DPIA

(DATA PROTECTION IMPACT ASSESSMENT)

by Ichnelios

Comune di San Teodoro

(Provincia di Sassari)

Settore Servizi alla Comunità

TRATTAMENTO dei DATI PERSONALI :

VIDEOSORVEGLIANZA di AREE di PUBBLICO INTERESSE

relazione e servizio DPIA a cura di ICHNELIOS S.C. ar.l.

il Legale Rappresentante

Il Referente presso il Garante

Il Responsabile della Protezione dei Dati

Ichnelios S.C.ar.l.

PIRAS ROBERTO
ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI SASSARI
Ingegnere
26.02.2024 17:04:38 GMT+01:00

Indice generale

PREMESSA

Il presente documento è redatto in conformità alle prescrizioni del GDPR 2016/679, in altri termini il Regolamento UE Generale sulla protezione dei dati personali 2016/679 (RGPD), in ordine della Valutazione di Impatto del Trattamento di Dati Personali sulle persone fisiche interessate. La metodologia utilizzata è conforme ai criteri fissati nell'allegato 2 Linee Guida WP248 rev.01 Garanti Europei.

1. Il Trattamento in VALUTAZIONE

Il Trattamento in valutazione consiste nella gestione di un sistema di videosorveglianza di aree di interesse pubblico, situate nel territorio del suddetto Comune.
L'impatto è valutato ponendo particolare attenzione ai diritti ed alle libertà degli interessati, la valutazione ha come obiettivo quello di verificare e garantire la protezione dei dati personali di tutti coloro che entrano in contatto o in relazione con l'attività di videosorveglianza.

1.1. Descrizione del trattamento

L'acquisizione e la raccolta dei dati è interamente automatizzata ed è effettuata mediante l'utilizzo degli impianti di videosorveglianza attivati nelle aree di competenza dell'ENTE.

1.2. Finalità

L'utilizzo degli impianti è finalizzato a:

a) attività di prevenzione, indagine e perseguimento di atti ed attività illecite, inclusi episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del decreto legge n. 14/2017 e s.m.i., delle attribuzioni del Sindaco in qualità di autorità locale di cui all'articolo 50 e di ufficiale di governo di cui all'articolo 54 comma 4 e 4-bis del D.Lgs. 267/2000;
b) prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare quelle condotte legate a fenomeni di degrado, di discarica di materiale e di sostanze pericolose o di abbandono di rifiuti;
c) svolgere i controlli diretti ad accertare, ed eventualmente sanzionare, le violazioni delle norme contenute nel regolamento di Polizia Urbana, nei Regolamenti locali in generale e nelle Ordinanze del Sindaco;
d) monitorare la tutela del patrimonio pubblico, comprendente gli istituti scolastici, il teatro comunale, il cimitero e gli impianti sportivi, per preservarli da atti di vandalismo e danneggiamento;
e) vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;
f) tutelare l'ordine, il decoro e la quiete pubblica;

g) migliorare l'efficienza ed efficacia degli interventi della forza pubblica;
h) supportare, quando richiesto e necessario, le attività di Protezione Civile.
i) inserire punti di monitoraggio del traffico per individuare eventuali infrazioni al codice della strada e accertare le responsabilità nell'eventualità che si verifichino situazioni di emergenza.

1.3. Dati, Processi, Asset e Risorse di Supporto al Trattamento.

Gli impianti, costituiti da telecamere fisse e mobili, consentono riprese video e foto a colori, sia in diurna sia in notturna, in condizioni di illuminazione naturale o artificiale.
Gli impianti sono sempre in funzione, pertanto l'acquisizione e la registrazione dei dati ha caratteristica di continuità.
Sono riprese unicamente immagini fotografiche e video (non è previsto il rilievo dei suoni); il flusso di informazioni che contiene i video è inviato dalle unità di ripresa attraverso gli apparati di rete, verso un sistema di monitoraggio e controllo posto presso il Comando di Polizia Locale, denominato Client, e verso sistema di memorizzazione, monitoraggio e controllo posto presso il Municipio denominato Server.
I locali sono dotati di una rete di comunicazione adeguata secondo gli standard di sicurezza informatica ed hanno caratteristiche antintrusione e dispositivi di limitazione di accesso.
In queste sedi le immagini sono visualizzate su monitor ed hardware client appositamente configurato, con accesso protetto, riservato e consentito unicamente al personale formalmente ed appositamente incaricato.

Le immagini consentono di identificare, in modo diretto o indiretto, le persone riprese; esse consentono inoltre di determinare informazioni associabili alla persona fisica relative al possesso / uso di proprietà e beni, a caratteristiche fisiche, ad abitudini, a stile di vita e di comportamento, alla posizione geografica, associabili.

