REPUBBLICA ITALIANA

Regione Siciliana
ASSESSORATO REGIONALE DELL'AGRICOLTURA, DELLO SVILUPPO RURALE
E DELLA PESCA MEDITERRANEA
DIPARTIMENTO REGIONALE DELL'AGRICOLTURA

Valutazione di impatto sui trattamenti di competenza del Dipartimento regionale dell'agricoltura

1 Contesto

1.1 Panoramica del trattamento

1.1.1 Quale è il trattamento in considerazione?

Il trattamento oggetto di valutazione DPIA è il sistema di video sorveglianza perimetrale della sede Assessoriale e dipartimentale. Il trattamento ha ad oggetto i dati personali (immagini) raccolti mediante il funzionamento di n.2 impianti di videosorveglianza attivi presso la sede Assessoriale di Viale Regione Siciliana, 2771 Palermo e la sede distaccata dipartimentale sita in via Cimabue, 2 Palermo. Gli impianti di videosorveglianza, installati per il perseguimento di finalità connesse alla tutela del patrimonio aziendale, pubblica sicurezza, sicurezza del lavoro ed esigenze organizzative e produttive, risultano proporzionati ed efficaci rispetto alle finalità prefissate ed sono tali da non comportare rischi eccessivi rispetto a quelli inseriti in un contesto di normale funzionalità dei sistemi.

Caratteristiche specifiche dei sistemi di videosorveglianza:

Sede assessoriale di Viale Regione Siciliana, 2771:

l'impianto è costituito da:

- Registratore NVR IP 16ch 4K con Hard Disk integrato (stanza 130);
- n. 6 telecamere esterne (IP Bullet);
- n.2 monitor: 2 (stanza 130 e portineria);
- n.1 sim alla quale il personale autorizzato, può, tramite apposita applicazione, visionare in tempo reale e da remoto le immagini in caso di allarme (servizio al momento non disponibile ed in corso di ripristino);
- software: quelli per il normale funzionamento degli NVR e pertanto insiti nell'apparato e difficilmente catalogabili;
- fascia oraria di funzionamento: 24h;
- tempi di conservazione: circa 7 giorni;
- gestione tecnico-informatica: ditta Energy Sistem di Sansone F.sco Paolo via Terrasanta n. 92 - 90141 Palermo.

Sede distaccata di Via Cimabue, 2:

l'impianto è costituito da:

- Registratore NVR IP 8ch PoE con Hard Disk integrato (stanza 105);
- Numero telecamere: 8 telecamere (IP Bullet) di cui 6 esterne e 2 nel box;
- n.1 monitor: 1 (stanza 105);
- n.1 sim alla quale il personale autorizzato, può, tramite apposita applicazione, visionare il tempo reale e da remoto le immagini in caso di allarme (servizio al momento non disponibile ed in corso di ripristino);
- software: quelli per il normale funzionamento degli NVR e pertanto insiti nell'apparato e difficilmente catalogabili;
- fascia oraria di funzionamento: 24h;
- tempi di conservazione: circa 7 giorni;
- gestione tecnico-informatica: a seguito di cessata attività da parte della ditta installatrice (Ditta "Calì Service"), è in corso di affidamento, nei confronti della ditta Energy Sistem di Sansone F.sco Paolo, il servizio di ripristino e manutenzione.

1.1.2 Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento:
Salvatore Barbagallo, Assessore dell'agricoltura, dello sviluppo rurale e della pesca mediterranea.
telefono: 091 7076324
fax: 091 7076093
email: assessore.risorseagricole@regione.sicilia.it
pec:

Responsabile del trattamento:
Dario Cartabellotta, Dirigente Generale del Dipartimento dell'Agricoltura
Incaricato con D.A. n. 35/Gab. del 18/07/2023
telefono: 091 7076237
fax: 091 7076093
email: agri.direzione@regione.sicilia.it
pec: dipartimento.agricoltura@certmail.regione.sicilia.it

Sub-Responsabile del trattamento:
Giuseppe Madonia, Dirigente responsabile dell'Area 1 "Affari generali, Bilancio ed URP" incaricato con contratto approvato con D.D.G. n. 2616 del 12/06/2023.
Nell'ambito delle competenze affidate e mediante apposito atto di designazione, il Sub-Responsabile provvede alla nomina degli incaricati del trattamento e mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali sia avvenuto conformemente ai contenuti del GDPR, a garanzia di tutela dei diritti dell'interessato e nel rispetto del principio di proporzionalità trattando i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini.

