DETERMINA DIRETTORE GENERALE

N. 02 del 04.01.2024

OGGETTO: SISTEMA DI VIDEO SORVEGLIANZA DELL'ENTE. VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) AI SENSI DEL REGOLAMENTO UE 2016/679. APPROVAZIONE

PREMESSO CHE ai sensi della L.R. n.69/2011, come modificata in ultimo dalla L.R. n. 10/2018:

- A far data dal 1° gennaio 2012 è stata istituita l'Autorità per il servizio di gestione integrata dei rifiuti urbani Ato Toscana Sud quale ente rappresentativo di tutti i Comuni appartenenti all'ambito territoriale ottimale comprendente i comuni delle province di Arezzo, Siena e Grosseto (art. 30 e 31);
- L'Autorità ha personalità giuridica di diritto pubblico ed è dotata di autonomia organizzativa, amministrativa e contabile (art. 31);
- ai sensi dell'art. 33 della citata L.R. 69/2011 "[…], all'autorità si applicano le disposizioni di cui al titolo IV della parte I e quelle di cui ai titoli I, II, III, IV, V, VI e VII della parte II del decreto legislativo 18 agosto 2000, n.267 (Testo unico delle leggi sull'ordinamento degli enti locali)";
- Gli organi delle autorità servizio rifiuti sono l'assemblea, il direttore generale e il revisore unico dei conti (art. 34);

PRESO ATTO CHE:

- con Deliberazione dell'Assemblea n. 12 del 30.11.2023 è stato approvato il bilancio di previsione 2024-2026 dell'Autorità Ato Toscana Sud;
- con Determinazione del Direttore Generale n. 140 del 27.12.2023 è stato approvato il Piano Esecutivo di Gestione (PEG) 2024-2026;

CONSIDERATO CHE al sottoscritto è stato affidato l'incarico di Direttore Generale dell'Autorità Ato Toscana Sud con delibera di Assemblea n. 24 del 06.07.2022, perfezionato con contratto stipulato con il Presidente dell'Assemblea il 12.09.2022 a valle dell'intesa rilasciata dal Presidente della Regione Toscana;

RISCONTRATA pertanto la propria competenza all'emanazione del presente atto ai sensi dell'art. 107 del D.Lgs. 267/2000, dell'art. 10 dello Statuto dell'Autorità Ato Toscana Sud e dell'art. 18 del vigente regolamento di organizzazione dell'Ente;

VISTO l'articolo 4, comma 1 della Legge 20 maggio 1970, n. 300 (c.d. Statuto dei lavoratori) il quale recita:

> "*1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di*

cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi"

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196";

DATO ATTO CHE la disposizione posta dalla norma è espressione del principio di salvaguardia della dignità del lavoratore, pertanto, il controllo sui dipendenti deve in ogni caso garantire un margine di riservatezza e di autonomia nello svolgimento della prestazione lavorativa;

TENUTO CONTO dei seguenti provvedimenti:

- provvedimento in materia di videosorveglianza dell'8 aprile 2010 (pubblicato sulla Gazzetta Ufficiale n. 99 del 29 aprile 2010) con cui il Garante per la protezione dei dati personali ha richiamato il già menzionato principio e individuato gli adempimenti e le prescrizioni specifiche da adottare, ivi comprese quelle inerenti alle misure di sicurezza;
- provvedimento del Garante ad oggetto "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento UE 2016/679;
- circolare n. 5 del 19 febbraio 2018 con cui l'Ispettorato Nazionale del Lavoro ha dettato indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e di altri strumenti di controllo ai sensi dell'art. 4 della Legge 300/1970;
- le Linee guida 3/2019 adottate dall'European Data Protection Board (Comitato Europeo per la protezione dei dati) in data 29/01/2020 ad oggetto il trattamento dei dati personali attraverso dispositivi video;
- La FAQ n. 9 in materia di videosorveglianza pubblicata dall'Autorità Garante per la protezione dei dati personali sul proprio sito istituzionale;

DATO ATTO CHE:

- L'Ente ha l'esigenza di installare un impianto di videosorveglianza, all'ingresso dell'Ente, in considerazione della particolare zona in cui è ubicata la sede legale (Via della Pace n. 37, int. 9 – Località Renaccio – SIENA), al fine di prevenire e contrastare eventi criminosi quali furti, atti vandalici e altri danni al patrimonio dell'Ente;
- in ottemperanza a quanto prescritto dall'art. 4 comma 1 della Legge 20 maggio 1970, n. 300 (c.d. Statuto dei lavoratori), in data 13/06/2013 è stato stipulato un accordo con le Organizzazioni sindacali territoriali firmatarie del CCNL relativo al personale del Comparto delle Funzioni Locali (Allegato n. 1);

