sistema.

Che cos'è il GDPR?

Il Regolamento generale sulla protezione dei dati (GDPR) è una serie di regole che governa tutte le forme di dati personali detenuti da un'organizzazione. Il GDPR assegna a ogni individuo la proprietà dei dati personali e, sul lato organizzazione, introduce la responsabilità in tutte le fasi del trattamento e della memorizzazione dei dati. Il GDPR realizza ciò fornendo diversi diritti agli individui e imponendo obblighi corrispondenti alle organizzazioni che trattano i dati personali.

Il GDPR armonizza le leggi sulla privacy dei dati in tutta l'UE e completa le normative nazionali esistenti su video sorveglianza e CCTV.

Sebbene il GDPR sia un regolamento dell'UE, riguarda molte altre parti del mondo.
Si applica al trattamento dei dati personali da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione europea, indipendentemente dal fatto che il trattamento avvenga nell'Unione europea o meno.
Si applica al trattamento dei dati personali da parte di un titolare del trattamento o di un responsabile del trattamento che non ha sede nell'Unione europea, dove le attività di trattamento sono correlate all'offerta di beni o servizi agli interessati nell'Unione europea o si applica al monitoraggio di questo comportamento purché avvenga all'interno dell'Unione europea.
Inoltre, molte altre parti del mondo stanno applicando normative di protezione della privacy simili, in base ai principi fondamentali del GDPR.

Il rispetto del GDPR è affidato alle autorità nazionali.

In caso di violazione vengono applicate ingenti sanzioni:

- Fino al 4% del reddito annuale mondiale dell'azienda
- Fino a 20 milioni di euro per incidente

Chi è responsabile di assicurarsi che un sistema di gestione video XProtect in esecuzione sia conforme al GDPR?

Il proprietario del VMS è responsabile della conformità al regolamento GDPR, incluso quanto segue:

- Installazioni effettive e utilizzo applicato
- Procedure e predisposizione organizzative
- Notifica di violazione dei dati e segnalazione alle autorità

Il GDPR non si applica a eventuali prodotti specifici, ma la combinazione del prodotto, dei dati che tratta e dell'utilizzo del prodotto e dei dati, tutti influiscono sulla conformità al GDPR.

Il GDPR ha implicazioni dirette per installatori, integratori di sistema e utenti della tecnologia di video sorveglianza.

Il proprietario del VMS è il titolare del trattamento (vedere Titolare del trattamento a pagina 14).

Il titolare del trattamento potrebbe esternalizzare parti o le intere operazioni del VMS a un responsabile del trattamento, ad esempio una società di sicurezza. In questo caso, il titolare del trattamento e il responsabile del trattamento devono applicare un *contratto del responsabile del trattamento*. Il *contratto del responsabile del trattamento* stabilisce quali dati vengono trattati e per quanto tempo vengono conservati (vedere Responsabile del trattamento a pagina 22 e Appendice: Contratto del responsabile del trattamento a pagina 52).

Tutte le installazioni per la video sorveglianza devono conformarsi al GDPR?

Il GDPR si applica a titolari del trattamento e responsabili del trattamento all'interno dell'Unione europea, indipendentemente da dove il video viene elaborato.

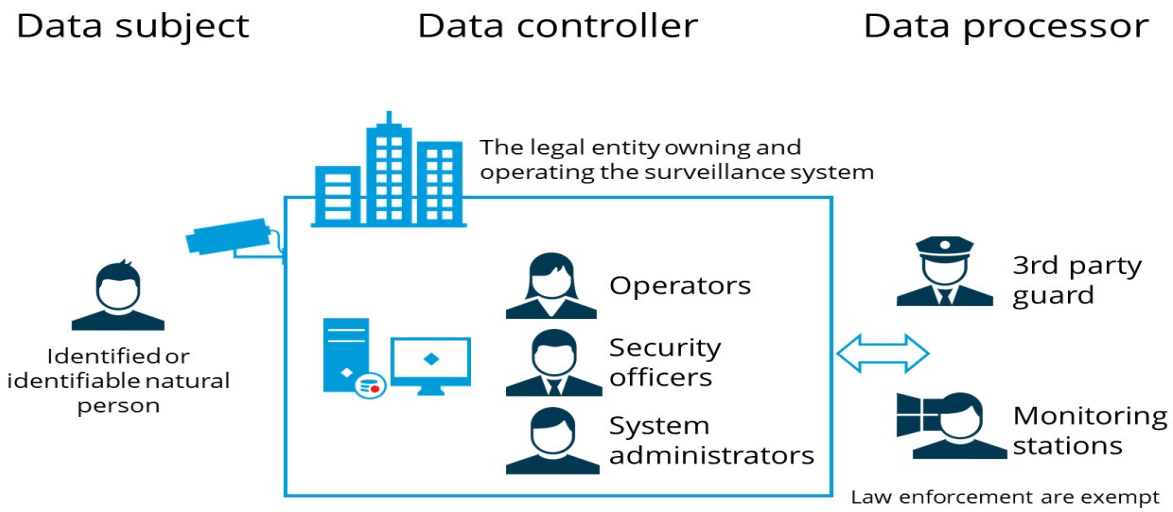
Inoltre, il GDPR protegge la privacy di qualsiasi residente dell'area geografica dell'UE, copre tutte le forme di video sorveglianza all'interno dell'UE e protegge i cittadini di tutti i Paesi che risiedono nell'UE (articolo 3, GDPR).

Per ulteriori informazioni sul GDPR, in particolare in relazione alla video sorveglianza, vedere Appendice: Conformità al GDPR a pagina 26.

Quali sono le parti interessate chiave del GDPR correlate alla video sorveglianza?

Quando si tratta di GDPR e video sorveglianza, esistono tre classi di parti interessate. Questa sezione del documento definisce ogni parte interessata e descrive le rispettive responsabilità rispetto al GDPR.

- Interessato a pagina 9
- Titolare del trattamento a pagina 14
- Responsabile del trattamento a pagina 22



Interessato

L'interessato è qualsiasi persona i cui dati personali vengono raccolti, conservati o trattati.

Gli interessati sono gli oggetti visualizzati della video sorveglianza, sia intenzionali che accidentali.

Gli interessati sono anche qualsiasi persona registrata coinvolta nel funzionamento del VMS, ad esempio, operatori o guardie di terze parti nominate.

L'obiettivo chiave del GDPR è salvaguardare i dati personali di questi interessati.

Diritti dell'interessato

Gli articoli da 12 a 23 del GDPR riguardano i diritti dell'interessato.

- Sezione 1: Trasparenza e modalità
  - Articolo 12: Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato
- Sezione 2: Informazione e accesso ai dati personali
  - Articolo 13: Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato
  - Articolo 14: Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato
  - Articolo 15: Diritto di accesso dell'interessato (vedere Diritto di accesso a pagina 33)
- Sezione 3: Rettifica e cancellazione
  - Articolo 16: Diritto di rettifica
  - Articolo 17: Diritto alla cancellazione ("diritto all'oblio") (vedere Diritto all'oblio (diritto alla cancellazione) a pagina 34)
  - Articolo 18: Diritto di limitazione del trattamento (vedere Diritto di limitazione del trattamento a pagina 36)
  - Articolo 19: Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento
  - Articolo 20: Diritto alla portabilità dei dati
- Sezione 4: Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche
  - Articolo 21: Diritto di opposizione
  - Articolo 22: Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione
- Sezione 5: Limitazioni
  - Articolo 23: Limitazioni

Di questi, i diritti più pertinenti nel contesto di video sorveglianza sono:

Il diritto all'informazione (articoli da 12 a 14 e 34, GDPR)	L'articolo 12 riguarda trasparenza e modalità, mentre l'articolo 13 e 14 concerne informazioni e accesso ai dati personali. Questi articoli forniscono all'interessato la capacità di essere informato in merito a quali dati personali vengono raccolti e per quanto tempo vengono conservati. Nel contesto del VMS, vedere Appendice: Avviso sul posto a pagina 47. L'articolo 34 fornisce all'interessato il diritto di essere informato in caso di una violazione dei dati se probabilmente determinerà un alto rischio per i diritti e le libertà dell'interessato stesso.

Il diritto di accesso (articolo 15, GDPR)	Questo diritto assegna all'interessato la capacità di ottenere l'accesso ai suoi dati personali in fase di trattamento, ad esempio, le sue videoregistrazioni. All'interessato viene concesso il diritto di chiedere a un'azienda informazioni su quali dati personali che lo riguardano vengono trattati e il motivo di tale trattamento.
Il diritto alla cancellazione ("diritto all'oblio") (articolo 17, GDPR)	Questo diritto fornisce all'interessato la capacità di chiedere l'eliminazione dei suoi dati. Nel contesto del VMS, la cancellazione in base alle richieste dell'interessato è eccezionale dovuta agli interessi del titolare del trattamento e ai periodi di conservazione brevi. Vedere Appendice: Politica di video sorveglianza a pagina 47 ed *Eliminazione parziale di registrazioni video* in Appendice: Il sistema Milestone XProtect VMS e il GDPR a pagina 53.
Il diritto di opposizione (articolo 21, GDPR)	Questo diritto fornisce all'interessato la capacità di opporsi al trattamento dei suoi dati personali. Nel contesto del VMS, altri interessi come interessi legittimi (rilevamento delle frodi, salute e sicurezza), obbligo giuridico (contabilità, antiriciclaggio) o anche adempimento contrattuale (contratti di lavoro) potrebbero prevalere sugli interessi e sui diritti dell'interessato. In tutti i casi, ciò deve essere completamente trasparente in modo che l'interessato possa sapere e opporsi. Se l'interessato si oppone, il titolare del trattamento deve valutare l'obiezione o altrimenti potrebbe incorrere in una sanzione.

Richiesta dell'interessato

L'azienda deve disporre di una procedura per la gestione delle richieste dei diritti dell'interessato, ad esempio eseguire il diritto di richiesta di accesso. Tale richiesta deve essere gestita entro un intervallo di tempo ragionevole. In base all'articolo 12 (3) del GDPR, ciò avviene "senza indebito ritardo e in ogni caso entro un mese dal ricevimento della richiesta". Si consiglia di utilizzare un modello di *richiesta dell'interessato* per documentare tali richieste, poiché può essere essenziale in un caso del GDPR con le autorità nazionali di protezione dei dati. Per un modello di esempio di una richiesta dell'interessato, vedere il modello di richiesta dell'interessato di *Milestone*.

La politica di video sorveglianza descrive la richiesta dell'interessato (vedere Appendice: Politica di video sorveglianza a pagina 47).

Cosa sono i dati personali?

Per essere conformi al GDPR, occorre sapere cosa sono i dati personali e limitare la raccolta ai soli dati necessari.

Secondo la normativa, i dati personali sono qualsiasi informazione correlata a una persona identificata o identificabile.

Una persona identificabile è qualcuno che può essere identificato direttamente o indirettamente, per riferimento a un identificatore come:

- Un nome
- Un numero di identificazione
- Dati sull'ubicazione
- Identificatore online come indirizzi IP o identificatore di cookie
- Dati utente
- Immagini video
- O per uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona

I dati personali sono qualsiasi tipo di informazione che direttamente o indirettamente può essere utilizzata per identificare una persona fisica (interessato). Sono i dati che possono essere utilizzati per identificare gli oggetti visualizzati della video sorveglianza, sia che si tratti di dati raccolti intenzionalmente che accidentalmente.

I dati personali protetti dal GDPR sono:

- Dati trattati dal prodotto IT o dal servizio basato sull'IT (ad esempio, nome e indirizzo di una persona, immagine video, dati di pagamento, dati sanitari).
- Dati generati accidentalmente quando viene utilizzato il prodotto o il servizio (ad esempio, dati sull'utilizzo, file di registro, dati statistici, dati per l'autorizzazione, dati di configurazione). Possono essere i dati personali degli utenti del servizio, i dati personali delle persone che utilizzano il prodotto o il servizio (possono includere sia il personale del fornitore di servizi che il personale degli utenti del prodotto o del servizio) o dati di configurazione pertinenti per la privacy (vedere Titolare del trattamento a pagina 14).

I dati personali sono definiti come qualsiasi informazione correlata a una persona fisica identificata o identificabile o l'interessato, ad esempio:

• Nome completo • Indirizzo dell'abitazione • Indirizzo e-mail • Numero di telefono • Dati sull'ubicazione • Identità digitale	• Targa del veicolo • Numero di patente del conducente • Numeri di carte di credito • Informazioni identificabili, immagini, ecc., come registrazioni video e fermi immagine • Attività utente, come quelle nei file di registro

Questi dati non sono necessariamente solo una relazione diretta con l'oggetto. I dati personali possono anche essere un quasi-identificatore. I quasi-identificatori sono parti di informazioni che non sono di per sé identificatori univoci ma sono sufficientemente ben correlati a qualcosa in modo da poterli unire con altri quasi-identificatori per creare un identificatore univoco. I quasi-identificatori sono particolarmente importanti quando si tratta di categorie speciali dei dati personali.

Le categorie speciali dei dati personali includono i dati che indicano origine razziale ed etnica, opinioni politiche, credi religiosi o filosofici, appartenenza a sindacati, dati genetici, dati biometrici, dati riguardanti lo stato di salute o dati relativi alla vita o all'orientamento sessuale, ad esempio:

• Anamnesi • Dati biometrici (inclusi foto, video, impronte digitali) • Fedina penale • Identità razziale o etnica	• Informazioni genetiche • Opinioni e impegni politici • Credi religiosi o filosofici • Storia e orientamento sessuali

Questi sono i dati personali potenzialmente raccolti da un sistema di video sorveglianza:

Quali tipi di descrizioni dei dati personali, memorizzati da XProtect, rientrano nell'ambito del GDPR?

I dati personali sono qualsiasi tipo di informazione che direttamente o indirettamente può essere utilizzata per identificare una persona fisica (interessato). Possono essere flussi di video sorveglianza, una singola immagine o una sequenza di video combinata con informazioni sull'ubicazione provenienti da telecamere e/o mappe a più

livelli, un'integrazione di controllo accesso che identifica una carta d'accesso personale e che la combina con un'ubicazione specifica o dati derivanti dalla funzione di riconoscimento del numero di targa (License Place Recognition, LPR) con o senza eventuali dati sull'ubicazione.

Per categorie speciali dei dati personali si intende quando la video sorveglianza è vicina a ospedali (dati correlati alle informazioni sanitarie) e carceri (condanne penali), riguarda l'attività politica (appartenenza ad associazioni), l'attività religiosa o immagini che rivelano l'orientamento sessuale (ad esempio, locali gay).

Per dati personali si intendono anche i dati utente (operatore, supervisore e amministratore), attività e registrazione attività utente. Include i registri utente personali di XProtect Smart Client, comprese le etichette temporali di connessione/disconnessione e la registrazione attività utente di flussi video, audio o metadati a cui si è avuto accesso, nonché la riproduzione e l'esportazione delle registrazioni.

Per assicurarsi di non violare i diritti personali, vedere Rischi inerenti con l'uso del VMS a pagina 51.

Titolare del trattamento

Nel contesto della video sorveglianza, i titolari del trattamento possiedono e utilizzano i sistemi di video sorveglianza. I titolari del trattamento sono l'ente giuridico che raccoglie, tratta e condivide i dati sull'interessato.

Quali sono le responsabilità del titolare del trattamento

I titolari del trattamento sono tenuti a rispettare i principi di protezione dei dati e adempiere ad alcuni obblighi specifici. Il titolare del trattamento deve implementare misure tecniche e organizzative appropriate per garantire ed essere in grado di dimostrare che il trattamento venga eseguito in conformità al GDPR. Ciò include anche:

- Applicazione e gestione di procedure e politiche di sicurezza delle informazioni per proteggere i dati personali. Tali procedure e politiche interne devono essere approvate al livello più alto all'interno dell'organizzazione e pertanto essere vincolanti per i tutti i membri del personale.
- Visualizzazione di una panoramica dei flussi di trattamento e dei registri dei dati personali, ad esempio registro delle attività di trattamento (articolo 30, GDPR) e un elenco di sistemi e archivi che gestiscono i dati personali (il sistema XProtect VMS e altri sistemi che contengono dati personali come registri del personale, contratti del responsabile del trattamento, ecc., incluse informazioni su come e dove avviene il flusso dei dati personali). Per un modello di esempio di un registro delle attività di trattamento, vedere il modello di registro delle attività di trattamento di *Milestone*.
- Implementazione di meccanismi che eseguono procedure e politiche interne, incluse le procedure di reclamo, per rendere effettive tali politiche. Include la creazione di un corso di formazione di sensibilizzazione sulla protezione dei dati e istruzioni per il personale. Il corso di formazione di sensibilizzazione è disponibile all'indirizzo https://www.milestonesys.com/solutions/services/learning-and-performance/.
- Definizione della politica di video sorveglianza (vedere Appendice: Politica di video sorveglianza a pagina 47). Questa politica deve fare riferimento alle leggi interne sulla video sorveglianza.