1.1.3 Ci sono standard applicabili al trattamento?

Le disposizioni contenute nel D.P.R. n.62 del 16aprile 2013 *"codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165*" e le successive modifiche introdotte con l'art.1 del D.P.R. n.81 del 13 giugno 2023 definiscono un quadro esaustivo circa ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Il Dipartimento al fine di fornire, a tutti i soggetti dipartimentali coinvolti nel trattamento dei dati personali, le informazioni essenziali per assicurare la riservatezza e la tutela dei diritti delle persone fisiche nel trattamento dei dati personali, ha realizzato un documento denominato *"Istruzioni e norme comportamentali di carattere generale per il trattamento dei dati personali di competenza del Dipartimento regionale dell'Agricoltura*", periodicamente aggiornato, pubblicato nella specifica sezione web dipartimentale dedicata alla privacy e formalmente notificato a tutti i dirigenti responsabili di struttura intermedia al fine di darne la massima diffusione nell'ambito dei propri uffici.

1.2 Dati, processi e risorse di supporto

1.2.1 Quali sono i dati trattati?

Il trattamento ha ad oggetto, esclusivamente, dati personali (immagini) raccolti mediante il funzionamento di n.2 impianti di videosorveglianza attivi presso la sede Assessoriale di Viale Regione Siciliana, 2771 Palermo e la sede distaccata dipartimentale sita in via Cimabue, n. 2 Palermo.

1.2.2 Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Le immagini di videosorveglianza consentono l'immediato riconoscimento della persona fisica (dipendente/visitatore/collaboratore esterno/fornitore) che sarà identificata, laddove previsto, attraverso esibizione e registrazione delle informazioni contenute nel documento di riconoscimento.
Il Titolare del trattamento raccoglie i dati personali mediante il funzionamento degli impianti di videosorveglianza attivi presso la sede Assessoriale e quella dipartimentale distaccata di Via Cimabue 2, Palermo. Le immagini, oltre che visibili in tempo reale attraverso l'ausilio di supporti monitor, vengono registrate su Hard Disk integrato nel registratore NVR, il quale trasmette le immagini acquisite su monitor dedicati e controllati da personale formalmente incaricato al trattamento. L'accesso alle immagini registrate avviene solo nel caso si verifichino eventi criminosi o eventi che rendano necessario un intervento. Ad eccezione di formali istanze dell'Autorità giudiziaria e/o di polizia per rispondere a particolari esigenze d'indagine, le immagini acquisite non vengono diffuse e/o divulgate. Alla fine del periodo di conservazione (circa una settimana), le riproduzioni video vengono cancellate mediante sovrascrizione automatica fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura degli uffici, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria e/o di pubblica sicurezza.

1.2.3 Quali sono le risorse di supporto ai dati?

Per le caratteristiche tecniche relative agli impianti si rimanda alle informazioni già declinate al punto 1.1.1 . I sistemi non sono collegati ad alcun server; gli NVR sono dotati di hard disk autonomi dove vengono registrate le riprese delle telecamere e quando la memoria sarà piena le stesse vengono sovrascritte a quelle precedenti a partire dalle meno recenti (da questo la durata delle conservazioni delle riprese). In entrambi le sedi oggetto di videosorveglianza, gli NVR ed i monitor sono allocati in ambienti chiusi a chiave e pertanto inaccessibili al personale non autorizzato. Fa eccezione la sede di Viale Regione Siciliana, 2771 nella quale è presente un secondo monitor (con funzione esclusiva di visualizzazione) posizionato, per motivi si sicurezza, all'interno della guardiola della portineria.

