AUTORITA' DI SISTEMA PORTUALE DEL MAR TIRRENO CENTRALE

Regolamento di videosorveglianza dei Porti della Circoscrizione dell'AdSP del Mar Tirreno Centrale

ALLEGATO AL DPS ED. 2022

NAPOLI - 2022

Sommario

INDICE DELLE REVISIONI

La tabella sottostante riporta la storia cronologica della Relazione e delle sue revisioni. Di ogni revisione, oltre alla data e alla tipologia d'intervento, successivo alla prima emissione, viene qui indicato il nome dell'estensore della revisione specifica, e del Titolare che ha approvato la revisione.

Edizione	Data	Revisore	Approvazione	Tipo di revisione

CAPO I

PRINCIPI GENERALI

Articolo 1 – Premessa

Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza gestiti ed impiegati dall'**Autorità di Sistema Portuale del Mar Tirreno Centrale**, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Garantisce altresì i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento.

Inoltre, nel rispetto del Provvedimento Generale emesso in data 8 aprile 2010 dal Garante della Privacy in cui viene stabilito che la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configurano un trattamento di dati personali, il presente Regolamento descrive un Sistema di Gestione della Sicurezza delle Informazioni (denominato da adesso SGSI) idoneo a ridurre al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini secondo quanto previsto dal GDPR. A tale scopo, quindi, verranno descritte le specifiche misure tecniche adottate ed i provvedimenti organizzativi che consentano al titolare dei dati di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).

Articolo 2 - Principi generali

1. Le prescrizioni del presente Regolamento si fondano sui principi di liceità, necessità, proporzionalità e finalità.
2. In ossequio al principio di liceità, l'A. P., Ente pubblico non economico, utilizza un sistema di videosorveglianza soltanto per lo svolgimento delle funzioni istituzionali e per conformarsi alle disposizioni in materia di sicurezza e security che di seguito vengono indicate:
    - Regolamento Eu n. 725/2004, relativo al miglioramento della sicurezza delle navi e del trasporto marittimo;

- direttiva comunitaria 2005/65/CE del Parlamento Europeo e del Consiglio del 26 ottobre 2005 che prevede, tra l'altro, l'individuazione di misure, procedure e azioni volte a limitare e mitigare le conseguenze di eventuali attentati dagli effetti devastanti;
- D.Lgs. n.203 del 06.11.2007 "Attuazione della Direttiva 2005/65/CE relativa al miglioramento della sicurezza nei porti";
- "Valutazione di Sicurezza" redatta dall'Autorità Portuale di Napoli ai sensi del D.Lgsl. 06.11.2007 n.203 ed approvata dalla Capitaneria di Porto di Napoli con Decreto n. 199 del 17.12.2018, riportante l'individuazione e la valutazione dei beni e delle infrastrutture da proteggere, le possibili minacce nonché le contromisure e gli adattamenti procedurali;
- "Piano di Sicurezza del Porto di Napoli" approvato con provvedimento del Prefetto della Provincia di Napoli con decreto n. 90/19/NC/AREA I^ (O.S.P.) in data 08.05.2019, redatto in forma congiunta dall'Autorità di Sicurezza del porto di Napoli e dall'Autorità Portuale di Napoli ai sensi del su indicato D.Lgs n.203;
- Decreto n.154 del 15.09.2009 con il quale viene adottato il "Regolamento recante disposizioni per l'affidamento dei servizi di sicurezza sussidiaria nell'ambito dei porti, delle stazioni ferroviarie e dei relativi mezzi di trasporto e depositi; delle stazioni delle ferrovie metropolitane e dei relativi mezzi di trasporto e depositi; nonché nell'ambito delle linee di trasporto urbano per il cui espletamento non è richiesto l'esercizio di pubbliche potestà adottato ai sensi dell'art.18, comma 2, del Decreto Legge 27.07.2005 n.144, convertito con modificazioni, dalla legge 31.07.2005 n.155".

3. Nel rispetto del principio di necessità, l'AdSP del Mar Tirreno Centrale utilizza un sistema di videosorveglianza configurato in modo da ridurre al minimo la registrazione di dati personali e di dati identificativi e da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate, rispettivamente, mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
4. Secondo quanto previsto dal principio di proporzionalità, nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, è stata evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra una effettiva esigenza di deterrenza. La proporzionalità è stata valutata in ogni fase o modalità del trattamento. Laddove l'installazione degli impianti di videosorveglianza è stata finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, di danneggiamento o di furto, è perché sono risultati comunque inefficaci altri idonei accorgimenti, vale a dire controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi.

5. Secondo il principio di finalità, gli scopi perseguiti devono essere determinati, espliciti e legittimi pertanto, la videosorveglianza è stata realizzata in piena conformità con le disposizioni del Reg. EU 725/2004, come misura complementare volta a prevenire atti illeciti intenzionali (ad ex atti terroristici) e comunque per migliorare la sicurezza all'interno dell'ambito portuale nei siti ove si svolgono attività produttive, industriali, commerciali o di servizi ed in particolare in quei siti o banchine o accosti destinati alle navi che esigono un particolare controllo.