VISTO l'art. 35 del Regolamento Europeo n. 679/2016 ed in particolare l'art. 35, comma 1, avente ad oggetto "*Valutazione d'impatto sulla protezione dei dati*" il quale recita: "*Quando un tipo di*

trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali";

RISCONTRATO CHE in base ai provvedimenti sopra menzionati ed alla disposizione normativa del Regolamento UE 2016/679, i trattamenti di dati personali effettuati tramite sistemi di videosorveglianza necessitano della valutazione d'impatto;

VISTA l'allegata Valutazione di Impatto (DPIA) predisposta con la consulenza del Data Protection Officer e dallo stesso validata con parere positivo rilasciato con comunicazione del 17/11/2023 assunta agli atti in data 20/11/2023 prot. n. 4374 (Allegati n. 2 e n. 3);

RITENUTO per quanto sopra esposto, di provvedere all'approvazione del documento di Valutazione di impatto (DPIA) relativa al trattamento dei dati personali acquisiti con il sistema di videosorveglianza;

DETERMINA

1. Le premesse formano parte integrante e sostanziale del presente atto.
2. di approvare il documento di valutazione di impatto sulla protezione dei dati personali (DPIA), relativa al trattamento dei dati personali acquisiti con il sistema di videosorveglianza, che viene allegata al presente atto a formarne parte integrante e sostanziale (Allegato n. 2);
3. di dare atto che le misure di sicurezza individuate nella DPIA saranno adottate dalle strutture organizzative dell'Ente;
4. di trasmettere il presente atto:
   a) Al Dirigente ed al personale dipendente;
   b) al Responsabile della Protezione dei Dati dell'Ente;
   c) al Responsabile del procedimento di Pubblicazione per la pubblicazione dello stesso:
      - all'Albo pretorio *on-line* per la durata di 15 gg. consecutivi;
      - nella sezione "*Privacy*" presente sul sito istituzionale dell'Ente.

IL DIRETTORE GENERALE
Ing. Enzo Tacconi (*)
(*) *Documento amministrativo informatico sottoscritto con firma digitale ai sensi dell'art.24 del D.Lgs. 82/2005*

AUTORITA' PER IL SERVIZIO DI GESTIONE INTEGRATA DEI RIFIUTI URBANI ATO TOSCANA SUD

Visto di regolarità contabile attestante la copertura finanziaria

(D.lgs. 18.08.2000, n.267 art. 153)

Si attesta la copertura finanziaria della spesa prevista dalla presente determinazione ai sensi dell'art. 153 e la compatibilità del programma dei conseguenti pagamenti con i relativi stanziamenti di cassa.

Data ___04.01.2024_

IL DIRIGENTE DELL'AREA
AMMINISTRATIVA E CONTABILE
Marco Morgione (*)
(*) *Documento amministrativo informatico sottoscritto con firma digitale ai sensi dell'art.24 del D.Lgs. 82/2005*

ACCORDO EX ARTICOLO 4 DELLA LEGGE 300/70 (STATUTO DEI LAVORATORI) IN MATERIA DI CONTROLLI A DISTANZA.

Tra l'Autorità per il servizio di gestione integrata dei rifiuti urbani, ATO Toscana Sud, rappresentato nel presente accordo dal Direttore Generale Ing. Enzo Tacconi, il quale agisce nel presente atto nella sua qualità Legale Rappresentante, nonché Presidente della delegazione trattante di parte datoriale

E

- le Organizzazioni sindacali territoriali firmatarie del CCNL relativo al personale del Comparto delle Funzioni Locali;
- la Rappresentanza sindacale unitaria di ATO Toscana Sud (RSU);
- la Rappresentanza sindacale aziendale di ATO Toscana Sud (RSA);

PREMESSO che:

- l'articolo 4, comma 1 della Legge 20 maggio 1970, n. 300 (c.d. Statuto dei lavoratori) stabilisce che

  "1. *Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi*"

  2. *La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*

  3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196";

- la disposizione posta dalla norma è espressione del principio di salvaguardia della dignità del lavoratore, sicché il controllo sui dipendenti deve in ogni caso garantire un margine di riservatezza e di autonomia nello svolgimento della prestazione lavorativa;
- con provvedimento in materia di videosorveglianza in data 8 aprile 2010 (pubblicato sulla Gazzetta Ufficiale n. 99 del 29 aprile 2010) il Garante per la protezione dei dati personali ha richiamato il predetto principio e individuato gli adempimenti e le prescrizioni specifiche da adottare, ivi comprese quelle inerenti alle misure di sicurezza;
- con circolare n. 5 del 19 febbraio 2018 l'Ispettorato Nazionale del Lavoro ha dettato indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e di altri strumenti di controllo ai sensi dell'art. 4 della Legge 300/1970;
- l'European Data Protection Board (Comitato Europeo per la protezione dei dati) ha adottato in data 29/01/2020, le Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video;
- La FAQ n. 9 in materia di videosorveglianza pubblicata dall'Autorità Garante per la protezione dei dati personali sul proprio sito istituzionale;