- Esecuzione delle valutazioni dell'impatto sulla protezione dei dati, in particolare per alcune operazioni di trattamento dei dati ritenute in grado di porre rischi specifici per i diritti e le libertà degli interessati, ad esempio, in virtù delle loro natura, del loro ambito o della loro finalità (vedere Appendice: Valutazione dell'impatto sulla protezione dei dati a pagina 49).
- Garanzia della trasparenza di queste misure adottate relativamente agli interessati e al pubblico in generale. I requisiti di trasparenza contribuiscono alla responsabilità dei titolari del trattamento (ad esempio, pubblicazione delle informative sulla privacy su Internet, trasparenza relativa alle procedure di reclami interne e pubblicazione in report annuali).
- Pubblicazione dell'informativa del diritto all'informazione (vedere Appendice: Avviso sul posto a pagina 47). Questa informativa informa gli individui interessati dalla finalità della sorveglianza, chi conserva i dati raccolti (titolare del trattamento) e la politica di conservazione.
- Assegnazione della responsabilità della protezione dei dati alle persone designate con responsabilità diretta della conformità alle leggi sulla protezione dei dati da parte delle loro organizzazioni. In particolare, nominare il responsabile della protezione dei dati (RDP).

Responsabile della protezione dei dati (RDP)

Ogni organizzazione deve disporre di un RPD incaricato o almeno un responsabile per la privacy assegnato.

Dall'inizio, i piani per installare o aggiornare un sistema di video sorveglianza devono essere comunicati all'RPD.

L'RPD deve essere consultato in tutti i casi e in maniera tempestiva per tutte le questioni correlate alla protezione dei dati personali trattati quando viene fornito o utilizzato il servizio.

L'RPD deve essere coinvolto in tutte le fasi del processo decisionale.

Le responsabilità dell'RPD includono:

- Partecipare alla definizione della finalità aziendale della video sorveglianza, ad esempio, prevenzione del crimine, rilevazione di frodi, verifica della qualità del prodotto o salute e sicurezza a livello pubblico e così via.
- Fornire commenti sulla bozza della politica di video sorveglianza dell'organizzazione, inclusi gli allegati (vedere Appendice: Politica di video sorveglianza a pagina 47), e correggere eventuali errori e suggerire miglioramenti
- Assistere nelle comunicazioni con le autorità di protezione dei dati nazionali o regionali
- Controllare i contratti con terze parti durante la condivisione di dati. Ossia, mantenimento e gestione del *contratto del responsabile del trattamento* (vedere Appendice: Contratto del responsabile del trattamento a pagina 52)
- Stilare report di conformità ed eseguire verifiche per ottenere la certificazione di terze parti che approva le misure interne adottate per garantire che la conformità gestisca, protegga e tuteli i dati personali in maniera efficiente

- Memorizzare e assicurarsi che il registro delle attività di trattamento e le valutazione dell'impatto sulla protezione dei dati (vedere Appendice: Valutazione dell'impatto sulla protezione dei dati a pagina 49) vengano aggiornati ogni volta che vengono apportate al VMS modifiche pertinenti alla protezione dei dati. Per un modello di esempio di un registro delle attività di trattamento, vedere il modello di registro delle attività di trattamento di *Milestone*.

Ruolo dei titolari del trattamento

Le seguenti sezioni descrivono le responaibilità dei rispettivi titolari del trattamento:

- Funzionario di sicurezza (supervisore del VMS) a pagina 16
- Amministratore di sistema del VMS a pagina 18
- Operatore del VMS a pagina 19

Funzionario di sicurezza (supervisore del VMS)

I supervisori o i funzionari di sicurezza sono responsabili dell'applicazione di un ambiente conforme al GDPR. I funzionari di sicurezza devono:

- Definire i diritti utente (vedere Gestione dei diritti utente a pagina 16)
- Rendere obbligatorio un corso di formazione di sensibilizzazione del personale (vedere Formazione sulla protezione dei dati a pagina 18)
- Contattare il responsabile della protezione dei dati (RPD) se si sospetta una non conformità al GDPR, ad esempio, nel caso di una violazione dei dati dei materiali video (vedere Appendice: Conformità al GDPR a pagina 26)
- Applicare e mantenere un livello di sicurezza generale alto. Per ulteriori informazioni su come proteggere le installazioni di XProtect VMS da attacchi informatici, vedere la Guida di rafforzamento.

Gestione dei diritti utente

Chi deve accedere alle risorse del VMS

Le organizzazioni devono:

- Limitare l'accesso utente a un numero ridotto di individui chiaramente identificati in base alla necessità di conoscere.
- Gestire i registri di attività e accessi utente.

I diritti di accesso devono essere limitati a un numero ridotto di individui chiaramente identificati in base alla rigorosa necessità di conoscere. Assicurarsi che gli utenti autorizzati possano accedere solo ai dati a cui i diritti di accesso si riferiscono. I criteri di controllo accesso devono essere definiti seguendo il principio del “privilegio minimo”: agli utenti del diritto di accesso deve essere concesso l'accesso solo a quelle risorse che sono strettamente necessarie per svolgere i loro compiti.

Durante la condivisione di un computer, Milestone consiglia agli operatori del VMS di non condividere l'account di accesso in Windows. Ciascun operatore deve disporre di un account individuale.

Inoltre, gli operatori del VMS non devono selezionare l'opzione che consente di memorizzare la password all'accesso al sistema VMS.

Solo il funzionario di sicurezza, l'amministratore di sistema o altri membri del personale specificamente nominati dal funzionario di sicurezza per questa finalità devono essere in grado di concedere, modificare o annullare i diritti di accesso di eventuali persone. Qualsiasi concessione, alterazione o annullamento dei diritti di accesso deve avvenire secondo i criteri stabiliti nella politica di video sorveglianza (vedere Appendice: Politica di video sorveglianza a pagina 47).

Coloro che dispongono dei diritti di accesso devono sempre essere individui chiaramente identificabili. Ad esempio, non devono essere allocati nomi utente e password generici o comuni a una società di sicurezza esternalizzata che impiega diverse persone per lavorare per l'organizzazione.

La politica di video sorveglianza deve chiaramente specificare e documentare l'architettura tecnica del sistema di video sorveglianza, chi ha accesso al video di sorveglianza e per quale finalità e in cosa consistono tali diritti di accesso. In particolare, occorre specificare chi ha il diritto di:

• Visualizzare o accedere al video in tempo reale • Azionare le telecamere PTZ (Pan/Tilt/Zoom) • Visualizzare o accedere al video registrato	• Esportare registrazioni e audit trail • Eliminare o rimuovere dispositivi (telecamere) ed eliminare eventuali registrazioni • Alterare eventuali dati dopo la configurazione iniziale

Inoltre, è necessario assicurarsi che solo coloro che necessitano dell'accesso alle seguenti funzioni del VMS ottengano queste autorizzazioni:

• Amministrare il VMS	• Leggere i registri attività utente • Avviare/Arrestare la registrazione

• Creare/Modificare/Visualizzare/Eliminare i segnalibri • Creare/Modificare/Visualizzare/Eliminare le protezioni prove • Rimuovere maschere privacy • Esportare nei percorsi definiti (ad esempio, esportare solo il formato XProtect, con crittografia, su un'unità condivisa)	• Creare/Modificare/Eliminare/Attivare/Bloccare/Rilasciare le preimpostazioni PTZ • Creare/Modificare/Eliminare/Avviare/Arrestare gli schemi di ronda PTZ • Autorizzazioni per audio, metadati, I/O ed eventi

Formazione sulla protezione dei dati

Tutto il personale con diritti di accesso, incluso il personale esternalizzato che svolge le operazioni CCTV giornaliere o la manutenzione del sistema, deve seguire un corso di formazione sulla protezione dei dati e deve aver acquisito familiarità con le disposizioni del GDPR nella misura pertinente ai suoi compiti. La formazione deve prestare particolare attenzione alla necessità di impedire la divulgazione del video di sorveglianza a chiunque diverso da individui autorizzati.

La formazione del personale è obbligatoria e deve includere:

- Sicurezza informatica
- Esportazione dei dati del VMS

La formazione deve tenersi quando viene installato un nuovo sistema, quando vengono apportate modifiche significative al sistema, quando un nuovo dipendente entra a far parte all'organizzazione e periodicamente successivamente a intervalli regolari. Per i sistemi esistenti, la formazione iniziale deve tenersi durante il periodo di transizione e periodicamente successivamente a intervalli regolari.

Per ulteriori informazioni sul GDPR per l'operatore del VMS, vedere la Guida alla privacy in base al GDPR di Milestone per operatori del VMS e il corso di e-learning sul GDPR di Milestone per operatori del VMS.

Amministratore di sistema del VMS

Gli amministratori di sistema sono responsabili della configurazione dell'ambiente di sistema conforme al GDPR. Gli amministratori di sistema, tra le altre cose, svolgono quanto segue:

- Applicare e mantenere un livello di sicurezza generale alto. Per ulteriori informazioni su come proteggere le installazioni di XProtect VMS da attacchi informatici, vedere la Guida di rafforzamento.
- Applicare un criterio per la password protetta
- Condurre verifiche della sicurezza

- Assicurarsi che i dispositivi registrino in base alla finalità definita, ad esempio, in base a evento, movimento, sempre attivi e così via
- Assicurarsi che il periodo di conservazione dei registri attività utente e delle registrazioni sia impostato in base alle legge locale e alla finalità definita del VMS
- Garantire la gestione degli utenti (aggiungere o rimuovere utenti)
- Assicurarsi, per quanto riguarda le telecamere, di seguire le leggi sulla privacy e di non registrare le aree con divieto di registrazione; mascherare tali aree per escluderle
- Contattare il responsabile della protezione dei dati (RPD) se si sospetta una non conformità al GDPR, ad esempio, nel caso di una violazione dei dati dei materiali video (vedere Appendice: Conformità al GDPR a pagina 26)

Operatore del VMS

Gli operatori del VMS devono seguire le procedure e le istruzioni di lavoro durante l'accesso ai dati nel sistema, ad esempio, durante la visualizzazione o l'esportazione di video e così via.

Per essere conformi al GDPR, gli operatori devono disporre di quanto segue:

- Una descrizione generale del GDPR e le regole per l'esportazione dei dati
- Formazione sul GDPR

  Gli operatori devono disporre di formazione adeguata sul sistema di video sorveglianza per garantire che la privacy e altri diritti fondamentali degli interessati ripresi dalle telecamere non vengano violati. Devono essere istruiti in merito a quali politiche di video sorveglianza definire (ad esempio, procedure di consegna delle prove video), chi contattare in caso di dubbi (persone da contattare per l'escalation come il supervisore o il responsabile della protezione dei dati) e così via (vedere Funzionario di sicurezza (supervisore del VMS) a pagina 16).

  Per ulteriori informazioni sul GDPR per l'operatore del VMS, vedere la Guida alla privacy in base al GDPR di Milestone per operatori del VMS e il corso di e-learning sul GDPR di Milestone per operatori del VMS.

Gestione dei dati esportati

L'esportazione viene eseguita quando si è verificato un incidente che richiede la condivisione della prova con le autorità. Se si dispone dei diritti utente per esportare la prova, si ha la responsabilità nel gestirla. Il motivo per cui sono dati sensibili è dovuto sia al contenuto sia al fatto che i dati escono dal sistema di sorveglianza. Molto probabilmente, si è verificato un incidente che può coinvolgere l'attività criminale. Potrebbero esserci anche dettagli privati sensibili nella prova. Quando si esportano, i dati vengono di solito memorizzati su un supporto di memorizzazione rimovibile dello stesso tipo (unità USB, disco ottico, ecc.).

Se tali dati finiscono nelle mani sbagliate, la privacy degli interessati nella prova andrebbe persa.

Occorre una procedura chiara per l'esportazione della prova, che includa:

- Chi può esportare la prova
- Dove viene conservata la prova finché non viene consegnata alle autorità
- Chi dispone dell'accesso
- Quali formati si devono utilizzare
- Se deve essere applicata la crittografia (fortemente consigliata)
- Quando viene distrutta la prova

I titolari del trattamento devono adottare misure tecniche e organizzative per proteggere i dati che escono da Milestone XProtect VMS. Tali misure potrebbero essere:

- Limitare l'autorizzazione per esportare video e registri attività utente solo al personale speciale
- Considerare la crittografia dei dati prima o dopo la loro esportazione
- Applicare maschere privacy prima di esportare i dati video, laddove appropriato
- Proteggere fisicamente i supporti rimovibili con i dati personali in essi contenuti
- Stabilire politiche per garantire che i dati personali vengano eliminati dai supporti in base al periodo di conservazione
- Tenere un registro di supporti rimovibili; chi ha esportato quali dati nei supporti? A chi sono stati inoltrati o per quale finalità? Il destinatario è stato informato di distruggere i supporti o di tornarvi dopo che la finalità è stata raggiunta? Ecc.
- Utilizzare criteri di gruppo Windows per disabilitare le porte USB o l'accesso ai supporti sui PC client
- Monitorare i registri attività utente per eventi di esportazione non autorizzati
- Far rispettare ai dipendenti la politica sulla protezione dei dati
- Purificare correttamente i supporti o eliminarli fisicamente se la purificazione non è possibile (ad esempio, DVD)

Per ulteriori informazioni sulla gestione delle esportazione dei dati, vedere il corso di e-learning del GDPR di Milestone per operatori del VMS.

Gestione dei dati esportati nelle notifiche ed e-mail

Oltre alle esportazioni, i dati possono essere estratti dal VMS anche tramite allegati alle notifiche. Le notifiche sono messaggi e-mail inviati all'indirizzo e-mail specificato. Durante la creazione di una notifica, l'amministratore può scegliere di includere una serie di istantanee o un'AVI di una sequenza. Poiché le istantanee e le sequenze AVI allegate presenti nelle notifiche escono dal VMS, sono fuori del controllo del VMS per quanto riguarda l'accesso utente e la conservazione. Si consiglia di non allegare immagini o sequenze AVI alle notifiche e-mail. Se sono necessari allegati, occorre almeno assicurarsi che esistano procedure e controlli organizzativi per chi riceve i messaggi e-mail e per come vengono gestiti.

Occorre una procedura chiara, che includa:

- Dove vengono conservati i dati

  Assicurarsi che i server e-mail di invio e ricezione siano sotto il controllo dell'organizzazione che è il titolare del trattamento/responsabile del trattamento della video sorveglianza. In particolare, i destinatari non devono essere account e-mail gratuiti come Gmail o Hotmail e così via.

- Chi dispone dell'accesso
- Quali formati si devono utilizzare
- Se deve essere applicata la crittografia SMTP

  Tenere presente quanto segue: Utilizzare un server di posta SMTP/SMTPS. È necessario crittografare la connessione tra il VMS e i server di posta in uscita, nonché tra i server SMTP di invio e ricezione per essere coperti dal marchio di certificazione europeo della tutela della privacy europeo. Una connessione crittografata e non protetta violerebbe il marchio di certificazione europeo della tutela della privacy (European Privacy Seal, EuroPriSe) e porterebbe alla perdita della conformità al marchio stesso.

- Quando vengono distrutti i dati

  Milestone consiglia di allineare il periodo di conservazione dei dati video nelle caselle postali in uscita e in entrata con il periodo di conservazione del database di supporti o con il periodo di conservazione di allarmi che potrebbero essere attivati dagli stessi eventi che hanno causato la notifica.

  Il periodo di conservazione nelle caselle postali deve essere limitato a un periodo che sia ragionevole per la finalità alla base del processo di notifica.

  Milestone consiglia di utilizzare solo caselle postali del titolare del trattamento/responsabile del trattamento e di configurare l'eliminazione automatica dei messaggi e-mail al termine del periodo di conservazione definito.

  I titolari del trattamento/responsabili del trattamento devono assicurarsi che queste caselle postali non vengano automaticamente archiviate dal sistema e-mail.

Violazione dei dati personali

Il GDPR definisce una "violazione dei dati personali" come "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati".

Nel caso di una violazione della sicurezza, l'RDP deve determinare se avvisare l'autorità di protezione dei dati e gli interessati coinvolti, ai sensi degli articoli 33 e 34 del GDPR.

Ai sensi dell'articolo 33 (1) del GDPR:

Nel caso di una violazione dei dati personali, il titolare del trattamento senza eccessivo ritardo e, laddove possibile, non oltre 72 ore dal momento in cui ne è venuto a conoscenza, comunicherà la violazione dei dati personali all'autorità di controllo competente ai sensi dell'articolo 55, a meno che non risulti improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Laddove la notifica all'autorità di controllo non sia stata presentata entro 72 ore, sarà accompagnata dai motivi del ritardo.

