agentzia sarda pro su traballu
agenzia sarda per le politiche attive del lavoro

REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

Servizio: DIREZIONE GENERALE
Settore: SEGRETERIA DI DIREZIONE

DETERMINAZIONE DEL DIRETTORE GENERALE N° 272 del 30-01-2023

OGGETTO:	**REGOLAMENTO INTERNO ASPAL RELATIVO ALLA PROTEZIONE DEI DATI PERSONALI IN APPLICAZIONE DEL REGOLAMENTO UE 2016/679 E DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**

IL DIRETTORE GENERALE

VISTO il Regolamento Generale sulla protezione dei dati, Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016, in particolare l'art. 6 il quale, nel prevedere le basi giuridiche del trattamento, dispone che con riferimento al paragrafo 1, lettere c) ed e), la base su cui si fonda il trattamento deve essere prevista dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento;

VISTO il d. lgs. 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali", e ss.mm.ii.;

VISTA la legge regionale n. 9 del 17 maggio 2016, recante "Disciplina dei servizi e delle politiche per il lavoro", in particolare l'art. 10 della predetta legge che istituisce l'Agenzia sarda per le politiche attive per il lavoro (per brevità ASPAL), con sede a Cagliari, quale Organismo tecnico della Regione dotato di personalità giuridica, di autonomia organizzativa, amministrativa, patrimoniale e contabile;

VISTO l'articolo 13 della legge regionale n. 9 del 17 maggio 2016 che individua, quali organi dell'ASPAL, il Direttore ed il Collegio dei revisori dei conti e l'articolo 14 della predetta legge che disciplina i compiti di coordinamento, direzione e controllo da parte del Direttore generale dell'ASPAL;

VISTA la deliberazione della Giunta regionale n. 36/5 del 16 giugno 2016 recante "Approvazione preliminare Statuto Agenzia sarda per le politiche attive del lavoro", approvato in via definitiva con deliberazione della Giunta Regionale n. 37/11 del 21 giugno 2016;

VISTO lo Statuto dell'ASPAL, in particolare l'art. 5 che disciplina i compiti e le funzioni del Direttore Generale e visto l'art. 11 il quale dispone che l'ASPAL sia organizzata in Direzione generale e Servizi, così come disposto dal Titolo II della legge regionale n. 31/1998 e ss.mm.ii.;

VISTA la legge regionale n. 31 del 13 novembre 1998 e ss.mm.ii., avente ad oggetto: "Disciplina del personale regionale e dell'organizzazione degli uffici della Regione", in particolare l'art. 8, comma 3 e l'art. 14 - che attribuiscono rispettivamente "Ai dirigenti dell'Amministrazione e degli enti […] l'adozione degli atti e provvedimenti amministrativi, compresi tutti gli atti che impegnano le amministrazioni verso l'esterno" e individuano la procedura per la costituzione delle posizioni funzionali dirigenziali di staff;

VISTO lo Statuto Speciale della Regione Autonoma della Sardegna e le relative norme di attuazione;

VISTA la Deliberazione della Giunta Regionale n. 17/3 del 7 maggio 2021 con la quale la scrivente è stata individuata Direttrice Generale dell'ASPAL;

VISTA la deliberazione della Giunta regionale n. 21/8 del 24.04.2018 riguardante il modello organizzativo e adempimenti finalizzati all'applicazione del Regolamento (UE) 2016/679 relativo alla

protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circol azione di tali dati;

CONSIDERATO che la deliberazione n. 21/8 del 24.04.2018 e le direttive in essa contenute non sono direttamente applicabili all'ASPAL in virtù della legge regionale n. 9 del 19 maggio 2016, in particolare l'art.10, comma 1 per il quale l'ASPAL è dotata di personalità giuridica e autonomia organizzativa e l'art.14, comma 1 che individua il rappresentante legale dell'Agenzia nel Direttore Generale pro tempore;

ATTESO che è intenzione dell'ASPAL attenersi alle disposizioni di cui alla sopracitata deliberazione 21/8 del 24.04.2018 e alle direttive in essa contenute, così come a tutte le altre disposizioni e adeguamenti previsti per il sistema Regione in materia di protezione dei dati;

VISTA la determinazione n. 841 del 2018 che approvava il Regolamento dell'ASPAL in materia protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati;

VISTA la determinazione n. 1417 del 2020 che approvava il regolamento dell'ASPAL in materia protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati in sostituzione del precedente Regolamento adottato con determinazione n. 841 del 2018;

CONSIDERATO che al fine di soddisfare il principio di *accountability*, si è reso necessario modificare il precedente Regolamento interno adottato con determinazione n. 1417 del 2020, affinché vengano resi noti gli attori del trattamento dei dati personali svolti dall'ASPAL e venga pubblicato l'organigramma privacy;

CONSIDERATO, inoltre, che si è reso opportuno specificare i ruoli e le funzioni degli attori del trattamento dei dati personali, nonché disciplinare la procedura *data breach* e la metodologia da adottare in linea con quella della Regione Autonoma della Sardegna;

VISTO l'art. 4, lettera c) dello Statuto che prevede che i regolamenti ed altri atti a contenuto generale sono soggetti al controllo e alla vigilanza di cui alla legge regionale 15 maggio 1995, n.14;

DATO ATTO che la presente determinazione non comporta impegno di spesa;

Per le motivazioni esposte in premessa:

DETERMINA

Art. 1) di approvare quanto in narrativa esposto che qui si intende integralmente riportato;

Art. 2) di approvare il "Regolamento interno ASPAL relativo alla protezione dei dati personali in applicazione del regolamento UE 2016/679 e del Codice in materia di protezione dei dati personali", che allegato alla presente ne fa parte integrante e sostanziale, così come gli allegati: "1) - Procedura *data breach* ASPAL", "2) – Modello di segnalazione breve *data breach*", "3) - Metodologia *data breach*";

Art. 3) di dare atto che il predetto Regolamento entrerà in vigore con il perfezionarsi della procedura di controllo prevista per i regolamenti interni dall'art. 4 della Legge Regionale n. 14 del 15 maggio 1995;

Art. 4) di dare atto che il presente provvedimento non necessita di regolarità contabile e attestazione di copertura finanziaria.