Articolo 3 – Definizioni

Ai fini del presente Regolamento si intende:

DPIA	Data Protection Impact Assessment – Valutazione d'Impatto sulla protezione dei dati
DPO	Data Protection Officer – Responsabile della Protezione dei Dati
EDPB	European Data Protection Board – Comitato europeo per la Protezione dei Dati. Organismo europeo indipendente il cui scopo è garantire un'applicazione coerente del GDPR.
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation – Regolamento Generale sulla Protezione dei Dati, n. 2016/679
IT	Information Technology
WP29	Working Group 29: gruppo istituito ai sensi dell'art. 29 della direttiva 95/46 CE. Dal 25 Maggio 2018 prende il nome di European Data Protection Board.
D.lgs. n. 101/2018	Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (GDPR).
D.lgs. n. 196/2003	Decreto Legislativo n. 196 del 30 giugno 2003, contenente il "Codice in materia di protezione dei dati personali", n. c. "Codice Privacy".
Regolamento UE 2016/679	Regolamento del Parlamento Europeo e del Consiglio, 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 (regolamento generale sulla protezione dei dati).
Legge n. 300/1970	Statuto dei Lavoratori.
Linee guida EDPB 3/2019	Linee guida in materia di videosorveglianza secondo il regolamento (UE) 2016/679, rilasciate dall'EDPB il 29 gennaio 2019.

a. *per "banca di dati"*, il complesso di dati personali, formatosi presso la sala di coordinamento, e trattato esclusivamente mediante riprese televisive che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti che transitano nelle aree portuali gestite o di proprietà dell'Ente.
b. *per il "trattamento"*, tutte le operazioni o complesso di operazioni svolte con l'ausilio dei mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto,

l'utilizzo, l'interconnessione, il blocco, la comunicazione, l'eventuale diffusione, la cancellazione e la distribuzione di dati;

c. *per "dato personale"*, qualunque informazione relativa a persona fisica, persona giuridica, Ente o associazione, identificati o identificabili, anche direttamente, e rilevati con trattamenti di immagini effettuati attraverso l'impianto di videosorveglianza;
d. *per "titolare"*, l'Autorità di Sistema portuale del Mar tirreno Centrale, nelle sue articolazioni interne, cui compete assumere decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;
e. *per "responsabile"*, la persona fisica, legata da rapporto di servizio al titolare e preposto dal medesimo al trattamento dei dati personali;
f. *per "interessato"*, la persona fisica, la persona giuridica, l'Ente o associazione cui si riferiscono i dati personali;
g. per "comunicazione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
h. *per "diffusione"*, il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
i. *per "dato anonimo"*, il dato che in origine a seguito di inquadratura, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
j. *per "blocco",* la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;
k. *per "Codice"*, il Codice in materia di protezione dei dati personali di cui al D. L.vo 196 del 30 giugno 2003.

Articolo 4 - Ambito di applicazione

Il presente Regolamento disciplina le modalità di raccolta, trattamento e conservazione di dati personali mediante sistemi di videosorveglianza attivati nell'ambito della circoscrizione portuale gestita dall'Autorità di Sistema Portuale del Mar Tirreno Centrale e collegati alle Sale di coordinamento.

Articolo 5 – Informativa

1. Gli interessati saranno informati che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale relativa registrazione, mediante un modello semplificato di informativa "breve", ovvero cartelli informativi posizionati agli ingressi e nelle varie zone delle aree portuali. Una prima informazione, quindi, è costituita dalla cartellonistica, che deve essere

ben visibile immediatamente prima che l'Interessato possa accedere nell'area videosorvegliata. Qualora la videocamera effettui anche riprese notturne, il cartello deve essere visibile anche di notte. L'informativa breve deve essere collocata nelle immediate vicinanze dei luoghi ripresi, deve avere un formato ed una dimensione che ne permetta un'agevole leggibilità e un posizionamento tale da essere chiaramente visibile agli interessati. L'informativa breve deve identificare il Titolare del trattamento e specificare le finalità della sorveglianza, nonché i riferimenti (collegamento al sito web aziendale) dove acquisire da parte dell'utenza, senza oneri ed agevolmente, il testo completo dell'informativa estesa sulla videosorveglianza.

2. Il Titolare del trattamento comunicherà agli interessati in ambito portuale l'attivazione del sistema di videosorveglianza e il conseguente avvio del trattamento dei dati personali, l'eventuale incremento dimensionale degli impianti e l'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo, mediante l'affissione di appositi manifesti informativi e/o altri mezzi di diffusione locale.

Articolo 6 – Finalità istituzionali del sistema di videosorveglianza

1. Le finalità perseguite mediante l'attivazione del sistema di videosorveglianza sono del tutto conformi alle funzioni istituzionali attribuite all'AdSP ai sensi della legge n.84/94 e s.m.i. relativa alla costituzione delle Autorità Portuali, del Reg. EU 725/04 e dalla parte "A" del codice I.S.P.S. in tema di sicurezza delle navi e dei traffici marittimi.
2. Il trattamento dei dati personali è effettuato ai fini:
   a. di monitorare, in tempo reale, i luoghi e le aree soggette agli accosti delle navi;
   b. di garantire la sicurezza dei trasporti marittimi e dei cittadini che ne fanno uso nonché la sicurezza dell'ambiente ed infine per contrastare la minaccia di atti illeciti intenzionali, quali atti terroristici, atti vandalici e danneggiamenti.
3. Il sistema di videosorveglianza comporta il trattamento di dati personali rilevati mediante le riprese televisive a circuito chiuso che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti ed i mezzi di trasporto che transitano nelle aree portuali.

