REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

AGENTZIA REGIONALE PRO S'AMPARU DE S'AMBIENTE DE SARDIGNA
AGENZIA REGIONALE PER LA PROTEZIONE DELL'AMBIENTE DELLA SARDEGNA
ARPAS

Direzione Generale

Determinazione n. 1435 del 09-08-2024

OGGETTO: REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO 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) □ APPROVAZIONE REGOLAMENTO PER LA VIDEOSORVEGLIANZA DELLE SEDI DELL'ARPAS

VISTA la Legge Regionale 6/2006 e ss.mm.ii. della Regione Autonoma della Sardegna (RAS), istitutiva dell'Agenzia regionale per la protezione dell'ambiente della Sardegna (ARPAS);

VISTA la Deliberazione della Giunta regionale n. 23/62 del 3 luglio 2024 relativa alla *Revoca delle funzioni di direzione generale dell'Agenzia regionale per la protezione dell'ambiente della Sardegna (ARPAS). L.R. n. 31/1998, articolo 28, comma 9, e L.R. n. 6/2006, art. 10, comma 8*;

VISTO il Decreto dell'Assessora della Difesa dell'ambiente n. 11 dell'8 luglio 2024 con il quale il Dott. Livio Sanna è stato nominato Direttore Generale sostituto dell'ARPAS fino alla nomina e all'insediamento del nuovo Direttore Generale;

VISTA la Legge Regionale 24/2014 della RAS, sull'organizzazione della Regione;

VISTO il *Regolamento generale e di organizzazione dell'ARPAS*, approvato con Determinazione del Direttore Generale n. 31/2015, modificato con Determinazione del Direttore Generale n. 922/2017;

VISTO il *Dettaglio organizzativo*, approvato con Determinazione del Direttore Generale n. 78/2015, modificato con Determinazione del Direttore Generale n. 5/2016, con Determinazione del Direttore Generale n. 992/2017, con Determinazione del Direttore Generale n. 9/2022 e con Determinazione del Direttore Generale n.

1770/2023;

VISTI il Regolamento (UE) 2016/679, regolamento generale sulla protezione dei dati, ed il Decreto legislativo 196/2003, come modificato dal Decreto legislativo 101/2018;

VISTA la Determinazione del Direttore Generale n. 721 dell'8 giugno 2018, relativa all'adozione del *Regolamento in materia di attuazione del Regolamento (UE) 2016/679*;

VISTA la Determinazione del Direttore Generale n. 846 del 20 giugno 2022, relativa alla revisione ed all'aggiornamento del *Regolamento in materia di attuazione del Regolamento (UE) 2016/679*;

VISTO l'articolo *2-quaterdecies*, Attribuzione di funzioni e compiti a soggetti designati, del Decreto legislativo n. 196/2003, Codice in materia di protezione dati personali, come modificato ed integrato dal Decreto legislativo n. 101/2018;

VISTA la Determinazione del Direttore Generale n. 854 del 20 giugno 2022, relativa al sistema delle deleghe delle funzioni del Titolare del trattamento e l'individuazione dei/delle Delegati/e del Titolare del trattamento come declinati nel documento *Sistema delle deleghe delle funzioni del Titolare del trattamento ed incarichi– Istruzioni*;

VISTA la Determinazione del Direttore Generale n. 2496 del 20 dicembre 2023 con la quale conferisce, per la posizione e per i compiti indicati rispettivamente nell'articolo 38 e nell'articolo 39 del Regolamento (UE) 2016/679, l'incarico di Responsabile della Protezione dei Dati (RPD) dell'ARPAS alla società Dasein Srl e nomina, come proposto dalla società Dasein Srl, il dott. Giovanni Maria Sanna Referente del Responsabile della Protezione dei Dati nei rapporti con il Titolare del trattamento dei dati;

VALUTATO che sia un servizio di guardiania/vigilanza diurno e notturno in presenza, sia altre misure di sicurezza, risultano attualmente soluzioni ragionevolmente troppo onerose e non attivabili e/o insufficienti per tutelare persone, beni mobili e beni immobili nelle sedi e nei siti in possesso/uso dell'ARPAS;

CONSIDERATO che i sistemi di videosorveglianza sono intesi come strumento di prevenzione e di razionalizzazione/potenziamento dell'azione e degli interventi di chi è preposto, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (articolo 6, comma 1, lettera e) Regolamento (UE) 2016/679), a tutelare anche esigenze di sicurezza;

ATTESO che l'ARPAS nelle proprie sedi/siti ha pertanto attivato sistemi di videosorveglianza; le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto cui si riferiscono, costituiscono dati personali e la videosorveglianza dà luogo, pertanto, a trattamento di dati personali;

TENUTO CONTO che nel Registro delle attività di trattamento dell'ARPAS (Titolare del trattamento) - costituito dall'applicativo informatico realizzato e amministrato dall'Ufficio speciale del Responsabile della protezione dei dati per il sistema Regione della Regione Autonoma della Sardegna - è stato individuato e decritto il trattamento denominato Videosorveglianza;

ATTESO che anche per il trattamento Videosorveglianza è stata condotta l'analisi del rischio intrinseco, esplicitata nel documento *Valutazione del rischio e misure di sicurezza per i dati personali* – 14/03/2024 aggiornamento 26/07/2024, allegato alla presente per farne parte integrante e sostanziale;

RITENUTO opportuno disciplinare con un Regolamento i sistemi di videosorveglianza dell'ARPAS e le correlate operazioni di trattamento delle immagini registrate, dalla fase di progettazione e installazione alla fase di gestione e manutenzione dei sistemi;

VISTO il documento *Proposta Regolamento per la videosorveglianza delle sedi dell'ARPAS – Luglio 2024* redatto congiuntamente dal Servizio Supporti direzionali e dal Servizio Tecnico dell'ARPAS;

ATTESO che il Responsabile della Protezione dei Dati (RPD) dell'ARPAS ha fornito consulenza e parere espresso sul suddetto documento (Comunicazione protocollo ARPAS 28337/2024 del 31 luglio 2024).

DETERMINA

Per le motivazioni espresse in premessa, che qui si intendono integralmente trascritte,

1. di approvare il documento *Regolamento per la videosorveglianza delle sedi dell'ARPAS – Luglio 2024*, allegato alla presente per farne parte integrante e sostanziale;

2. di trasmettere la presente Determinazione al Responsabile della Protezione dei Dati (RPD) dell'ARPAS;

3. di pubblicare la presente Determinazione nell'Albo pretorio on-line e nella sezione Amministrazione trasparente – Altri contenuti – Trattamento dati personali del sito *web* istituzionale dell'ARPAS.