Art. 5) di dare atto che, per quanto previsto in materia di pubblicità, trasparenza e diffusione di informazioni, si provvederà ai sensi delle disposizioni normative e amministrative richiamate in parte narrativa.

Visto
Del direttore del DIREZIONE GENERALE
F.to DOTT.SSA MAIKA AVERSANO

La Direttrice Generale
F.to MAIKA AVERSANO

Documento informatico firmato digitalmente ai sensi del TU 445/2000 e del D.Lgs. 82/2005 e rispettive norme collegate

REGOLAMENTO INTERNO ASPAL
RELATIVO ALLA PROTEZIONE DEI DATI PERSONALI
IN APPLICAZIONE DEL REGOLAMENTO UE 2016/679 E DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Sommario

Art. 1 Definizioni

1. Ai fini del presente Regolamento si intende per:
   a. **"ASPAL"**: Agenzia Sarda per le Politiche attive del Lavoro.
   b. "**Regolamento**": Regolamento interno ASPAL relativo alla protezione dei dati personali in applicazione del regolamento (UE) 2016/679 e del codice in materia di protezione dei dati personali.
   c. "**Regolamento UE**" o "**GDPR**": Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.
   d. "**Codice Privacy**": D. Lgs. 30 giugno 2003, n. 196, modificato dal D. Lgs. 10 agosto 2018, n. 101 e dal D.L. 8 ottobre 2021, n. 139 convertito dalla L. 3 dicembre 2021, n. 205.
   e. "**Titolare del trattamento**" o anche solo "**Titolare**": è l'Agenzia Sarda per le Politiche Attive del Lavoro – ASPAL.

f. "**Delegato del titolare**": è il Direttore del Servizio, nominato mediante determinazione del Direttore Generale, al quale vengono attribuite le deleghe, per ciascun ambito di competenza, delle funzioni relative all'attuazione dei principi dettati dall'articolo 5 del GDPR, in materia di trattamento dei dati personali e, in particolare, per lo svolgimento dei compiti e delle funzioni previste dal Regolamento.

g. "**Responsabile data breach**": è il Direttore del Servizio con competenze adeguate a valutare le conseguenze sui diritti degli interessati e a gestire la procedura del data breach, incluse le notifiche. Viene nominato mediante determinazione del Direttore Generale e ad esso viene attribuita la funzione di coordinatore del Gruppo di gestione del data breach.

h. "**Referente Privacy**": è il funzionario, referente unico per l'ASPAL, con competenze in materia di privacy.

i. "**Referente del Servizio**": è il funzionario, referente per ogni singolo Servizio, in materia di privacy.

j. "**Gruppo di lavoro privacy**": costituito dal Referente privacy e dai Referenti del Servizio.

k. "**RPD**" o "**DPO**": Responsabile della Protezione dei Dati o Data Protection Officer.

l. "**DPIA**": Valutazione d'impatto sulla protezione dei dati, come disciplinata dall'art. 35 GDPR.

m. "**Analisi del rischio**": è la valutazione che deve essere effettuata dal Titolare del trattamento o dal suo Delegato prima dell'inizio di ogni trattamento e consiste nella valutazione del rischio inteso come lo scenario descrittivo di un evento e delle relative conseguenze che sono stimate in termini di gravità e probabilità per i diritti e le libertà.

n. "**DPA**": Data Protection Agreement o Nomina del Responsabile del trattamento, come disciplinato dall'art. 28 GDPR.

o. "**Autorizzati al trattamento**": sono i dipendenti e i collaboratori che agiscono sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento, come disciplinato dall'art. 29 GDPR.

p. "**EDPB**": European Data Protection Board – Comitato Europeo per la protezione dei dati – ex Article 29 Working Party o WP29 - Gruppo di Lavoro Articolo 29.

q. "**Garante privacy**" o anche solo "**Garante**": Autorità Garante per la protezione dei dati personali.

2. Per quanto non espressamente definito al precedente comma 1, si intendono integralmente richiamate le definizioni di cui all'art. 4 del Regolamento (UE) 2016/679.