Il ciclo di vita dei dati - esclusivamente in formato digitale - prevede i seguenti trattamenti:

- ***Acquisizione***, avviene esclusivamente dalle unità di ripresa di cui alla relazione tecnica allegata. Eventuali implementazioni o modifiche comporteranno il tempestivo adeguamento di ogni documento riferibile.
- ***Registrazione***, avviene esclusivamente sui server dedicati e nelle unità di backup previste, non è consentita la copia su supporti rimovibili o la trasmissione su altri server o su cloud (salvo che ciò venga disposto dall'Autorità Giudiziaria per finalità di indagine o giustizia).
- ***Organizzazione***, le riprese per tutto il periodo di conservazione mantengono le riferibilità temporale e geografica.

- ***Conservazione***, i dati sono conservati per una durata non superiore a sette giorni dalla data di rilevazione, decorso tale periodo i dati registrati sono cancellati con modalità automatica (D.L. 11/2009 art. 6, comma 8) . La conservazione può essere prolungata, con limitazioni di accesso, sia per ragioni di pubblico interesse sia per disposizioni dell'Autorità Giudiziaria, comunque non oltre i termini massimi consentiti dalla legge.
- ***Consultazione***, consentita, con limitazioni di accesso, solo agli operatori autorizzati nei limiti previsti dal Regolamento, per ragioni di pubblico interesse o per disposizioni dell'Autorità Giudiziaria .
- ***Raffronto o interconnessione***, consentita, con limitazioni di accesso solo agli operatori autorizzati nei limiti previsti dal Regolamento, per ragioni di pubblico interesse o per disposizioni dell'Autorità Giudiziaria.
- ***Limitazione***, il trattamento è consentito esclusivamente nei limiti previsti dal Regolamento, per ragioni di pubblico interesse o per disposizioni dell'Autorità Giudiziaria.
- ***Pseudonimizzazione,*** il trattamento dei dati avviene mediante opportune procedure di pseudonimizzazione al fine di rafforzare la sicurezza e la protezione dei dati.

1.4. Gestione del Trattamento

Il Trattamento è gestito attraverso il personale dell'ENTE, designato al Trattamento ed appositamente formato per la sua gestione; sono specificatamente coinvolti i ruoli organizzativi della Polizia Locale, con l'individuazione del Comandante quale referente degli incaricati del trattamento.
Sono definite specifiche procedure operative affidate al referente per la corretta gestione del trattamento (v. documento Regolamento videosorveglianza).
La gestione dei dati esclusivamente interna all'Ente esclude destinatari esterni o stranieri, salvo le eccezioni previste ex lege che ne consentono la consultazione
Il Trattamento in futuro potrà essere affidato ad un Responsabile esterno che gestisca parzialmente o integralmente il servizio attraverso le proprie risorse tecniche, tecnologiche ed umane.
In tale caso alla nomina formale seguiranno tutti gli adempimenti che il RGPD assegna al ruolo di Responsabile del trattamento e saranno formalmente definite le procedure di gestione e di coordinamento con il personale preposto dell'ENTE.

1.5. Quadro normativo applicabile

L'utilizzo del sistema della videosorveglianza viene attuato attraverso un corretto impiego delle applicazioni e nel rispetto dei principi di cui all'art. 5, del RGPD :

a) Liceità, correttezza e trasparenza, in piena ottemperanza della normativa vigente, nei confronti dell'interessato.

b) Adeguatezza, in modo tale da essere pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

c) Integrità e riservatezza, in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

d) Proporzionalità, con sistemi attuati con attenta valutazione.

e) Finalità, nell' attuare il trattamento dei dati solo per scopi determinati, leciti ed espliciti.

f) Necessità, con esclusione di uso superfluo della videosorveglianza.

Il trattamento dei dati, effettuato mediante l'attività di videosorveglianza, è realizzato nel rispetto delle seguenti disposizioni normative:

a) Art. 615-bis del Regio Decreto 19 ottobre 1930, n. 1398 successive modifiche apportate dal D.Lgs. 11 maggio 2018, n. 63, dal D.Lgs. 10 aprile 2018, n. 36 e dal D.Lgs. 1° marzo 2018, n. 21.

b) Legge 20 maggio 1970, n. 300.

c) Legge 7 marzo 1986 n. 65.

d) D.Lgs. 31 marzo 1998, n. 112.

e) D.Lgs. 18 agosto 2000, n. 267.

f) D.Lgs. 30 giugno 2003, n. 196 e relative modifiche D.lgs. 14 marzo 2013, n. 33.

g) Circolare del Ministero dell'Interno n° 558/A/421.2/70/456, del 08.02.2005.

h) L. R. Sardegna 02 agosto 2007, n. 9.

i) Legge 24 luglio 2008, n. 125, di conversione, con modifiche, del D. L. 23 maggio 2008, n. 92.

j) D.M. Interno 5 agosto 2008 (G.U. N. 186, del 09/08/2008)

k) Legge. 23 aprile 2009, n. 38, di conversione, con modifiche del D.L. 23 febbraio 2009, n. 11.

l) Provvedimento del Garante per la protezione dei dati personali in materia di videosorveglianza 8 aprile 2010 (G.U. N. 99, del 29/04/2010)

m) Circolare del Ministero dell'Interno n. 558/A421.2/70/195860, del 6 agosto 2010.

n) Circolare del Ministero dell'Interno n. 558/SICPART/421.2/70/224632 del 2 marzo 2012.

o) Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera

circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

p) Regolamento UE n. 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

q) Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia".

r) D.Lgs.10 agosto 2018, n. 101.

s) Statuto Comunale.

t) Regolamenti Comunali vigenti.

