REGOLAMENTO AZIENDALE PER LA VIDEOSORVEGLIANZA

Olbia, 01.04.2020

SOMMARIO

Art. 1 – Obiettivi e ambito di applicazione

Il presente Regolamento definisce i criteri e le modalità di installazione ed utilizzo dell'impianto di videosorveglianza, al fine di garantire che il relativo trattamento dei dati personali, effettuato presso le sedi ed i mezzi di ASPO S.p.A., si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale e soltanto per finalità di controllo e sicurezza delle suddette sedi del Titolare del Trattamento.

Le prescrizioni indicate nel presente documento vengono dettate in ottemperanza a quanto prescritto dalle seguenti fonti normative e Provvedimenti del Garante per la tutela dei dati personali:

- Regolamento Europeo n. 679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- D.Lgs. 196/2003 (Codice Privacy) ed allegato tecnico nella sua versione aggiornata al D.Lgs. 101/2018 e ss. mm.;
- Provvedimento Generale sulla Videosorveglianza emanato dal Garante per la protezione dei dati personali in data 8 aprile 2010 e ss. mm.;
- Linee Guida n. 3/2020 sul trattamento di dati personali attraverso la Videosorveglianza.

Per tutto quanto non risulti essere dettagliatamente disciplinato nel presente regolamento, si fa rinvio alla normativa vigente in materia di protezione dei dati personali ed ai provvedimenti del Garante in materia di videosorveglianza.

Art. 2 – Definizioni ai sensi dell'Articolo 4 del Regolamento Europeo 2016/679

Ai fini del presente Regolamento si intende:

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Particolari categorie di dati: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 del GDPR).

Dati personali relativi a condanne penali e reati: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR).

Dato anonimo: il dato che a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

"Blocco": la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;

Titolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

DPO – Data Protection Officer: persona designata dal Titolare o dal Responsabile come centro di competenza per il corretto trattamento dei dati personali.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratti dati personali per conto del titolare del trattamento.

Persone autorizzate al trattamento: le persone fisiche autorizzate, in base a specifiche istruzioni, a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro

Art. 3 – Finalità del trattamento

Il trattamento dei dati personali effettuato a seguito dell'attivazione dell'impianto di videosorveglianza persegue le suddette finalità:

a) salvaguardia e protezione del patrimonio aziendale, attraverso l'acquisizione dei dati utili ad impedire o comunque reprimere eventuali condotte contrarie alla legge (quali, a solo titolo esemplificativo, la commissione di furti, danneggiamenti, atti di vandalismo) nelle sedi o a bordo dei mezzi di trasporto;
b) sicurezza sul lavoro, mediante il costante monitoraggio, sia preventivo che successivo al verificarsi di un eventuale sinistro, del rispetto delle disposizioni in materia di sicurezza e infortuni sul lavoro;
c) prevenzione incendi, al fine di consentire un intervento immediato in caso di principio di incendio;
d) tutela della sicurezza dei passeggeri/utenti e dei dipendenti da attività illecite ed episodi di criminalità, sia presso le sedi di ASPO S.p.A., che a bordo dei mezzi di trasporto pubblico;
e) ricostruzione della dinamica di eventuali atti lesivi del patrimonio aziendale e dell'incolumità delle persone, al fine di consentire ed agevolare l'eventuale esercizio, in sede di giudizio civile e penale, del diritto di difesa del titolare del trattamento o dei soggetti che abbiano subito lesioni o danneggiamenti;
f) collaborazione con le forze di polizia e giudiziarie nello svolgimento delle indagini e nella raccolta di prove.

Art. 4 – Base giuridica del trattamento

Il trattamento dei dati personali effettuati tramite il sistema di videosorveglianza può essere considerato lecito sia in quanto effettuato in ottemperanza alle disposizioni di legge che regolano l'esercizio dell'attività di trasporto pubblico, ai sensi dell'art. 6, lett. c) del Reg. UE 2016/679, sia in quanto necessario per il perseguimento del legittimo interesse del titolare del trattamento alla tutela del patrimonio aziendale da furti e atti di vandalismo, oltre che alla fondamentale tutela della sicurezza dei propri dipendenti, collaboratori, utenti e di tutti i passeggeri di ASPO S.p.A., valido e prevalente sugli interessi, i diritti e le libertà dell'interessato, ai sensi dell'art. 6, comma1, lett. *f*) del Reg. UE 2016/679.