Art. 2 Principi generali e ambito di applicazione

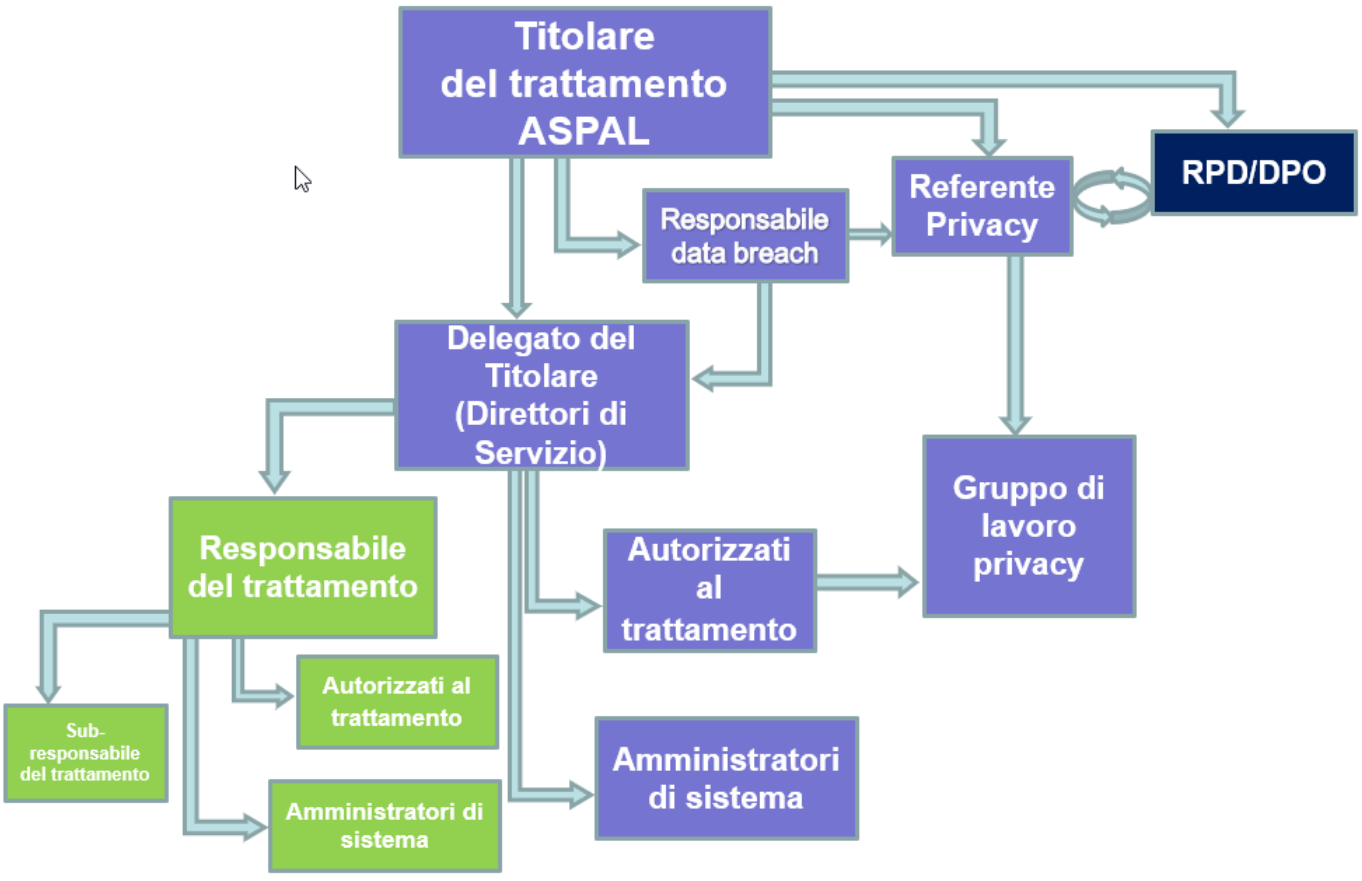
1. Il presente Regolamento interno, adottato ai sensi dello Statuto dell'ASPAL, ha per oggetto le misure organizzative e procedimentali mediante le quali l'ASPAL attua i principi e le disposizioni del Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 (di seguito indicato come GDPR) nonché quelle previste dal D. Lgs. n. 196/2003 Codice in materia di protezione dei dati personali come modificato dal D. Lgs. n. 101/2018 (di seguito Codice Privacy).
2. L'ASPAL (di seguito "Agenzia" o "Titolare"), in qualità di Titolare del trattamento, è il soggetto che garantisce che i trattamenti dei dati personali effettuati per l'adempimento delle proprie attività istituzionali si svolgano nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

3. Il presente Regolamento – che sostituisce il precedente Regolamento interno adottato con deliberazione n. 1417 del 23/09/2020 – disciplina il sistema di gestione dei dati personali all'interno dell'ASPAL e rappresenta lo strumento con il quale il Titolare individua le regole e i procedimenti ai quali devono attenersi tutti dipendenti e, in generale, i Delegati dal titolare e gli autorizzati al trattamento dei dati. Il presente regolamento interno si applica a tutti i trattamenti dei dati personali effettuati dall'Agenzia.

Art. 3 Normativa di riferimento

1. Ai fini del presente Regolamento si applica la seguente normativa:
   - *a.* Regolamento (UE) 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;
   - *b.* D. Lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali" come novellato dal D. Lgs. 10 agosto 2018, n.101 e dal D.L. 8 ottobre 2021, n. 139 convertito dalla L. 3 dicembre 2021, n. 205.
   - *c.* Le linee guida adottate dall'EDPB – ex Article 29 Working Party o WP29, oggi Comitato Europeo per la protezione dei dati.
   - *d.* I provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali in materie specifiche.

Art. 4 Organigramma privacy



Art. 5 Titolare del trattamento

1. Il Titolare del trattamento è l'Agenzia sarda per le politiche attive del lavoro, di seguito ASPAL, che esercita i poteri propri del Titolare per mezzo del legale rappresentante, il quale può agire d'ufficio o su impulso e/o proposta del Responsabile della Protezione dei Dati (RPD o DPO).
2. Il Titolare, a cui competono le decisioni in ordine alle finalità, modalità, mezzi di trattamento, compreso il profilo della sicurezza, provvede alla corretta applicazione della normativa in materia di protezione dei dati e si avvale dei Delegati del titolare, del Referente privacy, del Gruppo di lavoro privacy e di tutti i dipendenti e collaboratori che agiscono sotto la sua autorità.
3. Il Titolare e/o i Delegati del Titolare provvedono a istruire e a nominare gli autorizzati al trattamento e gli amministratori di sistema; inoltre, al fine di adempiere all'obbligo di cui all'art. 28 del Regolamento UE, provvedono a designare i Responsabili del trattamento – mediante apposito atto in forma scritta – tutti i soggetti terzi che, in esecuzione di un contratto, di una convenzione o di un affidamento, effettuino un trattamento di dati personali per conto del Titolare.
4. Il Titolare impartisce ai soggetti delegati al trattamento le istruzioni e gli adempimenti connessi a una compiuta e corretta attività di protezione dei dati.
5. Laddove finalità e mezzi del trattamento vengano determinati congiuntamente da due o più titolari, si rientra nelle ipotesi di contitolarità del trattamento. Per la determinazione dei casi di contitolarità del trattamento si richiamano integralmente le "*Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*" versione 2.0 adottate il 7 luglio 2021 dall'EDPB.
6. Il Titolare, tenendo conto degli articoli 37 e ss. del GDPR, nonché delle "Linee Guida sui responsabili della protezione dei dati" adottate dal WP29 e del "Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico" adottato dal Garante per la protezione dei dati personali, nomina il Responsabile della protezione dei dati.