1.6. Informativa e base giuridica del trattamento dati

Nelle strade, nei parchi e nelle piazze in cui sono posizionate le telecamere, in prossimità o nelle immediate vicinanze, ma non necessariamente a contatto, L'ENTE si obbliga ad affiggere ed a mantenere in sito, una adeguata segnaletica che riporti la seguente dicitura o equipollente " … ENTE ... - area video sorvegliata" con inclusione delle finalità e dei riferimenti normativi "per fini di prevenzione e sicurezza [Regolamento Europeo sulla protezione dei dati personali RGPD 2016/679]

Tale segnaletica

- *ha un formato che la renda accessibile e chiaramente visibile;*
- *è posizionata nel rispetto del provvedimento del Garante Privacy datato 8 aprile 2010, richiamato nel Regolamento videosorveglianza approvato dal Consiglio Comunale con delibera n. 12 del 14.4.2022*
- *ingloba simboli ed icone che comunicano se le immagini sono visionate, registrate o trattate con entrambe le modalità e include l'indicazione dei tempi di conservazione*
- *include l'informativa di primo livello e rimanda ad un luogo (fisico o anche virtuale) ove si possa prendere visione della informativa completa con le informazioni di secondo livello.*

In merito alle disponibilità delle informative accessibili mediante la pubblicazione sul sito web del Comune, preferibilmente in una sezione apposita, viene evidenziata la determina di affidamento, registro generale n.1063 del 15-09-2023 CIG A0107C4B61 CUP H91F22001180006 PNRR DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA PA MISURA 1.4.1 PNRR CITTADINANZA ATTIVA

La base giuridica del trattamento dei dati è individuata nell'art. art. 6, comma 1, lettera e) del RGPD 2016/679.

Nel D.L. n. 11/2009 convertito in legge 38/2009, l' art. 6 comma 7, precisa che "i Comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico", per la tutela della sicurezza urbana, nella accezione chiarita dall'art. 4 D.L. 14/2017, convertito in Legge 48/2017, per cui "si intende per sicurezza urbana il bene pubblico che afferisce alla vivibilità e al decoro della città, da perseguire anche attraverso ,,, la prevenzione della criminalità, in particolare di tipo predatorio."

Il trattamento dei dati personali **non necessita del consenso degli interessati** in quanto viene effettuato nello svolgimento di un compito di interesse pubblico e nell'esercizio di pubblici poteri.

In relazione al principio di minimizzazione dei dati (art. 5 n. 1 c RGPD) il sistema informativo e i programmi informatici, di cui al trattamento dei dati personali, sono configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzati mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
L'Ente dopo attenta valutazione ha escluso la possibilità di far ricorso ad alternative meno impattanti, quali ad esempio servizi di appostamento del personale di polizia o sistemi di allarme nell'area del territorio che si deve sorvegliare.

1.7. Diritti dell'Interessato

L'interessato, ai sensi degli articoli artt. 12, 13, comma 2, lettere (b) e (d) e 14, comma 2, lettere (d) e (e) nonché degli artt. 15-22 del RGPD, potrà ottenere dall' ENTE la conferma dell'esistenza o meno di propri dati personali.

Per l'esercizio dei diritti l'utente può contattare il TITOLARE del TRATTAMENTO dei DATI PERSONALI inviando una istanza **ai riferimenti di contatto contenuti nell'Informativa** e il Titolare risponderà nel rispetto della normativa vigente (art. 12 RGPD).

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dal RGPD hanno il diritto:

- di proporre reclamo al Garante della Privacy, come previsto dall'art. 77 del Regolamento stesso, seguendo le procedure e le indicazioni pubblicate sul sito ufficiale dell'Autorità www.garanteprivacy.it ;
- di adire le opportune sedi giudiziarie (art. 79 RGPD).

2. Documentazione Tecnica

2.1. Relazione Tecnica delle risorse dedicate al Servizio di Videosorveglianza (allegato 1)

E' riportata in allegato la relazione Tecnica delle risorse dedicate al servizio di videosorveglianza elaborata dai competenti uffici dell'Ente.
Va evidenziato che il documento deve essere aggiornato periodicamente, o in occasione di modifiche al sistema di videosorveglianza, anche mediante addendum con data certa che riporti le modifiche intercorse.
Al fine di garantire l'adeguatezza della versione in uso, annualmente il documento deve essere revisionato da un preposto che verbalizza l'avvenuta verifica.
In tale occasione, se opportuna per finalità di chiarezza, può essere emessa la versione aggiornata con le variazioni intercorse in sostituzione della versione obsoleta.