L'interesse legittimo predetto deve avere una reale consistenza, dimostrata dal fatto che si sia verificata una situazione di disagio nella vita reale, danni o incidenti gravi in

passato. Alla luce del principio di responsabilità, gli incidenti rilevanti si dovrebbero documentare, annotando in un apposito registro la data, le modalità, la perdita finanziaria e le relative accuse penali. Questi incidenti documentati possono rilevare un adeguato interesse legittimo.

Nel caso in cui le Forze di Polizia o l'Autorità Giudiziaria richiedano la consegna di alcuni video per lo svolgimento delle indagini, la base giuridica del trattamento deve essere rinvenuta nell'adempimento ad un obbligo di legge a cui è soggetto il Titolare del trattamento, ai sensi dell'art. 6, par. 1, lett. *c*), del Reg. UE 2016/679.

Art. 5 – Necessità del trattamento

I dati personali raccolti devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali sono trattati, nel rispetto di quanto previsto dal principio di "*minimizzazione dei dati*" dettato dall'art. 5, par. 1, lett. *c*) del Reg. UE 2016/679.

Deve essere valutata l'eventuale sussistenza di altri mezzi meno invasivi dei diritti e delle libertà fondamentali dell'interessato rispetto all'installazione di un sistema di videosorveglianza e procedere alla sua installazione solo nel caso in cui la ritenga l'unica misura adatta per raggiungere l'obiettivo desiderato, adeguata e necessaria al raggiungimento delle relative finalità.

Il sistema di videosorveglianza deve comportare esclusivamente il trattamento di dati personali rilevati mediante le riprese televisive che, in relazione ai luoghi di installazione delle videocamere, interessino i soggetti ed i mezzi di trasporto che transitino nell'area interessata di esclusiva proprietà del Titolare del Trattamento.

Nel caso in cui risultasse necessario estendere la videosorveglianza nelle immediate vicinanze dei locali, devono essere bloccate o oscurate tutte le aree non rilevanti.

L'attività di videosorveglianza deve raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando (quando non indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza. La localizzazione delle telecamere e le modalità di ripresa devono essere stabilite in modo conseguente a quanto qui precisato.

Nel caso in cui le apparecchiature vengano posizionate in aree nelle quali transitino lavoratori e collaboratori del titolare, le telecamere dovranno essere posizionate con un

angolo di ripresa che inquadri esclusivamente le parti dei locali più esposte a rischi e dalle quali derivi, in via del tutto accidentale ed occasionale, la possibilità di inquadrare i lavoratori.

In ogni caso è proibita la ripresa audiovisiva di singole postazioni o di singoli lavoratori durante l'orario lavorativo e sono da evitare telecamere ed apparecchiature che registrino l'audio. Al fine di tutelare il diritto alla riservatezza degli interessati, le telecamere non dovranno mai riprendere luoghi riservati esclusivamente al personale dipendente, come gli spogliatoi o i servizi igienici.

Art. 6 – Periodo di conservazione e obbligo di cancellazione

I dati personali non devono essere conservati più a lungo di quanto necessario per le finalità per le quali essi sono trattati. Tenendo conto dei principi di cui all'articolo 5, paragrafo 1, lettere c) ed e), del GDPR, in particolare la minimizzazione dei dati e la limitazione della conservazione, i dati personali dovrebbero essere cancellati automaticamente entro le 24 o 48 ore successive alla loro raccolta. Nel caso in cui sussistano comprovate esigenze, il tempo di conservazione delle immagini può essere esteso alle 72 ore successive alla loro raccolta.

Maggiore è il periodo di conservazione (in particolare se oltre le 72 ore), maggiori devono essere le argomentazioni fornite a sostegno della legittimità e necessità del trattamento. In ogni caso il periodo di conservazione deve essere chiaramente definito e impostato individualmente per ogni ciascuna finalità, nel rispetto dei principi di necessità e proporzionalità, conformemente alle disposizioni del Reg. UE 2016/679.

Art. 7 – Obblighi di trasparenza e informazioni agli interessati

Ai sensi dell'art. 13 del Reg. UE 2016/679, il titolare del trattamento deve fornire agli interessati dettagliate informazioni in merito al trattamento dei dati effettuato. Alla luce del volume di informazioni che è necessario fornire all'interessato, è preferibile seguire un approccio a più livelli: le informazioni più importanti dovrebbero essere visualizzate sul cartello di avvertimento stesso (primo livello o informativa semplificata) mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello).