Art. 6 Compiti e funzioni dei Delegati del titolare

1. L'ASPAL, con determinazione del Direttore Generale N. 628 del 21/03/2022, utilizzando lo strumento della delega, ha attribuito compiti e funzioni proprie del Titolare connesse al trattamento dei dati personali ai Direttori di Servizio.
2. I Direttori di Servizio, stante la delega ad essi attribuita, si avvalgono della collaborazione del Referente privacy e del Gruppo di lavoro privacy (anche dei singoli componenti), nonché di tutti i dipendenti e collaboratori che agiscono sotto la loro autorità, per lo svolgimento dei seguenti compiti e funzioni previste dal Regolamento UE:
    a. predisposizione delle informative da fornire agli interessati ai sensi degli articoli 13 e 14 del Regolamento UE 2016/679;
    b. predisposizione dei riscontri da fornire agli interessati in merito all'esercizio dei loro diritti previsti dagli articoli 15-22 GDPR;
    c. compilazione e aggiornamento del Registro delle attività di trattamento di cui all'art. 30 GDPR;
    d. adozione, riesame e aggiornamento delle misure tecniche e organizzative affinché esse siano adeguate e conformi secondo quanto previsto dagli articoli 24 e 32 GDPR;
    e. adozione delle misure tecniche e organizzative adeguate fin dalla progettazione del trattamento (privacy by design) e per impostazione predefinita (privacy by default), così come previsto dall'art. 25 GDPR;

f. tenendo conto delle lettere c) ed e) del presente articolo, effettuazione dell'analisi del rischio prima dell'inizio di ogni trattamento. Per la valutazione del livello di rischio e per testare le misure di sicurezza implementate, si utilizzano gli strumenti messi a disposizione dall'ENISA alla pagina https://www.enisa.europa.eu/risk-level-tool/

g. predisposizione dell'accordo di contitolarità ai sensi dell'art. 26 GDPR e adozione dei conseguenti adempimenti, quali ad esempio la redazione dell'estratto dell'accordo di contitolarità da mettere a disposizione degli interessati;

h. predisposizione dei contratti, atti o convenzioni e contestuale stipula e sottoscrizione dell'atto di designazione del Responsabile del trattamento a norma dell'art. 28 GDPR, qualora le attività della parte contrattuale comportino il trattamento di dati personali per conto del Titolare del trattamento;

i. istruire e nominare gli incaricati del trattamento facenti parte del proprio Servizio secondo quanto previsto dall'art. 29 GDPR;

j. nei casi in cui è prevista, collaborare con il Referente privacy e mettere a disposizione le risorse necessarie al fine di effettuare la valutazione d'impatto sulla protezione dei dati di cui all'art. 35 GDPR, collaborando altresì, ove necessario, anche alla consultazione preventiva ai sensi dell'articolo 36 GDPR;

k. coinvolgimento del Referente privacy e del DPO in tutte le questioni riguardanti la protezione dei dati;

l. garantire la cooperazione, per quanto di competenza, con l'Autorità di controllo nell'esecuzione dei compiti ad essa attribuiti.

3. I Delegati vigilano sulla conformità dell'operato dei propri preposti alle istruzioni e alle direttive indicate al comma 2 e verificano periodicamente lo stato di adeguamento alla normativa in oggetto. Verificano, altresì, che i dati oggetto di trattamento siano esatti, aggiornati, indispensabili, pertinenti e non eccedenti rispetto alle finalità per cui vengono trattati e si attengono alle indicazioni di sicurezza dettate dal Titolare del trattamento.
4. Partecipano ai momenti formativi organizzati dall'ASPAL o dall'RPD e assicurano la partecipazione dei propri preposti.
5. Sono componenti del Gruppo di analisi e gestione del *data breach* in relazione alle violazioni che riguardano il proprio Servizio.
6. Provvedono all'applicazione della Procedura *data breach*, disciplinata dall'allegato 1 e che è parte integrante del presente Regolamento.
7. Sensibilizzano le risorse afferenti al proprio servizio affinché sia data piena applicazione al Regolamento UE e alle disposizioni provenienti dal DPO.
8. Individuano il Referente del Servizio in tema di privacy e ne danno tempestiva comunicazione al Referente privacy affinché provveda all'aggiornamento della composizione del Gruppo di lavoro privacy e alla relativa comunicazione a tutto il personale.
9. Richiedono le autorizzazioni al rilascio delle abilitazioni agli applicativi informatici per i preposti appartenenti al proprio servizio.

Art. 7 Compiti e funzioni del Referente privacy

1. Il Referente privacy, incardinato sotto la Direzione Generale, è il funzionario referente unico per l'ASPAL con competenze specifiche e con esperienza in materia di protezione dati personali; ad esso sono attribuite le funzioni di supporto al Titolare e ai Delegati che concernono l'attuazione delle disposizioni comunitarie e nazionali in tema di trattamento dei dati personali.
2. Svolge le funzioni di coordinamento delle attività del Gruppo di lavoro privacy. In caso di inerzia dei Referenti dei Servizi o nei casi di necessità e urgenza, può in agire in autonomia

dietro autorizzazione, anche verbale, del Titolare o dei Delegati.

3. È membro del Gruppo di gestione del data *breach* e fornisce supporto al Responsabile del data *breach* per tutte le attività legate all'analisi e alla gestione della violazione.
4. Il Referente privacy, avvalendosi del supporto e della collaborazione del Gruppo di lavoro privacy o dei singoli Referenti dei Servizi, svolge le seguenti attività:
    a. fornisce riscontri e pareri alle richieste in tema di trattamento dei dati personali che pervengono dai Servizi;
    b. fornisce riscontro alle istanze che pervengono dagli utenti, comprese quelle relative ai diritti degli interessati, senza ingiustificato ritardo ed entro i termini previsti dall'art. 12 GDPR;
    c. predispone le informative ai sensi degli artt. 13 e 14 del Regolamento UE;
    d. compila e aggiorna il registro delle attività di trattamento di cui all'art. 30 GDPR;
    e. garantisce il supporto alle attività del Responsabile della Protezione Dati (RPD/DPO);
    f. collabora con il responsabile del *data breach* alla compilazione e all'aggiornamento del registro delle violazioni dei dati personali (*registro data breach)*;
    g. collabora con il responsabile del *data breach* alla predisposizione della notifica della violazione dei dati personali all'Autorità di controllo ai sensi dell'art. 33 GDPR e provvede, se del caso, alla comunicazione della violazione agli interessati, secondo quanto previsto dall'art. 34 GDPR;
    h. collabora con il Referente del Servizio alla predisposizione della nomina del Responsabile del trattamento ai sensi dell'art. 28 GDPR (anche DPA);
    i. collabora con i Delegati del titolare (Direttori di Servizio) alla predisposizione degli accordi di contitolarità e agli adempimenti connessi;
    j. comunica a tutto il personale ASPAL i nominativi dei funzionari facenti parte del Gruppo di lavoro privacy e tutti gli eventuali aggiornamenti sulla composizione del predetto Gruppo;
    k. promuove l'osservanza del Regolamento aziendale sulla privacy fornendo la necessaria consulenza in ordine alle problematiche in tema di riservatezza;
    l. promuove e supporta la formazione dei dipendenti in materia di privacy;
    m. promuove azioni di sensibilizzazione verso la materia.