CAPO II

TRATTAMENTO E RACCOLTA DEI DATI

Art. 7 – Responsabile ed incaricati del trattamento

1. Il Presidente dell'Autorità di sistema Portuale del Mar Tirreno Centrale, ovvero il Titolare del trattamento, designa con nomina il Delegato al trattamento dei dati, dell'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, della visione delle registrazioni.
2. Il Delegato, designerà per iscritto, tutte le persone fisiche incaricate del trattamento dei dati, dell'utilizzazione degli impianti e, nei casi in cui risulta indispensabile per gli scopi perseguiti, della visione delle registrazioni.
3. Il Delegato e gli incaricati conformeranno la propria azione al pieno rispetto di quanto prescritto dalle leggi vigenti e delle disposizioni nel presente Regolamento.
4. Il Delegato e gli incaricati procedono al trattamento attenendosi alle istruzioni impartite dal titolare il quale, con il supporto dell'Ufficio Privacy, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari.
5. I compiti affidati al Delegato ed agli incaricati devono essere analiticamente specificati nell'atto di designazione.

Articolo 8 – Trattamento e conservazione dei dati

1. I dati personali oggetto di trattamento sono:
   a. trattati in modo lecito e secondo correttezza;
   b. raccolti e registrati per le finalità di cui al precedente art. 6 comma 2, e resi utilizzabili per operazioni non incompatibili con tali scopi;
   c. monitorati, in tempo reale, presso le sale di coordinamento dell'AdSP - sedi di Napoli, Salerno e Castellammare di Stabia, dove sarà gestito e controllato il corretto funzionamento dell'impianto, nonché presso le sale operative delle FFOO locali e dell'Autorità Marittima;
   d. raccolti in modo pertinente, completo e non eccedente il rispetto delle finalità per le quali sono raccolti o successivamente trattati;
   e. trattati con modalità volta a salvaguardare l'anonimato degli interessati;
   f. conservati per un periodo non superiore a *sette giorni* successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in caso di specifica richiesta, con finalità

investigativa, inoltrata dall'Autorità Giudiziaria o dalla Polizia Giudiziaria. L'eventuale allungamento dei tempi di conservazione rivestirà carattere di eccezionalità in relazione a necessità cogenti imposte da un evento già accaduto o realmente incombente, oppure dalla necessità di consegnare una copia su specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria in relazione ad attività investigative in corso.

Si precisa che in tutti i casi in cui si renda necessario procedere ad un allungamento dei tempi di conservazione per un periodo superiore alla settimana, occorre che una richiesta in tal senso sia sottoposta ad una verifica preliminare da parte del Garante. L'allungamento dei tempi di conservazione, oltre i termini previsti, deve in ogni caso ritenersi di carattere eccezionale, e ciò nel pieno rispetto del principio di proporzionalità.

Al trattamento dei dati attraverso sistemi di videosorveglianza e/o videocontrollo è applicato il principio di necessità, come stabilito dal GDPR: qualsiasi trattamento non conforme a questo principio è da ritenersi illecito.

Il sistema a supporto degli impianti di videosorveglianza e/o videocontrollo è conformato in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi.

L'eventuale registrazione di dati personali non necessari deve essere cancellata ed i relativi supporti distrutti.

Per l'installazione di sistemi di videosorveglianza che prevedono un intreccio delle immagini con altri particolari sistemi (es. dati biometrici) o in caso di digitalizzazione delle immagini o di sorveglianza che valuti percorsi e lineamenti (es. riconoscimento facciale) deve essere effettuata da parte del Titolare una valutazione d'impatto sulla protezione dei dati personali (DPIA).

2. Il trattamento dei dati viene effettuato con strumenti elettronici, nel rispetto delle misure di sicurezza in conformità a quanto indicato all'art. 32 del Regolamento UE 679/2016 (GDPR). In particolare:

Il trattamento dei dati personali attraverso l'impiego di un sistema di videosorveglianza è equiparato al trattamento dei dati personali a mezzo di strumenti elettronici.

Tra le misure che il Titolare adotta o può adottare per tale trattamento, si segnalano:

- **Credenziali di autenticazione distinte per livello di accesso**
  In presenza di differenti competenze specificatamente attribuite ai singoli incaricati, devono essere configurati diversi livelli di accesso e trattamento delle immagini.
- **Abilitazione in base alla mansione**

Se i sistemi di videosorveglianza prevedono la registrazione e la conservazione delle immagini, deve essere limitata la possibilità, per i soggetti abilitati, di prendere visione delle immagini stesse.

- **Cancellazione automatica**
  Il sistema deve prevedere la cancellazione in automatico delle immagini registrate mediante sovrascrittura, rispettando le scadenze contenute nel presente regolamento.
- **Cautele nelle attività di manutenzione**
  L'accesso alle immagini è limitato ai casi ove si renda indispensabile compiere delle verifiche tecniche.
- **Protezione da accessi abusivi**
  Nel caso in cui il sistema di ripresa sia collegato a reti telematiche, trova applicazione il disposto di cui all'art. 615ter c.p.
- **Cifratura delle comunicazioni su reti pubbliche**
  La trasmissione tramite reti pubbliche di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche di crittografia che garantiscano la riservatezza.

È compito del Responsabile esterno, del Delegato interno per la videosorveglianza (qualora designato) e del dirigente dell'Ufficio competente alla gestione degli impianti di videosorveglianza e videocontrollo verificare il rispetto delle misure di sicurezza contenute nel presente regolamento e della normativa di settore e comunicare eventuali misure che si rendano necessarie per evitare il rischio di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta.

Della adozione di tali misure di sicurezza sarà fatta menzione nella eventuale DPIA effettuata dal Titolare.