DATO ATTO che:

- ATO Toscana Sud, in considerazione della zona in cui è ubicata la sede legale, ha la necessità di installare impianti di videosorveglianza, al fine di prevenire e contrastare eventi criminosi quali furti, atti vandalici e altri danni al patrimonio dell'Ente, e precisamente: nell'immobile adibito a sede legale, in Via della Pace n. 37, int. 9 – Località Renaccio ed in particolare nelle seguenti zone: all'ingresso della sede

tutto quanto sopra ritenuto e premesso, le parti convengono quanto segue:

Art. 1 Le parti convengono e si danno reciprocamente atto che ATO Toscana SUD intende installare e utilizzare ulteriori sistemi di videosorveglianza negli ambienti sopra indicati;

Art. 2 Le parti convengono che l'installazione e l'utilizzazione degli impianti di videosorveglianza di cui all'articolo precedente siano finalizzati esclusivamente alla prevenzione ed al contrasto di possibili eventi criminosi, quali furti, atti vandalici e altri danni al patrimonio dell'Ente restando esclusa ogni altra finalità, diretta o indiretta, di controllo a distanza dell'attività lavorativa dei dipendenti.

Le parti si danno reciprocamente atto che:

- la telecamera è posizionata solo nell'area di ingresso dell'Ente in cui effettivamente esiste un rischio concreto e non altrimenti controllabile di danni al patrimonio dell'ente, in modo da riprendere unicamente le zone specificatamente individuate. La telecamera viene attivata solo all'atto della chiusura degli uffici e disattivata al momento dell'apertura dei medesimi. A ciò consegue che le immagini che sono registrate sono limitate al soggetto che attiva il sistema prima della chiusura e lo disattiva al momento dell'apertura;

- la gestione del sistema di videosorveglianza verrà effettuata nel rispetto di quanto risportato nel documento allegato (allegato n. 1);

Letto, confermato e sottoscritto.

Siena, 13 giugno 2023

Delegazione trattante di parte datoriale

Direttore Generale Ing. Enzo Tacconi_____

Delegazione trattante di parte sindacale

CGIL FP Siena Tiziana Tarquini_____

RSU Lucia Criscione_____

AUTORITA' PER IL SERVIZIO DI GESTIONE INTEGRATA DEI RIFIUTI URBANI ATO TOSCANA SUD

Documento di Valutazione di impatto sulla protezione dei dati

(DPIA - *DATA PROTECTION IMPACT ASSESSMENT*)

Redatto ai sensi dell'articolo 35 del Regolamento UE 679/2016 e delle Linee Guida WP248 rev. 01 adottate il 4 Aprile 2017 in materia di valutazione d'impatto sulla protezione dei dati e determinazione delle possibilità che il trattamento "possa presentare un rischio elevato".

Sede Legale Via della Pace 37, int. 9 - Loc. Renaccio
53100 Siena – C.F.: 92058220523
Tel. 0577 247075 – Fax 0577 279500
e-mail: segreteria@atotoscanasud.it – Pec: segreteria@pec.atotoscanasud.it

Titolare del trattamento:

Titolare del trattamento dei dati è l'Autorità per il servizio di Gestione dei Rifiuti Urbani ATO Toscana Sud, nella persona del Direttore Generale (Legale Rappresentante)
E-mail: segreteria@atotoscanasud.it
PEC: segreteria@pec.atotoscanasud.it

Responsabile della protezione dei dati (RPD/DPO):

Avv. Marco Giuri

Sede

Via della Pace, 37, int. 9 – Località Renaccio – 53100 SIENA

Data

3 gennaio 2024

MOTIVAZIONE DELLA VALUTAZIONE

Il presente documento viene elaborato ai sensi dell'articolo 35 del Regolamento UE 679/2016. La valutazione d'impatto si rende necessaria alla luce di un'attenta autoanalisi compiuta circa il trattamento dei dati personali.

L'Autorità per il servizio di gestione integrata dei rifiuti urbani, ATO Toscana Sud, con sede in Via della Pace, 37, int. 9 – Località Renaccio – 53100 SIENA, quale Ente Pubblico, ritiene necessario procedere ad una valutazione di impatto, stante il rischio elevato che il trattamento di dati di seguito citato possa avere sui diritti e le libertà delle persone fisiche:

trattamento effettuato mediante sistemi di videosorveglianza;

DEFINIZIONI

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 (art. 4 del Regolamento UE 2016/679).

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 (art. 4 del Regolamento (UE) 2016/679).

Titolare del trattamento: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4 del Regolamento (UE) 2016/679).

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (art. 4 del Regolamento (UE) 2016/679).