Art. 8 Compiti e funzioni del Referente del Servizio e del Gruppo di lavoro privacy

1. Il Referente del Servizio è il funzionario individuato quale referente in materia di privacy. Ciascun Direttore può indicare non più di due referenti per Servizio. Ogni Referente del Servizio è componente del Gruppo di lavoro privacy.
2. Di seguito vengono indicati i compiti e le funzioni del Referente del Servizio:
    a. segnala tempestivamente al Referente privacy qualsiasi questione in tema di trattamento dei dati personali che non possa gestire in autonomia e collabora con esso alla gestione del quesito o all'analisi dei fatti;
    b. segnala tempestivamente al Referente privacy le istanze che pervengono dagli utenti, comprese quelle relative ai diritti degli interessati e collabora con esso affinché possa essere dato riscontro all'utente entro i termini previsti dal Regolamento UE;
    c. collabora con il Referente privacy alla predisposizione delle informative relative ai trattamenti del proprio Servizio;

d. collabora con il Referente privacy alla predisposizione delle nomine dei Responsabili del trattamento *ex* art. 28 GDPR;

e. comunica al Referente privacy, con congruo anticipo e in ogni caso prima che sia dato inizio al trattamento, ogni nuovo trattamento di dati personali che verrà effettuato nell'ambito del proprio Servizio e collabora con esso affinché possa provvedere alla compilazione del Registro dei trattamenti;

f. segnala tempestivamente al proprio Direttore o al Referente privacy qualsiasi episodio che possa comportare una violazione dei dati personali e si attiene scrupolosamente alle disposizioni di cui alla Procedura *data breach* allegata al presente Regolamento;

g. cura la propria formazione in tema di privacy e partecipa alle iniziative, agli incontri e alle attività formative promosse dal DPO, dal Referente privacy o dal Servizio Risorse Umane e Formazione.

3. Il Gruppo di lavoro privacy fornisce risposte alle istanze che pervengono dai Servizi o dagli utenti e promuove azioni di sensibilizzazione verso la materia, in particolare:

a. garantisce il supporto alle attività del Responsabile della protezione dati (DPO/RPD), al Referente privacy e al Responsabile del *data breach*;

b. provvede alla predisposizione degli atti necessari, ai fini dell'adempimento degli oneri previsti dalla normativa suddetta;

c. promuove l'osservanza del Regolamento sulla privacy fornendo la necessaria consulenza in ordine alle problematiche in tema di riservatezza.

Art. 9 Autorizzati al trattamento: compiti e istruzioni

1. Il Titolare e/o i suoi Delegati autorizzano al trattamento dei dati personali i soggetti di cui l'ASPAL si avvale per il raggiungimento delle proprie finalità, nel limite di quanto necessario allo svolgimento delle mansioni affidate.
2. Sono soggetti autorizzati al trattamento i dipendenti e i collaboratori che agiscono sotto la diretta autorità del Titolare del trattamento, i quali ai sensi dell'art. 29 GDPR hanno accesso ai dati personali e al loro trattamento.
3. Il precedente comma 2 si applica anche in caso di accordo contitolarità.
4. I soggetti autorizzati vengono istruiti circa i limiti e le corrette modalità del trattamento dei dati connesso all'espletamento delle loro funzioni, con particolare riferimento ai seguenti doveri:

a. trattare i dati in modo lecito e secondo correttezza attenendosi alle direttive impartite dal Titolare o dal Delegato sia nell'atto di designazione sia in seguito;

b. trattare i dati esclusivamente per le finalità indicate dal Titolare o dal Delegato e unicamente per lo svolgimento delle mansioni affidate;

c. verificare che i dati personali siano pertinenti, completi, esatti, aggiornati e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;

d. trattare i soli dati necessari allo svolgimento delle operazioni da effettuare;

e. utilizzare le informazioni e i dati con cui si entra in contatto per ragioni lavorative, comprese le categorie particolari di dati personali e i dati giudiziari, di cui agli artt. 9 e 10 del GDPR, esclusivamente per lo svolgimento delle attività istituzionali, con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata del rapporto lavorativo e anche successivamente al termine di esso;

f. conservare i dati rispettando le misure di sicurezza, tecniche e organizzative, predisposte dal Titolare o dal Delegato;

g. segnalare al Titolare o al Delegato del titolare eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza, al fine di proteggere i dati da trattamenti non autorizzati o illeciti, dal rischio di perdita, di distruzione o di danno accidentale;

h. astenersi dal comunicare a terzi dati e informazioni senza la preventiva specifica autorizzazione del Titolare o del Delegato (salvo i casi previsti dalla legge o da contratti e convenzioni);

i. collaborare con il Referente privacy e con il Referente del Servizio ai fini della predisposizione di atti e adempimenti che riguardano il trattamento dei dati personali collegati alle proprie mansioni;

h. informare immediatamente il Titolare del trattamento, il proprio Direttore di Servizio o il Referente del Servizio per la privacy o il Referente privacy nel caso in cui si constati o si sospetti un incidente di sicurezza, come dalle disposizioni di cui alla Procedura *data breach* allegata al presente Regolamento;

j. collaborare con il Referente privacy e con il Gruppo di gestione del *data breach* nel caso in cui la violazione dei dati personali abbia attinenza con la propria attività o comunque sia collegata in maniera diretta o indiretta con lo svolgimento dei propri compiti e mansioni (es. nel caso in cui la violazione riguardi il dispositivo in dotazione o derivi da un comportamento doloso o colposo ascrivibile al dipendente).