L'Ufficio AA.GG. Risorse Umane e Segreteria, deputato alla formazione del personale e alla gestione degli adempimenti privacy, in accordo con il DPO, programma iniziative periodiche di formazione ai delegati ed agli incaricati in materia di videosorveglianza.

Il Titolare del trattamento, per il tramite dell'Ufficio Privacy, deve costituire apposito registro, o inserire un'apposita sezione per il trattamento dei dati della videosorveglianza nel registro dei trattamenti preesistente, per la disciplina di questo trattamento.

Per tutti i dettagli su tale registro, così come delineato dal GDPR, si rimanda alla procedura specifica conservata in azienda.

La valutazione di impatto si configura come un'autonoma valutazione che il Titolare del trattamento pone in essere per analizzare la necessità, la proporzionalità e i rischi di un determinato trattamento dati per i diritti e le libertà delle persone fisiche. Tale valutazione deve essere effettuata per tutti i trattamenti in materia di videosorveglianza che possono comportare tale livello di rischio e, in particolar modo, deve essere effettuata secondo il GDPR in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico. Per determinare se un trattamento è svolto su "larga scala" si deve far riferimento al numero degli interessati, al volume di dati e/o alle tipologie di dati, alla durata dell'attività di trattamento e all'ambito geografico dell'attività di trattamento.

Articolo 9 – Modalità di raccolta dei dati

1. I dati personali sono raccolti attraverso riprese video effettuate da telecamere a circuito chiuso installate in corrispondenza delle principali banchine, piazzali ed immobili appartenenti al demanio marittimo ubicati nell'ambito delle circoscrizioni portuali, nonché in corrispondenza del perimetro delle aree portuali.
2. Le telecamere di cui al precedente comma consentono riprese video a colori o in bianco/nero. Esse possono essere dotate di brandeggio e zoom ottico programmati, e sono collegate ad un centro di gestione ed archiviazione che consente di registrare le immagini esclusivamente per il perseguimento dei fini istituzionali.
3. I segnali video delle unità di ripresa saranno raccolti presso le stazioni di monitoraggio e controllo site nelle sedi dei porti della circoscrizione dell'AdSP del Mar Tirreno Centrale. In queste sedi le immagini saranno visualizzate in tempo reale su monitor e registrate in digitale su hard disk.
4. Le immagini videoregistrate sono conservate per il periodo indicato all'art. 8, comma 1, lettera e) presso le Sale di coordinamento. Al termine del periodo stabilito, il sistema di videoregistrazione provvede, in automatico, alla loro cancellazione mediante sovra-registrazione, con modalità tali da rendere non utilizzabili i dati cancellati.
5. Le immagini videoregistrate possono essere visionate dagli operatori della video centrale dal PSO, dai deputy PSO e dai rappresentanti delle FF.OO. o Autorità Giudiziaria che ne facciano richiesta scritta registrando l'accesso su apposito registro, predisposto dall'ufficio competente e custodito dagli operatori stessi, mentre possono essere estrapolate e consegnate esclusivamente alle FF. OO o Autorità Giudiziaria a seguito di apposita richiesta scritta che viene valutata ed autorizzata dal Dirigente Ufficio Security e Capo Settore Operativo.
6. Nel caso in cui i rappresentanti delle suddette FF.OO. si presentino in Sala di Videosorveglianza per la mera visualizzazione delle immagini, l'addetto in centrale è tenuto ad avvisare uno dei reperibili di turno dell'Ufficio Security per preventivo n/o all'accesso, nonché ad annotare nel registro il nominativo del richiedente con indicazione del relativo Comando di appartenenza.

Articolo 10 - Obblighi degli operatori

1. L'utilizzo delle telecamere è consentito solo per la sorveglianza di quanto si svolge nelle aree comprese nel demanio marittimo gestito dall'AdSP del Mar tirreno Centrale.
2. Fatti salvi i casi di richiesta degli interessati al trattamento dei dati registrati, questi ultimi possono essere riesaminati, nel limite del tempo ammesso per la conservazione di cui al precedente articolo, solo in caso di effettiva necessità e per esclusivo perseguimento delle finalità espresse dall'art. 6.

3. La mancata osservanza degli obblighi di cui al presente articolo comporterà l'applicazione di sanzioni disciplinari ed amministrative e, ove previsto dalla vigente normativa, l'avvio degli eventuali procedimenti penali a carico del trasgressore.
4. E' vietato fotografare e/o filmare con cellulari o altro tipo di dispositivo elettronico direttamente le immagini trasmesse dai monitor della sala di videosorveglianza.

CAPO III

DIRITTI, SICUREZZA E LIMITI NEL TRATTAMENTO DEI DATI

Articolo 11 - Diritti dell'interessato

Ai sensi del GDPR, all'interessato sono assicurati diversi diritti, in particolare:

a) accedere ai dati che lo riguardano (allegato n. 4);

b) verificare le finalità, le modalità e la logica del trattamento;

c) ottenere l'interruzione di un trattamento illecito, la cancellazione dei propri dati o la limitazione del trattamento degli stessi a determinate finalità (allegato n. 5).