Le informazioni sul sistema di videosorveglianza possono essere fornite in combinazione con un'icona al fine di fornire, in modo facilmente visibile, comprensibile e chiaramente leggibile, una panoramica significativa del trattamento previsto.

Il cartello contenente le informazioni dovrebbe essere posizionato ad una distanza ragionevole dai luoghi monitorati, in modo tale che l'interessato possa facilmente riconoscere l'esistenza della videosorveglianza prima di entrare nell'area monitorata (approssimativamente a livello degli occhi). Non è necessario specificare l'ubicazione precisa delle apparecchiature di sorveglianza, purché non vi siano dubbi su quali aree siano soggette a monitoraggio e sia chiaro in modo inequivocabile il contesto della sorveglianza.

L'interessato deve essere in grado di stimare quale area è acquisita da una telecamera in modo da poter evitare la sorveglianza o adattare il suo comportamento, se necessario.

I cartelli affissi dovrebbero trasmettere le informazioni più importanti, come:

a. i dettagli delle finalità del trattamento;
b. l'identità del Titolare del trattamento;
c. l'esistenza dei diritti dell'interessato;
d. le informazioni sui maggiori impatti del trattamento come, ad esempio, gli interessi legittimi perseguiti dal Titolare del trattamento (o da una terza parte) e i dettagli di contatto del Titolare della Protezione dei Dati;
e. le informazioni più dettagliate di secondo livello, dove e come trovarle;
f. tutte le informazioni che potrebbero impressionare l'interessato, come la trasmissione dei dati a terzi, in particolare se si trovano al di fuori dell'UE, o il relativo periodo di conservazione. Se queste informazioni non sono indicate, l'interessato dovrebbe presumere che esiste solo un monitoraggio in tempo reale (senza alcuna registrazione o trasmissione di dati a terzi);
g. dove trovare le ulteriori informazioni sul trattamento dei dati, disponibili in un luogo facilmente accessibile all'interessato tramite fonte digitale (ad esempio QR-code o indirizzo di un sito Web) o analogica (es. banco informazioni).

L'informativa completa deve contenere tutti i dati previsi dall'art. 13 del Reg. UE 2016/679 e deve essere messa a disposizione degli interessati con modalità di facile accesso.

Infine, tenuto conto del fatto che le riprese potrebbero, seppur in via esclusivamente incidentale, riguardare i dipendenti e collaboratori, il titolare deve mettere a disposizione del personale una copia del presente regolamento e una copia dell'informativa sul trattamento dei propri dati personali, consultabili in qualunque momento anche mediante estrazione di copia.

Nel rispetto di quanto previsto dall'art. 4, comma 1, della legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori), prima ancora di procedere all'installazione ed utilizzazione di un sistema di videosorveglianza dal quale possa derivare la possibilità di controllo dei dipendenti, il Titolare deve siglare un accordo con le rappresentanze sindacali per l'installazione dell'impianto (nel caso in cui superi la soglia occupazionale di 15 dipendenti) oppure richiedere l'Autorizzazione all'installazione alla Direzione Territoriale del Lavoro (nel caso in cui la soglia occupazionale non venga superata).

Art. 8 – Misure di sicurezza per la protezione dei dati

Come indicato nell'art. 25 del Reg. EU 2016/679, il Titolare del trattamento deve attuare misure tecniche e organizzative adeguate alla protezione dei dati sin dal momento in cui pianifichi la videosorveglianza, prima di iniziare la raccolta e il trattamento dei filmati video, tramite:

1. Misure di sicurezza organizzative, che definiscano con precisione i ruoli e le responsabilità connesse al sistema di videosorveglianza ed alla potenziale visualizzazione delle immagini.

2. Misure di sicurezza tecniche, per la protezione di tutti i componenti del sistema di videosorveglianza e i dati in tutte le fasi, vale a dire durante la memorizzazione (dati a riposo), la trasmissione (dati in transito) e l'elaborazione (dati in uso).