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 (art. 4 del Regolamento (UE)

2016/679).

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 (art. 4 del Regolamento (UE) 2016/679).

Rischio: scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità (Linee-guida 17/EN WP248).

Gestione del rischio: l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio (Linee-guida 17/EN WP248).

"Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario"[1].

La valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.

- *"una descrizione dei trattamenti previsti e delle finalità del trattamento";*
- *"una valutazione della necessità e proporzionalità dei trattamenti";*
- *"una valutazione dei rischi per i diritti e le libertà degli interessati";*
- *"le misure previste per:*
    - "*affrontare i rischi*"*;*

[1] Cfr. anche il Considerando 84:*"[l]'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento".*

- "*dimostrare la conformità al presente regolamento*".

In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

- valutando il contesto: *"tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio";*
- valutando i rischi: *" valutare la particolare probabilità e gravità del rischio";*
- trattando i rischi: *"attenuando tale rischio*", "*assicurando la protezione dei dati personali*" e "*dimostrando la conformità al presente regolamento*".

Nota: la valutazione d'impatto sulla protezione dei dati svolta ai sensi del Regolamento generale sulla protezione dei dati è uno strumento per gestire i rischi per i diritti degli interessati, di conseguenza, adotta la loro prospettiva, come avviene in taluni settori (ad esempio, la sicurezza sociale). Al contrario, la gestione del rischio in altri settori (ad esempio in quello della sicurezza delle informazioni) è incentrata sull'organizzazione.

CRITERI PER LA VALUTAZIONE DI RISCHIO E DI IMPATTO

In esplicazione di quanto detto nel presente documento, sono riportati gli elementi previsti dalla normativa vigente (art. 35, comma 7):

1. La descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
2. La valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
3. La valutazione dei rischi per i diritti e le libertà degli interessati;
4. Le misure previste per affrontare i rischi.

Le principali norme di riferimento in materia definiscono il rischio come "effetto dell'incertezza" (UNI

EN ISO 9000) ovvero "effetto dell'incertezza sugli obiettivi" (UNI ISO 31000), dove l'effetto è uno scostamento da quanto atteso.

Il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento e della verosimiglianza del suo verificarsi, dove per verosimiglianza (o possibilità) si intende la plausibilità di un accadimento ipotizzabile e, per conseguenze, si intendono gli esiti di un evento che influenza gli obiettivi.

La verosimiglianza può essere descritta come probabilità (o frequenza, con riferimento ad un dato intervallo di tempo). Le conseguenze di un evento possono avere effetti positivi o negativi sugli obiettivi.

Pertanto, la definizione di rischio contenuta nelle Linee-guida 17/EN WP 248 è sovrapponibile con queste definizioni: "scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità".

Pertanto il rischio può essere espresso come funzione di G (*gravità delle conseguenze) e di* P (*probabilità di accadimento dell'evento), cioè:*

R= f (G, P)

ove:

R = *entità del rischio*

G = *gravità delle conseguenze*

P = *probabilità di accadimento dell'evento*

Si assume in particolare che la funzione per determinare il rischio sia espressa dal prodotto di probabilità e gravità/rilevanza delle conseguenze, ovvero:

R (rischio) = P (probabilità) x G (gravità/rilevanza)

La procedura di valutazione dei rischi può essere riassunta come definito di seguito.

Ogni possibile minaccia viene analizzata sotto i seguenti profili:

- ✓ valutazione intrinseca della **probabilità** di accadimento dell'evento, in una scala da 1 a 4;
- ✓ valutazione della **gravità** delle conseguenze, in una scala da 1 a 4.

Per ogni possibile rischio identificato, come indicato al paragrafo 2.4 della "Procedura per la valutazione di impatto sulla protezione dei dati", è effettuata la valutazione dell'entità del rischio.

La valutazione è corretta (ossia ricalcolata) in presenza di misure di prevenzione e opportunità identificate e adeguatamente attuate, in relazione ai diversi aspetti esaminati. Si valuta così il rischio residuo, ossia il rischio che residua a seguito del trattamento del rischio stesso.

Per valutare la gravità, si tengono in considerazione il danno per la reputazione, la discriminazione, il furto d'identità, le perdite finanziarie, i danni fisici o psicologici, la perdita di controllo dei dati, altri svantaggi economici o sociali e, infine, l'impossibilità di esercitare diritti, servizi o opportunità.

Criteri di attribuzione dei livelli di Probabilità e Gravità.