Il Titolare, garantisce l'effettivo esercizio dei diritti dell'interessato, secondo le seguenti modalità:

1) l'Interessato, previa verifica dell'identità ed entro le settantadue ore successive alla rilevazione, può richiedere per iscritto l'accesso alle registrazioni che lo riguardano (allegato n. 4). L'eventuale accesso a registrazioni riferite direttamente o indirettamente a terzi sarà oggetto di apposito bilanciamento degli interessi da parte del Titolare, acquisito il parere dall'Ufficio Privacy e del DPO;

2) i dati sono estratti a cura dell'Incaricato e possono essere comunicati direttamente al richiedente mediante la visione delle registrazioni e, se vi è richiesta, si provvede alla duplicazione di tali registrazioni su adeguato supporto;

3) la visione e l'estrazione delle rilevazioni è gratuita per l'interessato; qualora, tuttavia, a seguito di questa operazione non risulti l'esistenza di dati che riguardano l'Interessato, potrà essergli addebitato un contributo spese, ai sensi del GDPR.

Articolo 12 - Cessazione del trattamento dei dati

In caso di cessazione, per qualsiasi causa, dell'attività di trattamento, i dati personali sono:

a. distrutti;
b. conservati per fini esclusivamente istituzionali.

Articolo 13 – Comunicazione

1. La comunicazione di dati personali da parte dell'AdSP ad altri soggetti pubblici è ammessa quando risulti comunque necessaria per lo svolgimento delle funzioni istituzionali e per gli scopi previsti dal presente Regolamento.

2. La comunicazione di dati personali da parte dell'AdSP a privati o a Enti pubblici economici è ammessa unicamente quando prevista da una norma di legge.

CAPO IV

NORME FINALI

Articolo 14 - Modifiche regolamentari

Le norme del presente Regolamento saranno adeguate alle modifiche normative e regolamentari che dovessero intervenire nonché allo sviluppo dei sistemi di sicurezza utilizzati.

Articolo 15 – Provvedimenti attuativi

Il competente Ufficio Security, Safety ed Ordinanze, previa intesa con il Segretario Generale dell'AdSP del Mar Tirreno Centrale, e con l'ausilio della società fornitrice del servizio, nominata quale Responsabile esterno del trattamento ex art. 28 del GDPR, assumerà i provvedimenti attuativi conseguenti. In particolare curerà la predisposizione dell'elenco dei siti di ripresa e la definizione di ogni ulteriore disposizione ritenuta utilmente applicabile in coerenza con i principi del presente Regolamento.

Articolo 16 - Norme finali

Per quanto non disciplinato dal presente Regolamento si rinvia al Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 200, n. 196 come modificato dal D.lgs. n. 101/2018, e al Provvedimento Generale del Garante in materia di videosorveglianza, emesso in data 8 aprile 2010 e pubblicato su G. U. del 29/04/2010, oltre che dal Regolamento UE 2016/679, dalla Legge n. 300/1970 e dalle Linee guida EDPB 3/2019

Articolo 17 - Pubblicità del Regolamento

Copia del presente Regolamento, a norma dell'art. 22 della legge n. 241/90 e successive modifiche, sarà resa disponibile al pubblico. Inoltre, copia dello stesso Regolamento sarà pubblicata sul sito istituzionale dell'AdSP del Mar Tirreno Centrale e trasmessa agli Uffici dell'Ente.

Articolo 18 - Entrata in vigore e durata

Il presente Regolamento entra in vigore a far data dalla sua approvazione e contestuale pubblicazione sul sito istituzionale dell'Ente.

ALLEGATO "A"

ALLEGATO "A" – VALUTAZIONE d'IMPATTO - ANALISI DEI RISCHI DEL SISTEMA DI GESTIONE DEI DATI

La Data Protection Impact Assessment (DPIA) o "Valutazione di impatto sulla protezione dei dati" rappresenta una delle fondamentali attività previste dal Regolamento UE 679/2016, di seguito sinteticamente indicato come "Regolamento" o "GDPR", relativamente agli obblighi dei Titolari (cfr. art 35), nell'ambito della gestione del rischio correlato al trattamento di dati personali.
La DPIA è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per ridurli.
In tale ottica l'analisi dei Rischi incombenti sui dati personali trattati dal Sistema di Videosorveglianza rappresenta una fase essenziale per la valutazione dell'impatto possibile sui soggetti interessati. Atteso il rispetto dei principi di necessità e proporzionalità del trattamento, un "rischio" **è uno scenario che descrive un evento e le sue conseguenze**. La valutazione dei rischi deve identificare gli **"scenari di rischio"** e, per ognuno di essi, stimare il "livello di rischio effettivo" per i diritti e le libertà dell'interessato connesso al trattamento in esame con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento.
I principali scenari di rischio da prendere in considerazione sono:

- perdita di riservatezza - accesso illegittimo ai dati personali;
- perdita di integrità - modifica non autorizzata dei dati personali;
- perdita di disponibilità - perdita, furto, cancellazione non autorizzata di dati personali.

In questa sezione sono descritti i rischi in relazione al contesto fisico–ambientale di riferimento e agli strumenti elettronici utilizzati per la videosorveglianza:

- *I principali eventi potenzialmente dannosi per la sicurezza dei dati*
- *Le possibili conseguenze e la gravità*

EVENTI	
EVENTI CONSEGUENTI A CALAMITÀ NATURALI	➢ Perdita di dati conseguente ad allagamento ➢ Perdita di dati conseguente ad incendio ➢ Perdita di dati conseguente ad evento sismico
EVENTI CONSEGUENTI A MINACCE INTENZIONALI	➢ Accessi non consentiti e Furti ➢ Accessi non autorizzati e Trattamenti non consentiti ➢ Furto e/o manomissione dati su supporti cartacei ➢ Furto e/o manomissioni dati su supporti informatici ➢ Furto di Strumenti Elettronici ➢ Sottrazione credenziali ➢ Carenza di consapevolezza – incuria ➢ Comportamenti sleali o fraudolenti ➢ Cessione involontaria di credenziali

