# Videosorveglianza in azienda: come redigere l’atto di “documentazione delle scelte”

Si chiama “documentazione delle scelte” ed è un adempimento che si rende necessario tutte le volte in cui il datore di lavoro pianifichi di raccogliere dati personali dei lavoratori con il sistema della videosorveglianza. Si tratta di un’evenienza molto frequente attesa la pluralità di ragioni per cui può essere avviato un trattamento di tale genere, e cioè esigenze produttive, esigenze di sicurezza e/o esigenze di protezione del patrimonio aziendale. Per la mancata redazione di un atto di documentazione delle scelte secondo gli articoli 5 e 25 del GDPR l’azienda rischia una sanzione fino a 20 milioni di euro.

Per mettere in conformità privacy la **videosorveglianza**ci vuole un atto di “documentazione delle scelte”.

L’adempimento documentale inserisce sotto i riflettori del **regolamento UE sulla protezione dei dati** una analoga incombenza prevista dal provvedimento generale del Garante italiano del 29 aprile 2004. In questo provvedimento, sul punto, solo formalmente sorpassato dalle sopravvenienze normative, ma sostanzialmente vigente in quanto assorbito dalle prescrizioni relative alla responsabilizzazione (articolo 5 Gdpr), trovano posto le ragioni delle scelte.

## **Atto di documentazione delle scelte: quando è necessario**

La documentazione delle scelte è un adempimento che si rende necessario tutte le volte in cui il **datore di lavoro** pianifichi di **raccogliere dati** con il sistema della videosorveglianza.

Si tratta di un’evenienza molto frequente attesa la pluralità di ragioni per cui può essere avviato un trattamento di tale genere, e cioè esigenze produttive, esigenze di sicurezza e/o esigenze di protezione del patrimonio aziendale.

La norma nella quale fare rientrare la redazione di un atto di documentazione delle scelte è il sopracitato articolo 5 del GDPR oltre che l’articolo 25 del medesimo GDPR (privacy by design e by default).

## **In cosa consiste l’adempimento**

L’adempimento consiste nella stesura di un **documento specifico** a corredo dei progetti tecnici, che serva da parametro anche per gli audit successivi all’installazione.

Il datore di lavoro, inoltre, deve programmare **sessioni di verifica** delle modalità di utilizzo dell’impianto per verificare il rispetto delle cautele specifiche indicate nell’atto di documentazione delle scelte.

## **Contenuto dell’atto: lo schema tipo**

Tornando all’atto di documentazione delle scelte, in via generale, quando si parla di privacy le scelte sono quelle relative alle finalità e alle modalità del trattamento così come quelle relative alle misure tecniche e organizzative.

Questa sequenza di argomenti costituisce l’indice dello **schema tipo**di atto di documentazione delle scelte.

Vediamo di analizzarne i contenuti, ripercorrendo le voci del sommario, riportato nel frontespizio.

**Premessa**

Nella premessa il datore di lavoro deve inserire le declaratorie di politica aziendale.

**Profili soggettivi**

Nella sezione dedicata ai profili soggettivi vanno indicati i **nominativi** e i **dati di recapito** di coloro che promuovono e realizzano i relativi trattamenti. In questa sezione l’indicazione delle qualifiche operative introduce alla divisione dei compiti e delle correlate responsabilità interne ed esterne. In particolare, va indicato **chi rivesta i ruoli** di titolare del trattamento, contitolare del trattamento, responsabile esterno, altri responsabili. I soggetti designati particolari funzioni o compiti e i soggetti autorizzati possono essere indicati per categorie con richiamo del ruolo rivestito.