R (entità del rischio)	**Probabilità**	Alta	**4**	Esiste una correlazione diretta tra la situazione rilevata ed il verificarsi dell'evento. Si sono già verificati eventi per la stessa situazione rilevata nel medesimo luogo, in ambienti simili o in situazioni simili. Il verificarsi dell'evento non susciterebbe

				alcuno stupore nell'organizzazione.
		Media	3	La situazione rilevata può provocare l'evento anche se non in modo automatico o diretto. E' noto qualche episodio in cui si è verificato l'evento. Il verificarsi dell'evento susciterebbe una moderata sorpresa nell'organizzazione.
		Bassa	2	La situazione rilevata può provocare l'evento al contemporaneo verificarsi di particolari condizioni. Sono noti rari episodi già verificatisi. Il verificarsi dell'evento susciterebbe una discreta sorpresa nell'organizzazione.
		Estremamente bassa/non rilevante	1	La situazione rilevata può provocare l'evento per concomitanza di più eventi poco probabili indipendenti. Non sono noti episodi già verificatisi. Il verificarsi dell'evento susciterebbe incredulità.
	Gravità	Alta	4	Seria violazione della privacy di un

				interessato. Alto impatto su altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione), con compromissione della fruizione. Conseguenze significative irreversibili o non eliminabili (minaccia per la vita, perdita o sospensione del rapporto di lavoro, danno finanziario ingente).
		Media	3	Violazione della privacy di un interessato con significativo disagio. Impatto su altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione, incolumità della vita) che, in concomitanza con altri elementi, potrebbe comprometterne la fruizione. Conseguenze ripristinabili con un certo dispendio di risorse.
		Bassa	2	Violazione della privacy di un interessato con basso impatto (es. la violazione

				comporta un disturbo/disagio facilmente ripristinabile). Nessuna violazione di altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione).
		Estremamente bassa/non rilevante	1	Impatto irrilevante per la privacy di un interessato. Nessuna violazione di altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione).

Il titolare del trattamento ed i soggetti di cui sopra, a seguito della valutazione condotta, effettuano la ponderazione dei rischi.

La ponderazione del rischio è definita come il processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio, per determinare se il rischio e/o la sua espressione quantitativa sia accettabile o tollerabile. La ponderazione del rischio agevola la decisione circa il trattamento del rischio, ossia il processo per modificare il rischio. La decisione sugli interventi necessita di stabilire a priori quale sia il livello di **rischio accettabile Ra**, in modo che si individuino le situazioni di intervento prioritarie, che presentano cioè un livello di rischio superiore al valore ritenuto accettabile (R>Ra).

La quantificazione del **rischio accettabile R < Ra** avviene in base alla tabella sottostante.

Area del rischio accettabile

R = P X G

Probabilità (P)

Alta	4	4 (eccezione)	8	12	16
Media	3	3	6	9	12
Bassa	2	2	4	6	8
Estrem. bassa / non rilevante	1	1	2	3	4
		1	2	3	4
Gravità (G)		Estrem. bassa / non rilevante	Bassa	Media	Alta

La matrice in tabella individua graficamente quelli che si considerano rischi non accettabili, ovvero quelli per cui è richiesto un intervento di miglioramento tale da riportare la situazione al di sotto della soglia di accettabilità. In base alla matrice dei rischi si individuano come **non accettabili** tutti quei **rischi che risultano avere valori di P x G superiori a 4**, unica eccezione le situazioni che si riferiscono

ad un alto livello di probabilità (P = 4). Poiché non si considera accettabile alcun tipo di danno, neppure di lieve entità, qualora si ritenga il suo verificarsi estremamente probabile.

La tabella che segue riporta i giudizi attribuiti alle classi di rischio. In base a quanto sopra detto, risultano **non accettabili**[2] i rischi classificati come **medio o alto**, oltre a tutti i rischi con un alto livello di probabilità (P = 4).

R (entità del rischio) normalizzata	**I ≥ 6**	**RISCHIO ALTO**
	4 ≤ I ≤ 5	**RISCHIO MEDIO**
	2 ≤ I ≤ 3	**RISCHIO BASSO**
	I ≤ 1	**RISCHIO ESTREMAMENTE BASSO, NON RILEVANTE**

Le carenze eventualmente evidenziate sono oggetto di **misure tecniche e organizzative e/o programmi di miglioramento** definiti al fine di **ridurre il rischio ad un livello accettabile**, secondo il criterio di accettabilità enunciato.

Tali misure e programmi tengono conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento.

[2] Il Regolamento (UE) 2016/679 considera non accettabile il rischio "elevato", che nella presente classificazione su quattro livelli accorpa anche il livello di rischio medio.

INDIVIDUAZIONE DEL TRATTAMENTO

Ai sensi dell'art. 30 del Regolamento UE 2016/679, il titolare del trattamento, insieme al DPO agli eventuali responsabili del trattamento e ad altre funzioni coinvolte provvedono a determinare le tipologie di trattamenti di dati personali effettuati dall'organizzazione o per conto di essa, mantenendo aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità.

Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento, e del responsabile della protezione dei dati;

b) le tipologie di trattamento;

c) le basi legali del trattamento;

d) le finalità del trattamento;

e) una descrizione delle categorie di interessati e delle categorie di dati personali;

f) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

g) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

h) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

i) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1, del Regolamento.

Tali informazioni sono documentate nel "Registro delle attività del trattamento", aggiornate, in caso di modifiche significative, e riesaminate, se necessario.

Per questa sezione relativa alla descrizione dei trattamenti previsti e delle finalità del trattamento si rinvia al documento "Registro del Trattamento" approvato con Determinazione del Direttore Generale n. 73 del 15/06/2023.

Sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea); in particolare il trattamento viene effettutato attraverso un impianto di videosorveglianza costituito da una videocamera posizionata all'ingresso della sede finalizzato alla prevenzione ed al contrasto di possibili eventi criminosi, quali furti, atti vandalici e altri danni al patrimonio dell'Ente restando esclusa ogni altra finalità, diretta o indiretta, di controllo a distanza dell'attività lavorativa dei dipendenti.

L'utilizzo del sistema di videosorveglianza viene eseguito con l'adozione delle misure di sicurezza di seguito indicate:

- sistemi di autenticazione mediante credenziali all'hardware dedicato collegato al server;
- aggiornamento periodico del software del sistema di videosorveglianza;
- antivirus;
- firewall;
- cancellazione dei dati dopo 24 ore;
- sistema di Intrusion Detection (IDS – misura adottata per il server);
- verifica periodica della "solidità" del sistema di sicurezza adottato;
- monitoraggio delle attrezzature obsolete al fine di assicurare gli standard minimi di sicurezza;
- utilizzo di screen saver dotati di password da attivare a tempo ed in ogni caso tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro;

- controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite

VALUTAZIONE SULLA NECESSITÀ E LA PROPORZIONALITÀ DEL TRATTAMENTO

- Sono state determinate le misure previste per garantire il rispetto del Regolamento, ai sensi e per gli effetti dell'articolo 35, paragrafo 7, lettera d) e del considerando 90):

1. Informative ai soggetti interessati (sia di primo livello attraverso il cartello di segnalazione;
2. Nomine interne di autorizzati, responsabili "interni", responsabile esterno del trattamento, responsabile per la protezione dei dati personali, responsabile IT;
3. Registro delle attività di trattamento e registro di *accountability* (o di rendicontazione);
4. Adozione di misure di sicurezza tecniche, organizzative e logistiche adeguate;
5. Procedure per la *'privacy by design'* e *'privacy by default'*;
6. Formazione.

- Sono state determinate le misure (di seguito elencate) che contribuiscono alla proporzionalità e alla necessità del trattamento:
  1. in considerazione della zona in cui è ubicata la sede legale, l'Ente ha la necessità di installare impianti di videosorveglianza, al fine di prevenire e contrastare eventi criminosi quali furti, atti vandalici e altri danni al patrimonio dell'Ente restando esclusa ogni altra finalità, diretta o indiretta, di controllo a distanza dell'attività lavorativa dei dipendenti;
  2. la telecamera è posizionata solo nell'area di ingresso dell'Ente in cui effettivamente esiste un rischio concreto e non altrimenti controllabile di danni al patrimonio dell'ente, in modo da riprendere unicamente le zone specificatamente individuate. La telecamera viene attivata solo all'atto della chiusura degli uffici e disattivata al momento dell'apertura dei medesimi. A

ciò consegue che le immagini che sono registrate (solo per 24 h), sono limitate al soggetto che attiva il sistema prima della chiusura e lo disattiva al momemto dell'apertura;

3. Le immagini potranno essere comunicate a soggetti che, qualora sia strettamente stabilito dalla legge, potranno accedere ai dati in forza di disposizioni di legge, nei limiti previsti dalle norme stesse (es. Forze di Polizia e Autorità competenti in caso di commissione di reati).
4. Accertamento, esercizio o difesa di un diritto in sede giudiziaria;
5. Consultazione preventiva del DPO qualora vi fossero dubbi relativamente al trattamento dei dati personali;

- Sono state individuate finalità di trattamento determinate e legittime, esplicitate (articolo 5, paragrafo 1, lettera b)) attraverso la stesura dell'informativa affissa all'entrata dell'Ente e pubblicata sul sito web dell'Ente, ove sono riportati i diritti dell'interessato e le modalità per esercitarli;

- È stato rispettato il principio di liceità del trattamento (articolo 6), attraverso la valutazione delle finalità. Preponderante è il trattamento dei dati per il legittimo interesse dell'Ente costituito dalla tutela del patrimonio aziendale in considerazione della particolare ubicazione della sede dell'Ente;

- I dati personali trattati sono adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c). La telecamera verrà attivata solo all'atto della chiusura degli uffici e disattivata al momento dell'apertura dei medesimi. A ciò consegue che le immagini che saranno registrate (solo per 24 h), sono limitate al soggetto che attiva il sistema prima della chiusura e lo disattiva al momemto dell'apertura

- È stata prevista la cancellazione delle registrazioni ogni 24 ore.