	➢ Incuria nella custodia dei supporti/dispositivi
EVENTI CONSEGUENTI A MINACCE INVOLONTARIE	➢ Blackout elettrico ➢ Anomalie e Guasti dell'Alimentazione e/o Sistema Elettronico ➢ Malfunzionamenti Software ➢ Malfunzionamenti Hardware ➢ Errore materiale
EVENTI CONSEGUENTI AD ATTACCHI AL SISTEMA INFORMATICO	➢ Perdita di Dati dovuta a virus o ad intrusione informatica ➢ Spamming e tecniche di sabotaggio ➢ Malfunzionamento o indisponibilità degrado degli strumenti ➢ Accessi esterni non autorizzati ➢ Intercettazione informazioni su rete

VALUTAZIONE DEL RISCHIO

LEGENDA

TERMINE	DESCRIZIONE		
EVENTO	Fatto o avvenimento preso in considerazione nell'analisi dei rischi		
PROBABILITA'	Probabilità che l'evento accada		
	1	Poco Probabile	
	2	Probabile	
	3	Molto Probabile	
	4	Altamente Probabile	
GRAVITA' AZIENDALE	Livello di criticità dell'evento e/o di non conformità di un comportamento ad una normativa aziendale		
	1	Molto Bassa	
	2	Bassa	
	3	Media	
	4	Alta	
RILEVANZA ECONOMICA	Entità del potenziale danno in termini di diminuzione di profitto, perdita di immagine, irrogazione di sanzioni amministrative e penali		
	1	Bassa	
	2	Media	
	3	Alta	
	4	Molto Alta	
CONSEGUENZE	Possibili Conseguenze a seguito del verificarsi dell'evento		
	A	Le conseguenze non incidono in maniera considerevole sulla sicurezza e tutela dei dati personali	
	B	Rischio di distruzione o perdita, anche accidentale, di dati personali	
	C	Rischio di accesso non autorizzato a dati personali	
	D	Rischio di trattamento non consentito o non conforme alle finalità della raccolta di dati personali	
RISCHIO	Livello di rischio aziendale = Probabilità x Gravità Aziendale x Rilevanza Economica		
	1 - 7	Molto Basso	Sono state correttamente definite ed implementate le misure di sicurezza previste dal Regolamento UE 2016/679 (art. 32 GDPR) ed il rischio residuo è stato definito accettabile dal Titolare.

	8 – 23	Basso	Sono state correttamente definite ed implementate tutte le misure minime di sicurezza previste dal Codice Privacy (art. 33 del D.Lg. 196/03) ma non tutte le misure di sicurezza previste dall'art. 32 Regolamento UE 2016/679. Il rischio residuo è stato comunque definito accettabile dal Titolare.
	24 – 35	Medio	Sono state correttamente definite e implementate tutte le misure idonee di sicurezza previste dall'art. 32 del Regolamento UE 2016/679 ma il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza adottate non configurano il livello minimo di protezione richiesto in relazione ai rischi ai sensi dell'31 del D.Lg 196/03.
	36 – 47	Alto	Sono state definite le misure idonee di sicurezza previste dall'art. 32 del Regolamento UE 2016/679 ma parte di esse sono ancora in fase di implementazione o non sono state correttamente implementate.
	48 – 64	Molto Alto	Non sono state definite e implementate tutte le misure idonee di sicurezza previste dall'art. 32 del Regolamento UE 2016/679 ed il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza adottate non configurano il livello minimo di protezione richiesto in relazione ai rischi ai sensi dell'art. 32 del Regolamento UE 2016/679 .

VALUTAZIONE DEL RISCHIO EFFETTIVO

ANALISI DEL RISCHIO RELATIVO A CALAMITÀ NATURALI

EVENTI CONSEGUENTI A CALAMITÀ NATURALI					
EVENTO	IMPATTO SULLA SICUREZZA				
	Probabilità	Gravità	Rilevanza	Conseguenze	Rischio
Perdita di dati conseguente ad allagamento	2	2	1	AB	4
Perdita di dati conseguente ad incendio	2	2	1	AB	4
Perdita di dati conseguente ad evento sismico	1	1	1	A	1

ANALISI DEL RISCHIO RELATIVO AD EVENTI CONSEGUENTI A MINACCE INTENZIONALI

EVENTI CONSEGUENTI A MINACCE INTENZIONALI					
EVENTO	IMPATTO SULLA SICUREZZA				
	Probabilità	Gravità	Rilevanza	Conseguenze	Rischio
Accessi non consentiti e Furti	1	3	4	BCD	12
Accessi non autorizzati e Trattamenti non consentiti	1	3	4	BCD	12
Furto e/o manomissione dati su supporti cartacei	1	3	4	A	12
Furto e/o manomissione dati su supporti informatici	1	3	4	BCD	12
Furto di Strumenti Elettronici	1	3	4	BCD	12
Sottrazione credenziali	1	3	4	BCD	12
Carenza di consapevolezza – incuria	1	3	3	BCD	9
Comportamenti sleali o fraudolenti	1	4	4	BCD	16

Cessione involontaria di credenziali	1	3	3	BCD	9
Incuria nella custodia dei supporti/dispositivi	1	3	3	BCD	9