Art. 10 Servizio sistemi informativi (IT)

1. Il servizio responsabile della gestione dei sistemi informativi provvede affinché vengano messe in atto le misure tecniche sui sistemi informatici al fine di garantire un livello di sicurezza adeguato al rischio, come previsto dall'art. 32 GDPR, nonché in coerenza con gli indirizzi forniti dal Responsabile per la Transizione Digitale.
2. All'interno del Servizio vengono individuati i dipendenti e i collaboratori ai quali vengono attribuite le funzioni di amministratore di sistema. La nomina, che compete al direttore del Servizio "Sistemi informativi, affari legali, anticorruzione e controlli", avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, compreso il profilo relativo alla sicurezza. La nomina viene effettuata in maniera individuale ed è formalizzata con l'indicazione analitica degli applicativi e dei sistemi di gestione di applicazione di operatività consentiti in base al profilo di autorizzazione assegnato.
3. Gli amministratori di sistema mantengono, configurano e gestiscono le reti e apparati di telecomunicazione di sicurezza; ad essi sono attribuiti i seguenti compiti:

    a. Attuano e verificano la corretta applicazione delle misure di sicurezza tecniche individuate dal Titolare del trattamento o dal Direttore del Servizio IT, al fine di assicurare l'integrità e la disponibilità dei dati e garantire la protezione dei dispositivi e dei programmi contro il rischio di intrusione o perdita;

    b. collaborano per il tempestivo ripristino dei dati personali in caso di incidente di sicurezza e collaborano con Gruppo di gestione del *data breach*;

    c. segnalano al Direttore del Servizio qualsiasi avvenimento, fatto o circostanza che possa determinazione un incidente di sicurezza o una violazione dei dati personali e suggeriscono altresì le misure tecniche o organizzative che, secondo la loro esperienza e professionalità, possano garantire un livello di sicurezza rispettoso dell'art. 32 GDPR;

    d. vigilano sul rispetto del regolamento interno sull'utilizzo degli strumenti informatici o delle disposizioni emanate dal Responsabile IT o dal Titolare del trattamento.

Art. 11 Tenuta della postazione lavorativa e della scrivania

1. Il personale dipendente e i collaboratori, nello svolgimento delle operazioni di trattamento, controllano e custodiscono con cura e diligenza gli atti e i documenti contenenti dati personali in modo che ad essi non accedano persone prive di autorizzazione. Garantiscono il rispetto delle istruzioni impartite dal Titolare del trattamento o dal Delegato, e in ogni caso, con riferimento alla tenuta delle scrivanie e delle postazioni lavorative, sono tenuti a:

    a. utilizzare password lunghe almeno dodici caratteri con un misto di lettere, numeri e segni di interpunzione, diversificarle tra i vari applicativi e non usare password troppo intuibili;

    b. assicurare la riservatezza delle credenziali di autenticazione assegnate. È vietata la conservazione su post-it, agende o bloc-notes lasciati incustoditi sulle scrivanie;

    c. non lasciare accessibile la postazione durante una sessione di trattamento e utilizzare uno *screen saver* che blocchi il dispositivo (laptop, notebook o PC) entro pochi minuti di inutilizzo;

    d. nel caso in cui pervengano richieste di comunicazione di dati, verificare l'identità del richiedente attraverso un diverso canale (mail/telefono);

    e. non utilizzare i supporti removibili (es. chiavette USB) salvo che sia indispensabile, in tal caso è necessario cancellare il contenuto dei supporti non appena possibile;

    f. ridurre al minimo lo spostamento di supporti informatici o cartacei contenenti dati personali;

    g. riporre i documenti e i fascicoli contenenti dati personali, al termine del loro utilizzo e comunque alla fine di ogni giornata lavorativa, negli armadi o nei cassetti dotati di serratura e chiuderli a chiave;

    h. far uso esclusivamente delle attrezzature e dei servizi forniti dal Titolare, salva diversa autorizzazione del Titolare o del Delegato;

    i. non creare banche dati senza espressa autorizzazione del Titolare o del Delegato;

    j. prestare attenzione nel caso in cui si debbano inviare documenti contenenti dati personali tramite posta elettronica, in particolare verificare il corretto inserimento dell'indirizzo di posta elettronica a cui inviare la comunicazione, ricontrollando sempre l'esattezza dell'indirizzo digitato prima dell'invio.

Art. 12 Responsabile Protezione dei Dati (R.P.D.) o Data Protection Officer (D.P.O.)

1. Il responsabile della protezione dei dati dell'ASPAL (di seguito anche RPD o DPO) dispone delle competenze e delle prerogative previste dagli articoli 37 e 38 del GDPR.
2. Si applicano, altresì, le "*Linee guida sui responsabili della protezione dei dati*" del Gruppo di lavoro articolo 29 adottate il 13 dicembre 2016 e modificate in data 5 aprile 2017, nonché le disposizioni di cui al "*Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico*" provvedimento n. 186 del 29 aprile 2021 e s.m.i. adottato dal Garante privacy.
3. L'ASPAL può far ricorso e procedere alla designazione del responsabile per la protezione dei dati personali nominato dall'Amministrazione regionale per gli enti del sistema Regione, come previsto dall'art. 37 par. 3 GDPR e dalla DGR 21/8 del 24/04/2018. In ogni caso, qualora se ne ravvisi l'esigenza, fermo restando il possesso delle competenze e prerogative di cui al comma 1, l'ASPAL potrà individuare l'RPD fra i propri dipendenti o procedere tramite procedura ad

evidenza pubblica.