Se ritenuto necessario, il titolare del trattamento deve pubblicare la notifica di violazione dei dati entro 72 dall'avvenuta rilevazione della violazione (vedere Violazione dei dati personali a pagina 21). Per un modello di esempio di una notifica di violazione dei dati, vedere il modello di notifica di violazione dei dati di *Milestone*. Gli interessati devono essere avvisati anche se la violazione dei dati personali "probabilmente determinerà un alto rischio per i diritti e le libertà degli individui".

I responsabili del trattamento che subiscono una violazione dei dati personali devono avvisare il titolare del trattamento, ma altrimenti non hanno altro obbligo di notifica o segnalazione ai sensi del GDPR.

Per informazioni sulle altre responsabilità dell'RPD, vedere Titolare del trattamento a pagina 14.

Responsabile del trattamento

Se un'organizzazione ha esternalizzato tutte o parte delle attività di video sorveglianza a una terza parte (un responsabile del trattamento), deve comunque conformarsi al GDPR come titolare del trattamento. Ad esempio, gli addetti alla sicurezza che si occupano del monitoraggio della video sorveglianza live nell'area della reception di un'organizzazione che lavora per privati a cui l'organizzazione ha esternalizzato il compito del monitoraggio live. In questo caso, l'organizzazione deve assicurarsi che gli addetti alla sicurezza svolgano le loro attività in conformità al GDPR.

Per essere conformi al GDPR, i responsabili del trattamento di terze parti (escluse le forze dell'ordine) devono:

- Soddisfare gli stessi requisiti dell'operatore (vedere Operatore del VMS a pagina 19)
- Firmare e rispettare un *contratto del responsabile del trattamento* (vedere Appendice: Contratto del responsabile del trattamento a pagina 52).

Riepilogo

Il GDPR è un regolamento che sta già influenzando il modo in cui le organizzazioni gestiscono i dati, inclusi i dati video.

Come requisito minimo, ciascuna organizzazione che tratta i dati personali deve avere una o più persone designate, responsabili di garantire che i dati personali vengano gestiti in linea con il GDPR e la politica aziendale (il numero di ore-uomo allocate per questo scopo dipenderà dalla dimensione dell'organizzazione e dalla quantità di dati personali raccolti e trattati). Inoltre, per alcune organizzazioni, il GDPR richiederà la nomina di un responsabile della protezione dei dati (RPD) formale per lo svolgimento di questi compiti.

Verranno anche apportate modifiche nella procedura amministrativa. In base al GDPR, le organizzazioni devono conservare un *registro delle attività di trattamento* dettagliato e accurato. Per un modello di esempio di un registro delle attività di trattamento, vedere il modello di registro delle attività di trattamento di *Milestone*. C'è un'ampia varietà di dettagli che devono essere registrati, inclusi tra gli altri:

- A quale categoria di individui sono correlati i dati personali trattati (ad esempio, clienti, dipendenti, visitatori di negozi e così via)
- Per quali finalità vengono utilizzati i dati personali
- Se i dati personali verranno trasferiti, ad altre aziende e/o al di fuori dell'UE
- Per quanto tempo i dati personali verranno conservati
- Misure adottate dall'organizzazione, in relazione a ciascun attività di trattamento dei dati separata, per garantire la conformità al GDPR

Tutto questo è pertinente quando si tratta dei video di sorveglianza memorizzati e definito nella politica di video sorveglianza (vedere Appendice: Politica di video sorveglianza a pagina 47).

Le organizzazioni sono obbligate a spiegare perché una videocamera si trova in un punto specifico, cosa viene ripreso e perché. Nel caso di video sorveglianza, occorre utilizzare un'adeguata segnaletica all'interno e intorno all'area dove il sistema stesso viene impiegato al fine di fornire informazioni in merito.

Il titolare del trattamento può essere obbligato a eseguire una valutazione dell'impatto sulla protezione dei dati (vedere Appendice: Valutazione dell'impatto sulla protezione dei dati a pagina 49) quando si tratta di configurare una telecamera in un luogo pubblico. Una valutazione dell'impatto deve includere:

- Una descrizione sistematica delle finalità e delle operazioni di trattamento previste
- Una valutazione della necessità e della proporzionalità delle operazioni di trattamento in termini di finalità (può richiedere assistenza esterna)
- Valutazione del rischio per i diritti e le libertà degli individui
- Misure pianificate per gestire questi rischi, inclusi misure di salvaguardia e meccanismi per garantire la protezione dei dati personali e la conformità al GDPR (si dovrebbero considerare i diritti e gli interessi legittimi di individui e altre persone interessate)

Una delle funzioni chiave del GDPR è che coloro che vengono monitorati devono essere completamente informati riguardo a quali dati vengono conservati su di essi e come vengono utilizzati. L'informativa sul diritto all'informazione informa gli individui interessati dalla finalità della sorveglianza, che gestiscono i dati raccolti (titolare del trattamento/responsabile del trattamento) e la politica di conservazione. Per un modello di esempio di un avviso sul posto, vedere il modello di *avviso sul posto di Milestone*.

Le organizzazioni che memorizzano i video hanno chiare responsabilità quando si tratta di memorizzare i dati personali e devono adottare misure efficienti per impedire l'accesso non autorizzato. Ciò significa che è importante definire, per iscritto, chi avrà accesso a telecamere e registrazioni.

Le organizzazioni devono anche applicare una procedura per quando un individuo sceglie di esercitare il suo diritto di accedere ai dati personali o richiederne l'eliminazione. In questo modo possono restare nella finestra prescritta di un mese entro cui devono conformarsi a queste richieste ai sensi del GDPR. Nel presentare tale richiesta, è ragionevole aspettarsi che il richiedente fornisca informazioni adeguate per individuare questi dati, ad esempio un intervallo di tempo approssimativo e l'ubicazione dove il video è stato acquisito. Ossia, il soggetto deve esibire documenti di riconoscimento ufficiali come prova della sua identità e l'organizzazione deve tenere traccia delle registrazioni mostrate o fornite all'individuo. Inoltre, nel video devono essere escluse tramite mascheratura altre persone, utilizzando strumenti di terze parti.

Le organizzazioni devono utilizzare misure efficaci per impedire l'accesso non autorizzato ai dati personali memorizzati. La tattica utilizzata da ciascuna organizzazione sarà specifica per le sfide che affronta. Tuttavia, in tutti i casi, le organizzazioni devono impiegare controlli di sicurezza efficienti, restare aggiornate con le best practice per la sicurezza informatica e assicurarsi di lavorare con partner fidati che forniscono hardware e software protetti e servizi di post-assistenza completi.

Gestione dei dati personali

Nella gestione dei dati personali, aderire a questi principi:

- Valutare: sapere quali informazioni personali sono presenti nei file e sui computer.
- Ridurre: conservare solo ciò che è necessario per l'azienda.
- Proteggere: proteggere le informazioni conservate.
- Eliminare: smaltire correttamente ciò che non è più necessario.
- Rispondere: riferire immediatamente tutte le violazioni della sicurezza effettive e sospette.

Per ulteriori informazioni

- Per la versione di testo completo del GDPR, vedere il *Regolamento generale sulla protezione dei dati*.
- Per ulteriori informazioni sul GDPR per l'operatore del VMS, vedere la Guida alla privacy in base al GDPR di Milestone per operatori del VMS e il corso di e-learning sul GDPR di Milestone per operatori del VMS.
- Per restare aggiornati e ottenere ulteriori informazioni sugli sviluppi del GDPR, visitare il sito Web della Commissione europea, Protezione dei dati.

- Per una guida al GDPR per aiutare le organizzazioni a conformarsi ai suoi requisiti, vedere la guida Guide to the UK General Data Protection Regulation dell'Information Commissioner's Office.
- Per un elenco dei concetti chiave sul GDPR, vedere i *concetti chiave del Regolamento generale sulla protezione dei dati*.
- Per consigli per le istituzioni e gli organismi europei su come progettare e utilizzare i sistemi di video sorveglianza, vedere le *linee guida del Garante europeo della protezione dei dati (GEPD)*.
- Per ulteriori informazioni su come proteggere le installazioni di XProtect VMS da attacchi informatici, vedere la Guida di rafforzamento.
- Per informazioni su come i componenti di Milestone XProtect VMS interagiscono, vedere il documento di Milestone che descrive l'architettura di sistema.

Milestone - Modelli del GDPR

- Modello di *avviso sul posto di Milestone*.
- Modello di *registro delle attività di trattamento di Milestone*.
- Modello di *di politica di video sorveglianza di Milestone*.

  È necessario obbedire ai requisiti del GDPR per la configurazione e lo sviluppo del sistema di video sorveglianza. Tenere presente che la raccolta di audio e metadati non è soggetta al marchio di certificazione europeo della tutela della privacy (EuroPriSe).

- Modello di *contratto del responsabile del trattamento di Milestone*
- Modello di *richiesta dell'interessato di Milestone*.

  Questo è solo un esempio. Non esistono requisiti formali per le richieste degli interessati.

- Modello di *notifica di violazione dei dati di Milestone*.

Appendici

Per informazioni aggiuntive, fare riferimento alle seguenti sezioni:

Appendice: Conformità al GDPR

Questa sezione fornisce una panoramica delle normative del GDPR pertinenti per la video sorveglianza. Descrive cos'è il GDPR e come influisce sull'utilizzo della video sorveglianza nelle seguenti sezioni:

- Si dispone di un fondamento giuridico per la raccolta di dati? a pagina 26
- Diritti individuali a pagina 31
- Privacy fin dalla progettazione a pagina 37
- Responsabilità a pagina 44
- Elenco di controllo per proteggere integrità e riservatezza a pagina 46

Si dispone di un fondamento giuridico per la raccolta di dati?

Il GDPR richiede che tutte le organizzazioni abbiano un valido fondamento giuridico per la raccolta e il trattamento dei dati personali.

La video sorveglianza sulla base del consenso o degli interessi vitali è possibile in situazioni eccezionali, ad esempio nel settore sanitario e dell'assistenza se una persona deve essere monitorata costantemente.

Si è obbligati a tenere traccia delle attività di trattamento in un *registro delle attività di trattamento* (articolo 30, GDPR). Per un modello di esempio di un registro delle attività di trattamento, vedere il modello di registro delle attività di trattamento di *Milestone*.

Controllare la legittimità del trattamento dei dati video e dei dati utente a seconda dei seguenti livelli del regolamento:

1. Regolamento generale sulla protezione dei dati (articolo 6, GDPR)

   In particolare, l'articolo 6 (1)(b) del GDPR:

   *Il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.*

   E l'articolo 6 (1)(e)(f) del GDPR:

   *Il trattamento sarà lecito se e nella misura in cui è necessario per le finalità degli interessi legittimi perseguiti dal titolare del trattamento o da una terza parte, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, **in particolare se l'interessato è un minore**.*

2. Direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie o la legge nazionale basata su tale direttiva

   Rispettare la legge nazionale basata sulla Direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie al fine di stabilire una base legale per controllare la legittimità del trattamento.

3. Legge nazionale

   Rispettare la legge nazionale, ad esempio, la sezione 4 della legge federale sulla protezione dei dati (Federal Data Protection Act, FDPA) tedesca, sebbene questa disposizione non si applichi alla video sorveglianza condotta dalle aziende.

Prima di implementare la video sorveglianza, valutare i potenziali vantaggi e l'impatto sui diritti alla privacy, nonché altri diritti fondamentali e interessi legittimi di coloro che sono presenti nell'area coperta.

Quando si decide di utilizzare la video sorveglianza, documentare la finalità del sistema video, quali informazioni vengono raccolte, per che cosa verranno usate, da chi e per quanto tempo e fornire un'adeguata prova di supporto come i dati statistici sul numero effettivo di incidenti di sicurezza avvenuti, nonché la prova dell'efficacia passata delle telecamere per scoraggiare, impedire, esaminare o perseguire penalmente tali incidenti.

La portata della valutazione dipende dalla dimensione del sistema proposto e dall'impatto sulla privacy delle persone e altri interessi legittimi o diritti fondamentali.

Trattamento basato su un obbligo legale o un compito di interesse pubblico

Quando probabilmente verrà applicato il fondamento giuridico per gli obblighi legali? In breve, quando si è obbligati a trattare i dati personali per rispettare la legge. L'articolo 6 (3) del GDPR richiede che l'obbligo legale debba essere stabilito dalla legge dell'UE o dalla legge dello Stato membro.

Non significa che deve esserci un obbligo legale che richiede appositamente l'attività di trattamento specifica. Il punto è che la finalità complessiva deve rispettare un obbligo legale che abbia una base sufficientemente chiara nel diritto comune o nello statuto. Ad esempio, un'ordinanza del tribunale potrebbe richiedere il trattamento dei dati personali per una finalità specifica e ha anche i requisiti per essere un obbligo giuridico.

Le istituzioni pubbliche di solito utilizzano la video sorveglianza per svolgere un compito di interesse pubblico. Tenere presente che la ponderazione degli interessi non è una base legale per le autorità pubbliche nello svolgimento di questi compiti.

Per le istituzioni pubbliche, la video sorveglianza è legittima solo se è necessaria per svolgere il compito di interesse pubblico. Durante l'esecuzione di un compito di servizio pubblico, è necessario condurre una valutazione della proporzionalità (vedere Ponderazione degli interessi/Valutazione della proporzionalità a pagina 28). Il titolare del trattamento deve considerare i principi di minimizzazione dei dati (ad esempio, mascheratura privacy), limitazione di memorizzazione (periodo di conservazione) e limitazione di finalità (articolo 5 (1), GDPR).

Ponderazione degli interessi/Valutazione della proporzionalità

Enti privati di solito utilizzano un VMS per perseguire gli interessi legittimi del titolare del trattamento o di una terza parte (articolo 6 (1)(f), GDPR). Pertanto, è necessaria una ponderazione degli interessi per controllare la legittimità del trattamento. Il titolare del trattamento deve identificare e ponderare i suoi interessi rispetto agli interessi o ai diritti e alle libertà fondamentali degli interessati, che richiedono la protezione dei dati personali.

Il trattamento dei dati della cronologia degli allarmi e delle verifiche possono di solito basarsi sull'interesse legittimo del titolare del trattamento (articolo 6 (1)(f), GDPR). La stessa cosa è applicabile per i dati sulla gestione degli utenti (dati sugli account, credenziali di autenticazione, dati di autorizzazione, dati di configurazione) se l'utente è un dipendente di una società di sicurezza.

È necessario essere chiari, aperti e onesti con le persone dall'inizio in merito a come verranno utilizzati i dati personali. Nella valutazione, affrontare le seguenti domande:

- Quali sono i vantaggi dell'uso della video sorveglianza? I vantaggi superano eventuali effetti negativi?
- La finalità del sistema è chiaramente specificata, esplicita e legittima? Esiste un motivo legittimo per la video sorveglianza?
- L'esigenza di utilizzare la video sorveglianza è chiaramente dimostrata? È uno strumento efficiente per raggiungere la finalità prevista? Sono disponibili alternative meno invadenti?

Inoltre, il titolare del trattamento può utilizzare i dati personali per una nuova finalità solo se è compatibile con la finalità originale o il titolare del trattamento ottiene il consenso o ha una chiara base giuridica.

Tipici interessi del titolare del trattamento

Solitamente, il titolare del trattamento:

- Esercita il diritto di determinare a chi sarà consentito o negato l'accesso ai dati
- Salvaguardia gli interessi legittimi per finalità specificamente definite

Nell'ambito dei rapporti di lavoro, il titolare del trattamento deve essere informato che il trattamento dei dati personali dei dipendenti (dati video e dati utente) può essere soggetto a regole più specifiche ai sensi della legge dello Stato membro (articolo 88, GDPR), ad esempio la sezione 26 della legge FDPA (Germania).

Tipici interessi e diritti degli interessati

Gli interessati hanno il diritto di:

- Nessuna sorveglianza per lungo tempo
- Nessun monitoraggio di situazioni intime
- Periodi di conservazione ridotti
- Misure di salvaguardia adeguate se vengono trattate categorie speciali dei dati personali (articolo 9, GDPR)

Come XProtect riduce l'impatto sugli interessi e sui diritti e sulle libertà fondamentali dell'interessato

Milestone XProtect riduce l'impatto sugli interessi e sui diritti fondamentali dell'interessato tramite:

- Protezione dei dati personali mediante:
  - Controllo accesso basato sul ruolo
    - Maschere privacy rimovibili solo dal supervisore
    - Registrazione degli accessi
  - Crittografia delle registrazioni
  - Conservazione automatica di video (eliminazione automatica)
  - Mascheratura privacy
  - Esportazione di video protetta e verificabile
- Sicurezza informatica
  - Rafforzamento del sistema. Per ulteriori informazioni su come proteggere le installazioni di XProtect VMS da attacchi informatici, vedere la Guida di rafforzamento.
  - Segnalazione di vulnerabilità note e applicazione di patch. Per ulteriori informazioni, vedere Segnalazione di vulnerabilità note e applicazione di patch.
- Formazione e sensibilizzazione
  - Programmi di certificazione della formazione per partner
  - Programmi di certificazione della formazione per partner (vedere il programma per partner tecnologici di Milestone e Milestone Marketplace)
  - Milestone - Corso di e-learning sul GDPR per operatori del VMS

Trasferimenti e divulgazioni

Esistono tre regole principali del GDPR che disciplinano i trasferimenti, a seconda del fatto che le registrazioni siano state trasferite:

- A un destinatario all'interno dell'organizzazione o in un'altra organizzazione

  In questo caso, il GDPR afferma che le registrazioni possono essere trasferite ad altri all'interno dell'organizzazione o in un'altra organizzazione se ciò è necessario per il legittimo espletamento di compiti di competenza del destinatario.