ANALISI DEL RISCHIO RELATIVO A EVENTI CONSEGUENTI A MINACCE INVOLONTARIE

EVENTI CONSEGUENTI A MINACCE INVOLONTARIE					
EVENTO	**IMPATTO SULLA SICUREZZA**				
	Probabilità	**Gravità**	**Rilevanza**	**Conseguenze**	**Rischio**
Blackout elettrico	1	1	2	A	2
Anomalie e Guasti dell'Alimentazione e/o Sistema Elettronico	2	3	2	B	12
Malfunzionamenti Software	2	3	3	B	18
Malfunzionamenti Hardware	2	3	3	B	18
Errore materiale	2	4	2	BC	16
Errori umani nella gestione della sicurezza fisica	1	4	4	CD	16

ANALISI DEL RISCHIO RELATIVO A EVENTI CONSEGUENTI AD ATTACCHI AL SISTEMA INFORMATICO

A EVENTI CONSEGUENTI AD ATTACCHI AL SITEMA INFORMATICO					
EVENTO	**IMPATTO SULLA SICUREZZA**				
	Probabilità	**Gravità**	**Rilevanza**	**Conseguenze**	**Rischio**
Perdita di Dati dovuta a virus o ad intrusione informatica	1	4	2	BCD	8
Spamming e tecniche di sabotaggio	1	4	2	B	8
Malfunzionamento o indisponibilità degrado degli strumenti	2	2	2	B	8
Accessi esterni non autorizzati	1	4	4	BCD	16
Intercettazione informazioni su rete	1	4	4	BCD	16

EXECUTIVE SUMMARY - TABELLE DI SINTESI

A conclusione delle attività fin qui descritte ed analizzate occorre definire ed individuare la strategia di gestione del rischio per i diritti e le libertà degli interessati. Pertanto, valutato i livelli di rischio sopra riportati occorre definire la strategia adeguata per il contenimento degli stessi entro il valore desiderato. A tale proposito il Titolare, per ogni tipologia di evento, ritiene che il livello di rischio massimo debba essere contenuto entro il livello definito **"Basso"** che rappresenta una adeguata tutela per i diritti e le libertà degli interessati. I risultati sopra riportati già soddisfano ampiamente tali aspettative, tuttavia a seguito di alcuni interventi minimi programmati in corrispondenza di particolari tipologie di eventi, si riducono ancor di più i corrispondenti livelli di rischio al punto di rendere quasi nulli i livelli di rischi residui

Le tabelle sottostanti mostrano appunto i livelli di rischio residuo raggiunti.

TERMINE	DESCRIZIONE
EVENTO	Fatto o avvenimento preso in considerazione nell'analisi dei rischi
MISURE IN ESSERE	Misure di sicurezza attualmente adottate dal Titolare

RISCHIO	Livello di rischio aziendale = Probabilità x Gravità Aziendale x Rilevanza Economica		
	1 - 7	Molto Basso	Sono state correttamente definite ed implementate le misure di sicurezza previste dal Regolamento UE 2016/679 (art. 32 GDPR) ed il rischio residuo è stato definito accettabile dal Titolare.
	8 – 23	Basso	Sono state correttamente definite ed implementate tutte le misure di sicurezza previste Regolamento UE 2016/679 (art. 32 GDPR) ma non tutte le misure di sicurezza previste dall'art. 32 del Regolamento UE 2016/679 . Il rischio residuo è stato comunque definito accettabile dal Titolare.
	24 – 35	Medio	Sono state correttamente definite e implementate tutte le misure di sicurezza previste dal Regolamento UE 2016/679 (art. 32 GDPR) , ma il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza adottate non configurano il livello minimo di protezione richiesto in relazione ai rischi ai sensi dell'art. 32 del Regolamento UE 2016/679 .
	36 – 47	Alto	Sono state definite le misure minime di sicurezza previste dal Regolamento UE 2016/679 (art. 32 GDPR) ma parte di esse sono ancora in fase di implementazione o non sono state correttamente implementate.
	48 – 64	Molto Alto	Non sono state definite e implementate tutte le misure di sicurezza previste dal Regolamento UE 2016/679 (art. 32 GDPR) ed il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza adottate non configurano il livello minimo di protezione richiesto in relazione ai rischi ai sensi dell'art. 32 del Regolamento UE 2016/679 .
MISURE DA ADOTTARE	Misure di sicurezza che il Titolare intende adottare per ridurre il rischio		
RISCHIO RESIDUO	Rischio Residuo dopo l'adozione delle nuove misure di sicurezza		
	1	Basso	
	2	Medio	
	3	Alto	
	4	Molto Alto	

MISURE DI SICUREZZA RELATIVE A CALAMITA' NATURALI

EVENTI RELATIVI A CALAMITA' NATURALI				
EVENTO	**MISURE DI SICUREZZA**			
	Misure in essere	**Rischio**	**Misure Programmate**	**Rischio Residuo**
Perdita di dati conseguente ad allagamento	Dispositivi antincendio Rilevatori di fumi Paratie di protezione accessi d'acqua Locali costruiti in cemento armato	**4**	Nell'ambito delle definizione delle procedure generali, sono previste procedure ad *hoc* per la gestione degli eventi	**N.A.**

Perdita di dati conseguente ad incendio		4		
Perdita di dati conseguente ad evento sismico		1		