4. Il Titolare del trattamento, anche attraverso i propri delegati, si assicura che il Responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardante la protezione dei dati personali. Inoltre, provvede alla pubblicazione dei dati di contatto del Responsabile della protezione dei dati e li comunica al Garante per la protezione dei dati personali.
5. I compiti del responsabile della protezione dei dati sono individuati dall'art. 39 del Regolamento UE.
6. Il Titolare del trattamento può prevedere ulteriori e diversi compiti a carico del DPO attraverso specifica previsione nell'atto di designazione.

Art. 13 Registro delle attività di trattamento

1. L'ASPAL, come previsto dall'art. 30 del Regolamento UE, ha adottato il Registro delle attività di trattamento in relazione allo svolgimento delle attività istituzionali che svolge come Titolare e come Responsabile del trattamento. Il modello in uso è quello del Sistema Regione, accessibile unicamente in modalità elettronica alla pagina https://rpd.regione.sardegna.it/registrotrattamento/login.php.
2. Il Registro delle attività di trattamento ha la funzione di rappresentare il flusso dei dati e dei trattamenti che vengono svolti dall'ASPAL sia come Titolare che come Responsabile del trattamento; per questo motivo la corretta tenuta del Registro, costituendo uno strumento di *accountability*, consente all'ASPAL di operare una valutazione dei rischi legati ai trattamenti. Il personale dipendente, qualora si avveda di un trattamento non presente sul Registro, deve tempestivamente segnalarlo al Referente del proprio Servizio o al Delegato del titolare.
3. Il Registro delle attività di trattamento è compilato dal Referente privacy con la collaborazione dei Referenti dei Servizi, i quali, tempestivamente e senza indugio, reperiscono e comunicano ogni informazione utile affinché il Registro possa essere compilato prima che abbia inizio il trattamento.
4. Il Registro è accessibile da tutti i dipendenti in modalità "visualizzazione" e da quelli appositamente incaricati anche in modalità "redattore".
5. Al Responsabile per la protezione dei dati compete la gestione, la manutenzione e lo sviluppo dell'applicativo del Registro delle attività di trattamento in uso all'ASPAL.
6. Il Registro è sempre a disposizione dell'Autorità Garante per la protezione dei dati personali.

Art. 14 Informazioni agli interessati

1. Il Titolare o i suoi Delegati sono tenuti a fornire agli interessati, prima che abbia inizio il trattamento, tutte le informazioni che riguardano le finalità e le modalità di utilizzo dei dati personali nell'ambito delle proprie attività istituzionali, secondo le disposizioni di cui agli articoli 13 e 14 GDPR. Tali informazioni sono fornite attraverso un modello predisposto dall'ASPAL che può essere adattato in funzione delle specificità di ogni singolo trattamento.
2. Il Referente del Servizio si adopera affinché la documentazione utile alla predisposizione delle informazioni di cui agli articoli 13 e 14 GDPR vengano rese disponibili al Referente privacy con un congruo preavviso, non inferiore a quindici giorni lavorativi dalla data attesa di pubblicazione del bando, dell'avviso o comunque dall'inizio del trattamento.
3. Le informative vengono pubblicate alla pagina https://www.aspalsardegna.it/privacy/ e rese disponibili agli interessati con gli strumenti più idonei al caso concreto.
4. Nei Centri per l'impiego (CPI) si procede all'affissione delle informative concernenti i trattamenti svolti nell'ambito dell'erogazione dei servizi all'impiego. In ogni caso, le predette informative sono sempre a disposizione presso il desk o lo sportello in cui si riceve il pubblico,

sia in modalità cartacea (plastificata) che digitale, attraverso, ad esempio, la messa a disposizione di un QR *code*.

5. Le informative che accompagnano i bandi di concorso, i bandi di gara, le lettere di invito e/o gli avvisi pubblici, a seconda delle circostanze concrete e del caso di specie, potranno essere integrate nell'articolato del documento principale o pubblicate alla pagina internet di cui al comma 2 del presente articolo.

Art. 15 Sistemi di videosorveglianza

1. Laddove necessario e in ossequio al principio di proporzionalità, il Titolare provvede all'installazione dei sistemi di videosorveglianza secondo le disposizioni di cui al Regolamento (UE) 2016/679, del Codice privacy e dell'art. 4 della legge n. 300/1970.
2. Il trattamento dei dati personali effettuato attraverso i sistemi di videosorveglianza avviene nel rispetto della dignità e dell'immagine delle persone, delle norme a tutela dei lavoratori e dei provvedimenti in materia emessi dall'Autorità Garante per la protezione dei dati personali.
3. L'informativa semplificata, ossia il cartello contenente le informazioni minime sul trattamento, viene esposto in prossimità degli accessi nei luoghi in cui gli interessati possano prenderne visione prima che abbia inizio il trattamento. L'informativa estesa viene pubblicata alla pagina https://www.aspalsardegna.it/privacy/
4. Con riferimento alla sede centrale di via is Mirrionis, il Titolare del trattamento ha ritenuto che - al fine di tutelare il patrimonio dell'Ente, in considerazione della localizzazione in una zona ad alto rischio di furti e danneggiamenti, data la delicata funzione sociale svolta dall'Agenzia, nonché tenuto conto dell'imminente riqualificazione dell'hangar e della sua destinazione a centro polifunzionale al quale avrà accesso il pubblico - sia necessario mantenere in funzione il sistema di videosorveglianza (senza captazione dell'audio).
5. L'impianto di videosorveglianza ha la finalità di tutelare altresì il patrimonio dei dipendenti e dei visitatori (es. autoveicoli, velocipedi, motocicli, etc.) da eventuali atti di vandalismo, danneggiamento o furto, nonché garantire la salvaguardia e l'incolumità del personale, compreso il personale terzo (utenti, fornitori, consulenti e visitatori). Le immagini potranno essere acquisite dall'Autorità Giudiziaria alla quale sia stata presentata una denuncia o una querela per l'esercizio e la tutela dei propri diritti.
6. Il trattamento non ha la finalità di controllo a distanza dei lavoratori: le immagini acquisite non saranno utilizzate in alcun modo nell'ambito di procedimenti disciplinari a carico dei lavoratori. A tal riguardo, il Titolare ha siglato un apposito accordo con le rappresentanze sindacali dei dipendenti ai sensi dell'art. 4 dello Statuto dei Lavoratori.
7. Il sistema di videosorveglianza è dotato di 14 telecamere. In ciascun angolo dell'edificio (4) sono posizionate tre telecamere; inoltre sono state posizionate altre due telecamere: una sul lato della via Ciociaria affinché possa essere sorvegliato l'accesso che conduce al sottopiano, l'altra sul lato della via Fontana Raminosa per presidiare l'accesso che conduce all'archivio.
8. La società di Vigilanza - nominata Responsabile del trattamento – è incaricata della verifica delle immagini in tempo reale che sono visibili tramite il monitor posizionato presso la guardiania. Inoltre, i codici d'accesso per estrarre i video sono in possesso unicamente della predetta società: nessun dipendente ASPAL è in grado di visionare i video registrati né di estrarne copia.
9. Le immagini vengono conservate per circa quattro giorni, ossia fino al raggiungimento della capacità massima di archiviazione dell'hard disk. La cancellazione delle immagini avviene in automatico per mezzo della sovrascrittura.