Gli eventuali accessi al sistema sono effettuati esclusivamente dal personale autorizzato e tramite credenziali (user e password) possedute anche dalla ditta che si occupa dell'assistenza tecnica dei sistemi. Come già evidenziato al punto 1.1.1, il personale autorizzato ha la possibilità, tramite App collegate attraverso SIM dedicate, di poter visionare in tempo reale e da remoto le immagini in caso di allarme. Si evidenzia che alla data del presente documento tale servizio risulta non attivo ed in corso di ripristino.

2 Principi Fondamentali

2.1. Proporzionalità e necessità

2.1.1 Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento delle immagini acquisite mediante i sistemi di videosorveglianza avviene per le finalità che sono espressamente manifestate nel Regolamento UE 2016/679 e nelle specifica informativa resa ai sensi dell'art.13 del GDPR pubblicata nella sezione web dipartimentale dedicata alla Privacy (link).
Gli scopi sono specifici, espliciti e legittimi, in quanto i dati personali sono raccolti e trattati dall'Amministrazione esclusivamente per finalità di sicurezza, controllo degli accessi, incolumità fisica delle persone ai sensi della normativa sulla sicurezza nei luoghi di lavoro e tutela di proprietà e patrimonio.

2.1.2 Quali sono le basi legali che rendono lecito il trattamento?

Nel rispondere ai requisiti di liceità, il trattamento si fonda sulla base giuridica prevista dall'art.6 , comma 1 lett. e) del GDPR "*esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento"*

2.1.3 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

Quanto alle misure giuridiche di contenimento, il trattamento risponde ai requisiti di limitazione delle finalità, minimizzazione ed esattezza dei dati. In termini di limitazione delle finalità, così come precedentemente evidenziato, il trattamento delle informazioni acquisite mediante i sistemi di videosorveglianza avviene per le finalità che sono espressamente previste nel Regolamento UE 2016/679 e nelle specifica informativa resa ai sensi dell'art.13 del GDPR. Quanto al requisito della minimizzazione, sono trattati solo ed esclusivamente i dati personali necessari e sufficienti per il raggiungimento delle finalità alla base del trattamento così come previsto dall'art.5 comma 1 lett.c) del GDPR.
In applicazione del principio della pertinenza delle immagini raccolte, le telecamere non sono installate, ad esempio, in luoghi dove i rischi connessi alle finalità di cui sopra sono del tutto assenti e, al contrario, è incentivata l'adozione di strumenti tecnologici conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi. In particolare, le telecamere sono installate affinché l'angolatura e la panoramica delle riprese venga effettuata con modalità tali da limitare l'angolo di visuale all'area da proteggere (per le caratteristiche tecniche degli impianti si rimanda alle informazioni contenute al punto 1.1.1

2.1.4 I dati sono esatti e aggiornati?

I dati sono raccolti in tempo reale e, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura degli uffici, nonché nel caso in cui si debba aderire ad una specifica richiesta dell'autorità giudiziaria e/o di pubblica sicurezza, sovrascritti decorso il termine di conservazione stimabile in circa 7 giorni. Quanto alle misure giuridiche di contenimento, il trattamento risponde ai requisiti di limitazione delle finalità, minimizzazione ed esattezza dei dati.

2.1.5 Qual è il periodo di conservazione dei dati?

La conservazione delle immagini acquisite dai registratori NVR è limitata ad un tempo pari a circa 7 giorni con modalità di sovrascrizione automatica dalle meno recenti e tali da rendere non riutilizzabili i dati cancellati.

2.2 Misure a tutela dei diritti degli interessati

2.2.1 Come sono informati del trattamento gli interessati?

Gli interessati al trattamento sono informati tramite le seguenti modalità:
- informativa semplificata (cartelli) appostia in prossimità delle aree videosorvegliate;
- informativa estesa, redatta ai sensi dell'art. 13 del Regolamento Generale sulla Protezione dei Dati (GDPR), è pubblicata nella specifica sottosezione web dipartimentale dedicata alla Privacy (link).

2.2.2 Ove applicabile: come si ottiene il consenso degli interessati?

Per il trattamento in oggetto non è richiesto il consenso dell'interessato, in quando si fonda su un presupposto di liceità diverso (art.6 , comma 1 lett. e) del GDPR "esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".