Il Direttore Generale
LIVIO SANNA

** Documento informatico sottoscritto con firma digitale ai sensi del Decreto legislativo 82/2005.*

REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

AGENTZIA REGIONALE PRO S'AMPARU DE S'AMBIENTE DE SARDIGNA
AGENZIA REGIONALE PER LA PROTEZIONE DELL'AMBIENTE DELLA SARDEGNA
ARPAS

Direzione Generale

CERTIFICATO DI PUBBLICAZIONE

Direzione Generale

Determinazione n. 1435 del 09-08-2024

Si certifica che la determinazione 1435/2024 trovasi in corso di pubblicazione nell'Albo pretorio on line dell'ARPAS per 15 giorni dal 09-08-2024 al 24-08-2024.

L'originale informatico dell'Atto è stato predisposto e conservato presso l'ARPAS in conformità alle regole tecniche di cui all'articolo 71 del Decreto legislativo 82/2005. Nella copia analogica la sottoscrizione con firma autografa è sostituita dall'indicazione a stampa del nominativo del soggetto responsabile secondo le disposizioni di cui all'articolo 3 del Decreto legislativo 39/1993.

Il Responsabile *
LIVIO SANNA

** Documento informatico sottoscritto con firma digitale ai sensi del Decreto legislativo 82/2005.*

REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

AGENTZIA REGIONALE PRO S'AMPARU DE S'AMBIENTE DE SARDIGNA
AGENZIA REGIONALE PER LA PROTEZIONE DELL'AMBIENTE DELLA SARDEGNA

ARPAS

Direzione Generale
Servizio Supporti direzionali
Servizio Tecnico

Regolamento per la videosorveglianza delle sedi dell'ARPAS

Versione 00 del 31/07/2024

Luglio 2024

Sommario

Prima emissione.

Parere del Responsabile della Protezione dei Dati (RPD) dell'ARPAS (Protocollo ARPAS 28337/2024).

Articolo 1 – Ambito di applicazione

1. Il presente Regolamento - in conformità alle finalità e agli obiettivi istituzionali perseguiti dall'ARPAS (Allegato n. 1 – *Definizioni*) ed alle disposizioni normative per la protezione dei dati personali (Allegato n. 2 – *Normativa di riferimento e regolamenti*), in particolare alle disposizioni impartite dall'Autorità garante - disciplina i sistemi di videosorveglianza dell'ARPAS e le correlate operazioni di trattamento delle immagini registrate, dalla fase di progettazione e installazione alla fase di gestione e manutenzione dei sistemi.

2. L'ARPAS attiva i sistemi di videosorveglianza in quanto sia un servizio di guardiania/vigilanza diurno e notturno in presenza, sia altre misure di sicurezza, risultano attualmente soluzioni ragionevolmente troppo onerose e non attivabili e/o insufficienti.

3. Le immagini riguardanti persone, qualora rendano possibile l'identificazione del soggetto cui si riferiscono, costituiscono dati personali. La videosorveglianza dà luogo, pertanto, a trattamento di dati personali e incide sul diritto alla riservatezza delle persone fisiche eventualmente presenti nell'area sottoposta a ripresa.

4. Il presente Regolamento garantisce che il trattamento dei dati personali, effettuato mediante sistemi di videosorveglianza di varia tipologia attivati dall'ARPAS si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

5. L'installazione di telecamere all'interno degli edifici delle sedi dell'ARPAS richiede un propedeutico accordo collettivo stipulato dalla rappresentanza sindacale unitaria (comma 1, articolo 4 Legge 300/1970).

Articolo 2 - Caratteristiche dei sistemi di videosorveglianza dell'ARPAS

1. I sistemi di videosorveglianza dell'ARPAS, costituiti da dispositivi analogici e digitali nonché da software dedicati, sono installati nelle sedi dell'ARPAS indicate nell'Allegato n. 3 - *Sedi/siti dell'ARPAS dotati di sistema di videosorveglianza e consistenza degli impianti*.

2. I sistemi di videosorveglianza sono configurati con una serie di telecamere poste a protezione del perimetro degli edifici, in prossimità degli accessi carrai e pedonali delle sedi, delle sale server (CED) e nelle zone di passaggio e a protezione delle aree esterne dove sono collocati altri impianti tecnologici (esempio gruppi elettrogeni, chiller).

3. Le telecamere installate sono in alta definizione e visione notturna, e le apparecchiature di registrazione sono dotate di archivio digitale sufficiente a garantire anche più giorni di registrazione continua ed in piena qualità secondo le normative di legge in vigore. Le apparecchiature di registrazione sono generalmente installate nei locali presidiati dal personale autorizzato del servizio di portierato diurno.

4. Sono installate tre postazioni di controllo remoto: due installate nella sede della Direzione generale, per il controllo di tutti i sistemi di videosorveglianza delle varie sedi; una installata nella sede del Dipartimento Meteoclimatico, per il controllo del sistema installato nel Dipartimento e del sistema installato nella Stazione RADAR. L'utilizzo dei personal computer dedicati è possibile solo mediante credenziali di accesso rilasciate al personale dell'ARPAS specificatamente autorizzato. L'accesso al software dedicato di ciascun sistema è possibile solo mediante credenziali rilasciate al personale dell'ARPAS specificatamente autorizzato.

5. Il sistema di videosorveglianza della sala server (CED) della sede della Direzione Generale opera autonomamente rispetto al sistema di videosorveglianza perimetrale.

6. Nella maggior parte delle sedi sono presenti postazioni dotate di videoterminale presidiato dal personale autorizzato del servizio di portierato diurno, oppure dal personale dell'ARPAS autorizzato, che hanno solamente la visione diretta (in sincronia con la ripresa) delle immagini rilevate dai sistemi di videosorveglianza. I monitor degli impianti di videosorveglianza sono collocati in modo tale da non permettere la visione diretta delle immagini, neanche occasionalmente, a persone estranee e non autorizzate.

7. L'hardware di tutti i sistemi di sorveglianza è collegato alla rete LAN presente in ogni sede dell'ARPAS.

8. Gli accessi alle sale server (CED) avvengono attraverso un lettore di badge e credenziali, rilasciati a personale dell'ARPAS specificatamente autorizzato.