- Verso altri all'interno dell'Unione europea

  In questo caso (i trasferimenti al di fuori delle organizzazioni ma all'interno dell'Unione europea), sono possibili se ciò è necessario per l'espletamento di un compito nel pubblico interesse o rientrano nell'esercizio della pubblica autorità o se il destinatario dimostra altrimenti la necessità del trasferimento e non sussistono ragioni per presumere che possano subire pregiudizio gli interessi legittimi di quelli le cui immagini sono oggetto di trasferimento.

- O all'esterno dell'Unione europea

  In questo caso, i trasferimenti al di fuori dell'Unione europea possono avvenire: (i) se eseguiti solamente per consentire l'espletamento dei compiti dell'organizzazione e (ii) solo soggetti a requisiti aggiuntivi, principalmente per garantire che i dati verranno adeguatamente protetti all'estero.

Riepilogo

Assicurarsi di non utilizzare i dati in violazione di eventuali altre leggi.

È necessario utilizzare i dati personali in modo equo. Ciò significa che non si devono trattare i dati in modo indebitamente dannoso, imprevisto o fuorviante per gli individui interessati.

È possibile utilizzare i dati personali per una nuova finalità solo se è compatibile con la finalità originale o si ottiene il consenso o si ha una chiara base giuridica.

In alcuni casi ritenuti ad alto rischio di violare la privacy, è necessario condurre una valutazione dell'impatto formalizzata (vedere Appendice: Valutazione dell'impatto sulla protezione dei dati a pagina 49).

Conduzione di una valutazione dell'impatto

Prima di installare e implementare sistemi di video sorveglianza, occorre condurre una valutazione della privacy e una *valutazione dell'impatto sulla protezione dei dati*.

La finalità di una valutazione dell'impatto è determinare l'impatto del sistema proposto sulla privacy degli individui e altri diritti fondamentali e individuare modi per mitigare o evitare effetti avversi.

Quanto sforzo deve richiedere una valutazione dell'impatto? Dipende dalle circostanze. Un sistema di video sorveglianza con un alto rischio di violare la privacy garantisce un maggiore investimento rispetto a un sistema di video sorveglianza con impatto limitato sulla privacy, ad esempio, un sistema CCTV statico convenzionale.

Come requisito minimo, ai sensi dell'articolo 35 (7) del GDPR, la valutazione deve contenere almeno:

- Una descrizione sistematica delle operazioni di trattamento previste e le finalità del trattamento, incluso, laddove applicabile, il legittimo interesse perseguito dal titolare del trattamento
- Una valutazione della necessità e della proporzionalità delle operazioni di trattamento in relazione alle finalità
- Una valutazione dei rischi per i diritti e le libertà degli interessati indicati nell'articolo 35 (1) del GDPR:

  Laddove un tipo di trattamento che in particolare utilizza nuove tecnologie e tiene conto della natura, dell'ambito, del contesto e delle finalità del trattamento stesso, probabilmente determinerà un alto rischio per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima del trattamento, eseguirà una valutazione dell'impatto delle operazioni previste sulla protezione dei dati personali. Una singola valutazione potrebbe riguardare una serie di operazioni di trattamento simili che presentano alti rischi simili.
- Le misure previste per gestire questi rischi, inclusi misure di salvaguardia, misure di sicurezza e meccanismi per garantire la protezione dei dati personali e la conformità al GDPR tenendo conto dei diritti e degli interessi legittimi degli interessati e di altre persone coinvolte

In ogni caso, è necessario valutare e giustificare se ricorrere alla video sorveglianza, come collocare le telecamere, selezionare e configurare i sistemi e come implementare le misura di salvaguardia per la protezione dei dati richieste. Per informazioni sulla protezione delle installazioni di XProtect VMS, vedere la Guida di rafforzamento e la Guida ai certificati.

Diritti individuali

Una delle principali finalità del GDPR è assegnare agli individui maggiore protezione e una serie di diritti che regolano i dati personali.

Esistono alcuni requisiti molto specifici ai sensi del regolamento, i quali tutti significano che la parte che tratta o memorizza i dati personali ha la responsabilità di tenere privati questi dati.

Il GDPR assegna agli individui il diritto di essere informati in merito a quando i loro dati personali vengono raccolti (al momento dell'acquisizione) e a come verranno utilizzati. Nel caso di video sorveglianza, ad esempio, sarà un'adeguata segnaletica all'interno e intorno all'area dove viene utilizzato il sistema stesso.

Gli articoli da 12 a 23 del GDPR riguardano i diritti dell'interessato.

- Sezione 1: Trasparenza e modalità
  - Articolo 12: Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

- Sezione 2: Informazione e accesso ai dati personali
  - Articolo 13: Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato
  - Articolo 14: Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato
  - Articolo 15: Diritto di accesso dell'interessato (vedere Diritto di accesso a pagina 33)
- Sezione 3: Rettifica e cancellazione
  - Articolo 16: Diritto di rettifica
  - Articolo 17: Diritto alla cancellazione ("diritto all'oblio") (vedere Diritto all'oblio (diritto alla cancellazione) a pagina 34)
  - Articolo 18: Diritto di limitazione del trattamento (vedere Diritto di limitazione del trattamento a pagina 36)
  - Articolo 19: Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento
  - Articolo 20: Diritto alla portabilità dei dati
- Sezione 4: Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche
  - Articolo 21: Diritto di opposizione
  - Articolo 22: Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione
- Sezione 5: Limitazioni
  - Articolo 23: Limitazioni

Di questi, i diritti più pertinenti nel contesto di video sorveglianza sono:

Il diritto all'informazione (articoli da 12 a 14 e 34, GDPR)	L'articolo 12 riguarda trasparenza e modalità, mentre l'articolo 13 e 14 concerne informazioni e accesso ai dati personali. Questi articoli forniscono all'interessato la capacità di essere informato in merito a quali dati personali vengono raccolti e per quanto tempo vengono conservati. Nel contesto del VMS, vedere Appendice: Avviso sul posto a pagina 47. L'articolo 34 fornisce all'interessato il diritto di essere informato in caso di una violazione dei dati se probabilmente determinerà un alto rischio per i diritti e le libertà dell'interessato stesso.
Il diritto di accesso (articolo 15, GDPR)	Questo diritto assegna all'interessato la capacità di ottenere l'accesso ai suoi dati personali in fase di trattamento, ad esempio, le sue videoregistrazioni.

	All'interessato viene concesso il diritto di chiedere a un'azienda informazioni su quali dati personali che lo riguardano vengono trattati e il motivo di tale trattamento.
Il diritto alla cancellazione ("diritto all'oblio") (articolo 17, GDPR)	Questo diritto fornisce all'interessato la capacità di chiedere l'eliminazione dei suoi dati. Nel contesto del VMS, la cancellazione in base alle richieste dell'interessato è eccezionale dovuta agli interessi del titolare del trattamento e ai periodi di conservazione brevi. Vedere Appendice: Politica di video sorveglianza a pagina 47 ed *Eliminazione parziale di registrazioni video* in Appendice: Il sistema Milestone XProtect VMS e il GDPR a pagina 53.
Il diritto di opposizione (articolo 21, GDPR)	Questo diritto fornisce all'interessato la capacità di opporsi al trattamento dei suoi dati personali. Nel contesto del VMS, altri interessi come interessi legittimi (rilevamento delle frodi, salute e sicurezza), obbligo giuridico (contabilità, antiriciclaggio) o anche adempimento contrattuale (contratti di lavoro) potrebbero prevalere sugli interessi e sui diritti dell'interessato. In tutti i casi, ciò deve essere completamente trasparente in modo che l'interessato possa sapere e opporsi. Se l'interessato si oppone, il titolare del trattamento deve valutare l'obiezione o altrimenti potrebbe incorrere in una sanzione.

Per la conformità al GDPR nei sistemi VMS, tre diritti sono particolarmente pertinenti: diritto all'informazione, diritto di accesso e diritto alla cancellazione.

Diritto di accesso

Ai sensi dell'articolo 15, il GDPR fornisce agli individui il controllo dei loro dati personali, incluso il diritto di vederli. Particolarmente importante è il diritto per cui gli interessati possono ottenere una copia dei loro dati e terze persone sono mascherate (utilizzando strumenti di terze parti).

Su richiesta, le organizzazioni devono fornire all'interessato tutti i dati personali raccolti nei suoi confronti, incluso il video raccolto da un sistema di video sorveglianza.

Assicurarsi di stabilire procedure e politiche formali per la gestione delle richieste del diritto di accesso, descritte in *Registro di trasferimenti e divulgazioni*.

Trasferimenti e divulgazioni

Esistono tre regole principali del GDPR che disciplinano i trasferimenti, a seconda del fatto che le registrazioni siano state trasferite:

- A un destinatario all'interno dell'organizzazione o in un'altra organizzazione

  In questo caso, il GDPR afferma che le registrazioni possono essere trasferite ad altri all'interno dell'organizzazione o in un'altra organizzazione se ciò è necessario per il legittimo espletamento di compiti di competenza del destinatario.

- Verso altri all'interno dell'Unione europea

  In questo caso (i trasferimenti al di fuori delle organizzazioni ma all'interno dell'Unione europea), sono possibili se ciò è necessario per l'espletamento di un compito nel pubblico interesse o rientrano nell'esercizio della pubblica autorità o se il destinatario dimostra altrimenti la necessità del trasferimento e non sussistono ragioni per presumere che possano subire pregiudizio gli interessi legittimi di quelli le cui immagini sono oggetto di trasferimento.

- O all'esterno dell'Unione europea

  In questo caso, i trasferimenti al di fuori dell'Unione europea possono avvenire: (i) se eseguiti solamente per consentire l'espletamento dei compiti dell'organizzazione e (ii) solo soggetti a requisiti aggiuntivi, principalmente per garantire che i dati verranno adeguatamente protetti all'estero.

Registro di trasferimenti e divulgazioni

Le organizzazioni devono conservare un registro, se possibile in formato elettronico, di trasferimenti e divulgazioni. In esso, deve essere registrato ciascun trasferimento a una terza parte. Le terze parti includono anche chiunque all'interno dell'organizzazione per cui venga eseguito un trasferimento da parte di coloro che hanno accesso alle registrazioni in primo luogo. Di solito include qualsiasi trasferimento al di fuori dell'unità di sicurezza. Il registro, inoltre, deve contenere tutte le istanze dove, sebbene non sia stata trasferita la copia della registrazione di video sorveglianza, alle terze parti sono state mostrate le registrazioni o quando il contenuto delle registrazioni è stato altrimenti divulgato a terze parti.

Il registro deve includere almeno quanto segue:

- Data delle registrazioni
- Parte richiedente (nome, titolo e organizzazione)
- Nome e titolo della persona che autorizza il trasferimento
- Breve descrizione del contenuto delle registrazioni
- Motivo della richiesta e motivo della concessione
- Se è stata trasferita una copia della registrazione, è stata mostrata la registrazione o sono state fornite informazioni verbali

Diritto all'oblio (diritto alla cancellazione)

Ai sensi dell'articolo 17, il GDPR fornisce agli individui il controllo dei loro dati personali, incluso il diritto di cancellarli se non sono più necessari per la finalità prevista del sistema.

Ai sensi dell'articolo 17 (1)(c) del GDPR, il titolare del trattamento deve gestire le obiezioni degli interessati. Poiché l'eliminazione di un soggetto specifico dal video non è pratica, i responsabili del trattamento devono limitare rigorosamente il periodo di conservazione del video secondo la finalità documentata del sistema.

Come occorre procedere?

Esaminare il periodo di conservazione per tutte le telecamere e assicurarsi che sia stato impostato in base alla finalità del sistema documentata.

Il diritto all'oblio non si applica spesso alla video sorveglianza, poiché il periodo di conservazione è di solito breve e altri fondamenti giuridici prevalgono su interessi tecnici e legali "ragionevoli" come obbligo legale (legge sul lavoro), interesse pubblico (prevenzione del crimine, salute e sicurezza pubbliche), interessi vitali (dati critici su vita e salute, ambienti rischiosi e pericolosi), interessi legittimi (rilevamento di frodi, occupazione, sviluppo di prodotti) o persino adempimento contrattuale (occupazione, abbonamenti e licenze). Un esempio di interesse legittimo è che le registrazioni di video sorveglianza devono essere una fonte attendibile di prove in qualsiasi momento specificato, pertanto, il VMS protegge principalmente le prove video impedendo che vengano manomesse e garantendone l'autenticazione, rendendo secondario il diritto all'oblio.

Esistono di solito due motivi per cui gli interessati si oppongono alla memorizzazione delle registrazioni video:

- Sugli interessi del titolare del trattamento nel memorizzare i dati prevalgono gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali (articolo 17 (1)(c), GDPR).
- I dati personali sono stati trattati illecitamente, ad esempio per la sorveglianza di una scuola materna o uno spogliatoio (articolo 17 (1)(d), GDPR).

Pertanto, ogni richiesta deve essere esaminata attentamente.

Per quanto tempo le registrazioni devono essere conservate?

Il principio generale è che le registrazioni non devono essere conservate più del necessario per le finalità specifiche per cui sono state eseguite. Occorre anche considerare se innanzitutto è necessaria la registrazione e se il monitoraggio live senza registrazione sarebbe sufficiente.

Se un'organizzazione opta per la registrazione, deve specificare il periodo in cui le registrazioni verranno conservate. Alla scadenza di questo periodo, le registrazioni devono essere cancellate. Milestone XProtect VMS automatizza il processo di cancellazione, eliminando automaticamente le registrazioni precedenti al periodo di conservazione impostato.

Quando i file contenenti i dati video registrati vengono eliminati dal VMS, i file e il relativo contenuto non vengono effettivamente cancellati dai blocchi di dati nel sistema di memorizzazione ma semplicemente contrassegnati come liberi nel file system, consentendo la scrittura di altri file in questa ubicazione del sistema stesso. Finché i blocchi di dati non vengono effettivamente sovrascritti con dati nuovi, i dati video eliminati precedenti potrebbero potenzialmente essere ripristinati, fornendo l'accesso a registrazioni meno recenti rispetto al periodo di conservazione impostato.

Per questo motivo, si consiglia di non sovradimensionare il sistema di memorizzazione, poiché il rischio diventa maggiore con la dimensione del sovraccarico.

Ad esempio, se il sistema di memorizzazione allocato è grande il doppio della quantità di dati video memorizzati per il periodo di conservazione impostato, diciamo sette giorni, i blocchi di dati eliminati contenenti i dati video eliminati precedenti possono comparire statisticamente nel sistema di memorizzazione per altri sette giorni prima di essere sovrascritti.

Per ridurre ulteriormente il rischio di accesso ai dati video precedenti che sono stati eliminati, e per la sicurezza in generale, si consiglia di abilitare la crittografia dei database di supporti. Quando la crittografia è abilitata, oltre a consentire il ripristino dei file eliminati, i database di supporti indicano anche quando sono stati manomessi.

Indipendentemente dal fatto che i dati video siano strati crittografati o meno, una volta che i dischi nel sistema di memorizzazione non sono più utilizzabili, è importante bonificare o distruggere fisicamente i dischi rigidi utilizzati per memorizzare i database di supporti prima di smaltirli (ad esempio, tramite shredding o altri mezzi equivalenti).

Per informazioni su come configurare questa impostazione in Milestone XProtect, vedere Informazioni su memoria e archiviazione (spiegazione) nel Manuale dell'amministratore per il sistema VMS XProtect.

Se la finalità della video sorveglianza è la sicurezza, si verifica un incidente di sicurezza e viene stabilito che le registrazioni sono necessarie per fare ulteriori indagini sull'incidente o utilizzare le registrazioni come prova, la registrazione pertinente potrebbe essere conservata oltre i normali periodi di conservazione purché sia necessaria per queste finalità. Successivamente, deve essere tuttavia cancellata.

Periodo di conservazione per tipiche finalità di sicurezza: da una settimana a un mese

Quando le telecamere sono state installate per finalità di sicurezza, da una settimana a un mese dovrebbe essere un periodo di tempo sufficiente per consentire al personale addetto alla sicurezza di prendere una decisione consapevole in merito a se conservare una registrazione per un periodo più lungo al fine di esaminare ulteriormente un incidente di sicurezza o utilizzarlo come prova.