2.2. Regolamento della Videosorveglianza (allegato 2)

E' riportato in allegato il Regolamento Comunale per la disciplina della videosorveglianza approvato dal Consiglio Comunale con deliberazione n. 12 in data 14/04/2022.
Il documento deve essere aggiornato periodicamente, o in occasione di modifiche al sistema di videosorveglianza, anche mediante addendum con data certa che riporti le modifiche intercorse.
Al fine di garantire l'adeguatezza della versione in uso, annualmente il documento deve essere revisionato da un preposto che verbalizza l'avvenuta verifica.
In tale occasione, se opportuna per finalità di chiarezza, può essere emessa la versione aggiornata con le variazioni intercorse in sostituzione della versione obsoleta.
Per il documento approvato in data 14.04.2022 è programmata l'attività di aggiornamento e revisione.

2.3. Procedure di gestione del Servizio di Videosorveglianza (allegato 3)

E' riportato in allegato il documento elaborato dall'Ente che contiene le procedure di gestione del servizio di videosorveglianza.
Va evidenziato che il documento deve essere aggiornato periodicamente, o in occasione di modifiche al sistema di videosorveglianza, anche mediante addendum con data certa che riporti le modifiche intercorse.
Al fine di garantire l'adeguatezza della versione in uso, annualmente il documento deve essere revisionato da un preposto che verbalizza l'avvenuta verifica.

In tale occasione, se opportuna per finalità di chiarezza, può essere emessa la versione aggiornata con le variazioni intercorse in sostituzione della versione obsoleta.

3. Metodologia di valutazione

L'attività di *Data Protection Impact Assessment* (DPIA) si sviluppa sulla base dei seguenti step metodologici:

Step 1: **Valutazione della criticità del TRATTAMENTO**
Step 2: **Valutazione del livello di Rischio Inerente**
Step 3: **Misure di attenuazione del Rischio e Controllo**
Step 4: **Definizione del livello di Rischio Residuo**
Step 5: **Classificazione del Rischio**

Nei paragrafi successivi si riporta il dettaglio degli step metodologici previsti ai fini dello svolgimento del *Data Protection Impact Assessment*.

3.1. Valutazione della criticità del TRATTAMENTO

La valutazione della criticità del Trattamento è condotta attraverso la valutazione di 24 parametri valorizzati ciascuno in base all'impatto potenziale dell'interessato.
È attribuito il valore:

- 3 per parametri di criticità elevata
- 2 per parametri di criticità mediante
- 1 per parametri di criticità bassa

Il valore da attribuire alla criticità è determinato con la somma del contributo di ciascun parametro che potrà assumere valori compresi tra 0 e 58 .

Il parametro contribuisce con il valore di criticità attribuito solo se ricorre nel Trattamento, se non ricorre il suo contributo è nullo.

La valutazione della criticità del Trattamento è assunta su tre livelli di criticità:

3	LIVELLO ALTO	>	20
2	LIVELLO MEDIO	[10 -	20]
1	LIVELLO BASSO	<	10

Per il livello di criticità BASSO la valutazione è facoltativa ed è condotta prevalentemente per definire gli eventuali margini di miglioramento del sistema di prevenzione.
Per il livello di criticità MEDIO ed ALTO la valutazione è NECESSARIA, al fine di valutare in modo esaustivo il Rischio Inerente del Trattamento e determinare le Misure di Attenuazione del Rischio.

3.2. Valutazione del LIVELLO di RISCHIO INERENTE

La valutazione del Rischio Inerente, attraverso il quale viene identificato il rischio del trattamento, senza considerare gli eventuali presidi di controllo posti in essere dall'Azienda per la sua mitigazione, combinando, sulla base di metriche predefinite, le seguenti due dimensioni:

- **Impatto**, ovvero il possibile effetto che la diffusione dei dati potrebbe avere per l'interessato;
- **Probabilità di accadimento**, ovvero la frequenza con cui il trattamento è effettuato.

Il Titolare del Trattamento, valuta qualitativamente l'impatto e la probabilità connessi al Trattamento sulla base dell'applicazione di specifiche scale di valutazione.

I valori di Impatto e Probabilità attribuiti sono tradotti quantitativamente su una scala da 1 a 4, dove:

1 corrisponde al valore minimo (es. Impatto = Trascurabile; Probabilità = Evento raro)
4 corrisponde al valore massimo (es. Impatto = Massimo; Probabilità = Evento probabile).

Il Rischio Inerente è calcolato quantitativamente come il prodotto tra i valori di Impatto e Probabilità associati al Trattamento in un *range* da 1 a 16

VALUTAZIONE RISCHIO INERENTE

scala impatto

4	8	12	16
3	6	9	12
2	4	6	8
1	2	3	4

probabilità accadimento

3.3. Misure di attenuazione del rischio e controllo

Ai fini della valutazione dei controlli previsti nell'ambito dello Step 3, il trattamento è classificato in funzione delle modalità con cui è svolto, in:

- Cartaceo: trattamento effettuato con l'utilizzo della carta
- Elettronico: trattamento effettuato unicamente in modalità elettronica;
- Cartaceo/Elettronico: trattamento effettuato in modalità cartacea ed elettronica.