9. I sistemi di videosorveglianza coesistono con i sistemi di controllo degli accessi/antintrusione e rivelazione incendi delle varie sedi dell'ARPAS, che operano in autonomia e in piattaforme software dedicate.

10. Nella maggior parte delle sedi dell'ARPAS è attivo un servizio di portierato diurno dalle ore 7:00 alle ore 19:00, dal lunedì al venerdì.

11. Nella sede del Dipartimento Meteoclimatico, struttura con lavoro a turno, il servizio di portierato è attivo il sabato, la domenica e nei giorni festivi dalle 14:00 alle 18.00. In caso condizioni meteorologiche avverse il servizio di portierato può essere attivato su richiesta tutti i giorni, ore notturne comprese.

12. In ogni sede dell'ARPAS è attivo un servizio di vigilanza, con ronda notturna ad intervalli casuali - dalle 19:00 alle 7:00 dal lunedì al venerdì; nel fine settimana, quando le sedi sono chiuse, dalle 19:00 del venerdì alle 7:00 del lunedì; h24 nei giorni festivi - delle aree esterne/perimetrali delle sedi e/o degli ambienti interni limitatamente ai casi di innescato allarme intrusione.

Articolo 3 – Trattamento dei dati personali

1. I dati personali – costituiti esclusivamente da immagini registrate con videocamera - sono raccolti e trattati limitatamente alla seguente **finalità**:

a) tutelare l'integrità dei beni mobili e dei beni immobili in possesso/uso dell'ARPAS, prevenendo atti di vandalismo, danneggiamenti e furti;

b) sviluppare un'azione deterrente verso atti illeciti o verso atti o comportamenti in grado di compromettere la sicurezza, la salute e la incolumità dell'utenza, del personale dipendente e del personale dei fornitori presenti/che transitano nelle aree delle sedi dell'ARPAS;

c) ricostruire in tempo reale la dinamica, e acquisire prove utili per la contestazione, di fatti illeciti;

d) rilevare situazioni di pericolo per la sicurezza pubblica, consentendo l'intervento del personale autorizzato e delle Autorità competenti.

2. I sistemi di videosorveglianza dell'ARPAS sono intesi come strumento di prevenzione e di razionalizzazione/potenziamento dell'azione e degli interventi di chi è preposto, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (articolo 6, comma 1, lettera e) Regolamento (UE) 2016/679), a tutelare anche esigenze di sicurezza.

3. I dati sono raccolti e trattati secondo i principi di minimizzazione, di esattezza, di limitazione della conservazione, di integrità, di riservatezza e di responsabilizzazione indicati nel Regolamento (UE) 2016/679.

5. Gli impianti videosorveglianza devono raccogliere solo i dati strettamente necessari per il raggiungimento della finalità di cui al comma 1, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese all'area effettivamente da proteggere, evitando (quando non indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti.

6. Il trattamento delle immagini nell'ambito definito dal presente Regolamento non necessita del consenso degli interessati in quanto viene effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e comunque nello svolgimento delle funzioni istituzionali dell'ARPAS.

Articolo 4 – Analisi del rischio e Valutazione d'impatto

1. Qualora il trattamento delle immagini registrate con videocamera presenti un rischio intrinseco elevato per i diritti e le libertà delle persone fisiche, ai sensi dell'articolo 35, paragrafo 1, del Regolamento (UE) 2016/679, l'ARPAS condurrà la valutazione d'impatto sulla protezione dei dati.

2. L'ARPAS, considerate le funzioni istituzionali, non esegue una videosorveglianza sistematica su larga scala (articolo 35, paragrafo 3, del Regolamento (UE) 2016/679).

Articolo 5 – Conservazione, modifica, estrazione, comunicazione, cancellazione delle immagini

1. Le immagini, considerata la chiusura della maggior parte delle sedi dell'ARPAS nei giorni di sabato, di domenica e nei giorni festivi, devono essere conservate per un periodo non superiore ai 5 giorni successivi alla raccolta.

2. Eccezionalmente sono fatte salve speciali esigenze di ulteriore conservazione (e operazioni di adattamento o di modifica, di estrazione e di comunicazione) in relazione sia a specifica richiesta investigativa dell'Autorità giudiziaria o di Polizia giudiziaria, in presenza di provvedimenti da questi emanati, sia per il perseguimento del legittimo interesse di terzi.

3. I supporti su cui sono conservate le immagini per le speciali esigenze di cui al comma 2 sono custoditi in idoneo locale chiuso a chiave. Le chiavi sono in possesso del Titolare del trattamento dei dati, o del Delegato/a di cui all'articolo 6 e/o dell'autorizzato/a al trattamento e/o Responsabile del procedimento di accesso. Nei documenti di risposta/rilascio alle richieste di accesso, registrati nel Protocollo informatico e nel Registro degli accessi in dotazione dell'ARPAS, saranno indicate la data e l'ora della registrazione e la data e l'ora di cancellazione dell'immagine, applicando le misure di sicurezza indicate nell'articolo 9 del presente Regolamento.

4. La cancellazione delle immagini registrate, ad esclusione di quelle di cui al comma 2, dovrà avvenire automaticamente, in modo definitivo, con modalità tali da rendere non utilizzabili i dati cancellati, al termine del periodo di 5 giorni di cui al comma 1.

Articolo 6 – Titolare del trattamento dei dati e Delegati/e

1. Il Titolare del trattamento dei dati, o il Delegato/a del Titolare del trattamento dei dati, con il supporto del/della Dirigente responsabile della Struttura organizzativa di riferimento per il trattamento - come individuati nel *Regolamento in materia di attuazione del Regolamento (UE) 2016/679* e nel documento *Sistema delle deleghe delle funzioni del Titolare del trattamento ed incarichi - Istruzioni* (Allegato n. 2 – *Normativa di riferimento e regolamenti*)- è responsabile della gestione dei sistemi di videosorveglianza dell'ARPAS e del trattamento delle relative immagini raccolte e registrate.

2. Il Titolare, o il Delegato/a, vigila sull'utilizzo dei sistemi di videosorveglianza e sul trattamento delle immagini in conformità alla finalità e i principi di cui all'articolo 3, alle disposizioni normative che disciplinano la materia e, in particolare, alle eventuali disposizioni dell'Autorità Garante per la protezione dei dati personali.