8.1 Misure di sicurezza organizzative

8.1.1 Persone autorizzate al trattamento

Ai sensi dell'art. 2-quaterdecies del D. Lgs. 196/2003, così come modificato dal d.lgs. 101/2018 e del Reg. UE 2016/679, il titolare del trattamento deve individuare formalmente i soggetti che, all'interno di ASPO S.p.A., siano autorizzati ad accedere ai dati raccolti attraverso il sistema di videosorveglianza e, di conseguenza, a visualizzare le immagini nei casi in cui sia necessario per perseguire le finalità indicate al punto 3.

Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate

condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

Tali soggetti, il cui numero deve essere limitato a quanto strettamente necessario, devono essere nominati per iscritto e devono ricevere tutte le istruzioni in merito al corretto utilizzo del sistema.

Tali istruzioni vengono fornite dal fornitore/installatore del sistema ad integrazione del presente regolamento e del Regolamento aziendale per il trattamento dei dati personali, i cui principi devono essere sempre tenuti a mente ed applicati:

- Le persone autorizzate al trattamento devono accedere ai locali dove sono situate le postazioni di controllo solo ove sia indispensabile per gli scopi perseguiti, con l'obbligo di prestare la massima attenzione al fine di evitare che altri soggetti, anche inavvertitamente, possano prendere visione delle predette immagini.
- Il monitor dal quale sia possibile visualizzare le immagini deve sempre essere rivolto in modo tale da evitare che i altri soggetti non autorizzati possano, volontariamente o meno, prendere visione delle immagini.
- Nessun soggetto non autorizzato al trattamento dei dati deve poter accedere alle aree di controllo del sistema di videosorveglianza. Nel caso in cui queste ultime non siano costantemente presidiate, il dipendente o collaboratore dovrà assicurarsi di mettere in stand-by il monitor e di chiudere a chiave la stanza nella quale sia posizionato il monitor.
- In nessun caso le immagini acquisite tramite il sistema di videosorveglianza potranno essere utilizzate per scopi di natura personale né per scopi differenti da quelli per i quali i dati sono raccolti.
- Le registrazioni contenenti i dati personali potranno essere estratte solamente su autorizzazione scritta del Titolare, in seguito a potenziali eventi anomali (furti, danni, intrusioni non autorizzate, malfunzionamenti del sistema, etc) o su richiesta delle Autorità per finalità di indagini di polizia o giudiziaria. Tali richieste dovranno necessariamente essere formalizzate in forma scritta e conservate, quale evidenza della necessità di accedere i dati.

Tutte le persone autorizzate al trattamento devono attenersi strettamente alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle stesse.

Il mancato rispetto delle predette istruzioni può comportare l'irrogazione di sanzioni disciplinari, oltre che responsabilità di natura civilistica.

L'elenco dei soggetti autorizzati ad accedere ai dati raccolti tramite il sistema di videosorveglianza di ASPO S.p.A. è indicato nell'allegato n. 3.

8.1.2 Responsabili esterni del trattamento

Nel caso in cui l'installazione e la successiva gestione del sistema di videosorveglianza vengano effettuati da una società esterna, quest'ultima deve essere preliminarmente nominata Responsabile esterno del trattamento ai sensi dell'art. 28 del Reg. UE 2016/679, in relazione all'ambito di trattamento definito. La predetta nomina, con valenza contrattuale, deve essere redatta in forma scritta e deve contenere le istruzioni in merito al corretto trattamento dei dati personali.

A seguito della sua sottoscrizione, il responsabile è tenuto al rispetto di tutti gli obblighi dettati dall'art. 28 del Reg. UE 2016/679, tra i quali mettere a disposizione del Titolare del trattamento le informazioni necessarie per dimostrare il rispetto degli obblighi normativi e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento.

8.2 Misure di sicurezza tecniche

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.

La sicurezza del sistema e dei dati, ovvero la protezione da interferenze intenzionali e non intenzionali durante la normale attività dovrebbe includere:

a. protezione dell'intera infrastruttura VSS (comprese telecamere remote, cavi e alimentatore) contro manomissioni fisiche e furti;
b. protezione della trasmissione di filmati con canali di comunicazione sicuri contro l'intercettazione;
c. crittografia dei dati;
d. utilizzo di soluzioni basate su hardware e software come firewall, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici;
e. rilevamento di guasti di componenti, software e interconnessioni;

f. mezzi per ripristinare la disponibilità e l'accesso al sistema in caso di incidente fisico o tecnico.