2.2.3 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati, al fine di esercitare i diritti riconosciutigli dagli artt.15-22 del GDPR, possono inoltrare istanza al Titolare del Trattamento ai seguenti indirizzi: assessore.risorseagricole@regione.sicilia.it, pec: assessorato.risorse.agricole.alimentari@certmail.regione.sicilia.it utilizzando il *"modello unificato per l'esercizio dei diritti dell'interessato"* scaricabile al seguente link:
https://www.regione.sicilia.it/sites/default/files/2023-04/Modello%20unificato%20esercizio%20diritti%20interessato%20-%20Agrico_0.pdf
Considerata la base giuridica su cui si fonda il trattamento, il diritto alla portabilità non è esercitabile (art. 20 par. 3 del GDPR).

2.2.4 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati, al fine di esercitare i diritti riconosciutigli dagli artt.15-22 del GDPR, possono inoltrare istanza al Titolare del Trattamento ai seguenti indirizzi: assessore.risorseagricole@regione.sicilia.it, pec: assessorato.risorse.agricole.alimentari@certmail.regione.sicilia.it utilizzando il *"modello unificato per l'esercizio dei diritti dell'interessato"* scaricabile dal seguente link:
https://www.regione.sicilia.it/sites/default/files/2023-04/Modello%20unificato%20esercizio%20diritti%20interessato%20-%20Agrico_0.pdf.
Considerata la base giuridica su cui si fonda il trattamento, il diritto alla cancellazione non è esercitabile (art. 17 par. 3 lett. b del GDPR).

2.2.5 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati, al fine di esercitare i diritti riconosciutigli dagli artt.15-22 del GDPR, possono inoltrare istanza al Titolare del Trattamento ai seguenti indirizzi: assessore.risorseagricole@regione.sicilia.it, pec: assessorato.risorse.agricole.alimentari@certmail.regione.sicilia.it utilizzando il *"modello unificato per l'esercizio dei diritti dell'interessato"* scaricabile dal seguente link:
https://www.regione.sicilia.it/sites/default/files/2023-04/Modello%20unificato%20esercizio%20diritti%20interessato%20-%20Agrico_0.pdf

2.2.6 Gli obblighi dei Responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Tutti i Responsabili che operano nell'ambito del trattamento hanno ricevuto apposite istruzioni in forma scritta da parte del Titolare o, nel caso di sub-Responsabili, da parte del Responsabile ai sensi della deliberazione della Giunta regionale n.297 del 8 agosto 2019.

Di seguito gli estremi dei provvedimenti con i quali vengono definiti obblighi ed oneri dei soggetti coinvolti nei procedimenti:

1) Responsabile del trattamento	D.A. n.35 del 18/07/2023
2) Sub-responsabile	D.D.G. n.2263 del 14/05/2023
3) Autorizzati al trattamento	provvedimento di autorizzazione notificato a mezzo email del 10/08/2023

Cosi come già evidenziato al paragrafo 1.1.3 *"standard applicati al trattamento",* Il Dipartimento, al fine di fornire, a tutti i soggetti dipartimentali coinvolti nel trattamento dei dati personali, le informazioni essenziali per assicurare la riservatezza e la tutela dei diritti delle persone fisiche nel trattamento dei dati personali, il Dipartimento ha realizzato un documento denominato *"Istruzioni e norme comportamentali di carattere generale per il trattamento dei dati personali di competenza del Dipartimento regionale dell'Agricoltura*", periodicamente aggiornato, pubblicato nella specifica sezione web dipartimentale dedicata alla privacy e formalmente notificato a tutti i dirigenti responsabili di struttura intermedia al fine di darne la massima diffusione nell'ambito dei propri uffici.