MISURE DI SICUREZZA RELATIVE AD EVENTI CONSEGUENTI A MINACCE INTENZIONALI

EVENTI CONSEGUENTI A MINACCE INTENZIONALI				
EVENTO	**MISURE DI SICUREZZA**			
	Misure in essere	**Rischio**	**Misure Programmate**	**Rischio Residuo**
Accessi non consentiti e Furti	Controllo elettrocico degli accessi con tracciabilità alle aree di ubicazione dei server e dei moduli di archiviazione di massa Limitazione nel numero di persone autorizzate all'accesso alle impostazioni di sistema e ai moduli di archiviazione dei dait Registrazione e tracciabilità delle login d'accesso	12	Aggiornamento professionale	N.A.
Accessi non autorizzati e Trattamenti non consentiti		12		
Furto e/o manomissione dati su supporti cartacei		12		
Furto e/o manomissione dati su supporti informatici		12		

Furto di Strumenti Elettronici		12		
Sottrazione credenziali		12		
Carenza di consapevolezza – incuria		9		
Comportamenti sleali o fraudolenti		16		
Cessione involontaria di credenziali		9		
Incuria nella custodia dei supporti/dispositivi		9		

MISURE DI SICUREZZA RELATIVE A EVENTI CONSEGUENTI A MINACCE INVOLONTARIE

EVENTI CONSEGUENTI A MINACCE INVOLONTARIE				
EVENTO	MISURE DI SICUREZZA			
	Misure in essere	Rischio	Misure Programmate	Rischio Residuo
Blackout elettrico	Sistema UPS interfacciato con generatore di corrente alimentato a disel Rete elettrica dedicata CKup di sistema continui Aggiornamento continuo del software Aggiornamento professionale del personale addetto	2	Aggiornamento professionale del personale addetto	N.A.
Anomalie e Guasti dell'Alimentazione e/o Sistema Elettronico		12		
Malfunzionamenti Software		18		
Malfunzionamenti Hardware		18		

Errore materiale		16		
Errori umani nella gestione della sicurezza fisica		16		

MISURE DI SICUREZZA RELATIVE AD EVENTI CONSEGUENTI AD ATTACCHI AL SISTEMA INFORMATICO

EVENTI CONSEGUENTI AD ATTACCHI AL SISTEM AINFORMATICO				
EVENTO	**MISURE DI SICUREZZA**			
	Misure in essere	**Rischio**	**Misure Programmate**	**Rischio Residuo**
Perdita di Dati dovuta a virus o ad intrusione informatica	*	8		N.A.
Spamming e tecniche di sabotaggio		8		
Malfunzionamento o indisponibilità degrado degli strumenti		8		
Accessi esterni non autorizzati		16		
Intercettazione informazioni su rete		16		

PERDITA DI DATI DOVUTA A VIRUS O AD INTRUSIONI INFORMATICHE

1. PREVENZIONE
   a. ANTIVIRUS NOD32/FIREWALL KERIO
2. IN CASO SI VERIFICHI L'EVENTO
   a. SERVER DI BACKUP
   b. UNITA' DI BACKUP OTTICA
   c. UNITA' NAS DI RETE

SPAMMING E TECNICHE DI SABOTAGGIO

1. SE RIFERITA ALLO SPAMMING (invio di posta indesiderata) o di SPAM BOMB (attacco indirizzato ad ottenere il "fuori servizio" di un server di posta) nessuno dei nostri server è utilizzato come server di posta – il servizio è affidato alla Verticaltech
2. SE RIFERITO AD AZIONI DI SABOTAGGIO COME ATTACCHI DDos (Denial of Service) su nessuno dei nostri server risiedono servizi esterni di norma attaccati con tale tecnica. L'unico collegamento con l'esterno avviene per il sistema PTS WORK tramite VPN gestita dal FIREWALL KERIO

MALFUNZIONAMENTO O INDISPONIBILITA' DEGRADO DEGLI STUMENTI

1. PREVENZIONE
   a. Manutenzione/verifica dei strumenti/supporti informatici
2. IN CASO SI VERIFICHI L'EVENTO
   a. La suddivisione dei servizi su tre unità separate (DOMINIO / GATAWEY E SICUREZZA/ BACKUP) permette di rimpiazzare velocemente l'ipotetica unità danneggiata garantendo ripercussioni minime su i servizi di rete

ACCESSI ESTERNI NON AUTORIZZATI

1. IL SISTEMA DI DOMINIO/FIREWALL PERMETTE DI LIMITARE L'ACECSSO ALLE RISORSE DI RETE AI SOLI UTENTI/PC REGISTRATI AL SUO INTERNO
2. TUTTO IL PERSOANLE HA UNA PROPRIA PASSWORD DI ACCESSO
3. LE POLICY DI SICUREZZA PREVEDONO IL CAMBIO PASSWORD PERIODICO
4. VENGONO ACCETTTATE LE SOLE COMUNICAZIONI IN INGRESSO TAMITE LA VPN KERIO

INTERCETTAZIONE INFORMAZIONI SU RETE

1. IL SISTEMA DI DOMINIO/FIREWALL PERMETTE DI LIMITARE L'ACECSSO ALLE RISORSE DI RETE AI SOLI UTENTI/PC REGISTRATI AL SUO INTERNO .

ALLEGATO “C”

ALLEGATO “C” – MODULISTICA

INFORMATIVA BREVE

Al fine di garantire una nuova informativa breve della registrazione video si suggerisce di predisporre un numero adeguato di tabelle secondo il presente fac-simile.

Testo da inserire:
La rilevazione è effettuata da (…) per fini di (…).
Videosorveglianza collegata con le centrali delle forze dell’ordine.
Per ulteriori informazioni: (sito web……).
L’accesso alle immagini è consentito esclusivamente al personale autorizzato.
Linee Guida EDPB 3/2019 e Reg. UE 2016/679 GDPR.