In base alle caratteristiche dei sistemi utilizzati, i soggetti autorizzati al trattamento o, eventualmente, responsabili esterni del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza.

Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (controllo dei log). Il controllo degli accessi garantisce infatti che solo le persone autorizzate possano accedere al sistema e ai dati, mentre viene impedito agli altri di farlo. Le misure che supportano il controllo dell'accesso fisico e logico devono:

a) garantire che tutti i locali in cui viene effettuato il monitoraggio della videosorveglianza e vengono archiviate le riprese video siano protetti contro l'accesso non controllato da parte di terzi;
b) definire ed applicare le procedure per la concessione, la modifica e la revoca dell'accesso fisico e logico;
c) implementare metodi e mezzi di autenticazione e autorizzazione dell'utente, incluso ad esempio la lunghezza delle password e la frequenza di modifica;
d) registrare e rivedere periodicamente le azioni eseguite dall'utente (sia sul sistema che sui dati) tramite il controllo dei log di accesso;
e) effettuare il monitoraggio e il rilevamento degli errori di accesso in modo continuo e affrontare tempestivamente le carenze.

Nel caso in cui il sistema sia configurato per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione.

Nel caso in cui sia necessario effettuare interventi di manutenzione, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini.

Art. 9 – DPIA (DATA PROTECTION IMPACT ASSESSMENT)

Ai sensi dell'articolo 35, paragrafo 1, Il Titolare è tenuto ad effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) quando un tipo di trattamento dei dati può comportare un rischio elevato per i diritti e la libertà delle persone fisiche e se il trattamento costituisce un monitoraggio sistematico di un'area accessibile al pubblico su larga scala.

Nello specifico, secondo il chiarimento interpretativo fornito dal Garante per la protezione dei dati personali con l'Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018 [doc. web n. 9058979 - Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018 contenente l' Elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto] la valutazione d'impatto è obbligatoria quando "*dai trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).*"

Il Titolare del trattamento dei dati dovrebbe quindi effettuare tale valutazione e, sulla base del risultato della DPIA eseguita, dovrebbe determinare la scelta delle misure di protezione dei dati da implementare.

È anche importante notare che se i risultati della DPIA indicano che il trattamento comporta rischi elevati nonostante le misure di sicurezza pianificate dal Titolare del trattamento, sarà necessario prima di iniziare il trattamento consultare l'Autorità di controllo competente.

Art. 10 – Diritti degli interessati

In relazione al trattamento dei dati personali, agli interessati identificabili deve essere assicurato l'effettivo esercizio dei propri diritti, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento e di ottenere l'interruzione di un trattamento illecito.

La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti alla persona istante identificabile e può comprendere eventuali dati riferiti a terzi, solo nei limiti previsti dalla legge. A tal fine può essere opportuno che la verifica dell'identità del richiedente avvenga mediante esibizione o allegazione di un documento di riconoscimento che evidenzi un'immagine riconoscibile dell'interessato.

10.1 – Diritto di accesso

L'interessato ha il diritto di ottenere la conferma dal Titolare del trattamento in merito al trattamento dei propri dati personali. Una volta trascorso il momento di monitoraggio in tempo reale, se nessun dato viene archiviato o trasferito in alcun modo, il Titolare del trattamento potrebbe solo fornire l'informazione che nessun dato personale verrà più trattato. Se tuttavia i dati sono ancora in fase di trattamento al momento della richiesta (vale a dire se i dati sono archiviati o continuano ad essere trattati in un altro modo), l'interessato dovrebbe ricevere accesso alle informazioni ai sensi dell'articolo 15, con alcune limitazioni:

☐ Se la richiesta incide negativamente sui diritti di terzi.

Può accadere che nella stessa sequenza di videosorveglianza possa essere registrato un numero qualunque di soggetti interessati, che causerebbe quindi un trattamento aggiuntivo dei dati personali di altre persone interessate. Se l'interessato desidera ricevere una copia del materiale, la soddisfazione di tale richiesta potrebbe influire negativamente sui diritti e sulle libertà di altre persone interessate presenti nel video. A causa della natura invasiva del filmato, il Titolare del trattamento non dovrebbe mai distribuire a terzi filmati in cui è possibile identificare altri soggetti. La protezione dei diritti di terzi non dovrebbe tuttavia essere utilizzata come un vincolo per prevenire legittime richieste di accesso da parte di individui e il Titolare del trattamento dovrebbe invece implementare misure tecniche per soddisfare la richiesta di accesso (ad esempio, modifica delle immagini con funzioni di mascheramento o annebbiamento).

