Video sorveglianza adempimenti

Nota: l'intera relazione va allegata all'informativa privacy linkata dal cartello con le indicazioni semplificate e link per conoscere le modalità di funzionamento nel dettaglio.

Premesse

Introduzione

La presente guida riguarda l'uso di impianti solo per la tutela del patrimonio aziendale (furti, danni, manomissioni).

Immagini statiche vs video

Video sorveglianza include anche la registrazione di immagini fisse solo se attivate da sensore di movimento. Sarà considerata meno invasiva per le caratteristiche, ma gli adempimenti sono gli stessi.

Autorità

Due sono le autorità competenti prima dell'installazione dell'impianto:

- Ispettorato del lavoro
- Garante

Gli adempimenti, datati, DEVONO PRECEDERE l'installazione, non solo l'attivazione. Entrambe considerano "negativamente" la sola installazione indipendentemente che sia gestita in autonomia dai dipendenti.

Principi

I principi base sono:

- trasparenza
- chiarezza nei trattamenti che saranno fatti
- documentare il tutto

Differenza tra videosorveglianza e firewall, antivirus e controlli informatici e geolocalizzatori

La circolare 5 del 19 febbraio 2018 dell'ispettorato nazionale del lavoro, rivolta agli ispettorati regionali e territorialmente competenti, spiega (alla fine) che:

- i sistemi di sorveglianza a distanza sono quelli non installati sul pc affidato al dipendente.
- antirivirus e firewall vanno considerati parte della macchina affidata al dipendente, necessari per il funzionamento, e non per controlli da remoto.

Quindi antivirus e firewall non sono trattati come videocamere SOLO SE presenti sui singoli dispositivi in quanto considerati indispensabili a rendere la prestazione lavorativa. Una gestione centralizzata richiede altra domanda su altro modulo.

I moduli sono su: https://www.ispettorato.gov.it/it-it/strumenti-e-servizi/Modulistica/Pagine/Home-Modulistica.aspx

Step pratici

- invio istanza
  - relazione con
    - finalità
    - motivazioni
    - modalità
      - durata
      - accesso remoto
    - ipotesi trattamento di illecito
  - modulo istanza (si compila online)
  - modulo marche (si compila online)
  - documento identità
  - indicazione della pec
  - inviare a INL territorialmente competente
- informative
  - cartello
  - informativa completa
  - mansioni per addetto
- installazione
  - dopo risposta dell'ispettorato competente
- verifiche periodiche
  - controllo responsabile

Ispettorato del lavoro

La procedura pratica:

- Tutte le istruzioni sono su: https://www.ispettorato.gov.it/it-it/strumenti-e-servizi/Modulistica/Pagine/Home-Modulistica.aspx

- La domanda può essere compilata online su: https://www.ispettorato.gov.it/it-it/strumenti-e-servizi/Modulistica/Documents/Autorizzazione%20per%20impianti%20di%20videosorveglianza,%20localizzazione%20satellitare,%20altri%20strumenti%20di%20controllo/Modulo-INL-1-Istanza-autorizzazione-installazione-impianti-audiovisivi.pdf

La domanda (modulo inl1): - si puo' mandare via pec - allegando documento d'identità - allegando modulo sostitutivo per le marche d'identità (modulo inl1.4)

Istanza di autorizzazione

Su: https://www.ispettorato.gov.it/it-it/strumenti-e-servizi/Modulistica/Pagine/Home-Modulistica.aspxhttps://www.ispettorato.gov.it/it-it/strumenti-e-servizi/Modulistica/Pagine/Home-Modulistica.aspx

INL 1 - Modulo istanza di autorizzazione all'installazione di impianti audiovisivi Compila il modulo

- inserire i dati del richiedente l'autorizzazione
- rispondere alle domande molto semplici. Di solito:
  - non aver ricevuto visita ispettiva
  - tutela del patrimonio aziendale
  - numero di lavoratori attualmente in forza
  - che non vi sono rappresentanze sindacli
  - che si chiede una autorizzazione preventiva
- indicare la pec per ricevere l'autorizzazione in forma elettronica

Ricorda: in caso di modifiche, si dovrà chiedere la modifica, non una nuova autorizzazione.