3. Il Titolare, o il Delegato/a, rilascia al personale dell'ARPAS specificatamente autorizzato le credenziali per l'utilizzo delle postazioni di controllo remoto dei sistemi e del software di ciascun sistema di videosorveglianza.

Articolo 7 – Responsabile del trattamento dei dati

1. Il Responsabile del trattamento dei dati, soggetto esterno all'ARPAS, nominato con contratto o da altro atto giuridico in forma scritta dal Titolare del trattamento dei dati (articolo 28, paragrafo 3, del Regolamento (UE) 2016/679), tratta le immagini per conto del Titolare e opera limitatamente alla finalità di cui all'articolo 3.

2. È consentita al Responsabile del trattamento solamente l'operazione di visione diretta (consultazione) delle immagini videoregistrate nell'ambito del servizio di portierato, del servizio di manutenzione dei sistemi di videosorveglianza, e comunque nell'ambito di prestazioni strumentali e subordinate alle scelte del Titolare del trattamento dei dati.

3. Il Responsabile del trattamento, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni normative e regolamentari da parte dei/delle propri/proprie autorizzati/e.

Articolo 8 – Autorizzati/e al trattamento

1. Il Titolare del trattamento, o il Delegato/a del Titolare del trattamento, come individuato nel documento *Sistema delle deleghe delle funzioni del Titolare del trattamento ed incarichi - Istruzioni*, e/o il Responsabile del trattamento di cui all'articolo 7, designa per iscritto tra i propri dipendenti gli/le autorizzati/e, in numero sufficiente a garantire la gestione dei sistemi di videosorveglianza, le operazioni di trattamento delle immagini e la finalità del trattamento di cui all'articolo 3.

2. Con la designazione, agli/alle autorizzati/e saranno affidate specifiche operazioni di trattamento delle immagini e dovranno utilizzare i sistemi di videosorveglianza nel rispetto delle istruzioni indicate nel documento di cui al comma 1 e nel *Regolamento informatico dell'ARPAS* vigente. In ogni caso, prima dell'utilizzo dei sistemi di videosorveglianza, con apposite istruzioni organizzative e operative saranno istruiti/e al corretto utilizzo dei sistemi di videosorveglianza, sulla normativa di riferimento e sul presente Regolamento e dovranno conformare la propria condotta al pieno rispetto del medesimo.

3. Gli/le autorizzati/e devono procedere a cambiare le credenziali (password) di accesso per l'utilizzo delle postazioni di controllo remoto dei sistemi ogni 45 giorni e per l'utilizzo del software di ciascun sistema di videosorveglianza ogni 6 mesi.

Articolo 9 – Misure di sicurezza tecniche ed organizzative

1. Il Titolare del trattamento implementa le misure di sicurezza individuate sia durante il processo di analisi del rischio intrinseco sia durante la valutazione d'impatto di cui all'articolo 4.

2. Il Titolare del trattamento implementa comunque le seguenti misure di sicurezza:

a) Controllo degli accessi e autenticazione. L'uso di credenziali di accesso - ai personal computer e ai software dedicati di ciascun sistema di videosorveglianza - condivise tra più autorizzati/e non è consentita. Come misura minima deve essere utilizzata una combinazione di nome utente e password e la password deve rispettare un certo livello (configurabile) di complessità.

b) Cancellazione. La cancellazione delle immagini registrate dovrà avvenire automaticamente. Quando sia necessario memorizzare le immagini in altri supporti/archivi portatili, terminata la speciale esigenza di cui al comma 2, articolo 5, deve essere eseguita la sovrascrittura delle immagini e, nei casi in cui ciò non è possibile, eseguire la distruzione fisica del supporto/archivio.

c) Installazione telecamere. Le telecamere devono essere installate in modo tale da limitare l'angolo visuale delle riprese, evitando quando non indispensabili, immagini dettagliate o ingrandite.

d) Manutenzione sistemi di videosorveglianza. Durante gli interventi di manutenzione gli/le autorizzati/e dal Responsabile del trattamento potranno accedere alle immagini oggetto di ripresa solo se ciò si renda indispensabile al fine di effettuare le necessarie verifiche tecniche. Dette verifiche avverranno sempre in presenza del personale dipendente autorizzato dal Titolare del trattamento, o dal/dalla Delegato/a del Titolare del trattamento, dotato di credenziali di autenticazione ed autorizzato alle operazioni di trattamento delle immagini.

Articolo 10 – Trasparenza, informazione e diritti dell'interessato/a

1. Ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679, l'ARPAS fornisce agli/alle interessati/e che stanno per accedere a un'area videosorvegliata le informazioni più importanti di primo livello (titolare, responsabile protezione dati, conservazione, finalità, diritti dell'interessato/a, dove trovare l'informativa estesa - codice QR o indirizzo web) tramite cartelli (informativa breve) affissi in tutte le sedi

e i luoghi nei quali sono installate le telecamere, tenuto conto del loro numero, delle modalità di ripresa e della vastità dell'area sorvegliata.

2. I cartelli - che devono anticipare l'area videosorvegliata, anche nelle sue immediate vicinanze e non necessariamente a contatto con le telecamere, posizionati approssimativamente all'altezza degli occhi, chiaramente visibili anche in ore notturne - devono essere in linea con il modello adottato dal Comitato europeo per la protezione dei dati (EDPB).

3. Le informazioni ulteriori di dettaglio obbligatorie, di secondo livello, sono fornite, senza alcun onere, con l'informativa estesa, messa a disposizione, prima di entrare nell'area videosorvegliata, tramite codice QR e/o indirizzo web indicato nell'informativa breve. L'informativa estesa è comunque resa disponibile, affissa in un luogo di facile accesso, all'interno di ogni sede dell'ARPAS.

4. L'ARPAS agevola l'esercizio dei seguenti diritti dell'interessato/a:

a) conferma di un trattamento di immagini in corso, accesso alle immagini e informazioni (articolo 15 del Regolamento (UE) 2016/679);

b) cancellazione (articolo 17 del Regolamento (UE) 2016/679);

c) limitazione di trattamento (articolo 18 del Regolamento (UE) 2016/679);

d) obbligo di notifica in caso di cancellazione o limitazione (articolo 19 del Regolamento (UE) 2016/679);

e) opposizione (articolo 21 del Regolamento (UE) 2016/679);

f) comunicazione di una violazione dei dati personali (articolo 34 del Regolamento (UE) 2016/679);

g) proporre reclamo all'Autorità Garante per la Protezione dei dati personali (articolo 77 del Regolamento (UE) 2016/679;

h) proporre ricorso giurisdizionale (articolo 79 del Regolamento (UE) 2016/679),

come ulteriormente esplicitati nell'informativa estesa di cui al punto 3 del presente articolo.