3.3.1. Tipologia di Trattamento cartaceo

valutazione dei seguenti 4 controlli, definiti sulla base delle *best practices* di *Risk Management* e tenendo conto della Metodologia di *Risk Management* ISO 31001, di seguito riportata:

1. *chiara identificazione di ruoli e responsabilità del controllo;*
2. *periodico svolgimento delle attività di controllo;*
3. *formale definizione dei controlli/ norme comportamentali in policy/procedure aziendali;*
4. *presenza di misure di sicurezza fisiche per la gestione del cartaceo (es. presenza armadi/distruggi documenti).*

3.3.2. Tipologia di Trattamento elettronico

valutazione di 14 controlli, coincidenti con i domini dello standard ISO/IEC 27001/2013, associati a specifici obiettivi in materia di Sicurezza delle Informazioni di seguito riportati:

1. *politiche per la sicurezza delle informazioni;*
2. *organizzazione della sicurezza delle informazioni;*
3. *sicurezza delle risorse umane;*
4. *gestione degli asset;*
5. *controllo degli accessi;*
6. *crittografia;*
7. *sicurezza fisica e ambientale;*
8. *sicurezza delle attività operative;*
9. *sicurezza delle comunicazioni;*
10. *acquisizione, sviluppo e manutenzione dei sistemi;*
11. *relazioni con i fornitori;*
12. *gestione degli incidenti relative alla sicurezza delle informazioni;*
13. *disaster recovery – business continuity;*
14. *compliance.*

3.3.3. Tipologia di Trattamento cartaceo/elettronico

NON RICORRE

3.4. Definizione del RISCHIO RESIDUO

Ogni controllo è valutato quantitativamente sulla base di una scala a tre livelli:

(**a**)	**0**	*Controllo nullo/assente;*
(**p**)	**0,5**	*Controllo parzialmente soddisfatto;*
(**s**)	**1**	*Controllo totalmente soddisfatto.*

Ai fini del calcolo del Livello di Controllo, distintamente per le due tipologie di controlli (per trattamenti elettronici/Per trattamenti cartacei) è associato un peso uniforme.
La valutazione del controllo per ogni trattamento è ottenuta come somma ponderata della valutazione associata a ciascun controllo per il relativo peso.
Ai fini della definizione del livello di Rischio Residuo previsto nello step 4, per i Trattamenti effettuati in modalità Cartaceo/Elettronico è considerata la minore tra le valutazioni del controllo associate.

Il valore del **Rischio Residuo** per il trattamento è definito a partire dal **Valore di Rischio Inerente** tenendo in debita considerazione del **Valore del Controllo** mediante l'applicazione del seguente algoritmo di calcolo:

Rischio Residuo = Valore di Rischio Inerente x (1 - Valore del Controllo)

3.5. Classificazione del RISCHIO del TRATTAMENTO

Il valore ottenuto è successivamente ricondotto a una scala qualitativa ad 8 LIVELLI.

1. Trascurabile
2. Molto-Basso
3. Basso
4. Medio-Basso
5. Medio
6. Medio Alto
7. Alto
8. Molto Alto

Dunque, in considerazione del livello di Rischio Residuo, i trattamenti sono classificati in:

Trattamenti a rischio trascurabile:
trattamenti che presentano un valore del Rischio Residuo minore di 4

(corrispondente ai Livelli Trascurabile / Molto-Basso)

NON È NECESSARIO indirizzare azioni di adeguamento;

Trattamenti a rischio basso:
trattamenti che presentano un valore del Rischio Residuo minore di 8 e maggiore di 4 (corrispondente ai livelli Basso / Medio-Basso)

NON È NECESSARIO indirizzare azioni di adeguamento, ma È POSSIBILE VALUTARE delle azioni per il miglioramento/ottimizzazione del sistema di prevenzione e protezione del rischio;

Trattamenti a rischio medio:
trattamenti che presentano un valore di Rischio Residuo minore di 12 e maggiore di 8 (corrispondenti ai livelli Medio / Medio Alto)

*È RACCOMANDATO di individuare e indirizzare azioni di adeguamento e di miglioramento/ottimizzazione del sistema di prevenzione e protezione del risch*io;

Trattamenti a rischio alto:
trattamenti che presentano un valore del Rischio Residuo maggiore di 12 (corrispondenti ai livelli Alto / Molto Alto),

È NECESSARIO individuare e indirizzare azioni di adeguamento e di miglioramento/ottimizzazione del sistema di prevenzione e protezione del rischio.

In questo caso il Titolare del trattamento è obbligato a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento.

3.6. Consultazione PREVENTIVA

Nel caso in cui la valutazione d'impatto sulla protezione dei dati produca come risultato finale che il trattamento presenta un Rischio Residuo elevato (c.d. Trattamenti a Rischio Alto), anche sulla base dei presidi di controllo in essere, il Titolare del trattamento pone in essere le attività necessarie a effettuare una c.d. consultazione preventiva con l'Autorità di controllo.