Le dichiarazioni nell'istanza

Le dichiarazioni (prestampate) indicano le condizioni per poter ottenere e mantenere l'autorizzazione:

- che le apparecchiature riprenderanno i luoghi di lavoro connessi alle esigenze per le quali viene richiesta la presente autorizzazione;
- che le telecamere non riprenderanno luoghi riservati esclusivamente ai lavoratori (spogliatoi o servizi);
- ove possibile le telecamere non riprenderanno postazioni di lavoro in maniera continuativa;
- che le immagini non saranno in alcun modo diffuse all'esterno, tranne che per la necessità di tempestiva consegna all'Autorità giudiziaria competente qualora si verifichi una fattispecie delittuosa;
- che si provvederà ad informare tutti i lavoratori nelle forme previste dall'art.4, comma 3, della legge n.300/1970;
- che sarà rispettata la disciplina dettata dal Regolamento UE 2016/679 in materia di trattamento dei dati personali;

Gli allegati all'istanza

- La relazione da allegare, firmata dal legale rappresentante deve contenere le ragioni di tutela del patrimonio aziendale (o le altre previste nelle istruzioni)
- le modalità di funzionamento del sistema
- la modalità di conservazione dei dati
- la gestione dei dati
- le caratteristiche tecniche del sistema (allegando marca e modello)
- copia del documento d'identità del rappresentante legale, se istanza inviata via pec
- modulo INL 1.4 - Dichiarazione sostitutiva per marca da bollo compilabile online

La relazione

L'associazione UAAR | Unione degli Atei e degli Agnostici Razionalisti (d'ora in aventi "ente")con sede in Via Francesco Negri, 67/69, 00154 Roma RM, pec: uaar@pec.it in persona del Roberto Grendene in qualità di legale rappresentante pro tempore allega all'istanza di autorizzazione all'installazione di impianti audiovisivi la presente:

Relazione

- l'ente non ha RSA nè RSU (rappresentanti sindacali aziendali nè unitari);
- gli uffici dell'ente ospitano i dispositivi informatici per l'accesso e gestione all'intera attività associativa e una biblioteca non aperta al pubblico per la consultazione e richiesta in prestito di opere;
- La video sorveglianza verrà attivata fuori degli orari di apertura per la tutela aziendale da:
  - intromissioni o furti denunciati;
  - presenza di risorse componenti e beni immateriali di levato valore intrinseco, tra i quali:
    - i dati degli associati e trattati nello svolgimento delle attività dell'ente, da tutelare anche ex privacy;
    - la documentazione dei soci e delle attività dell'ente;
    - le comunicazioni informatiche dell'ente;
    - gli strumenti hardware per gestire tali dati;
    - la cassa per i contanti;
    - il nas senza accesso da remoto per i backup;
  - i locali con risorse informatiche, armadi, arredi e la libreria sono attigui e negli orari di chiusura non sono accessibili; l'uso dei sensori è ovviamente ragionevole solo in assenza di personale fuori dell'orario di lavoro e in assenza di personale autorizzato.
- l'impianto di videosorveglianza Verisure (con sensori di movimento sulla camera) che scatterà sequenze di immagini sui beni aziendali quando attivo;
  - l'impianto verrà attivato quando l'ultimo dipendente esce dagli uffici, e disattivato al primo accesso;
  - le immagini potranno essere consultate o scattate da remoto tramite app sulla cloud di verisure solo su evidenze concrete di pericolo per il patrimonio aziendale;
  - l'addetto sarà il sig. David Schacherl che utilizza le credenziali di accesso fornite da Verisure anche sui dispositivi personali in caso di avviso remoto;
- le aree che saranno interessate:

    - le porte di accesso ai locali, sala lettura, riunione, entrata, retro e limitrofe;
    - le vetrine
- le immagini saranno cancellate dalla cloud di verisure automaticamente dopo 30 giorni se non cancellate manualmente prima come da procedure qui indicate;
- l'addetto è un dipendente incaricato di attivare in assenza e disattivare in presenza di personale, così come indicato nel registro privacy
- l'accesso in remoto può avvenire solo previa segnalazione di anomalia da documentare e annotare nel registro privacy.
- l'accesso in remoto al servizio di Verisure resta nei log per sei mesi;
- idoneo cartello verrà apposto ben visibile prima di entrare nel raggio di azione della videocamera con link all'informativa completa sul sito;
- le immagini sono conservate fino a 48 ore dalla riapertura degli uffici in caso di acquisizione su segnalazione del sensore; si ricorda che per lunghi periodi di chiusura per vacanze il cloud di verisure cancella tutto dopo 30 giorni dall'acquisizione. 48 ore sono considerate sufficienti per predisporre l'eventuale denuncia alle autorità, insieme al legale ove necessario.
- i dati acquisiti, una volta controllati, possono essere inviati alle autorità, sentito il consulente dell'ente; se non ci sono motivi per ulteriori accertamenti, da documentare, vanno cancellati tempesticamente e non oltre 24 ore.
- i dati inviati alle autorità saranno trattati per tutta la durata delle investigazioni, del procedimento e per i procedimenti legali e le procedure assicurative connesse (appelli, risarcimento danni, etc.).
- l'acquisizione di immagini solo successivamente all'attivazione di un sensore di movimento, acceso solo durante la chiusura degli uffici, esclude un trattamento in larga scala e in luogo pubblico; cosi' come il controllo sistematico dei lavoratori. Il fornitore Verisure Italy srl, ben più che autorevole, garantisce il rispetto del GDPR.

Rischi, mansioni e misure di sicurezza

- il rischio di acquisizione di immagini statiche di individui, per errore, e' ridotto al minimo per le modalità di funzionamento del sistema;
- il rischio del trattamento di tali dati influisce, in caso di riconoscimento dell'autore dell'illecito, per l'avvio di attività giudiziarie solo previa valutazione dei soggetti preposti alle indagini e non automaticamente.
- il rischio è mitigato ulteriormente in quanto l'impianto è gestito solo in orari di chiusura e secondo queste direttive dagli stessi addetti, i cui log sono tracciati.
- il rischio di un accesso remoto da parte di terzi alla cloud è residuale, acquisendo dati in orari non consentiti, ma i sistemi di avviso consentono di intervenire immediatamente cancellando e modificando le credenziali di accesso, tenendone traccia nel registro privacy.
- l'accesso alla biblioteca, che non è aperta al pubblico, avviene solo negli orari di apertura degli uffici; il controllo della consultazione e/o prestito librario tramite videocamera negli orari di apertura è vietato.
- detto questo vi sono motivi per ritenere basso il rischio sui dati personali e i diritti degli interessati. Non essendovi trattamento di dati nè in pubblico nè in larga scala non si considera necessaria la DPIA.
- Andranno affidate all'incaricato le seguenti mansioni:
    - effettuare dei test di funzionamento periodicamente per verificare il funzionamento;
    - eventuali aggiornamenti software;
    - il funzionamento delle notifiche di allerta e
    - l'aggiornamento delle credenziali di accesso con altre sempre complesse;
    - I dispositivi personali che possano accedere in remoto dovranno prevedere un ulteriore blocco all'accesso del dispositivo se non anche della singola app;
    - con divieto di qualsiasi utilizzo che non sia quello di condividere entro 48 ore dal rientro sul posto di lavoro, con la dirigenza, per l'incarico al consulente la valutazione, dell'eventuale azione legale;
    - cancellare entro 48 ore dal rientro sul posto di lavoro ogni immagini irrilevante.
- In relazione al decreto trasparenza, d.lgs. 104/2022, direttiva UE 1152/2019, si precisa che il sistema non comporta decisioni automatizzate.

Si aggiunge espressamente, anche ai fini dell'informativa, la modalità di funzionamento che Verisure indica sul propri sito:

"Quando rilevano un movimento sospetto, questi sensori di movimento per antifurto scattano 5 immagini dell’evento e le inviano alla Centrale Operativa Verisure per la verifica dell’evento. La Centrale Operativa gestisce lo scatto d’allarme in meno di 60 secondi, elimina possibili falsi allarmi ed intervenire tempestivamente."