5. L'interessato/a può esercitare il diritto di accesso e gli altri diritti presentando apposita richiesta all'ARPAS, Titolare del trattamento, e al Responsabile della Protezione dei Dati, da inviare mezzo Posta Elettronica Certificata ovvero mezzo Raccomandata con Avviso di Ricevimento, nonché mezzo Posta Elettronica Ordinaria agli indirizzi indicati nelle informative di cui al punto 1 e al punto 3 del presente articolo e nella sezione Trattamento dati personali del sito web istituzionale dell'ARPAS.

6. Per esercitare i diritti di cui al presente articolo l'interessato/a può utilizzare lo specifico modello pubblicato nella sezione Trattamento dati personali del sito web istituzionale dell'ARPAS.

7. Nel caso di accesso alle immagini, nella richiesta l'interessato/a dovrà indicare:

a) il luogo, la data e la fascia oraria della possibile ripresa;

b) l'abbigliamento indossato al momento della possibile ripresa;

c) gli eventuali accessori in uso al momento della possibile ripresa;

d) l'eventuale presenza di accompagnatori al momento della possibile ripresa;

e) l'eventuale attività svolta al momento della possibile ripresa;

f) eventuali ulteriori elementi utili all'identificazione dell'interessato/a.

8. L'accesso alle immagini videoregistrate e alle informazioni, limitatamente alla finalità di cui all'articolo 3 e al periodo di conservazione di cui all'articolo 5, è consentito:

a) all'interessato/a, soggetto a cui si riferiscono le immagini oggetto di trattamento, nell'ambito del diritto di accesso di cui all'articolo 15 del Regolamento (UE) 2016/679;

b) al Titolare del trattamento o al/dalla Delegato/a del Titolare del trattamento, e agli/alle autorizzati/e da questi designati/e per specifiche operazioni di trattamento e richieste di accesso;

c) al Responsabile del trattamento, e agli/alle autorizzati/e da questo designati/e, nell'ambito dei servizi e delle prestazioni di cui all'articolo 7, solamente per l'operazione di visione diretta (consultazione) delle immagini;

d) all'Autorità giudiziaria e alla Polizia giudiziaria sulla base di richiesta scritta e in presenza di provvedimenti da queste emanati/adottati;

e) ai soggetti legittimati all'accesso ai documenti amministrativi ai sensi e per gli effetti degli articoli 22 e successivi della Legge 241/90 e s.m.i. e, in particolare, nei casi in cui, in ossequio alle previsioni di cui all'articolo 24, comma 7, della Legge 241/90 e s.m.i., l'accesso alle immagini sia necessario per curare o per difendere gli interessi giuridici del richiedente. L'accesso sarà garantito mediante l'utilizzo di tecniche di oscuramento dei dati identificativi delle persone fisiche eventualmente presenti non strettamente indispensabili per la difesa degli interessi giuridici del soggetto richiedente.

9. L'autorizzato/a al trattamento e/o Responsabile del procedimento di accesso accerterà l'effettiva esistenza delle immagini. In caso positivo e di accoglimento della richiesta di accesso, all'interessato/a viene comunicato il nominativo del soggetto autorizzato/a e/o Responsabile del procedimento di accesso dell'ARPAS, il giorno, l'orario, la struttura dell'ARPAS presso cui, entro un periodo di tempo non inferiore a quindici (15) giorni - l'interessato/a o la persona delegata/con procura - può prendere visione (consultazione) ed eventualmente estrarre copia delle immagini che lo/la riguardano.

10. Qualora l'interessato/a chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei *files* contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in rispetto alla previsione di cui all'articolo 15, comma 4 del Regolamento (UE) 2016/679.

11. Le richieste di accesso alle immagini e informazioni ed i relativi documenti di risposta/rilascio saranno registrati nel Protocollo informatico e nel Registro degli accessi in dotazione dell'ARPAS. Il documento di risposta/rilascio, a cura del Titolare del trattamento dei dati, o del Delegato/a di cui all'articolo 6 e/o dell'autorizzato/a e/o Responsabile del procedimento di accesso, dovrà contenere le seguenti informazioni:

a) identificazione del soggetto autorizzato/a alle operazioni di trattamento e di accesso;

b) estremi e motivazione della richiesta di accesso;

c) data e ora registrazione delle immagini;

d) data ed ora di accesso alle immagini e delle operazioni di trattamento;

e) tipologia di accesso indicando visione (consultazione) e/o rilascio copia (con o senza operazioni di adattamento o di modifica) delle immagini.

12. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato/a o per ragioni familiari meritevoli di protezione, ferme restando le limitazioni individuate dall'articolo 2-*terdecies* Decreto legislativo 196/2003 e s.m.i..

13. Nell'esercizio dei diritti di cui al presente articolo l'interessato/a può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato/a può altresì farsi assistere da persona di fiducia.

14. Nel caso di esito negativo alle richieste di cui ai punti precedenti del presente articolo, l'interessato può rivolgersi all'Autorità Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Articolo 13 - Mezzi di ricorso, responsabilità e sanzioni

1. Per quanto attiene al diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali, nonché ad ogni altro diritto a un ricorso amministrativo o giurisdizionale, si rinvia integralmente all'articolo 77 e seguenti del Regolamento (UE) 2016/679 e all'articolo 140-*bis* e seguenti del Decreto legislativo 196/2003 e s.m.i..

2. Chiunque subisca un danno materiale o immateriale per effetto del trattamento di dati personali, ha il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento ai sensi dell'articolo 82 del Regolamento (UE) 2016/679.

3. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2, del Regolamento (UE) 2016/679.

4. Il Titolare del trattamento o Responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Articolo 17 – Pubblicità, disposizioni attuative, di rinvio, di modifica e di abrogazione

1. Il presente Regolamento entra in vigore dalla data di pubblicazione nell'Albo Pretorio online della Determinazione di approvazione da parte del/della Direttore/Direttrice generale. Con l'entrata in vigore si devono considerare abrogate le disposizioni regolamentari con esso contrastanti.