- Sono stati disciplinati i rapporti con il Responsabile esterno del trattamento (articolo 28) attrasverso l'atto di nomina; Ai sensi dell'art. 39, comma 1, lett. c del Regolamento, in ordine alla presente valutazione di impatto il DPO, dietro richiesta dell'Ente, ha rilasciato un parere.

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEI SOGGETTI INTERESSATI

- I rischi per i diritti e le libertà degli interessati (articolo 35, paragrafo 7 lettera c)) sono valutati ed indicati nella tabella di valutazione dei rischi. Tali rischi vengono così riassunti:
  - rischio distruzione
  - rischio perdita
  - rischio modifica
  - rischio divulgazione non autorizzata
  - rischio accesso non consentito ai dati personali trasmessi, conservati o comunque trattati (art. 32, comma 2).
- L'origine, la natura, la particolarità e la gravità dei rischi (cfr. Considerando 84) vengono determinate, tenendo in considerazione le diverse prospettive degli interessati e l'impatto sui relativi diritti e libertà.

ORIGINE INTERNA ED ESTERNA

1) Vi sono rischi causati dal **comportamento degli operatori/dipendenti difforme o non consapevole** (per dolo o colpa) e concretantesi in (a titolo esemplificativo):

- Furto di credenziali di autentificazione che potrebbe comportare un accesso non autorizzato ai dati;
- Perdita, diffusione e danneggiamento dei dati, e più in generale un trattamento illecito e non corrispondente alla finalità per cui i dati sono stati raccolti;
- Errore materiale nell'esecuzione dell'ufficio che potrebbe determinare il rischio di trattamenti illeciti, diffusioni, omissioni nel corretto e lecito trattamento;

- Errori umani nella gestione della struttura fisica (si pensi alla perdita e al danneggiamento dei dati per mancato inserimento del sistema di allarme, alla mancata revisione del sistema di antincendio o alla fortuita dimenticanza di aperture che facilitano l'ingresso di terzi non autorizzati).

2) Vi sono rischi **causati dolosamente, ma anche fortuitamente, derivanti da eventi esterni che colpiscono gli strumenti di lavoro e la struttura**. Si pensi ad un:

- Attacco al sistema informatico da parte di virus, che potrebbe causare danneggiamento ai software e, per l'effetto, danneggiamento, perdita, alterazione e diffusione non autorizzata dei dati;
- Attacco *criptolocker* che potrebbe causare danneggiamento ai software e conseguente danneggiamento, perdita, diffusione non autorizzata dei dati.
- *Spamming*, che potrebbe determinare un danneggiamento ai software con conseguente alterazione, perdita, diffusione non autorizzata dei dati;
- Malfunzionamento per vetustà degli elaboratori e degli strumenti di lavoro;
- Accesso ai locali da parte di soggetti non autorizzati che potrebbero impossessarsi dei dati e dei dispositivi che li contengono, diffondendo illecitamente i dati;
- Accessi in rete non autorizzati. Il rischio *de quo* è anche ricollegabile agli interventi operati da parte dell'assistenza tecnica da remoto sulle macchine, sui software, sui computer e sui server, che potrebbero determinare, in modo del tutto inconsapevole, la cancellazione di dati, la loro diffusione e/o modificazione.

3) Vi sono rischi causati da **eventi causali, prevedibili pur in astratto.**

In tal caso si fa riferimento al verificarsi di eventi distruttivi naturali o artificiali che possono causare la perdita e il danneggiamento delle macchine delle strutture e, conseguentemente, dei dati ivi conservati.

NATURA DOLOSA E COLPOSA

I rischi sopra declinati possono essere ricondotti ad eventi di natura sia **dolosa** che **colposa**.

PARTICOLARITÀ RISCHI INFORMATICI

Come evidenziato, si considerano come fonti di rischio, anche prevedibili (cfr. Considerando 90):

- l'errore umano dell'operatore e del personale dipendente;
- i rischi provenienti dall'esterno (virus, *troianhorse*, *ramsomware*, intrusione informatica ecc.);
- accessi non autorizzati nei locali e nelle strutture di soggetti terzi non autorizzati, il cui unico scopo è quello di sottrarre, con intento doloso, hardware, software o dispositivi elettronici o documenti cartacei;
- eventi fortuiti

GRAVITÀ; TIPOLOGIA DI CONSEGUENZE (perdita, accesso, danno di immagine, ecc.)