Un esempio di legge locale: secondo alcune autorità tedesche competenti per la protezione dei dati personali e la maggior parte della letteratura in materia di protezione dei dati, questo periodo di conservazione è compreso tra 48 e 72 ore come linea guida per il controllo accesso e le indagini sui reati.

Territorio dello Stato membro o di un paese terzo: 48 ore

Nel caso in cui la sorveglianza copra qualsiasi area all'esterno degli edifici nel territorio dello Stato membro (o di un paese terzo) (di solito quelli vicino alle aree di entrata e uscita) e non è possibile evitare che i passanti o le auto in transito vengano ripresi dalle telecamere, si consiglia di ridurre il periodo di conservazione a 48 ore o altrimenti tenere conto delle preoccupazioni locali, se possibile.

Diritto di limitazione del trattamento

L'interessato può, con riferimento all'articolo 18 (1) del GDPR, reclamare il diritto di limitazione del trattamento. In uno scenario del VMS di base, l'interessato può sostenere che il trattamento del VMS sia illegittimo, ad esempio se è inconsapevole che la video sorveglianza di uno spazio pubblico viene eseguita con la protezione tramite maschera privacy. Si consiglia di utilizzare un modello di *richiesta dell'interessato* per documentare il reclamo (vedere Richiesta dell'interessato a pagina 11). Per un modello di esempio di una richiesta dell'interessato, vedere il modello di richiesta dell'interessato di *Milestone*.

Il reclamo deve essere trattato in un intervallo di tempo ragionevole, più rapidamente del periodo di conservazione, per evitare l'eliminazione o la conservazione automatizzata della prova del VMS nel reclamo stesso. In generale, si consiglia di cercare assistenza legale relativamente alla limitazione di trattamento. Un modo per gestire questa richiesta è consentire all'amministratore del VMS di limitare i supervisori o gli operatori del VMS mediante l'assegnazione di ruoli solo per poter riprodurre le registrazioni entro un breve periodo di tempo dopo che sono state eseguite, ad esempio, quatto ore o un giorno (vedere Come occorre procedere? a pagina 37: "Considerare la restrizione dell'accesso al video registrato per operatori, completamente, al solo video registrato nelle poche ore passate o solo con doppia autorizzazione"). Le limitazioni della riproduzione si applicano anche alle protezioni prove. Se sono richieste ulteriori limitazioni di trattamento, si consiglia di condurre una valutazione dell'impatto sulle imprese e una valutazione dell'impatto sulla privacy (vedere Conduzione di una valutazione dell'impatto a pagina 30) come parte della gestione dei reclami.

Privacy fin dalla progettazione

Il GDPR prevede che la privacy debba essere una priorità in tutto il processo di progettazione e messa in funzione del sistema. L'approccio adottato rispetto alla privacy dei dati deve essere proattivo, non reattivo. I rischi devono essere previsti e l'obiettivo deve essere impedire gli eventi prima che accadano.

Le organizzazioni devono considerare e documentare attentamente come sono stati progettati i sistemi per essere conformi agli obiettivi prefissati.

Prestare attenzione a non acquisire i dati personali di soggetti che non rientrano nel dominio del sistema (ad esempio, aree pubbliche adiacenti).

Prestare attenta considerazione di chi ha bisogno di vedere quali informazioni (ad esempio, live/registrate, intervallo di tempo, risoluzione) e chi può accedere a quali funzioni (ad esempio, ricerca).

Come occorre procedere?

- Documentare la risoluzione di punti differenti nella scena della telecamera
- Documentare il periodo di conservazione previsto
- Considerare l'applicazione della mascheratura privacy, permanente o rimovibile
- Considerare la configurazione di autorizzazioni per la visualizzazione di video live, registrazioni
- Considerare la restrizione dell'accesso per l'esportazione di registrazioni e per la rimozione di maschere privacy
- Valutare ed esaminare regolarmente ruoli e responsabilità per operatori, investigatori, amministratori di sistema e altri con accesso al sistema
- Considerare la restrizione dell'accesso a gruppi incaricati di indagini per telecamere specificamente posizionate per acquisire l'identità (ad esempio, facce di persone che entrano in un negozio)
- Considerare la restrizione dell'accesso al video registrato per operatori, completamente, al solo video registrato nelle poche ore passate o solo con doppia autorizzazione
- Limitare il numero di utenti che hanno un ruolo di amministratore

Requisiti di privacy fin dalla progettazione

Minimizzazione dei dati	È necessario garantire che i dati personali trattati siano: • adeguati; sono sufficienti per realizzare correttamente la finalità indicata. • pertinenti; hanno un legame razionale con tale finalità. • limitati a ciò che è necessario; non conservare più di quello che serve per tale finalità.
Accuratezza	In generale, per dati personali: • Occorre adottare tutte le misure ragionevoli per garantire che i dati personali detenuti non risultino inesatti o fuorvianti come dato di fatto. • Potrebbe essere necessario tenere aggiornati i dati personali, sebbene ciò dipenderà dallo scopo per cui vengono utilizzati. • Nel caso in cui i dati personali dovessero risultare inesatti o fuorvianti, è necessario adottare misure ragionevoli per correggerli o cancellarli prima possibile. • È necessario considerare attentamente eventuali problemi legati all'accuratezza dei dati personali.
Limitazione del periodo di conservazione	• Non conservare i dati personali per un periodo più lungo del necessario. • È necessario pensare a, ed essere in grado di giustificare, quanto tempo conservare i dati personali. Dipenderà dalle finalità della conservazione dei dati. • Serve una politica che imposti periodi di conservazione standard, laddove possibile, per soddisfare i requisiti documentati. • Occorre rivedere periodicamente i dati detenuti e cancellarli o anonimizzarli quando non sono più necessari. • È necessario considerare attentamente eventuali problemi legati alla conservazione dei dati. Gli individui hanno il diritto alla cancellazione se i dati non sono più necessari. • È possibile conservare i dati personali per un periodo più lungo solo per finalità di archiviazione nel pubblico interesse oppure per finalità scientifiche, storiche o statistiche.

Privacy fin dalla progettazione e privacy per impostazione predefinita

Ai sensi del GDPR, il titolare del trattamento dei dati personali, nel trattare tali dati, deve implementare misure tecniche o organizzative progettate per implementare i principi di protezione dei dati definiti nel GDPR. Il GDPR lo definisce "privacy fin dalla progettazione".

Nel contesto di una telecamera, un esempio pertinente di privacy fin dalla progettazione sarebbe una funzione che consente a livello digitale all'utente di restringere l'acquisizione di immagini a un determinato perimetro, impedendo alla telecamera di acquisire eventuali immagini al di fuori di questo perimetro che verrebbero altrimenti riprese.

Nel VMS XProtect, è disponibile il supporto per la mascheratura privacy in due forme: maschere permanenti che non possono essere rimosse e maschere rimovibili che (con le autorizzazioni adatte) possono essere rimosse per rivelare l'immagine dietro la maschera.

Il titolare del trattamento deve anche implementare misure tecniche o organizzative che, per impostazione predefinita, garantiscono il trattamento, minimamente invasivo per la privacy, dei dati personali in questione. GDPR la definisce privacy per impostazione predefinita. Nel contesto di una telecamera, un esempio pertinente di privacy per impostazione predefinita potrebbe essere utilizzare la mascheratura privacy per mantenere privata un'area sensibile all'interno della vista della telecamera.

Qual è un esempio di una funzione di XProtect che supporta l'approccio privacy fin dalla progettazione?

Milestone sviluppa il suo portfolio di prodotti continuamente e la privacy per impostazione predefinita è un criterio di valutazione chiave nel rendere XProtect conforme al GDPR. Per ulteriori informazioni, vedere la guida sul ciclo di vita di sviluppo protetto in Milestone. Questa guida fa parte integrante della privacy per impostazione predefinita, applicando principi quali "difesa approfondita", "privilegi minimi", evitando impostazioni predefinite meno protette e disattivando funzioni utilizzate meno di frequente per impostazione predefinita.

Come occorre procedere per assicurare la privacy fin dalla progettazione?

- Considerare la risoluzione di punti differenti nella scena della telecamera e documentare queste impostazioni

  Finalità differenti richiedono qualità delle immagini diverse. Quando non è necessaria l'identificazione, dovrebbero essere scelti la risoluzione della telecamera e altri fattori modificabili per assicurarsi di non acquisire immagini facciali riconoscibili.

- Crittografare le registrazioni

  Milestone consiglia di proteggere le registrazioni abilitando almeno la crittografia semplice negli archivi e nello spazio di memorizzazione dei server di registrazione. Milestone utilizza l'algoritmo AES-256 per la crittografia. Quando si seleziona la crittografia semplice, viene crittografata solo una parte della registrazione. Quando si seleziona la crittografia avanzata, viene crittografata l'intera registrazione.

- Proteggere la rete

  Milestone consiglia di selezionare le telecamere che supportano HTTPS. Si consiglia di impostare le telecamere su VLAN separate e utilizzare HTTPS per la telecamera per la comunicazione con i server di registrazione, nonché i client per la comunicazione con i server di registrazione.

  Si consiglia di abilitare la crittografia della comunicazione multimediale da Recording Server ad altri server e client.

  Si consiglia di collocare XProtect Smart Client e XProtect Smart Wall sulla stessa VLAN dei server.

  Utilizzare una rete VPN crittografata o simile se si usa Smart Client o Smart Wall da un'ubicazione remota.

- Abilitare e documentare il periodo di conservazione previsto

  In base all'articolo 17 (1)(a) del GDPR, le registrazioni non devono essere conservate più del necessario per le finalità specifiche per cui sono state eseguite. Milestone consiglia di impostare il periodo di conservazione appropriato. Ciò quindi automatizza lo smaltimento di video.

- Esportazioni protette

  Milestone consiglia di consentire l'accesso alla funzionalità di esportazione solo per un gruppo selezionato di utenti che richiedono questa autorizzazione.

  Milestone consiglia anche di cambiare il profilo di Smart Client per consentire solo l'esportazione in formato XProtect con la crittografia abilitata. Non consentire le esportazioni in formato AVI e JPEG perché non possono essere impostate come protette. Così l'esportazione di qualsiasi prova è protetta da password, crittografata e firmata digitalmente, garantendo che il materiale forense sia autentico, non manomesso e visualizzato solo dal destinatario autorizzato.

- Abilitare la mascheratura privacy, permanente o rimovibile

  Utilizzare la mascheratura privacy per aiutare a eliminare la sorveglianza di aree non pertinenti per l'oggetto di sorveglianza.

- Limitare i diritti di accesso con ruoli

  Applicare il principio del privilegio minimo (Principle of Least Privilege, PoLP).

  Milestone consiglia di consentire l'accesso alle funzionalità solo per un gruppo selezionato di utenti che richiedono questa autorizzazione. Per impostazione predefinita, solo l'amministratore di sistema può accedere al sistema ed eseguire i vari compiti. Tutti i nuovi ruoli e utenti creati non hanno accesso a eventuali funzioni finché non sono stati deliberatamente configurati da un amministratore.

  Configurare autorizzazioni per tutte le funzionalità, inclusi la visualizzazione di video live e registrazioni, l'ascolto dell'audio, l'accesso ai metadati, il controllo di telecamere PTZ, l'accesso e la configurazione di Smart Wall, la rimozione di maschere privacy, l'utilizzo di esportazioni, il salvataggio di istantanee e così via.

  Limitare l'accesso a video, audio e metadati registrati per operatori, completamente, o limitare l'accesso solo a video, audio o metadati registrati nelle poche ore precedenti.

  Valutare ed esaminare regolarmente ruoli e responsabilità per operatori, investigatori, amministratori di sistema e altri con accesso al sistema. Il principio del privilegio minimo si applica comunque?

- Limitare le autorizzazioni dell'amministratore

  Milestone consiglia di limitare il numero di utenti che hanno un ruolo di amministratore.

Impostazione e configurazione del sistema di video sorveglianza

Il principio guida in relazione a tutti gli argomenti trattati in questa sezione dovrebbe essere ridurre al minimo l'eventuale impatto negativo sulla privacy e su altri diritti fondamentali e interessi legittimi di coloro che sono sotto sorveglianza.

Ubicazioni delle telecamere e angoli di visualizzazione

Le ubicazioni delle telecamere devono essere scelte in modo da ridurre al minimo la visualizzazione di aree non pertinenti per le finalità previste.

Di norma, dove è installato un sistema di video sorveglianza per proteggere le risorse (proprietà o informazioni) dell'organizzazione o la sicurezza del personale e dei visitatori, l'organizzazione deve limitare il monitoraggio a

- aree attentamente selezionate contenenti informazioni sensibili, elementi di alto valore o altre risorse che richiedono una maggiore protezione per un motivo specifico,
- punti di entrata e di uscita verso gli edifici (incluse le uscite di emergenza e le uscite di sicurezza o le recinzioni che circondano l'edificio o la proprietà) e
- punti di entrata e di uscita all'interno dell'edificio che collegano aree differenti che sono soggette a diritti di accesso diversi e separate da porte chiuse a chiave o un altro meccanismo di controllo accesso.

Numero di telecamere

Il numero di telecamere da installare dipenderà dalla dimensione degli edifici e dalle esigenze di sicurezza, che, a loro volta, sono contingenti per una serie di fattori. Lo stesso numero e lo stesso tipo di telecamere possono essere appropriati per un'organizzazione e possono essere enormemente sproporzionati per un'altra. Tuttavia, se tutti gli altri fattori sono uguali, il numero di telecamere è un buon indicatore della complessità e della dimensione di un sistema di sorveglianza e può suggerire maggiori rischi per la privacy e altri diritti fondamentali. Con l'aumentare del numero di telecamere, è anche più probabile che non verranno utilizzate in modo efficiente e si verifica un sovraccarico di informazioni. Pertanto, il Garante europeo della protezione dei dati (GEPD) consiglia di limitare il numero di telecamere a quelle strettamente necessarie a realizzare le finalità del sistema. Il numero di telecamere deve essere incluso nella politica di video sorveglianza.

Periodi del monitoraggio

Il tempo di registrazione impostato per le telecamere deve essere scelto in modo da ridurre al minimo il monitoraggio in periodi non pertinenti per le finalità previste. Se la finalità della video sorveglianza è la sicurezza, se possibile, il sistema deve essere impostato per registrare solo durante questi periodi quando esiste una maggiore probabilità che si verifichino i problemi di sicurezza presumibili.

Risoluzione e qualità delle immagini

Si devono scegliere una risoluzione e una qualità delle immagini adeguate. Finalità differenti richiederanno qualità delle immagini diverse. Ad esempio, quando l'identificazione degli individuali è fondamentale, la risoluzione delle telecamere, le impostazioni di compressione in un sistema digitale, l'ubicazione, l'illuminazione e altri fattori dovranno tutti essere considerati e scelti o modificati in modo che la qualità delle immagini risultante sia sufficiente a fornire immagini facciali riconoscibili. Se non è necessaria l'identificazione, possono essere scelti la risoluzione della telecamera e altri fattori modificabili per assicurarsi di non acquisire immagini facciali riconoscibili.

Chi deve accedere al VMS?

I diritti di accesso devono essere limitati a un numero ridotto di individui chiaramente identificati in base alla rigorosa necessità di accesso. I criteri di accesso al VMS devono essere definiti seguendo il principio del “privilegio minimo”: agli utenti deve essere concesso il diritto di accesso solo a quelle risorse che sono strettamente necessarie per svolgere i loro compiti.

Solo il titolare del trattamento, l'amministratore di sistema o altri membri del personale specificamente nominati dal titolare del trattamento per questa finalità devono essere in grado di concedere, alterare o annullare i diritti di accesso di eventuali persone. Qualsiasi concessione, alterazione o annullamento dei diritti di accesso deve avvenire secondo i criteri stabiliti nella politica di video sorveglianza dell'organizzazione.

Coloro che dispongono dei diritti di accesso devono sempre essere individui chiaramente identificabili.

La politica di video sorveglianza deve chiaramente specificare e documentare chi ha accesso alle registrazioni di video sorveglianza e/o l'architettura tecnica, ad esempio i server VMS, del sistema di video sorveglianza, per quali finalità e in cosa consistono tali diritti di accesso. In particolare, occorre specificare chi ha il diritto di:

- Visualizzare il video/l'audio in tempo reale
- Azionare le telecamere PTZ (Pan/Tilt/Zoom)
- Visualizzare le registrazioni
- Esportare o
- Eliminazione di eventuali registrazioni

Inoltre, è necessario configurare l'accesso alle seguenti funzioni del VMS:

- Segnalibri
- Blocchi delle prove
- Rimuovi maschere privacy:
- Esporta
- Eventi di attivazione
- Avvio/Arresto della registrazione
- Creazione/Modifica/Eliminazione/Attivazione/Blocco/Rilascio delle preimpostazioni PTZ
- Creazione/Modifica/Eliminazione/Avvio/Arresto degli schemi di ronda PTZ
- Ricerca avanzata
- Autorizzazioni per audio, metadati, I/O ed eventi

Protezione dei dati memorizzati e trasmessi

Innanzitutto, deve essere eseguita un'analisi interna dei rischi per la sicurezza per determinare quali misure di sicurezza sono necessarie per proteggere il sistema di video sorveglianza, inclusi i dati personali trattati.