2. Il presente Regolamento è pubblicato nella sezione Trattamento dati personali della sezione Amministrazione trasparente del sito web istituzionale dell'ARPAS.

3. Con Determinazione del/della Direttore/Direttrice generale, il presente Regolamento sarà adeguato alle modifiche normative che dovessero intervenire e alle eventuali disposizioni emesse dall'Autorità garante per la protezione dei dati personali.

4. Per quanto non disciplinato dal presente Regolamento, si rinvia al Regolamento (UE) 2016/679 e ai provvedimenti dell'Autorità garante per la protezione dei dati personali.

ALLEGATI

Allegato n. 1 – Definizioni

1. Ai fini del presente Regolamento si intende:

a) per «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;

b) per «trattamento», qualsiasi operazione o insieme di attività, 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;

c) per "banca dati", il complesso organizzato di dati personali, formatosi attraverso le apparecchiature di registrazione e ripresa video che, in relazione ai luoghi di installazione delle telecamere, riguardano prevalentemente i soggetti e/o i mezzi di trasporto che transitano nelle aree interessate dalle riprese;

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

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

f) per «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, i mezzi e le modalità 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;

g) per «autorizzato del trattamento», la persona fisica che abbia accesso a dati personali e agisca sotto l'autorità del titolare o del funzionario designato al coordinamento delle attività e al controllo del trattamento;

h) per «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;

i) per «interessato», la persona fisica cui si riferiscono i dati personali oggetto di trattamento;

j) per «terzo», la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il funzionario designato al coordinamento delle attività e al controllo del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del funzionario designato al coordinamento delle attività e al controllo;

k) per «violazione dei dati personali», la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

l) per «autorità di controllo», l'autorità pubblica indipendente istituita da uno Stato membro (in Italia, il Garante per la protezione dei dati personali);

m) per «comunicazione», il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'Interessato, dal Rappresentante del Titolare nel territorio dell'Unione europea, dal Responsabile o dal suo Rappresentante nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

n) per «diffusione», il dare conoscenza generalizzata dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

o) per «dato anonimo», il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

p) per «blocco», la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;

q) per «sedi» beni immobili e altre infrastrutture strumentali dell'ARPAS dotati di impianto di video sorveglianza

r) per «ARPAS», l'Agenzia Regionale per la Protezione dell'Ambiente della Sardegna

s) per «EDPB», l'European Data Protection Board (Comitato europeo per la protezione dei dati)

Allegato n. 2 – Normativa di riferimento e regolamenti (Base giuridica)

- Regolamento (UE) n. 2016/679 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 («RGPD»)

- articolo 4, *Impianti audiovisivi e altri strumenti di controllo* - Legge 300/1970 - Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro enorme sul collocamento -

- articolo 23, *Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196* - Decreto legislativo 151/2015 - Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183

- Provvedimento Garante Protezione Dati Personali 8 aprile 2010 [1712680] - Provvedimento in materia di videosorveglianza (G.U. n. 99 del 29/04/2010)

- Linee guida European Data Protection Board 3/2019 (Comitato europeo per la protezione dei dati 3/2019) - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate il 29/01/2020

- Decreto legislativo 196/2003, così come modificato dal Decreto legislativo 101/2018

- Legge 241/1990 e s.m.i., Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi

- Regolamento informatico dell'ARPAS (approvato con Determinazione del Direttore Generale dell'ARPAS n. 1851/2023 del 13/10/2023)

- Regolamento in materia di attuazione del Regolamento (UE) 2016/679 (Determinazione del Direttore Generale dell'ARPAS n. 846/2022 del 20/06/2022)

- Sistema delle deleghe delle funzioni del Titolare del trattamento ed incarichi – Istruzioni (Determinazione del Direttore Generale dell'ARPAS n. 854/2022 del 21/06/2022)

Allegato n. 3 – Sedi/siti dell'ARPAS dotati di sistema di videosorveglianza e consistenza degli impianti

Cagliari - Via Contivecchi 7

Installate 5 telecamere esterne perimetrali e 3 telecamere nella sala CED.

Installate due postazioni per il controllo remoto di tutti i sistemi installati nelle varie sedi dell'ARPAS: una installata nella stanza del/della Direttore/Direttrice generale e una installata nella stanza degli/delle Autorizzati/e della sede di via Contivecchi 7 a Cagliari.

Presente videoterminale nel vano portineria all'ingresso della sede. Impianto non protetto da gruppo di continuità elettrica.

Cagliari - Via Carloforte 51

Installate 2 telecamere nell'ingresso alla sede. Videoterminale non presente. Impianto non protetto da gruppo di continuità elettrica.

Cagliari - Viale Ciusa 6

Installate 8 telecamere esterne perimetrali. Presente videoterminale nel vano portineria all'ingresso della sede. Impianto non protetto da gruppo di continuità elettrica.

Portoscuso - Via Napoli 7

Installate 6 telecamere esterne perimetrali. Presente videoterminale nel vano portineria all'ingresso della sede. Impianto non protetto da gruppo di continuità elettrica.

Oristano - Via Liguria 60

Installate 4 telecamere esterne perimetrali. Presente videoterminale spento nel vano portineria all'ingresso della sede. Impianto non protetto da gruppo di continuità elettrica.

Nuoro - Via Roma 85

Installate 2 telecamere esterne perimetrali ed una nell'ingresso alla sede. Presente videoterminale spento nel vano portineria all'ingresso della sede. Impianto non protetto da gruppo di continuità elettrica.

Sassari - Via Rockefeller 58-60

Installate 10 telecamere esterne perimetrali. Presente videoterminale nel vano portineria all'ingresso della sede. Impianto protetto da gruppo di continuità elettrica.

Sassari - Viale Porto Torres 119

Installate 4 telecamere esterne perimetrali ed una nell'ingresso alla sede.

Installata una postazione per il controllo remoto del sistema installato nel Dipartimento e del sistema installato nella Stazione RADAR del Monte Rasu. La postazione è installata nella stanza del/della Direttore/Direttrice del Dipartimento Meteoclimatico della sede di vilale Porto Torres 119 a Sassari.

Presente videoterminale spento nel vano portineria all'ingresso della sede. Impianto non protetto da gruppo di continuità elettrica.

Bono - Stazione RADAR installata nel Monte Rasu

Installate 4 telecamere esterne perimetrali. Presente videoterminale spento. Impianto protetto da gruppo di continuità elettrica.