Ai sensi dell'art. 36, paragrafo 3, del RGPD, la richiesta di consultazione inviata dovrà contenere indicazioni almeno relativamente a:

- ove applicabile, le rispettive responsabilità del Titolare del trattamento, di eventuali contitolari e responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
- le finalità e mezzi del trattamento previsto;
- le misure e le garanzie previste per la protezione dei diritti e delle libertà degli interessati;

- ove applicabile, i dati del RPD;
- le valutazioni di impatto sulla protezione dei dati dalle quali è risultato un livello di rischio elevato;
- eventuali ulteriori informazioni richieste da parte dell'Autorità di Controllo.

L'Autorità di controllo, entro un termine di otto settimane, al massimo prorogabile di ulteriori sei settimane, fornirà un parere scritto all'interno del quale sarà indicato se ritiene che il trattamento in esame violi i requisiti regolamentari oppure se lo stesso sia in linea con quanto disciplinato dal RGPD.

4. Esito della VALUTAZIONE

La valutazione è condotta con riferimento alle schede tecniche compilate ed allegate in calce :

scheda 1	Determinazione del livello di criticità del Trattamento
scheda 2	Valutazione del rischio inerente
scheda 3	Misure di Attenuazione e Controllo
scheda 4	Classificazione del Rischio Residuo

Step 1: Valutazione della criticità del TRATTAMENTO

scheda 1

note:

*Il livello di criticità del Trattamento si attesta su un valore pari a **19**, che corrisponde ad un livello di criticità classificato come **MEDIO** rappresentando in questo modo l'opportunità della presente valutazione.*

Step 2: Valutazione del livello di Rischio Inerente

scheda 2

note:

*Il Rischio Inerente si attesta su un valore pari a **8,** classificabile come livello di Rischio ALTO; il risultato è determinato dalla frequenza del Trattamento, che attinge al valore massimo della Probabilità dell'accadimento (valore pari a **4**), e dal possibile impatto su l'interessato, per il quale è stato scelto il parametro* LIMITATO *(valore pari a **2**) in quanto la diffusione di informazioni inerenti i comportamenti e la collocazione geografica possono avere uno spettro di conseguenze sull'interessato molto variabile, sia in considerazione del singolo individuo, sia per il medesimo nel tempo.*

Step 3: Misure di attenuazione del Rischio e Controllo

scheda 3

note:

Le misure di attenuazione e controllo conducono ad un parametro di Riduzione del rischio pari a 64% (Valore di controllo pesato)

Il Valore di controllo pesato necessita di un'azione di verifica periodica al fine di garantire la permanenza dei requisiti di Attenuazione, pertanto tale situazione dovrà essere monitorata con Audit di controllo specifici.

Step 4 / 5: Definizione del livello di Rischio Residuo e Classificazione del Trattamento

scheda 4

note:

*Il calcolo del Rischio Residuo si attesta su un valore pari a **5,1** che viene classificato come Trattamento a **RISCHIO BASSO** .*

*Il Trattamento presenta un valore del Rischio Residuo Tra **4** e **8** (corrispondente ai Livello Basso) pertanto SAREBBE NECESSARIA un azione di adeguamento;*

Preso atto della valutazione del rischio nella scheda 5.3 allegata al presente documento, si consiglia per la attenuazione del rischio, di adottare le misure 1 2 5 8 9 10 12 in modo che come evidenziato si arrivi a raggiungere un risultato parziale per attenuare il rischio.

La presente valutazione mantiene la sua validità esclusivamente nella situazione di permanenza di ogni requisito posto a verifica.
Ogni variazione in peius, determinata da deperimento od obsolescenza dei sistemi di supporto sia hardware, sia software, nonché l'attenuazione dell'applicazione di procedure o la diminuita attenzione e/o competenza dei preposti determinano un decadimento della valutazione del Rischio non determinabile aprioristicamente, e pertanto la carenza o la sola variazione di un solo requisito richiede di operare una nuova valutazione.

SONO RACCOMANDATI AUDIT PERIODICI PER IL CONTROLLO DELLA PERMANENZA DEI REQUISITI DI SICUREZZA SULLA PROTEZIONE DEI DATI.

Sassari 26/02/2024

il Legale Rappresentante
Il Referente presso il Garante

Il Responsabile della Protezione dei Dati
Ichnelios S.C.ar.l.

PIRAS ROBERTO
ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI SASSARI
Ingegnere
26.02.2024 17:04:38 GMT+01:00