**Profili oggettivi**

Nella sezione dedicata ai profili oggettivi devono essere inseriti gli **adempimenti documentali** realizzati e il loro contenuto. Tale sezione diventa la base per la redazione degli atti di informazione, della designazione di autorizzato e dei contratti con terzi responsabili. Rispetto alle singole voci si rileva quanto segue.

|  |
| --- |
| **Registri del trattamento**: costituiscono una attestazione descrittiva del trattamento e vanno aggiornati sia dal titolare sia dal responsabile.  **Finalità**: deve essere una finalità corrispondente agli scopi societari e, quindi, compatibile con l’attività economica e con la disciplina della stessa.  **Liceità/base giuridica**: deve corrispondere ad una o più delle voci elencate agli articoli 6 e 9 del gdpr.  **Proporzionalità (minimizzazione)**: bisogna indicare le circostanze di fatto che escludono raccolta o utilizzo di dati non pertinenti o eccedenti rispetto alle finalità e che escludono l’ultroneità dei trattamenti rispetto a quelli indicati nelle informative.  **Dati trattati**: bisogna selezionare ed elencare i dati personali oggetto del trattamento; necessario spigare se si procede ad elaborazione particolari, profilazioni e simili.  **Operazioni eseguite**: bisogna selezionare le operazioni eseguite avendo cura di distinguere trattamenti più pericolosi, come quelli “aperti” di comunicazione.  **Modalità**: si deve descrivere l’apparecchiatura utilizzata e la logica dei trattamento complessi.  **Comunicazione**: va indicato l’ambito eventuale di comunicazione dei dati.  **Diffusione**: va indicato l’ambito eventuale di diffusione dei dati.  **Decisioni automatizzate**: va indicato se le immagini sono inserite in un percorso di trattamento effettuato a mezzo di macchine, ma con l’intervento umano.  **Decisioni interamente automatizzate**: va indicato se il trattamento avviene senza l’intervento umano e quale sia la logica del trattamento stesso.  **Termini conservazione**: se del caso, differenziare i termini di conservazione in relazione a diverse finalità. |

**Misure organizzative**

La sezione dà conto di “**chi” fa “che cosa”** e quale è il procedimento autorizzatorio interno nonché le modalità di profilazione degli autorizzati quali utenti dei sistemi IT. Si descrive, altresì, il coinvolgimento di esterni nel flusso del trattamento, il loro ruolo, i loro compiti e la loro responsabilità.

**Misure di sicurezza**

|  |
| --- |
| **Valutazione del rischio:**è necessario verificare se i documenti relativi alla analisi del rischio debbano essere aggiornati in relazione a nuove fonti e tipi di rischio e/o alla necessità di disporre nuove precauzioni.  **Valutazione di impatto privacy**: di fatto sempre necessaria a fronte della casistica in cui l’adempimento è obbligatorio (art. 35 gdpr).  **Consultazione preventiva**: valutare e dare conto se sia necessario o meno ricorrere al parere del garante ex art. 36 gdpr.  **Protocollo violazioni della sicurezza**: è necessario verificare se debbano essere aggiornati i documenti relativi al data breach (registro delle violazioni, protocollo di intervento). |

**Rapporto con gli interessati e misure di sorveglianza**

Nelle sezioni citate occorre indicare i seguenti dati.

|  |
| --- |
| **Atti di informazione agli interessati**: bisogna individuare le modalità della fornitura dell’informativa sintetica (cartello) e analitica.  **Protocollo esercizio dei diritti degli interessati**: a seconda dei casi può essere necessario/opportuno predisporre punti di contatto dedicati a soddisfare le istanze degli interessati, anche a riguardo del diritto di accesso mediante consegna di fotogrammi.  **Pareri/informazioni del dpo**: anche a prescindere dalla necessità di stesura di una valutazione di impatto privacy, il dpo deve essere coinvolto in tutte le scelte che implichino il trattamento dei dati.  **Audit**: è una misura di mantenimento della conformità legale e tecnica dei trattamenti di videosorveglianza, da programmare con obbligo di azioni conseguenti. |

## **Sanzioni**

Eventuali inadempimenti saranno sanzionati, ai sensi dell’articolo 83, paragrafi 4 e 5 del GDPR, con una sanzione fino a 20 milioni di euro in caso di violazione dell’articolo 5 GDPR.