2.2.7 In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Non ricorre ipotesi

3 Rischi

3.1 Misure esistenti o pianificate

3.1.1 Controllo degli accessi logici

Le categorie di rischio possono essere: fonti umane interne, fonti umane esterne, fonti non umane.
Per la valutazione dell'impatto del trattamento dei dati dell'interessato sulle libertà ed i diritti del medesimo, si è partiti dai contenuti (criteri) del Registro dei trattamenti ex art.30 Reg.UE 2016/679 attribuendo specifiche categorie di rischio. Nello specifico, le misure a tutela del trattamento comportano le seguenti prescrizioni:

- Istruzioni per il trattamento fornite agli autorizzati
- Accesso controllato ai locali della struttura e videosorveglianza
- Accesso al sistema solo tramite autenticazione personale (nome utente e password)

Le autorizzazioni al trattamento non vengono rinnovate periodicamente ma mantengono la propria validità. Nel caso in cui il soggetto autorizzato al trattamento dovesse essere trasferito, collocato in quiescenza o rimosso dall'incarico, si procede alla formale revoca con immediata sospensione delle credenziali di accesso alle informazioni ed inibizione all'ingresso nei locali presso cui sono installati i registratori.

3.1.2 Tracciabilità

La tecnologia dell'NVR non prevede un sistema di log degli eventi in cui viene registrata, per un determinato tempo, ogni operazione effettuata (data, orario, e identificativo del soggetto che accede alle informazioni)..

3.1.3 Archiviazione

In entrambi i sistemi l'archiviazione dei dati, su hard disk, è automatica e permane per un periodo pari a circa 7 giorni dopo i quali vengono sovrascritti iniziando dalle immagini meno recenti.

3.1.4 Minimizzazione dei dati

Sono raccolte esclusivamente le video-immagini relative ai soggetti che fanno accesso ai locali sottoposti a sorveglianza. Quanto alle misure giuridiche di contenimento, il trattamento risponde ai requisiti di minimizzazione dei dati. Sono trattati esclusivamente dati personali necessari e sufficienti per il raggiungimento delle finalità alla base del trattamento così come previsto dall'art.5 comma 1 lett.c) del predetto GDPR. In applicazione del principio della pertinenza delle immagini raccolte, le telecamere collegate ai registratori NVR non sono installate, ad esempio, in quei luoghi dove i rischi connessi alle finalità di cui sopra sono del tutto assenti ed operano affinché l'angolatura e la panoramica delle riprese venga effettuata con modalità tali da limitare l'angolo di visuale all'area da proteggere.

3.1.5 Politiche di tutela della privacy

L'amministrazione regionale ha adottato diverse delibere di Giunta regionale in materia di politiche a tutela della privacy. Tra queste si segnalano la Delibera n.203 del 23/05/2018 con la quale è stato nominato il Responsabile per la protezione dei dati, la Delibera n. 483 del 29/11/2018 con la quale, fra l'altro, sono state fornite le prime istruzioni organizzative e tecniche per il trattamento dei dati personali e la gestione degli incidenti di sicurezza (c.d. data breach), e, infine, la Delibera n. 297 del 08/08/2019 con cui, allo scopo di accelerare il processo decisionale sui provvedimenti adottati in materia di protezione dei dati personali e rendere più agevole l'iter di approvazione dei documenti a carattere generale che si applicano a tutta l'amministrazione è stata prevista la possibilità di delegare alcuni adempimenti di competenza dei Titolari dei trattamenti ai Responsabili del trattamento dati. Il Dipartimento ha realizzato un documento denominato *"Istruzioni e norme comportamentali di carattere generale per il trattamento dei dati personali di competenza del Dipartimento regionale dell'Agricoltura*", periodicamente aggiornato, pubblicato nella specifica sezione web dipartimentale dedicata alla privacy (link) e formalmente notificato a tutti i dirigenti responsabili di struttura intermedia al fine di darne la massima diffusione nell'ambito dei propri uffici.

3.1.6 Vulnerabilità

Per quanto concerne le misure tecniche che sovrintendono al controllo sul grado di sicurezza dei sistemi utilizzati si rimanda alle informazioni contenute al punto 3.1.1 del presente documento. Ai fini valutativi in tema di vulnerabilità si è tenuto conto delle possibili minacce e dei corrispettivi livelli di probabilità. La seguente valutazione si fonda su una previsione di massima delle minacce tipo che possono paventarsi a seguito dell'uso dei sistemi oggetto di valutazione. Gli indicatori rappresentati in tabella costituiscono, laddove necessario, oggetto di costante e periodico aggiornamento alla luce delle criticità ovvero migliorie tecniche e di utilizzo che possono essere suggerite o rilevate. Considerata la tipologia degli impianti si espone, di seguito, una rappresentazione tabellare sulle possibili minacce correlate alla probabilità del verificarsi dell'evento:

Minacce	Livello di probabilità
Attacchi informatici	basso
Abusi di privilegi di accesso/utillizzo improprio	medio-basso
Modifica dei dati	basso
Errori nei processi di elaborazione	basso
Perdita dati per guasto/furto/smarrimento hardware	medio-basso
Cancellazione accidentale	basso
Inefficiente gestione del dato	basso

Si rimanda alle informazioni contenute al punto 1.1.1 circa la competenza in merito all'adozione ed alla gestione delle misure di protezione dei sistemi di videosorveglianza

3.1.7 Lotta contro il malware

Con riferimento alla difesa dal malware (software malevolo che può causare danni al computer o ai dati in esso memorizzati) e dallo spam (invio di messaggi email indesiderati o dannosi), la tecnologia dei sistemi di videosorveglianza (registratori NVR con Hard Disk integrato) non prevede alcuna esposizione a rischio.

3.1.8 Gestione delle postazioni

Le postazioni adibite al servizio di videosorveglianza NVR sono dotate di hard disk autonomi, non collegati in rete. La ditta che cura l'assistenza esegue, periodicamente, verifiche ed aggiornamenti; l'accesso avviene attraverso credenziali strettamente personali intestate ai soggetti, autorizzati al trattamento, che fanno accesso alla postazione e le cui password non sono soggette ad aggiornamento Gli account concessi al personale autorizzato e nel frattempo trasferito o collocato in quiescenza, vengono immediatamente cessati e inibito l'accesso fisico ai locali sede dei sistemi. Quanto alle informazioni relative alla società manutentrice si rimanda alle informazioni contenute al punto 1.1.1

3.1.9 Backup

Considerata la tipologia degli impianti e la durata di permanenza delle immagini acquisite, non è prevista l'esecuzione di periodici backup fatte salve le circostanze previste al punto 1.2.2 .

3.1.10 Sicurezza dei canali informatici

Le postazioni adibite al servizio di videosorveglianza NVR sono dotate di hard disk autonomi, non collegati in rete o a server e pertanto non sottoposte a procedure di salvaguardia oltre quelle indicate al punto 1.2.3

3.1.11 Sicurezza dei documenti cartacei

Il trattamento in questione non prevede l'acquisizione di documentazione cartacea contenente "dati sensibili" di cui agli artt. 9 e 10 del GDPR .

3.1.12 Controllo degli accessi fisici

I locali in cui sono allocati gli hardware dei sistemi di videosorveglianza (registratori NVR e monitor) sono debitamente chiusi a chiave e pertanto inaccessibili a soggetti non autorizzati. L'accesso da parte dei soggetti autorizzati avviene, comunque, per le circostanze già evidenziate al punto 1.2.2 ed a seguito di richiesta o incarico da parte del Sub-responsabile al trattamento.

3.1.13 Sicurezza fisica dell'hardware

I locali in cui sono allocati gli hardware dei sistemi di videosorveglianza (registratori NVR e monitor) sono debitamente chiusi a chiave e pertanto inaccessibili a soggetti non autorizzati. Tuttavia, qualora si verificassero intrusioni non autorizzate, gli NDR richiederebbero, comunque, per l'accesso alle informazioni, le credenziali rilasciate. Non sussistono, per gli ambienti, criticità ambientali riguardanti la sicurezza antincendio a protezione delle apparecchiature.

3.1.14 Prevenzione delle fonti di rischio

Al punto 3.1.1 sono già evidenziate le misure preventive di rilevamento o di protezione per ridurre o evitare che fonti di rischio (umane e non), anche se scarsamente probabili, arrechino pregiudizio ai dati personali . Quanto alla sicurezza degli ambienti in termini di rischio provocato da eventi non umani (fenomeni climatici, , incidenti interni o esterni, danni provocati da acqua, ecc.), il trattamento dei dati avviene nel pieno rispetto degli obblighi normativi in materia di prevenzione incendi.