VALUTAZIONE DEL RISCHIO E MISURE DI SICUREZZA PER I DATI PERSONALI

Valutazione del livello di rischio per l'operazione di trattamento **Videosorveglianza** e proposta di misure di sicurezza tecniche e organizzative appropriate.

Sezione I – Definizione e contesto dell'operazione di trattamento

DESCRIZIONE DELL'OPERAZIONE DI TRATTAMENTO	RISPOSTA	
Dati personali oggetto di trattamento	Immagini registrate con videocamera.	
Finalità del trattamento	Tutelare integrità beni mobili e beni immobili; azione deterrente atti illeciti, atti o comportamenti in grado di compromettere sicurezza, salute e incolumità utenza, personale dipendente e personale fornitori; dinamica e acquisire prove di fatti illeciti; sicurezza pubblica e intervento Autorità.	
Soggetti interessati	Utenti, dipendenti, fornitori.	
Strumenti impiegati nel trattamento	Sistema automatizzato con software e hardware dedicati.	
Destinatari dei dati	Interni	Nessuno
	Esterni	Autorità giudiziaria e Polizia giudiziaria
Responsabile del trattamento	Coopservice S.coop.p.a. (Cagliari, viale Ciusa e via Contivecchi) GRUPPO SERVIZI ASSOCIATI SPA S.U. (Sassari, via Rockefeller) COOPERATIVA DI VIGILANZA LA NUORESE (Sassari, viale Porto Torres) VEDETTA 2 MONDIALPOL S.P.A. (Portoscuso) Tepor S.p.A.	

Sezione II – Valutazione dell'impatto

Riservatezza impact assessment: **Basso**

Integrità impact assessment: **Basso**

Disponibilità impact assessment: **Basso**

VALUTAZIONE DELL'IMPATTO		
Riservatezza	**Integrità**	**Disponibilità**
Basso	Basso	Basso
	Valutazione globale di impatto	Basso

Sezione III – Analisi delle minacce per area di valutazione

Risorse di rete e tecniche threat probability: Basso

- **Qualche parte del trattamento dei dati personali viene eseguita tramite Internet? Sì**
- **È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)? Sì**
- **Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)? No**
- **Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati? No**
- **Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi? No**

Processi / Procedure relativi all'operazione di trattamento dei dati threat probability: Basso

- **I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti? No**
- **L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito? No**
- **I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali? No**
- **I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione? No**
- **Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file di registro (es: log)? Sì**

Parti / Persone coinvolte nel trattamento dei dati personali threat probability: Basso

- **Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti? No**
- **Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (responsabile del trattamento)? Sì**
- **Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti? No**
- **Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni? No**
- **Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali? No**

Settore di operatività e scala di trattamento threat probability: Basso

- **Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici? No**
- **La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni? No**
- **Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno? No**
- **Un'operazione di elaborazione riguarda un grande volume di individui e / o dati personali? No**

- **Esistono best practice di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente seguite?** **No**

AREA DI VALUTAZIONE	PROBABILITA	
Risorse di rete e tecniche	Basso	1
Processi / Procedure relativi all'operazione di trattamento dei dati	Basso	1
Parti / Persone coinvolte nel trattamento dei dati personali	Basso	1
Settore di operatività e scala di trattamento	Basso	1
Livello globale di probabilità di occorrenza della minaccia	Basso (4)	

Sezione IV – Valutazione del rischio

	LIVELLO DI IMPATTO			
PROBABILITÀ DI OCCORRENZA DELLA MINACCIA		Basso	Medio	Alto / Molto Alto
	Basso	X		
	Medio			
	Alto			

Sezione V – Misure di sicurezza organizzative

Va notato che l'abbinamento di misure a specifici livelli di rischio non dovrebbe essere percepito come assoluto. A seconda del contesto del trattamento dei dati personali, l'organizzazione può considerare l'adozione di misure aggiuntive, anche se sono assegnate a un livello di rischio più elevato. Inoltre, l'elenco proposto di misure non tiene conto di altri requisiti di sicurezza specifici settoriali aggiunti, nonché di obblighi normativi specifici, derivanti ad esempio dalla direttiva e-privacy o dalla direttiva NIS. Nel tentativo di facilitare ulteriormente questa procedura è inclusa anche una mappatura del gruppo di misure proposto con i controlli di sicurezza ISO/IEC 27001:2013.

Politica di sicurezza e procedure per la protezione dei dati personali

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
A.1	L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.	
A.2	La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.	
	Pertinente alla certificazione ISO 27001:2013 - A.5 Politica di sicurezza	

Ruoli e responsabilità

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
B.1	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.	
B.2	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e mezzi del trattamento.	
	Pertinente alla certificazione ISO 27001:2013 - A.6.1.1 Ruoli e responsabilità per la sicurezza delle informazioni	

Politica di controllo degli accessi

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
C.1	I diritti specifici di controllo degli accessi dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.	
	Pertinente alla certificazione ISO 27001:2013 - A.9.1.1 Politica di controllo degli accessi	

Gestione risorse/asset

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
D.1	L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete). Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).	
D.2	Il censimento delle risorse e degli apparati IT e il relativo registro dovrebbero essere rivisti e aggiornati regolarmente.	
	Pertinente alla certificazione ISO 27001:2013 - A.8 Gestione delle risorse	

Gestione delle modifiche apportate alle risorse, agli apparati ed ai sistemi IT

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
E.1	L'organizzazione deve assicurarsi che tutte le modifiche alle risorse, agli apparati ed al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, il Responsabile IT o sicurezza). Il monitoraggio regolare delle eventuali modifiche apportate al sistema IT dovrebbe avvenire a cadenza regolare e periodica.	
E.2	Lo sviluppo software dovrebbe essere eseguito in un ambiente speciale non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire un test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non sia possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test e nello sviluppo software.	
	Pertinente alla certificazione ISO 27001:2013 - A. 12.1 Procedure operative e responsabilità	

Responsabili del trattamento

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
F.1	Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcing) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione del Titolare del trattamento.	
F.2	Al rilevamento di una violazione dei dati personali (data breach), il responsabile del trattamento informa il titolare del trattamento senza indebiti ritardi.	
F.3	Requisiti formali e obblighi dovrebbero essere formalmente concordati tra il titolare del trattamento dei dati e il responsabile del trattamento dei dati. Il responsabile del trattamento dovrebbe fornire sufficienti prove documentate di conformità della sua organizzazione e dei trattamenti svolti alle prescrizioni in materia di sicurezza.	
	Pertinente alla certificazione ISO 27001:2013 - A.15 Rapporti con i fornitori	

Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
G.1	È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.	
G.2	Le violazioni dei dati personali (come definite dall'art. 4 del GDPR) devono essere segnalate immediatamente al Management competente secondo l'organizzazione interna.. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi degli art. 33 e 34 GDPR.	
	Pertinente alla certificazione ISO 27001:2013 - A.16 Gestione degli incidenti di sicurezza delle informazioni	

Business continuity

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
H.1	L'organizzazione dovrebbe definire le principali procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).	
	Pertinente alla certificazione ISO 27001:2013 - A. 17 Aspetti di sicurezza nella gestione della continuità operativa	

Obblighi di confidenzialità imposti al personale

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
I.1	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto. I ruoli e le responsabilità devono essere chiaramente definiti ed assegnati comunicati durante il processo di pre-assunzione e / o assunzione.	
	Pertinente alla certificazione ISO 27001:2013 - A.7 Sicurezza delle risorse umane	

Formazione

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
J.1	L'organizzazione dovrebbe garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento siano adeguatamente formati e informati sui controlli di sicurezza del sistema informatico relativi al loro lavoro quotidiano. I dipendenti coinvolti nel trattamento dei dati personali dovrebbero inoltre essere adeguatamente informati in merito ai requisiti e agli obblighi legali in materia di protezione dei dati attraverso regolari campagne di sensibilizzazione o iniziative di formazione specifica.	
	Pertinente alla certificazione ISO 27001:2013 - A.7.2.2 Consapevolezza, educazione e formazione sulla sicurezza delle informazioni	

Controllo degli accessi e autenticazione

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
K.1	Dovrebbe essere implementato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, la revisione e l'eliminazione degli account utente.	
K.2	L'uso di account utente comuni (con credenziali di accesso condivide tra più utenti) dovrebbe essere evitato. Nei casi in cui questo sia necessario, dovrebbe essere garantito che tutti gli utenti dell'account comune abbiano gli stessi ruoli e responsabilità.	
K.3	Dovrebbe essere attivo un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di nome utente / password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità.	
K.4	Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile).	
	Pertinente alla certificazione ISO 27001:2013 - A.9 Controllo degli accessi	

Generazione di file di log e monitoraggio

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
L.1	Dovrebbero essere generati file di log per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Essi dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).	
L.2	I file di log dovrebbero essere contrassegnati con data e ora e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento.	
	Pertinente alla certificazione ISO 27001:2013 - A.12.4 Generazione di file di log e monitoraggio	

Sicurezza di server e database

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
M.1	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente.	
M.2	I server ove risiedono database e applicazioni devono trattare solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR).	
	Pertinente alla certificazione ISO 27001:2013 - A. 12 Sicurezza delle operazioni	

Sicurezza delle Postazioni di lavoro

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
N.1	Gli utenti non dovrebbero essere in grado di disattivare o bypassare le impostazioni di sicurezza.	
N.2	Le applicazioni anti-virus e le firme di rilevamento devono essere configurate su base settimanale.	
N.3	Gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software non autorizzate.	

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
N.4	Il sistema dovrebbe attivare il timeout di sessione quando l'utente non è stato attivo per un certo periodo di tempo.	
N.5	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.	
	Pertinente alla certificazione ISO 27001:2013 - A. 14.1 Requisiti di sicurezza dei sistemi informativi	

Sicurezza della Rete e delle Infrastrutture di comunicazione Elettronica

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
O.1	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL)	
	Pertinente alla certificazione ISO 27001:2013 - A.13 Sicurezza delle comunicazioni	

Back-ups

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
P.1	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità.	
P.2	Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine.	
P.3	L'esecuzione dei backup deve essere monitorata per garantirne la completezza.	
P.4	I backup completi devono essere eseguiti regolarmente.	
	Pertinente alla certificazione ISO 27001:2013 - A.12.3 Back-Up	

Dispositivi mobili / portatili

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
Q.1	Le procedure di gestione dei dispositivi mobili e portatili dovrebbero essere definite e documentate stabilendo regole chiare per il loro corretto utilizzo.	
Q.2	I dispositivi mobili, ai quali è consentito accedere al sistema informativo, dovrebbero essere pre-registrati e pre-autorizzati.	
Q.3	I dispositivi mobili dovrebbero essere soggetti agli stessi livelli delle procedure di controllo degli accessi (al sistema di elaborazione dei dati) delle altre apparecchiature terminali.	
	Pertinente alla certificazione ISO 27001:2013 - A. 6.2 Dispositivi mobili e telelavoro	

Sicurezza del ciclo di vita delle applicazioni

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
R.1	Durante il ciclo di vita dello sviluppo, dovrebbero essere seguite le best practice, lo stato dell'arte e ben noti pratiche di sviluppo sicuro, framework o standard.	
R.2	Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo.	
R.3	Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET)) dovrebbero essere adottate in analogia con i requisiti di sicurezza.	
R.4	Dovrebbero essere seguiti standard e pratiche di codifica sicure.	
R.5	Durante le attività di sviluppo, dovrebbero essere eseguite attività di test e convalida dei requisiti di sicurezza inizialmente implementati.	
	Pertinente alla certificazione ISO 27001:2013 - A. 12.6 Gestione delle vulnerabilità tecniche e A. 14.2 Sicurezza nei processi di sviluppo e supporto	

Cancellazione / eliminazione dei dati

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
S.1	La sovrascrittura software dei dati dovrebbe essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), è necessario eseguire la distruzione fisica.	
S.2	È necessario eseguire la triturazione della carta e dei supporti portatili utilizzati per memorizzare i dati personali.	
	Pertinente alla certificazione ISO 27001:2013 - A. 8.3.2 Smaltimento dei supporti e A. 11.2.7 Smaltimento o riutilizzo sicuro dell'attrezzatura	

Sicurezza fisica

Identificatore della misura	Descrizione della misura di sicurezza	Livello di rischio
T.1	Il perimetro fisico dell'infrastruttura del sistema IT non dovrebbe essere accessibile da personale non autorizzato.	
	Pertinente alla certificazione ISO 27001:2013 - A.11 Sicurezza fisica e ambientale	