In tutti i casi, si devono adottare misure per garantire la sicurezza rispetto a

- Trasmissione
- Memorizzazione (come nei database di computer)
- Accesso (come accesso a server, sistemi di memorizzazione, rete e locali)

La trasmissione deve essere instradata tramite canali di comunicazione sicuri e protetta dalle intercettazioni, ad esempio per mezzo di:

- Crittografia dei supporti da Recording Server ai server e client
- Dalla telecamera HTTPS a Recording Server
- VPN per Smart Client o Management Client connesso tramite Internet

La protezione dalle intercettazioni è particolarmente importante se viene utilizzato un sistema di trasmissione wireless o se vengono trasferiti eventuali dati tramite Internet. In questi casi, i dati devono essere crittografati n transito o deve essere fornita una protezione equivalente.

Devono anche essere considerati in altri casi la crittografia o altri mezzi tecnici che garantiscono una protezione equivalente, durante la memorizzazione, se giustificati dall'analisi interna dei rischi di sicurezza. Ad esempio, nel caso in cui i dati sono particolarmente sensibili. A tale scopo, abilitare la crittografia del database di supporti.

Devono essere protetti tutti i locali in cui i dati di video sorveglianza vengono memorizzati e dove vengono visualizzati. Deve essere protetto l'accesso fisico alla sala di controllo e alla sala server dove sono stati collocati i server VMS. Nessuna terza parte (ad esempio, il personale addetto alla pulizia o alla manutenzione) deve avere accesso senza supervisione a questi locali.

Si deve scegliere l'ubicazione dei monitor in modo che il personale non autorizzato non possa visualizzarli. Se devono essere vicini alle aree pubbliche, i monitor devono essere posizionati in modo che siano visualizzabili solo dal personale addetto alla sicurezza.

Per impostazione predefinita, XProtect VMS registra le informazioni di base, ma si consiglia di abilitare la registrazione degli accessi utente in Management Client per il registro attività utente.

Questo sistema di registrazione digitale viene implementato per assicurare che una verifica possa determinare in qualsiasi momento chi ha avuto accesso al sistema, dove e quando. Il sistema di registrazione può identificare chi ha visualizzato, eliminato o esportato eventuali dati di video sorveglianza (ciò richiede l'abilitazione della registrazione degli accessi utente).

Per ulteriori informazioni, vedere il Manuale dell'amministratore per VMS XProtect.

In relazione a ciò e altrove, occorre prestare particolare attenzione alle funzioni chiave e ai poteri degli amministratori di sistema e alla necessità di bilanciare questi elementi con misure di salvaguardia e monitoraggio adeguati.

Responsabilità

L'articolo 5 (2) del GDPR dichiara:

Il titolare del trattamento sarà responsabile, e in grado, di dimostrarne la conformità, paragrafo 1 ("responsabilità").

Laddove i principi correlati al trattamento dei dati personali sono: legittimità, equità e trasparenza, limitazione di finalità, minimizzazione dei dati, accuratezza, limitazione di memorizzazione, integrità e riservatezza.

Il principio di responsabilità richiede di assumersi la responsabilità di cosa fare con i dati personali.

Più nello specifico, l'articolo 30 del GDP dichiara:

Ciascun titolare del trattamento e, laddove applicabile, il rappresentante di quest'ultimo, dovrà gestire un registro delle attività di trattamento sotto la sua responsabilità.

Il registro deve contenere le seguenti informazioni:

a. *il nome e i dettagli di contatto del titolare del trattamento e, laddove applicabile, il titolare congiunto, il rappresentante del titolare e il responsabile della protezione dei dati*

b. *le finalità del trattamento*

c. *una descrizione delle categorie degli interessati e delle categorie dei dati personali*

d. *le categorie dei destinatari a cui i dati personali sono stati o verranno divulgati inclusi i destinatari in paesi terzi o organizzazioni internazionali*

e. *laddove applicabile, i trasferimenti di dati personali in un paese terzo o un'organizzazione internazionale, inclusa l'identificazione di tale paese terzo o organizzazione internazionale e, in caso di trasferimenti riportati nel secondo sottoparagrafo dell'articolo 49 (1), la documentazione delle misure di salvaguardia appropriate*

f. *laddove possibile, l'orario previsto limita la cancellazione delle categorie differenti di dati*

g. *laddove possibile, una descrizione generale delle misure di sicurezza tecniche o organizzative riportate nell'articolo 32 (1).*

La responsabilità è uno dei principi della protezione dei dati; significa essere responsabili della conformità al GDPR e occorre essere in grado di dimostrare la propria conformità.

Occorre prendere misure tecniche e organizzative appropriate per soddisfare i requisiti di responsabilità.

Esistono diverse misure che è possibile adottare, e in alcuni casi è necessario prendere, inclusi:

- Adozione e implementazione delle politiche di protezione dei dati
- Adozione di un approccio di "protezione dei dati fin dalla progettazione e per impostazione predefinita" (per ulteriori informazioni, vedere Privacy fin dalla progettazione a pagina 37)
- Stipulazione di contratti scritti con organizzazioni che trattano i dati personali per proprio conto
- Gestione della documentazione delle attività di trattamento
- Implementazione di misure di sicurezza appropriate
- Registrazione e, dove necessario, segnalazione delle violazioni dei dati personali
- Esecuzione di valutazioni dell'impatto sulla protezione dei dati per usi di dati personali che probabilmente determineranno un alto rischio per gli interessi degli individui
- Nomina di un responsabile della protezione dei dati
- Aderire ai codici di condotta pertinenti e iscriversi a schemi di certificazione

Utilizzare un modello di registro delle attività di trattamento per identificare e monitorare i problemi di responsabilità. Per un modello di esempio di un registro delle attività di trattamento, vedere il modello di registro delle attività di trattamento di *Milestone*.

Gli obblighi di responsabilità sono vigenti. È necessario rivedere e, laddove necessario, aggiornare le misure adottate.

Se si implementa un framework di gestione della privacy, si possono incorporare misure di responsabilità e creare una cultura di privacy in tutta l'organizzazione.

Essere responsabili può aiutare a creare una relazione di fiducia con gli individui e a mitigare l'azione coercitiva del GDPR.

Elenco di controllo per proteggere integrità e riservatezza

Il GDPR richiede che le organizzazioni abbiano procedure e politiche complete volte a garantire che i dati personali restino sempre sotto il loro controllo. Inoltre, le violazioni dei dati personali devono essere segnalate entro 72 ore all'autorità di controllo competente nominata dal governo nazionale.

Adottare tutte le misure tecniche e organizzative appropriate per proteggersi dalla compromissione dei dati personali.

Come occorre procedere?

- Rivedere le politiche di sicurezza in merito a controllo delle password e utilizzo degli account.
- Considerare l'impostazione di requisiti minimi di complessità delle password per tutti i gruppi di domini. Considerare l'impostazione di requisiti più complessi per account amministrativi a livello di dominio.
- Applicare procedure per verificare lo stato della protezione e rilevare eventuali violazioni.
- Assicurarsi che gli utenti non condividano gli account, scambiandosi le password o evitando che si disconnettano/connettano all'inizio/alla fine del loro turno.
- Gestire una politica e una procedura documentate che regolino azioni appropriate nel caso di una violazione dei dati.
- Occorre anche assicurarsi di aver adottato misure di sicurezza appropriate per proteggere i dati personali detenuti.
- Un principio chiave del GDPR è che il trattamento protetto dei dati personali avviene per mezzo di "misure tecniche e organizzative appropriate"; questo è il "principio di sicurezza".
- In questo modo, occorre considerare aspetti come analisi del rischio, politiche organizzative e misure fisiche e tecniche.
- Occorre anche tenere conto di requisiti aggiunti per la sicurezza del trattamento e questi si applicano anche ai responsabili del trattamento.
- È possibile considerare lo stato dell'arte e i costi dell'implementazione nel decidere quali misure prendere, ma esse devono essere appropriate alle circostanze e al rischio che il trattamento pone.
- Laddove appropriato, si dovrebbe cercare di utilizzare misure come la pseudonimizzazione (ad esempio, utilizzando la protezione della privacy con una maschera di sfocatura) e la crittografia.
- Le misure adottate devono garantire "la riservatezza, l'integrità e la disponibilità" dei sistemi e dei servizi e dei dati personali trattati con essi.

- Le misure devono anche consentire di ripristinare la disponibilità e l'accesso ai dati personali in maniera tempestiva nel caso di un incidente fisico o tecnico.
- Occorre anche assicurarsi di aver adottato procedure appropriate per testare l'efficacia delle misure e apportare eventuali miglioramenti richiesti.

Appendice: Avviso sul posto

Gli avvisi sul posto devono includere un pittogramma, ad esempio, il pittogramma ISO o il pittogramma utilizzato abitualmente dove sorge l'edificio. Il pittogramma deve anche essere comprensibile per i bambini. È disponibile, ad esempio, nella pagina dei simboli grafici ISO (https://www.iso.org/obp/ui/#search/grs/). L'avviso deve:

- Identificare il titolare del trattamento
- Specificare la finalità della sorveglianza:
  - Per consentire agli organismi pubblici di eseguire i loro compiti
  - Per esercitare il diritto di determinare a chi sarà consentito o negato l'accesso
  - Per salvaguardare gli interessi legittimi per finalità specificamente definite
- Indicare chiaramente se le immagini sono state registrate
- Fornire dettagli di contatto e un collegamento alla politica di video sorveglianza online
- Se qualsiasi area al di fuori degli edifici è sotto sorveglianza, ciò deve essere indicato chiaramente

Il personale addetto alla sicurezza e alla reception deve essere formato sugli aspetti delle pratiche di video sorveglianza relativi alla protezione dei dati e deve essere in grado di creare copie dell'informativa dettagliata sulla protezione dei dati (vedere Appendice: Politica di video sorveglianza a pagina 47), disponibile su richiesta. Deve anche essere in grado di dire al pubblico chi contattare con domande aggiuntive o per accedere ai suoi dati.

Le insegne devono essere collocate in tali ubicazioni ed essere sufficientemente grandi che gli interessati le possano notare prima di entrare nella zona monitorata e le possano leggere senza difficoltà. Non significa che si deve collocare un avviso accanto a ogni singola telecamera.

Le insegne all'interno degli edifici devono essere in una o più lingue generalmente comprensibili ai membri del personale e ai visitatori più frequenti. Devono anche essere poste insegne al di fuori degli edifici (se vengono monitorate eventuali are esterne) in una o più lingue locali.

Per un modello di esempio di un avviso sul posto, vedere il modello di *avviso sul posto di Milestone*.

Appendice: Politica di video sorveglianza

La politica di video sorveglianza comprende molte finalità e serve a soddisfare le seguenti esigenze:

- L'adozione del presente documento è spesso necessaria per completare e specificare la base legale e quindi aiutare a stabilire un motivo legittimo per la video sorveglianza (vedere l'articolo 5 del GDPR).
- La stesura di pratiche per iscritto e un'attenta considerazione di quali altre misure aggiuntive occorre adottare possono migliorare le procedure e assicurare una migliore conformità.
- L'adozione di una politica e la sua pubblicazione aiuteranno a rispettare l'obbligo, ai sensi del GDPR, di fornire al pubblico le informazioni necessarie a garantire un trattamento equo.
- La politica stabilisce una serie di regole in base a cui si può misurare la conformità (ad esempio, durante una verifica).
- Aumentando la trasparenza e intraprendendo sforzi in materia di conformità, le organizzazioni inducono un senso di fiducia nei loro dipendenti e in terze parti, aiutando a facilitare la consultazione con le parti interessate.

La politica di video sorveglianza deve fornire quanto segue:

- Fornire una panoramica sul sistema di video sorveglianza e descriverne le finalità
- Descrivere come il sistema viene utilizzato, i dati personali vengono impiegati e quali misure di salvaguardia di protezione dei dati vengono adottate
- Confermare in modo esplicito la conformità al GDPR
- Definire eventuali misure necessarie richieste per l'implementazione

Le organizzazioni devono rendere pubbliche le loro politiche di video sorveglianza sui loro siti Intranet e Internet. Se il presente documento contiene informazioni riservate, deve essere resa pubblica una versione non riservata.

Per servire come informativa adeguata sulla protezione dei dati, le seguenti informazioni devono essere integrate nella politica di video sorveglianza in un formato e in una lingua intuitivi:

- Identità del titolare del trattamento (ad esempio, organizzazione, direzione generale, direzione e unità)
- Breve descrizione della copertura del sistema di video sorveglianza (ad esempio, punti di entrata e uscita, sale computer, sale di archivi)
- La base legale della video sorveglianza, ad esempio l'articolo 6 (1)(f) del GDPR
- I dati raccolti e la finalità della video sorveglianza (devono anche essere chiaramente specificate eventuali limitazioni sugli usi consentiti)
- Chi ha accesso al materiale di sorveglianza e a chi possono essere divulgate le registrazioni
- Come vengono protette e salvaguardate le informazioni
- Per quanto tempo i dati vengono conservati
- Come gli interessati possono verificare, modificare o eliminare le loro informazioni (inclusi i dettagli di contatto per ulteriori domande e informazioni su come ottenere il ricorso internamente)

Inoltre, la politica di video sorveglianza deve fornire riferimenti a:

- I report sulla verifica dell'organizzazione
- I report sulla valutazione dell'impatto dell'organizzazione

Per un modello di esempio di una politica di video sorveglianza, vedere il modello di politica di video sorveglianza di *Milestone*.

Declinazione di responsabilità: La politica di video sorveglianza di esempio deve essere controllata dal titolare del trattamento. La conformità al GDPR mediante questo esempio è la sua area di responsabilità.

Tenere presente quanto segue: la raccolta di audio e metadati non è soggetta al marchio di certificazione europeo della tutela della privacy. Una configurazione del VMS con la raccolta di audio e metadati non è autorizzata a utilizzare il profilo del prodotto certificato EuroPriSe. Un titolare del trattamento/responsabile del trattamento che agisce in questo modo non può indicare di utilizzare un prodotto che facilita in modo specifico la protezione dei dati e la conformità al GDPR.

Appendice: Valutazione dell'impatto sulla protezione dei dati

Ai sensi dell'articolo 35 del GDPR, è richiesta una *valutazione dell'impatto sulla protezione dei dati* se la sorveglianza

probabilmente determinerà un alto rischio per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima del trattamento, eseguirà una valutazione dell'impatto delle operazioni previste sulla protezione dei dati personali.

Il titolare del trattamento deve consultare l'autorità di controllo prima del trattamento dove una *valutazione dell'impatto sulla protezione dei dati* ai sensi dell'articolo 35 indica che il trattamento comporterebbe un alto rischio in assenza di misure adottate dal titolare del trattamento per mitigare il rischio (consultazione preventiva, articolo 36 del GDPR).

Creare e gestire una *valutazione dell'impatto sulla protezione dei dati*, un'informativa agli individui interessati. Il presente documento:

- Descrive la finalità della sorveglianza
- È conservata dal titolare del trattamento o dal responsabile del trattamento
- Definisce la politica di conservazione

Occorre condurre una *valutazione dell'impatto sulla protezione dei dati* prima di installare e implementare sistemi di video sorveglianza ogniqualvolta ciò aggiunge valore agli sforzi in materia di conformità dell'organizzazione. La finalità della *valutazione dell'impatto sulla protezione dei dati* è determinare l'impatto del sistema proposto sulla privacy degli individui e altri diritti fondamentali e individuare modi per mitigare o evitare eventuali effetti avversi.

Come requisito minimo, ai sensi dell'articolo 35 (7) del GDPR, la valutazione deve contenere almeno:

- Una descrizione sistematica delle operazioni di trattamento previste e le finalità del trattamento, incluso, laddove applicabile, il legittimo interesse perseguito dal titolare del trattamento
- Una valutazione della necessità e della proporzionalità delle operazioni di trattamento in relazione alle finalità
- Una valutazione dei rischi per i diritti e le libertà degli interessati indicati nell'articolo 35 (1) del GDPR:

  Laddove un tipo di trattamento che in particolare utilizza nuove tecnologie e tiene conto della natura, dell'ambito, del contesto e delle finalità del trattamento stesso, probabilmente determinerà un alto rischio per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima del trattamento, eseguirà una valutazione dell'impatto delle operazioni previste sulla protezione dei dati personali. Una singola valutazione potrebbe riguardare una serie di operazioni di trattamento simili che presentano alti rischi simili.
- Le misure previste per gestire questi rischi, inclusi misure di salvaguardia, misure di sicurezza e meccanismi per garantire la protezione dei dati personali e la conformità al GDPR tenendo conto dei diritti e degli interessi legittimi degli interessati e di altre persone coinvolte

Lo sforzo che sia appropriato per investire in una *valutazione dell'impatto sulla protezione dei dati* dipende dalle circostanze. Un sistema di video sorveglianza con rischi inerenti elevati o uno che pone problemi nuovi o complessi richiede un maggiore sforzo in termini di investimenti rispetto a uno con un impatto proporzionalmente limitato sulla privacy e altri diritti fondamentali, come un sistema CCTV statico convenzionale utilizzato per tipiche finalità di sicurezza.