☐ Il Titolare del trattamento non è in grado di identificare l'interessato.

Se per soddisfare la richiesta e trovare l'interessato in questione il Titolare del trattamento deve passare attraverso una grande quantità di materiale archiviato, potrebbe non essere in grado di identificare l'interessato. Per questi motivi l'interessato nella sua richiesta al Titolare del trattamento dovrebbe (oltre a identificarsi con un documento di identità o di persona), specificare quando - entro un termine ragionevole in proporzione alla quantità di soggetti registrati - è entrato nell'area monitorata. Il Titolare del trattamento deve comunicare preventivamente all'interessato quali informazioni sono necessarie affinché il Titolare del trattamento possa soddisfare la richiesta. Di conseguenza se il Titolare del trattamento è in grado di dimostrare di non essere in grado di identificare l'interessato, il medesimo Titolare deve, se possibile, informare l'interessato.

☐ Richieste eccessive.

In caso di richieste eccessive o manifestamente infondate da parte dell'interessato, il Titolare del trattamento può addebitare un costo ragionevole ai sensi dell'articolo 12, paragrafo 5, lettera a), del Reg. UE 2016/679 o rifiutare di dare seguito alla richiesta (articolo 12, paragrafo 5, lettera b). Il Titolare del trattamento deve essere in grado di dimostrare il carattere eccessivo o manifestamente infondato della richiesta.

10.2 – Diritto alla cancellazione

Se il Titolare del trattamento continua a trattare i dati personali dopo il monitoraggio in tempo reale (ad esempio memorizzando il video) l'interessato può richiedere la cancellazione dei dati personali ai sensi dell'articolo 17 del Reg. UE 2016/679.

Su richiesta, il Titolare del trattamento è tenuto a cancellare i dati personali senza indebito ritardo quando non sono più necessari per la finalità per cui sono stati inizialmente memorizzati o quando il trattamento è illegale.

Inoltre, i dati personali devono essere cancellati ogni volta che l'interessato esercita il diritto di opposizione e non vi sono motivi legittimi convincenti e prevalenti per il trattamento.

10.3 – Diritto di opposizione

L'interessato ha diritto in qualsiasi momento, per motivi relativi alla sua situazione particolare, di opporsi al trattamento ai sensi dell'articolo 21 del Reg. UE 2016/679, a meno che il Titolare del trattamento non dimostri validi motivi legittimi che prevalgano sui diritti e sugli interessi della persona interessata. Deve quindi essere interrotto il trattamento dei dati della persona che ha contestato.

Nel contesto della videosorveglianza, questa opposizione potrebbe essere fatta prima di entrare, durante la permanenza o dopo aver lasciato l'area monitorata. A meno che il Titolare del trattamento non abbia validi motivi legittimi, il monitoraggio di un'area in cui le persone fisiche potrebbero essere identificate è lecito solo se il Titolare del trattamento è in grado di interrompere immediatamente il trattamento dei dati personali da parte della telecamera, quando richiesto.

10.4 Modalità di esercizio dei diritti

Deve essere garantita all'interessato la possibilità di esercitare, in qualsiasi momento, i diritti previsti dagli articoli dal 15 al 21 del Reg. UE 2016/679, contattando il Titolare del Trattamento all'indirizzo di posta elettronica info@pec.aspo.it o tramite la posta ordinaria, presso la sede di Olbia, Via Indonesia 9, Zona Industriale.

Il Titolare del trattamento è tenuto a rispondere alle richieste dell'interessato senza indebito ritardo e al più tardi entro un mese. Un ulteriore periodo di un mese è giustificato solamente da impedimenti dovuti a difficoltà oggettive nel recupero dei dati: in ogni caso entro il mese dalla ricevuta richiesta occorre fornire una prima risposta all'interessato.

Allegati

Allegato 1 – Accordo sindacale per l'installazione e l'utilizzazione dell'impianto di videosorveglianza

Allegato 2 – Relazione tecnico descrittiva

Allegato 3 – Elenco persone autorizzate al trattamento e dei responsabili esterni