3.1.15 Integrazione della protezione della privacy nei progetti (privacy by design)

In ambito dipartimentale, la sicurezza dei dati personali tiene conto delle disposizioni di cui alle delibere di giunta n. 203/2018, 483/2018 e 297/2019. Conformemente alla disciplina del Reg. (UE) 2016/679, i dati i dati trattati sono soltanto quelli strettamente necessari per le finalità perseguite ed in ossequio al principio di minimizzazione. Sul trattamento della videosorveglianza non è stato applicato il principio della "privacy by design". La realizzazione degli impianti è avvenuta su incarico del Dirigente Generale e realizzato da ditte specializzate nel settore secondo dettagliate caratteristiche prodotte dall'amministrazione.

3.1.16 Gestione degli incidenti di sicurezza e delle violazioni dei dati personali

L'art. 4 del Reg. UE 2016/679 definisce la violazione dei dati personali (*data breach*) come "*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*". Quindi, un data breach può essere un evento doloso, come un attacco informatico, oppure un evento accidentale come un accesso abusivo, un incidente, la semplice perdita di una chiavetta USB, un malfunzionamento hardware o software.
Per stabilire cosa fare in caso di violazione dei dati personali occorre una valutazione del rischio, cioè dei possibili effetti. Il rischio viene valutato tenendo in considerazione natura, sensibilità e volume dei dati personali violati, numero degli interessati, grado di possibilità che si verifichino effetti dannosi sui diritti e le libertà personali degli interessati o eventuali ripercussioni di carattere economico-finanziario dovute a pretese risarcitorie nei confronti dell'Amministrazione regionale.
Una volta scoperta la violazione dei dati, qualora si potesse determinare un rischio alle libertà personali della persona a cui si riferiscono i dati, sarà necessario informare prontamente il Titolare e il Responsabile del trattamento, anche per il tramite dei Sub-Responsabili del Dipartimento regionale dell'Agricoltura. Il Titolare, così come stabilisce il GDPR, deve quindi notificare l'evento all'Autorità di controllo (Garante della privacy), tranne nel caso in cui "*sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*" (es. perdita di dati già pubblici). La notifica deve avvenire "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*" il Titolare. Qualora la notifica non avvenga nelle 72 ore, il Titolare dovrà precisare anche i motivi del ritardo. La norma prevede anche la possibilità di allegare ulteriori informazioni in un momento successivo.

3.2 Accesso illegittimo ai dati

3.2.1 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

L'accesso illegittimo può compromettere la riservatezza, l'integrità o la disponibilità dei dati personali con inevitabili refluenze sulla piano reputazionale, discriminatorio, possibile rischio di furto di identità ed impatto sul piano giurisdizionale nel caso in cui siano intraprese azioni legali per ottenere un risarcimento. La probabilità che possano verificarsi, da parte di fonti umane esterne o interne non abilitate, eventi di accesso illegittimo alle informazioni registrate nei sistemi NDR è da ritenersi di basso impatto considerate le misure di sicurezza già evidenziate al punto 3.1.1 . Va tenuto conto, tuttavia, di quelli intestabili a fonti umane interne autorizzate nel caso in cui le stesse, senza alcuna preventiva disposizione da parte del responsabile o sub-responsabile o in assenza di circostanze che ne giustificano l'arbitrario accesso, accedono alle informazioni oggetto di trattamento con il chiaro intento di recare nocumento al titolare degli stessi. I soggetti autorizzati hanno l'obbligo di conoscere i contenuti del documento *"Istruzioni e norme comportamentali di carattere generale per il trattamento dei dati personali di competenza del Dipartimento regionale dell'Agricoltura*", affinché siano comprese le proprie responsabilità e gli obblighi derivanti dal trattamento dei dati personali.

3.2.2 Quali sono le principali minacce che potrebbero concretizzare il rischio?

Le caratteristiche tecniche dei sistemi di videosorveglianza non prevedono , considerata la tecnologia utilizzata, rischi derivanti da fattori esterni quali attacchi informatici o inadeguatezza della rete informatica. Al netto dei danni o guasti tecnici alle apparecchiature, la probabilità deriva, fondamentalmente, dall'accesso abusivo da parte dei soggetti autorizzati al trattamento o dalla sottrazione, agli stessi, delle credenziali di accesso.