Sono stati, come evidenziato, valutati gli impatti potenziali per i diritti e le libertà degli interessati al verificarsi di eventi, quali l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati; le conseguenze derivanti dagli stessi, astrattamente individuabili nella diffusione e conoscenza di informazioni riservate e di dati personali, determinano un rischio per i diritti e libertà degli interessati (diritto alla riservatezza e la dignità della persona).

Vengono stimate, dunque, la probabilità e la gravità per determinarne il livello di rischio (Considerando 90):

Trattamento effettuato mediante sistemi di videosorveglianza

VALUTAZIONE SUI DATI INFORMATICI (con applicazione delle misure necessarie)					
	Gravità distruzione **2**	Gravità perdita **2**	Gravità modifica **2**	Gravità divulgazione non autorizzata	Gravità accesso non consentito

				2	3
Probabilità distruzione **1**	Rischio distruzione **2**				
Probabilità perdita **1**		Rischio perdita **2**			
Probabilità modifica **1**			Rischio modifica **2**		
Probabilità divulgazione non autorizzata **1**				Rischio divulgazione non autorizzata **2**	
Probabilità accesso non consentito **1**					Rischio accesso non consentito **3**

MISURE DI SICUREZZA APPLICATE:

- sistemi di autenticazione mediante credenziali all'hardware dedicato collegato al server;

- aggiornamento periodico del software del sistema di videosorveglianza;

- antivirus;

- Non è autorizzato l'accesso da postazione remota alle immagini "in tempo reale"

-firewall;

- cancellazione dei dati dopo 24 ore dalla rilevazione, salvo eventuali ulteriori periodi legati a festività o chiusura dell'esercizio o di specifiche richieste investigative da parte dell'Autorità Giudiziaria o di Polizia Giudiziaria;

- Informativa estesa e cartellonistica informativa;

- sistema di Intrusion Detection (IDS – misura adottata per il server);

- verifica periodica della "solidità" del sistema di sicurezza adottato;
- monitoraggio delle attrezzature obsolete al fine di assicurare gli standard minimi di sicurezza;
- utilizzo di screen saver dotati di password da attivare a tempo ed in ogni caso tutte le volte che ci si allontana, anche brevemente, dal posto di lavoro;
- controllo degli accessi alle apparecchiature e ai dati con registrazione su file di log delle operazioni che vengono eseguite
- formazione e sensibilizzazione del personale che accede, visiona, estrapola le immagini.

MISURE PREVISTE PER CONTRASTARE I RISCHI

Le altre misure ritenute adeguate a contrastare i rischi individuati sono le seguenti:

- Controlli interni del DPO;
- Regole scritte circa il trattamento dei dati per i soggetti autorizzati;
- Nomine scritte e responsabilizzazione dei responsabili esterni

- Si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2): questo viene sempre coinvolto nelle decisioni dell'Ente e viene richiesto il suo parere su singole questioni o quesiti che hanno a che fare con il trattamento dei dati personali.

Anche il presente documento verrà sottoposto al suo vaglio finale.

CONCLUSIONI

Considerato il livello di rischio basso, si ritiene superflua, in accordo con il DPO, la consultazione preventiva dell'Autorità Garante, ai sensi e per gli effetti dell'art. 36 Regolamento UE 679/2016.

Il Direttore Generale
Ing. Enzo Tacconi (*)

(*) Documento informatico sottoscritto con firma digitale
ai sensi del D.Lgs. 82/2005

Zimbra **c.senatore@atotoscanasud.it**

Re: P2503 ATS – DPO AVV GIURI VALUTAZIONE IMPATTO VIDEOSORVEGLIANZA

Da : pa@privacysolving.it Privacy Pubblica Amministrazione <pa@privacysolving.it> ven, 17 nov 2023, 18:09

3 allegati

Oggetto : Re: P2503 ATS – DPO AVV GIURI VALUTAZIONE IMPATTO VIDEOSORVEGLIANZA

A : Carmela Senatore <c.senatore@atotoscanasud.it>

Cc : Stefania Zelli <stefaniazelli31@gmail.com>, marcogiuri@studiogiuri.it

Buonasera,
in relazione all'oggetto il DPO esprime parere positivo.
Rimetto in allegato il documento con alcune integrazioni che troverete in verde.
Suggerisco di approvare la DPIA e di convertirla in pdf.
Cordiali saluti,
nicoletta giangrande

> Il 17/11/2023 11:00 CET Carmela Senatore <c.senatore@atotoscanasud.it> ha scritto:
>
> Buongiorno
>
> in allegato quanto richiesto
>
> Cordiali saluti
>
> Carmela Senatore

Avv. Nicoletta Giangrande

consolve STUDIO GIURI AVVOCATI
Consulting & Solutions, not else.

Via Cosseria, 28 - 50129 Firenze(FI); Mob: 377 6960858

Valutazione di impatto videosorveglianza RV NG 17.11.23.docx
434 KB