ALLEGATI

scheda 5.1 Determinazione del livello di criticità del Trattamento

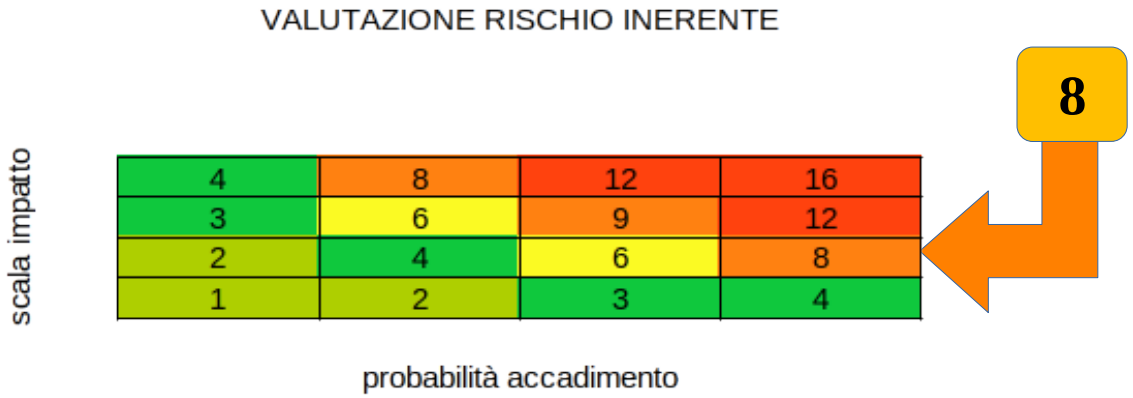
CARATTERISTICHE del TRATTAMENTO per la DETERMINAZIONE del LIVELLO di CRITICITA'			esito dell'AUDIT	19
	3	LIVELLO ALTO	>	20
	2	LIVELLO MEDIO	[10 -	20]
	1	LIVELLO BASSO	<	10
	DEVE ESSERE COMPILATO OGNI PUNTO DELLA TABELLA			

CATEGORIA VARIABILE	n.o	variabile	peso della variabile	valore AUDIT 0 – 1	risultato parziale
DATI PARTICOLARI	1	Dati che rivelano l'origine razziale o etnica	3	1	3
	2	Dati che rivelano le opinioni politiche	3	0	0
	3	Dati che rivelano le convinzioni religiose o filosofiche	3	0	0
	4	Dati che rivelano l'appartenenza sindacale	3	1	3
	5	Dati genetici	3	0	0
	6	Dati biometrici	3	0	0
	7	Dati relativi alla salute (Appartenenza a categoria protetta)	2	1	2
	8	Dati relativi alla salute (con evidenza del referto medico e/o informazioni su particolari disabilità)	3	0	0
	9	Dati relativi alla vita sessuale o all'orientamento sessuale di una persona	3	0	0
DATI di MINORI	10	Profilazione e/o marketing su minori	3	0	0
	11	Trattamento categorie particolari di dati su minori	3	1	3
ALTRI DATI COMUNI	12	Dati di identità per le finalità indicate per la videosorveglianza	2	1	2
	13	Carte di Credito / CC Bancari	3	0	0
	14	Dati di localizzazione	1	1	1
	15	Dati di Videosorveglianza	3	1	3
FINALITà	16	Finalità di marketing (invio comunicazioni commerciali)	2	0	0
	17	Finalità di profilazione	3	0	0
TERZI	18	Presenza di soggetti terzi (fornitori e non) con cui possono essere condivisi i dati	2	0	0
INFRA STRUTTURA	19	Infrastruttura (di [+] o di fornitori esterni) o parte delle infrastrutture coinvolte nel trattamento in Cloud (SaaS)	2	0	0
	20	Infrastruttura (di [+] o di fornitori esterni) o parte delle infrastrutture coinvolte nel trattamento in Cloud (Private Cloud)	1	0	0
DEVICE	21	MS Exchange in Private Cloud	1	0	0
	22	Dati Residenti fuori dall'UE	3	0	0
	23	Dati trattati attraverso l'utilizzo di device portatili (per es. tablet), anche da parte dei dipendenti	1	0	0
	24	Permesso l'utilizzo di supporto removibili per il trasferimento dei dati	2	1	2
			58		
		risultato complessivo			19

scheda 5.2 Valutazione del Rischio Inerente

Valutazione della probabilità di ACCADIMENTO			audit	
DEVE ESSERE COMPILATO SOLO UN PUNTO DELLA TABELLA				
valutazione criticità	valore criticità	descrizione	valore AUDIT 0 – 1	risultato parziale
EVENTO PROBABILE	4	Il Trattamento avviene con frequenza GIORNALIERA	1	4
EVENTO POSSIBILE	3	Il Trattamento avviene con frequenza SETTIMANALE	0	0
EVENTO IMPROBABILE	2	Il Trattamento avviene con frequenza MENSILE/TRIMESTRALE	0	0
EVENTO RARO	1	Il Trattamento avviene con frequenza SEMESTRALE/ANNUALE	0	0
		probabilità di ACCADIMENTO		**4**