3.2.3 Quali sono le fonti di rischio?

Si ribadisce quanto già espresso in punti precedenti. Gli ambienti presso cui sono allocati gli hardware non manifestano criticità riguardanti la sicurezza antincendio a protezione delle apparecchiature. In termini di accesso illegittimo alle informazioni, le fonti di rischio sono rappresentate, esclusivamente, dal comportamento improprio del personale interno, comportamento improprio del personale esterno, dal comportamento improprio da parte dei soggetti autorizzati nel caso in cui si manifesti un accesso abusivo per interessi personali o al fine di arrecare nocumento all'interessato oggetto di trattamento.

3.2.4 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

controllo dei accessi logici e fisici, attività di sensibilizzazione da parte dei soggetti con responsabilità nel trattamento corretto dei dati e richiamo alle disposizioni contenute nelle *"Istruzioni e norme comportamentali di carattere generale per il trattamento dei dati personali di competenza del Dipartimento regionale dell'Agricoltura*".

3.2.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

considerata la specificità tecnica degli hardware, la tipologia dei dati personali trattati, le misure di minimizzazione e la formazione del personale, la gravità del rischio di perdita del controllo dei dati e della riservatezza risulta trascurabile.

3.2.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

considerate le misure di minimizzazione, e la formazione del personale, la probabilità rischio di eventuale accesso illegittimo dei dati risulta trascurabile.

3.3 Modifiche indesiderate dei dati

3.3.1 Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

nessun impatto reale

3.3.2 Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

furto dei dati e problemi tecnici alle apparecchiature

3.3.3 Quali sono le fonti di rischio?

comportamento improprio del personale interno

3.3.4 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

controllo degli accessi fisici e logici

3.3.5 Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

impatto trascurabile

3.3.6 Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

considerate le caratteristiche dei supporti e le misure di controllo degli accessi fisici e logici,
la probabilità è trascurabile.

3.4 Perdita di dati

3.4.1 Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

perdita della riservatezza, perdita sul controllo dell'utilizzo dei dati, esposizione a ricatti.

3.4.2 Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

problemi tecnici alle apparecchiature, accesso fisico e logico non autorizzato.

3.4.3 Quali sono le fonti di rischio?

attaccante esterno, comportamento improprio personale esterno, comportamento improprio personale interno.

3.4.5 Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

istruzioni per il trattamento fornite agli autorizzati, accesso controllato ai locali della struttura e videosorveglianza, accesso al sistema solo tramite autenticazione personale (nome utente e password).

3.4.6 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

considerate le caratteristiche dei supporti, la minimizzazione dei dati e le misure di controllo degli accessi fisici e logici, la probabilità è trascurabile.

3.4.7 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

considerate le caratteristiche dei supporti, la minimizzazione dei dati, le misure di controllo degli accessi fisici e logici, la probabilità è trascurabile.

<u>Conclusioni</u>

La considerazione del contesto in cui si sviluppa l'azione dei sistemi di videosorveglianza adottati dal Dipartimento dell'agricoltura nonché le sue finalità, le modalità con cui avviene il trattamento dei dati, la tipologia dei medesimi e le misure giuridiche di contenimento dei rischi consentono di poter considerare il rischio per le libertà e di diritti dei cittadini di livello complessivamente "basso". Per quanto attiene le misure indicate al punto 3.1, si ritiene che le stesse siano, allo stato attuale, idonee. Affinché i sistemi in uso consentano lo svolgimento delle finalità di rilevanza pubblica nel pieno rispetto delle libertà e diritti dei cittadini, la congruità ed adeguatezza della presente DPIA andrà verificata ogni volta che dovesse essere rilevata qualche criticità ovvero appalesarsi la necessità di rivalutare l'adeguatezza e la conformità del funzionamento dei sistemi in uso.

Il Responsabile dei trattamenti
Dirigente Generale
Dario Cartabellotta

DARIO CARTABELLOTTA

Firmato digitalmente da DARIO CARTABELLOTTA
Data: 2024.11.19 12:58:13 +01'00'