In ogni caso, in una *valutazione dell'impatto sulla protezione dei dati* formale o altrimenti, le organizzazioni devono valutare e giustificare se ricorrere alla video sorveglianza, come collocare, selezionare e configurare i loro sistemi e come implementare misure di salvaguardia volte alla protezione dei dati.

Inoltre, ci possono essere dei casi in cui un'organizzazione propone un sistema non standard. In questo caso, l'organizzazione deve valutare attentamente le differenze pianificate dalla pratica e dai consigli, discuterli con il responsabile della protezione dei dati e con altre parti interessate e documentarne la valutazione per iscritto, in una *valutazione dell'impatto sulla protezione dei dati* formale o altrimenti. Anche la verifica del sistema dell'organizzazione deve rispettare la legittimità della personalizzazione del sistema stesso.

Infine, per la sua complessità, novità, specificità o rischi inerenti, si consiglia di eseguire una *valutazione dell'impatto sulla protezione dei dati* nei seguenti casi:

- Video sorveglianza per finalità diverse dalla sicurezza (tra cui per scopi di indagine)
- Video sorveglianza di spazi pubblici
- Monitoraggio dei dipendenti
- Monitoraggio sul territorio dello Stato membro o di paesi terzi
- Categorie speciali di dati
- Aree incluse in aspettative elevate di privacy

- Video sorveglianza high-tech e/o intelligente
- Sistemi interconnessi
- Registrazione audio

La *valutazione dell'impatto sulla protezione dei dati* può essere eseguita internamente o da un appaltatore indipendente. La valutazione deve essere condotta nella fase iniziale del progetto. In base ai risultati della *valutazione dell'impatto sulla protezione dei dati* un'organizzazione può decidere:

- Di astenersi da o modificare il monitoraggio pianificato e/o
- Di implementare misure di salvaguardia aggiuntive

Rischi inerenti con l'uso del VMS

Durante la gestione della *valutazione dell'impatto sulla protezione dei dati*, occorre essere al corrente in merito ai rischi inerenti con l'uso del VMS.

La *valutazione dell'impatto sulla protezione dei dati* deve essere adeguatamente documentata. In linea di principio, un report di *valutazione dell'impatto sulla protezione dei dati* deve chiaramente specificare i rischi per la privacy e/o altri diritti fondamentali che l'organizzazione ha identificato, nonché le misure di salvaguardia aggiuntive proposte. Tenere presente i seguenti rischi di violazione dei diritti personali:

- Azienda/Datore di lavoro, utilizzando feed video, allarmi o registri attività utente per:
    - Monitorare gli orari di lavoro dei dipendenti nel sito oggetto di indagine, ad esempio, l'ora di arrivo e di partenza
    - Monitorare l'efficienza dei dipendenti controllando dove trascorrono il loro tempo, la quantità di tempo passata presso la macchinetta del caffè, il tempo impiegato nei bagni, purché lavorino in maniera efficiente per qualsiasi compito loro abbiano
    - Monitorare ciò che il dipendente osserva sugli schermi dei computer
    - Monitorare se i dipendenti rispettano i requisiti di lavoro o di sicurezza, ad esempio nei cantieri
    - Mostrare registrazioni video di dipendenti ad altri dipendenti o manager per bullizzare il dipendente o minacciare altri dipendenti di fare la stessa cosa
    - Controllare se addetti alla sicurezza/operatori svolgono le loro mansioni in modo efficiente, ad esempio verificando se utilizzando in maniera attiva i client, selezionando le telecamere, eseguendo le riproduzioni, ecc.
- Azienda/Proprietario/Operatore/Guardie, utilizzando feed video per:
    - Condividere registrazioni video di persone (dipendenti aziendali o il pubblico in generale) in situazioni imbarazzanti o sensibili sui social media
    - Utilizzare le telecamere PTZ per lo zoom avanti delle persone e ottenere registrazioni ravvicinate intime/inappropriate a loro insaputa.

- Società/Proprietario/Operatore/Guardie
  - Esportare video o fornire l'accesso al video registrato in maniera non critica a chiunque lo richieda

Fonti aggiuntive per identificare il rischio sono:

- La *Guida di rafforzamento di Milestone* fornisce Cyber Risk Management Framework, che descrive i sei passaggi consigliati di categorizzazione, selezione, implementazione, valutazione, autorizzazione e monitoraggio dei rischi. La *Guida di rafforzamento di Milestone* fornisce una serie di rischi tecnici e implementazioni consigliate per mitigare i rischi. Includono, tra le altre cose, la protezione della privacy del VMS in termini di una serie di violazioni dei dati e rischi di accesso non autorizzato dovuti a operazioni non efficienti di manutenzione, progettazioni e configurazione tecnica. Per ulteriori informazioni su come proteggere le installazioni di XProtect VMS da attacchi informatici, vedere la Guida di rafforzamento.
- La *Guida alla privacy di Milestone* (il presente documento) fornisce consigli su gestione dei rischi operativi non tecnici, inclusa la gestione di diritti e richieste dell'interessato, ruoli e responsabilità di un VMS, modelli per l'avviso sul posto, politica di video sorveglianza e *contratti del responsabile del trattamento*.
- Il corso di e-learning sulla privacy dell'utente finale di Milestone fornisce una formazione di sensibilizzazione per operazioni e supervisori del VMS su come, nel funzionamento quotidiano, gestire i rischi per la privacy correlati al VMS. Per ulteriori informazioni, vedere il sito Web della certificazione GDPR di Milestone.

Appendice: Contratto del responsabile del trattamento

Il titolare del trattamento deve aver stipulato un *contratto del responsabile del trattamento* con qualsiasi terza parte con cui il titolare del trattamento condivide i supporti di video sorveglianza, tranne la condivisione di tali supporti con le forze dell'ordine.

Se un'organizzazione ha esternalizzato tutte o parte delle attività di video sorveglianza a una terza parte (un responsabile del trattamento), deve comunque conformarsi al GDPR come titolare del trattamento. Ad esempio, gli addetti alla sicurezza che si occupano del monitoraggio della video sorveglianza live nell'area della reception di un'organizzazione che lavora per privati a cui l'organizzazione ha esternalizzato il compito del monitoraggio live. In questo caso, l'organizzazione deve assicurarsi che gli addetti alla sicurezza svolgano le loro attività in conformità alle disposizioni del GDPR.

Per un modello di esempio di un contratto del responsabile del trattamento, vedere il modello di contratto del responsabile del trattamento di *Milestone*.

Declinazione di responsabilità: Il *contratto del responsabile del trattamento* di esempio deve essere controllato dal titolare del trattamento. La conformità al GDPR mediante questo esempio è la sua area di responsabilità.

Appendice: Il sistema Milestone XProtect VMS e il GDPR

Tenere presente quanto segue: questa sezione descrive i requisiti e le restrizioni per essere un prodotto certificato con il marchio di certificazione europeo della tutela della privacy (EuroPriSe). Un titolare del trattamento/responsabile del trattamento che devia da questi requisiti non può indicare di utilizzare un prodotto che facilita in modo specifico la protezione dei dati e la conformità al GDPR.

Componenti e dispositivi non coperti dal marchio di certificazione europeo della tutela della privacy

I seguenti componenti non sono coperti dal marchio di certificazione europeo della tutela della privacy:

- Plug-in disponibili su Milestone Marketplace
- Server XProtect Mobile (disabilitato per impostazione predefinita)
- Client XProtect Mobile
- XProtect Web Client
- XProtect Access (disabilitato per impostazione predefinita)
- XProtect LPR (disabilitato per impostazione predefinita)
- XProtect Transact (disabilitato per impostazione predefinita)
- Milestone Interconnect
- XProtect DLNA Server
- Milestone Open Network Bridge (integrazione video pubblico-privato protetta)
- XProtect Event Server - Plug-in
- Trattamento dei dati audio (disabilitato per impostazione predefinita)
- Trattamento dei metadati (disabilitato per impostazione predefinita)
- Trattamento dei dati di dispositivi di input e output (disabilitato per impostazione predefinita)
- XProtect BYOL come fornito tramite https://aws.amazon.com/marketplace/pp/B089DKW36G

Affinché l'installazione di Milestone XProtect VMS sia coperta dal marchio di certificazione europeo della tutela della privacy, questi componenti non devono essere installati.

Inoltre, il prodotto standard non esegue riconoscimento facciale, analisi del comportamento, monitoraggio automatico o riconoscimento di persone nel feed live o nei supporti registrati. Anche queste funzionalità non sono conformi al marchio di certificazione europeo della tutela della privacy.

Ciò significa che, quando si installa XProtect VMS, non utilizzare l'opzione **Computer singolo** nel programma di installazione perché viene installato automaticamente Mobile Server.

Installare il sistema XProtect VMS con le opzioni **Distribuita** o **Personalizzata**. Non comporta l'installazione di Mobile Server.

Dopo aver installato XProtect VMS, la pagina di download in Management Server elencherà i componenti aggiuntivi DLNA Server e Mobile Server. Non installare questi server.

Guida all'aggiornamento

Se si sta eseguendo l'aggiornamento di un'installazione di Milestone XProtect VMS versione 2018 R2 o precedente, i vecchi file di registro devono essere eliminati manualmente affinché l'installazione sia conforme al GDPR.

Dopo l'aggiornamento di XProtect VMS, i file di registro precedenti possono essere eliminati utilizzando le informazioni e lo strumento descritto in questo articolo della Knowledge Base.

Rete protetta per dati di autenticazione e autorizzazione

Progettare un'infrastruttura di rete che utilizza la rete fisica o la segmentazione VLAN il più possibile.

Milestone consiglia di selezionare le telecamere che supportano HTTPS. Si consiglia di impostare le telecamere su VLAN separate e utilizzare HTTPS per la telecamera per la comunicazione con i server di registrazione, nonché i client per la comunicazione con i server di registrazione.

Si consiglia di collocare XProtect Smart Client e XProtect Smart Wall sulla stessa VLAN dei server.

Utilizzare una rete VPN crittografata o simile se si usa Smart Client o Smart Wall da un'ubicazione remota.

Abilitare la crittografia per tutte le comunicazioni. Per informazioni sulla protezione delle installazioni di XProtect VMS, vedere la Guida di rafforzamento e la Guida ai certificati.

> Tenere presente quanto segue: Il trasporto crittografato e non protetto dei dati video violerebbe il marchio EuroPriSe e porterebbe alla perdita della conformità al marchio di certificazione europeo della tutela della privacy EuroPriSe.

Mascheratura di individui in caso di accesso

Ai sensi dell'articolo 15 del GDPR, l'interessato ha il diritto di ottenere l'accesso ai suoi dati personali in fase di trattamento, ad esempio, le sue videoregistrazioni.

All'interessato viene concesso il diritto di chiedere a un'azienda informazioni su quali dati personali che lo riguardano vengono trattati e il motivo di tale trattamento.

Poiché XProtect VMS non supporta l'identificazione automatica di individui, occorre adottare misure aggiuntive per salvaguardare i diritti degli stessi. Nel contesto del VMS, vedere Appendice: Avviso sul posto a pagina 47.

Inoltre, XProtect VMS non supporta la mascheratura di altre persone in movimento e che vengono registrate insieme al ricorrente del diritto di accesso.

Diverse soluzioni di partner tecnici di Milestone per la sfocatura dinamica di tutte o altre persone prima dell'esportazione sono disponibili in Milestone Marketplace. In alternativa, può essere aggiunta una sfocatura a singole immagini o flussi video manualmente o assistita dopo l'esportazione. Alcune aziende offrono la sfocatura come servizio (ad esempio, FACIT Data Systems).

Eliminazione parziale di registrazioni video

Ai sensi dell'articolo 17 del GDPR, l'interessato ha il diritto di chiedere l'eliminazione dei suoi dati. Nel contesto del VMS, ciò spesso non si realizza a causa di interessi legittimi prevalenti (rilevamento delle frodi, salute e sicurezza) o altre finalità aziendali indicate nella politica di video sorveglianza (vedere Diritto all'oblio (diritto alla cancellazione) a pagina 34 e Appendice: Politica di video sorveglianza a pagina 47). La politica di video sorveglianza definisce la conservazione automatica (il valore predefinito è 7 giorni) che garantisce l'eliminazione automatica delle riprese e deve tenere nel debito conto sia i diritti degli interessati sia le finalità aziendali ragionevoli.

Se un interessato richiede di eliminare i suoi dati, si consiglia al titolare del trattamento di utilizzare una *richiesta dell'interessato* per documentare il reclamo (vedere Richiesta dell'interessato a pagina 11). Per un modello di esempio di una richiesta dell'interessato, vedere il modello di richiesta dell'interessato di *Milestone*.

È necessario eliminare tutte le registrazioni dalla telecamera o dalle telecamere in questione.

Per conservare tutte le altre registrazioni che non devono essere eliminate, esportare tutti i dati e tenerli al sicuro. Non è possibile ripristinare questi dati nel VMS.

Qualsiasi esportazione deve essere crittografata e firmata digitalmente e infine escludere gli intervalli di tempo specificati da una o più telecamere specifiche. Ossia, l'esportazione deve avvenire fino all'ora/alla data specificate e dopo l'ora/la data specificate. Questo può determinare backup in più periodi di tempo.

Smart Client – Player può quindi essere utilizzato per visualizzare i dati.

Si consiglia al titolare del trattamento di richiedere consulenza legale, condurre una valutazione dell'impatto sulle imprese e una valutazione dell'impatto sulla privacy (vedere Conduzione di una valutazione dell'impatto a pagina 30) prima di esercitare il diritto all'oblio dell'interessato, poiché l'eliminazione può introdurre nuovi rischi aziendali che potrebbero compromettere la ponderazione degli interessi e introdurre rischi che influiscono negativamente sulla protezione della privacy di altri interessati.

Uso di sfondi geografici in XProtect Smart Client

XProtect Smart Client supporta l'uso di sfondi geografici. Questi sfondi visualizzano gli sfondi delle mappe.

Si rischia di violare il GDPR se si utilizza uno qualsiasi dei seguenti servizi di mappe e non si sarà conformi al GDPR nell'ambito della certificazione EuroPriSe:

- Bing Maps
- Google Maps
- Milestone Map Service

Questi servizi non forniscono misure di salvaguardia adeguate relative al trattamento dei dati personali negli Stati Uniti. Il cliente diventa il titolare del trattamento (congiunto) per quanto riguarda il trattamento dei dati utente.

Fare riferimento a eventuali aggiornamenti alla sentenza Schrems II da parte della Commissione UE sul sito Web ufficiale.

In alternativa, si consiglia di configurare il servizio **OpenStreetMap** privato per lo sfondo geografico.

Integrazioni di partner registrati

Quando viene attivata una licenza, Milestone raccoglie dati per ciascuna integrazione. XProtect VMS raccoglie i dati sui plug-in e sui produttori di plug-in, nonché sui plug-in e sull'integrazione utilizzata dal cliente.

I dati raccolti da ciascuna installazione sono:

- Nome dell'integrazione
- Produttore dell'integrazione
- Versione dell'integrazione
- Tipo di integrazione (autonomo, Smart Client, Management Client, Event Server) e numero di istanze di ciascun tipo (ossia, su quanti client è in esecuzione il plug-in)

Gli sviluppatori di plug-in non devono mai utilizzare nomi personali durante la registrazione del loro prodotto. Utilizzare solo il nome dell'azienda.

I dati vengono trattati da Milestone solo se il produttore del plug-in è elencato nel marketplace e ha approvato il trattamento dei dati allo scopo di migliorare Milestone XProtect Corporate (e non per finalità di marketing e di ricerche di mercato). Se il plug-in non è stato registrato, i dati vengono eliminati immediatamente. La base legale del trattamento è l'articolo 6 (1)(f) del GDPR, che mostra interessi legittimi di Milestone e degli utenti del VMS.

Misure di salvaguardia aggiuntive

Per meglio garantire la conformità della configurazione di Milestone XProtect VMS al GDPR, questo elenco fornisce alcune misure di salvaguardia aggiuntive da tenere a mente quando si configura il sistema.