Valutazione di IMPATTO			audit	
DEVE ESSERE COMPILATO SOLO UN PUNTO DELLA TABELLA				
	scala impatto		valore AUDIT 0 – 1	risultato parziale
MASSIMO	4	Informazioni che, se divulgate potrebbero avere conseguenze gravi e/o irreversibili per l'interessato	0	0
SIGNIFICATIVO	3	Informazioni che, se divulgate potrebbero avere significative conseguenze per l'interessato	0	0
LIMITATO	2	Informazioni che, se divulgate potrebbero causare all'interessato problemi di carattere personale	1	2
TRASCURABILE	1	Informazioni comuni note con limitazioni di diffusione che, se divulgate, determinano un impatto trascurabile sull'interessato.	0	0
		Valutazione di IMPATTO		**2**
				x
		probabilità di ACCADIMENTO		**4**
				=
		RISCHIO INERENTE		**8**



scheda 5.3 Misure di Attenuazione e Controllo

misure di ATTENUAZIONE e CONTROLLO			controllo nullo /assente	parzialmente soddisfatto	soddisfatto	
	controlli per trattamenti elettronici	DEVE ESSERE COMPILATA UNA SOLA OPZIONE per OGNI PUNTO DELLA TABELLA	a	p	s	
n.o.	dominio ISO/IEC	Obiettivo	valore AUDIT			risultato parziale
1	Politiche per la sicurezza delle informazioni	Fornire indicazioni di gestione e supporto per la sicurezza delle informazioni in accordo con i requisiti di business e regolamenti cogenti.	a			0
2	Organizzazione della sicurezza delle informazioni	Stabilire un quadro di gestione per avviare e controllare l'implementazione della sicurezza delle informazioni all'interno dell'organizzazione.	a			0
3	Sicurezza delle risorse umane	Assicurare che il personale comprenda le proprie responsabilità e sia adeguato al ruolo loro assegnato.		p		0,5
4	Gestione degli asset	Identificare gli asset dell'organizzazione e definire appropriate responsabilità per la loro protezione.		p		0,5
5	Controllo degli accessi	Prevenire l'accesso di utenti non autorizzati ai sistemi ed alle applicazioni.	a			0
6	Crittografia	Proteggere la riservatezza, l'autenticità o l'integrità delle informazioni attraverso strumenti di crittografia.	a			0
7	Sicurezza fisica e ambientale	Prevenire accessi fisici non autorizzati, intromissioni e danni alle infrastrutture informative ed alle informazioni.			s	1
8	Sicurezza delle attività operative	Assicurare una gestione operativa corretta e sicura delle apparecchiature per l'elaborazione delle informazioni.	a			0
9	Sicurezza delle comunicazioni	Assicurare la salvaguardia delle informazioni in rete e la protezione dell'infrastruttura di supporto.	a			0
10	Acquisizione, sviluppo e manutenzione dei sistemi informativi	Assicurare che la sicurezza sia parte integrante dei sistemi informativi in tutto il ciclo di vita. Esso include anche i requisiti per i sistemi informativi che forniscono servizi sulle reti pubbliche.	a			0
11	Relazioni con i fornitori	Assicurare la protezione degli asset dell'organizzazione accessibili ai fornitori.			s	1
12	Gestione degli incidenti relativi alla sicurezza delle informazioni	Assicurare un approccio efficace e consistente alla gestione degli incidenti di sicurezza informatica, inclusi tutti gli eventi e le vulnerabilità di sicurezza delle comunicazioni.	a			0
13	Disaster Recovery / Business Continuity	La continuità della sicurezza delle informazioni dovrebbe essere integrata all'interno del sistema di gestione della continuità operativa dell'organizzazione.			s	1
14	Conformità	Evitare la violazione di obblighi legali, regolamentari o contrattuali relativi alla sicurezza delle informazioni e di eventuali requisiti di sicurezza.			s	1
		VALUTAZIONE PESATA di CONTROLLO				0,357143

scheda 5.4 Classificazione del Rischio Residuo

CLASSIFICAZIONE RISCHIO RESIDUO				
		valore del RISCHIO		
Trattamenti a rischio trascurabile	trattamenti che presentano un valore del Rischio Residuo minore di 4 (corrispondente ai Livelli Trascurabile / Molto-Basso) e per i quali non è necessario indirizzare azioni di adeguamento;		**<**	**4**
Trattamenti a rischio basso	trattamenti che presentano un valore del Rischio Residuo minore di 8 e maggiore di 4 (corrispondente ai livelli Basso / Medio-Basso) per i quali non è necessario indirizzare azioni di adeguamento, ma è possibile valutare delle azioni per il miglioramento/ottimizzazione del sistema di prevenzione e protezione del rischio;	**[4**	**-**	**8 [**
Trattamenti a rischio medio	trattamenti che presentano un valore di Rischio Residuo minore di 12 e maggiore di 8 (corrispondenti ai livelli Medio / Medio Alto), per i quali è consigliato di individuare e indirizzare azioni di adeguamento e di miglioramento/ottimizzazione del sistema di prevenzione e protezione del rischio;	**[8**	**-**	**12 [**
Trattamenti a rischio alto	trattamenti che presentano un valore del Rischio Residuo maggiore di 12 (corrispondenti ai livelli Alto / Molto Alto), per i quali è necessario individuare e indirizzare azioni di adeguamento e di miglioramento/ottimizzazione del sistema di prevenzione e protezione del rischio. In questo caso il Titolare del trattamento è obbligato a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento.		**>**	**12**

6 ALTRI ALLEGATI

allegato 1	**Relazione Tecnica delle risorse dedicate al Servizio di Video-sorveglianza**
allegato 2	**Regolamento della videosorveglianza**
allegato 3	**Procedure di gestione del Servizio di Video-sorveglianza**