Problema	Impatto negativo sulla privacy	Suggerimenti per il titolare del trattamento
Le telecamere PTZ e la mascheratura privacy non funzionano insieme. Le mascherature non seguono i	La privacy che esalta l'effetto della mascheratura può essere aggirata.	Milestone consiglia di effettuare una delle seguenti operazioni:

Problema	Impatto negativo sulla privacy	Suggerimenti per il titolare del trattamento
movimenti PTZ.		• Non utilizzare la funzione di mascheratura privacy incorporata di XProtect sulle telecamere PTZ perché la maschera è statica rispetto ai pixel decodificati dell'immagine e non alla direzione/all'ubicazione effettiva della telecamera PTZ. • Disattivare la funzionalità PTZ quando si utilizzano maschere. • Acquistare telecamere PTZ che supportano la mascheratura privacy dinamica (così le aree selezionare sono sempre mascherate indipendentemente dall'ubicazione e dallo zoom della telecamera).
L'uso del microfono o dei dispositivi dei metadati può violare la privacy personale. In XProtect Corporate, queste opzioni sono disattivate per impostazione predefinita.	L'utilizzo dei microfoni può facilmente violare la conformità al GDPR.	Prima di attivare i microfoni o i dispositivi di metadati, occorre assicurarsi di avere una finalità chiaramente giustificata per la raccolta di dati. Vedere Si dispone di un fondamento giuridico per la raccolta di dati? a pagina 26

Problema	Impatto negativo sulla privacy	Suggerimenti per il titolare del trattamento
	Tenere presente quanto segue: L'uso di microfoni e dispositivi di metadati non è coperto dal marchio di certificazione europeo della tutela della privacy. La loro attivazione violerebbe il marchio EuroPriSe.	
Operatori e amministratori possono esportare o copiare dati video, archivi video, backup di configurazione e registri attività utente in dischi rigidi locali o supporti rimovibili come CD, DVD, unità USB flash, ecc.	I dati personali escono dai limiti di governance di XProtect VMS. I dati non vengono più protetti da meccanismi di controllo accesso di XProtect VMS e non possono essere eliminati da XProtect VMS al termine del periodo di conservazione. Ciò comporta il rischio per cui i dati vengono memorizzati per più tempo di quello consentito, che vengono utilizzati per finalità differenti e che la riservatezza dei dati venga violata.	I titolari del trattamento adotteranno misure tecniche e organizzative per proteggere i dati che escono dal confine di XProtect VMS. Per le possibili misure da adottare, vedere Gestione dei dati esportati a pagina 19.
I dati di registri attività utente e altri dati personali non vengono crittografati dal prodotto prima che siano stati memorizzati nei	In particolare, i dati sensibili dei registri attività utente possono essere divulgati a utenti non autorizzati. Vedere Protezione dei	Effettuare le seguenti operazioni:

Problema	Impatto negativo sulla privacy	Suggerimenti per il titolare del trattamento
database SQL. Gli amministratori di database possono accedere ai dati di registri attività utente utilizzando client di database. XProtect Corporate non è in grado di controllare o registrare questo accesso.	dati memorizzati e trasmessi a pagina 43. Per ulteriori informazioni su come proteggere le installazioni di XProtect VMS da attacchi informatici, vedere la Guida di rafforzamento.	• Implementare un concetto di ruolo adeguato per l'amministrazione di database. • Limitare l'accesso al database solo al personale autorizzato. • Se possibile, attivare la crittografia del database utilizzando i meccanismi corrispondenti.
Il prodotto implementa una funzione di backup. Questa funzione consente di eseguire il backup della configurazione del VMS ma non del database di registri attività utente.	La distruzione fisica del supporto di dati che contiene il database di registri attività utente potrebbe impedire al titolare del trattamento di adempiere ai suoi doveri di responsabilità quando non esistono backup dei registri stessi.	Considerare la creazione di backup di database di registri attività utente. Se il titolare del trattamento decide di creare backup del database di registri attività utente, dovrebbe anche stabilire una procedura per eliminare i backup al termine del periodo di conservazione e proteggerli dall'accesso non autorizzato (ad esempio, crittografando il backup, mettendo sotto chiave i supporti di backup, ecc.). Per ulteriori informazioni, vedere il Manuale dell'amministratore per VMS XProtect.
XProtect VMS utilizza per la comunicazione client-server e server-server token di autenticazione/autorizzazione non protetti a livello di	Gli autori degli attacchi con accesso alla rete potrebbero acquisire di nascosto i token e utilizzarli per fingersi utenti del VMS o componenti server. Ciò potrebbe compromette la	Effettuare le seguenti operazioni:

Problema	Impatto negativo sulla privacy	Suggerimenti per il titolare del trattamento
crittografia su canali di comunicazione non protetti.	riservatezza dei dati video o l'integrità dell'intero sistema. Tenere presente quanto segue: Configurare VPN e/o HTTPS per proteggere le comunicazioni non protette in modo da essere conformi al marchio EuroPriSe.	• Utilizzare VPN protette a livello di crittografia. Per ulteriori informazioni su come proteggere le installazioni di XProtect VMS da attacchi informatici, vedere la Guida di rafforzamento. • Separare le reti. Per ulteriori informazioni su come proteggere le installazioni di XProtect VMS da attacchi informatici, vedere la Guida di rafforzamento. • Configurare l'indirizzo HTTPS per Recording Server. Per informazioni sulla protezione delle installazioni di XProtect VMS, vedere la Guida di rafforzamento e la Guida ai certificati.
Il funzionamento di una VPN in modalità suddivisione potrebbe mostrare l'indirizzo IP privato degli utenti di XProtect VMS.	Quando è abilitato il tunneling suddiviso, gli utenti aggirano le misure di sicurezza a livello di gateway che potrebbero essere stata applicate all'interno dell'infrastruttura di rete.	Effettuare le seguenti operazioni:

Problema	Impatto negativo sulla privacy	Suggerimenti per il titolare del trattamento
		• Utilizzare una connessione VPN protetta (una VPN è protetta per impostazione predefinita, ma alcuni protocolli VPN precedenti non crittografano i dati scambiati tra il server e il client) • Utilizzare sempre il tunneling completo • Utilizzare i protocolli di autenticazione più alti supportati (se presenti) • Utilizzare Active Directory per autenticare utenti VPN Per ulteriori informazioni su come proteggere le installazioni di XProtect VMS da attacchi informatici, vedere la Guida di rafforzamento.
Il prodotto consente l'impostazione dei periodi di conservazione per registri attività utente, dati video, allarmi e altri dati personali.	L'impostazione di periodi di conservazione troppo lunghi potrebbe violare i requisiti del GDPR per le limitazioni di memorizzazione (articolo 5 (1)(e) e articolo 17 del GDPR).	I periodi di conservazione devono essere adattati alle finalità di trattamento (vedere Diritto all'oblio (diritto alla cancellazione) a pagina 34).
Gli amministratori possono configurare i destinatari e-mail che potrebbero riceve frammenti di video o fermi	Un errore di digitazione potrebbe eventualmente portare a una violazione dei dati quando una terza parte riceve messaggi e-mail con	Rendere il titolare del trattamento consapevole di questo rischio.

Problema	Impatto negativo sulla privacy	Suggerimenti per il titolare del trattamento
immagine dal VMS quando si verificano determinati eventi. Non è possibile configurare un elenco di domini consentiti per tali destinatari e-mail.	dati video e allarmi di sistema.	Milestone consiglia di stabilire una procedura organizzativa come il principio dei quattro occhi che riduce il rischio di errori durante l'immissione degli indirizzi e-mail.
Le notifiche sono messaggi e-mail inviati all'indirizzo e-mail specificato. Durante la creazione di una notifica, l'amministratore può scegliere di includere una serie di istantanee o un'AVI di una sequenza.	Poiché le istantanee e le sequenze AVI allegate presenti nelle notifiche escono dal VMS, sono fuori del controllo del VMS per quanto riguarda l'accesso utente e la conservazione.	Poiché i messaggi e-mail e il relativo contenuto esulano dal controllo del VMS in termini di accesso utente e conservazione, si consiglia di non allegare immagini o sequenze AVI alle notifiche e-mail. Se il cliente necessita di questa funzione, deve almeno assicurarsi che esistano procedure e controlli organizzativi per chi riceve i messaggi e-mail e per come vengono gestiti. Consultare Gestione dei dati esportati nelle notifiche ed e-mail a pagina 20.

Appendice: Trattamento dei dati nell'ambiente Milestone XProtect VMS

La *Documentazione dell'architettura del sistema di Milestone* descrive i componenti del sistema e il modo in cui interagiscono tra di loro e con componenti di sistema dell'ambiente. Per ciascuno dei casi d'uso pertinenti del prodotto, è disponibile un diagramma che illustra il flusso di comunicazione tra i componenti coinvolti nei casi d'uso. Questi diagrammi forniscono una panoramica generale dei dati trasferiti. Per informazioni su come i componenti di Milestone XProtect VMS interagiscono, vedere il documento di Milestone che descrive l'architettura di sistema.

Questa sezione elenca i processi di installazione di XProtect predefiniti di dati personali, dati di autenticazione e configurazione pertinenti per le impostazioni di privacy e sicurezza.

Dati personali del sistema VMS

Il tipo di dati principale è rappresentato dai dati video delle videocamere. Questi dati vengono memorizzati dal servizio Recording Server. I dati video possono essere eseguiti in streaming live o in modalità riproduzione in XProtect Smart Client. L'altra parte di dati riguarda i dati master degli utenti del VMS che sono memorizzati nel database SQL.

Dati personali dell'ambiente

I dati personali sugli utenti del VMS provengono dall'ambiente Windows dove Active Directory (AD) viene utilizzato per l'autenticazione utente e come sorgente per l'appartenenza a gruppi. Il servizio Milestone XProtect Management Server esegue query su AD tramite il protocollo LDAP per ottenere informazioni sugli utenti che si stanno connettendo al sistema.

Dati personali del sistema

Questi dati personali comprendono tutti i tipi di dati necessari per proteggere, configurare, utilizzare, sottoporre a manutenzione o altrimenti supportare il sistema. I tipi di dati personali includono:

- Dati dei registri

  I sistemi IT di solito registrano dati di utente e sistema nei file di registro attività utente e di debug per aiutare ad azionare e sottoporre a manutenzione i sistemi. XProtect Corporate agisce nello stesso modo. Il VMS registra le informazioni sulla maggior parte delle azioni utente nel database SQL. Questo registro attività utente viene utilizzato per comprendere la responsabilità delle azioni passate e il comportamento del sistema e quindi tenere traccia dell'uso improprio del sistema. I file di registro di debug vengono utilizzati per identificare vizi e difetti nel sistema. I dati di debug possono contenere o meno dati personali.

  Le voci di registro e i dati di debug possono rivelare informazioni dettagliate sull'utilizzo del sistema da parte di operatori e amministratore e potrebbero essere adatti a monitorare comportamento e rendimento dei dipendenti.

- Registrazione dell'autenticazione

  Il server di autorizzazione OAuth Duende e Identity Provider (IDP) creano file di registro attività utente con i dati personali sul nodo server sui cui è in esecuzione IDP.

  La registrazione si verifica quando:

  - Un utente modifica la password
  - Accesso non riuscito
  - Bloccato una volta superato il numero consentito di tentativi di accesso corretto
  - Accesso riuscito

  Il file di registro viene memorizzato in \\ProgramData\Milestone\IDP\Logs\idp-audit.log.

  Il file di registro è accessibile solo all'utente IIS e agli amministratori locali. Se l'utente IIS cambia, queste autorizzazioni devono essere aggiornate.

  I registri vengono riprodotti in maniera ciclica in un intervallo di 24 ore e vengono eliminati dopo 30 giorni, per impostazione predefinita. L'impostazione del registro è configurabile nel file NLog.config.

Dati di autenticazione e autorizzazione

- Autenticazione utente nel VMS

  Esistono due opzioni per autenticare gli utenti del VMS di XProtect Management Client e XProtect Smart Client. È possibile utilizzare i meccanismi di accesso Windows o l'autenticazione nativa del VMS.

  In un ambiente Windows Active Directory, è possibile configurare l'uso del meccanismo di accesso Windows incorporato. Per impostazione predefinita, l'autenticazione con accesso Windows si basa sul protocollo Kerberos. Questa è l'opzione più protetta. In ambienti legacy, i controller di dominio potrebbero non supportare Kerberos. In questo caso, si verifica automaticamente il fallback dell'accesso Windows al protocollo NT Lan Manager (NTLMv2), che è ritenuto meno protetto di Kerberos.

  In ambienti senza un controller di dominio Windows, è possibile utilizzare il metodo di autenticazione nativa di XProtect, che è l'autenticazione di base con ID utente e password in SQL Server o l'autenticazione di Windows per Workgroup, se disponibile.

  Esistono quindi tre tipi di credenziali di autenticazione:

  - Token di accesso Windows (token Kerberos o NTLM)
  - Credenziali dell'autenticazione di base
  - Autenticazione di Windows per Workgroup

  Dopo la corretta autenticazione, l'utente è connesso al VMS e viene creata una sessione utente dal servizio Management Server, dove viene visualizzata la schermata di accesso. Il client può ora accedere alle funzionalità del servizio Management Server nel contesto di questa sessione utente. Quando l'utente desidera accedere alle funzionalità del servizio Recording Server, XProtect Smart Client richiede una sessione utente anche con questo servizio server.

- Autenticazione utente nel servizio Recording Server

  Poiché la sessione utente tra XProtect Smart Client/XProtect Management Client e il servizio Management Server non può essere riutilizzata per accedere a Recording Server, Recording Server deve autenticare anche l'utente. Per autenticarsi nel servizio Recording Server, il servizio Management Server fornisce al client un token di autenticazione, richiesto dal client stesso per presentarsi al servizio Recording Server. Allo stesso tempo, il servizio Management Server invia il token di autenticazione a tutti i servizi Recording Server nell'installazione del VMS. A loro volta possono essere utilizzati per autenticare gli utenti successivamente.

  XProtect VMS utilizza un semplice GUID come un token di autenticazione, che il client invia al servizio Recording Server. I GUID vengono creati e gestiti dal servizio Management Server, che rinnova questi token dopo un periodo specificato. Il GUID è semplicemente un identificatore per l'utente nel database SQL Server.

  Tenere presente quanto segue: questi token non sono stati trasmessi in un modo protetto a livello di crittografia dal VMS e ciò richiede misure di salvaguardia aggiuntive a livello di rete dell'ambiente. Per i dettagli, vedere Misure di salvaguardia aggiuntive a pagina 56 e per informazioni sulle reti protette, vedere Appendice: Il sistema Milestone XProtect VMS e il GDPR a pagina 53.
  È importante adottare ulteriori misure per assicurarsi di disporre di un prodotto conforme a EuroPriSe.

- Dati di autorizzazione

  I dati di autorizzazione per gli utenti del VMS vengono memorizzati nel database SQL in SQL Server. All'avvio, i servizi Management Server e Recording Server estraggono i dati di autorizzazione pertinenti, inclusi i token di autenticazione per tutti gli utenti del database SQL, per essere pronti per l'accesso utente successivo ai server. Quando un amministratore cambia le autorizzazioni o i ruoli o qualsiasi altro aspetto che influisce sull'autorizzazione dell'utente, questo aggiornamento viene memorizzato dal servizio Management Server nel database SQL in SQL Server e anche attivamente propagato a tutti i servizi Recording Server. I servizi Recording Server memorizzano localmente i dati di autorizzazione utente e tutti i token di autenticazione e quindi possono immediatamente autenticare gli utenti client che presentano il loro token di autenticazione.

- Dati di configurazione

  A parte i dati di visualizzazione, impostati da XProtect Smart Client, tutti i dati di configurazione per il sistema VMS vengono configurati tramite XProtect Management Client del VMS e memorizzati nel database SQL. Esistono diversi tipi di dati di configurazione:

  - Impostazioni e preferenze dell'utente
  - Autorizzazioni dell'utente
  - Configurazione del server
  - Impostazioni di sistema
  - Configurazione di telecamere e dispositivi

  Sebbene i dati di configurazione potrebbero non contenere dati personali, possono influire sulla modalità di trattamento dei dati personali da parte del VMS. Solo per la valutazione, sono pertinenti le informazioni di autorizzazione e le impostazioni di sicurezza e privacy tra i dati di configurazione elencati sopra.

helpfeedback@milestone.dk

Informazioni su Milestone

Milestone Systems è un produttore leader mondiale di software di gestione video a piattaforma aperta che offre una tecnologia in grado di garantire sicurezza, proteggere le risorse ed aumentare l'efficienza aziendale. Milestone Systems supporta una comunità di partner e tecnologie che stimola la collaborazione e l'innovazione nello sviluppo e nell'uso di tecnologia video di rete, con soluzioni affidabili e scalabili testate in oltre 150.000 siti al mondo. Fondata nel 1998, Milestone Systems è un'azienda indipendente del Canon Group. Per ulteriori informazioni, visitare https://www.milestonesys.com/.