Art. 16 Valutazione d'impatto sulla protezione dei dati – DPIA

1. L'art. 35 GDPR dispone che qualora il trattamento presenti un rischio elevato per i diritti e le

libertà delle persone fisiche, il Titolare del trattamento effettui, prima di procedere al trattamento, la Valutazione d'impatto sulla protezione dati, di seguito anche solo "valutazione d'impatto" o "DPIA".

2. Si applica quanto previsto nelle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento «possa presentare un rischio elevato» ai fini del regolamento (UE) 2016/679*" adottate dal Gruppo di lavoro Articolo 29 del 4/04/2017 come modificate il 4/10/2017 e s.m.i., nonché le "*Linee guida sui responsabili della protezione dei dati*" adottate dal Gruppo di lavoro Articolo 29 del 13/12/2016 come modificate il 5/04/2017 con particolare riferimento a "Il *ruolo del RPD nella valutazione di impatto sulla protezione dei dati*"
3. La necessità di procedere alla valutazione d'impatto può emergere in sede di progettazione di un nuovo trattamento, in sede di compilazione del Registro dei trattamenti o a seguito del mutamento delle circostanze di fatto o della normativa nazionale e comunitaria.
4. Sono competenti alla predisposizione della DPIA il Referente privacy e il Referente del Servizio o il funzionario responsabile dello specifico progetto o comunque il personale dipendente individuato dal Delegato del Titolare.
5. Il Delegato del Titolare si assicura che il Referente del Servizio o i soggetti indicati al comma precedente garantiscano ogni più ampia e fattiva collaborazione affinché venga predisposta la valutazione d'impatto e sia trasmesso il documento al DPO per il relativo parere.
6. Il software per la valutazione d'impatto adottato dall'ASPAL è quello messo a disposizione del CNIL e scaricabile alla pagina https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil . In ogni caso, il Responsabile per la protezione dati potrà suggerire l'adozione di un software o di uno strumento diverso che si renda opportuno, anche in considerazione delle innovazioni e dell'avanzamento tecnologico e digitale.

Art. 17 Violazione dei dati personali – *Data Breach*

1. La violazione dei dati personali, o *data breach*, è una violazione di sicurezza che comporta la distruzione accidentale o illecita, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
2. La procedura di gestione del *data breach* è regolata dall'Allegato 1 al presente documento di cui ne costituisce parte integrante.

Art. 18 Entrata in vigore del Regolamento e forme di pubblicità

1. Il presente Regolamento è redatto allo stato della vigente legislazione ed è soggetto a variazioni o integrazioni a seguito di eventuali successivi interventi normativi o provvedimenti dell'Autorità Garante per la protezione dei dati personali che dovessero incidere sul suo contenuto.
2. Attraverso la pubblicazione di apposite note interne, verranno resi noti e aggiornati i nominativi e i dati di contatto delle seguenti figure: Responsabile del data *breach*, Referente privacy, componenti del Gruppo di gestione del data *breach* e dei loro sostituti, Referenti del Servizio e componenti del Gruppo di lavoro privacy.
3. Per tutto quanto non previsto si applica la normativa di settore.
4. Il presente Regolamento entra in vigore dalla data di pubblicazione della determinazione di approvazione; si provvede altresì a darne pubblicità tramite la sua pubblicazione alla pagina https://www.regione.sardegna.it/agenziaregionaleperillavoro/ nella sezione "Atti Generali", sotto-sezione "Regolamenti" e nell'intranet dell'Agenzia.

Allegato 1
Procedura *data breach*

Sommario

1. Fonti normative e regolamentari di riferimento

1. Ai fini del presente Regolamento si applica la seguente normativa:
    a. Regolamento (UE) 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, di seguito anche indicato come “GDPR”; in particolare gli articoli 33 e 34 e i Considerando 85, 87 e 88.
    b. D.lgs. 30 giugno 2003 n. 196 – Codice in materia di protezione dei dati personali – così come modificato dal D.lgs. n. 101/2018, e dal D.L. 8 ottobre 2021, n. 139 convertito dalla L. 3 dicembre 2021, n. 205.
    c. Parere 03/2014 sulla notifica delle violazioni dei dati personali adottato il 25 marzo 2014 dall’EDPB (ex Gruppo di lavoro art. 29 – Working party art. 29).
    d. Linee guida sulla notifica delle violazioni dei dati personali - WP250 (ex Gruppo di lavoro art. 29 – Working party art. 29) adottate il 3 ottobre 2017 e modificate in data 6 febbraio 2018.

2. Scopo del documento e ambito di applicazione

1. Con il presente documento l’ASPAL, in qualità di Titolare del trattamento, stabilisce le corrette modalità di gestione del *data breach* alla luce della normativa vigente in materia di trattamento dei dati personali.

3. Violazione dei dati personali o *data breach*

1. Come disciplinato dall'art. 4 par. 12 del Regolamento (UE) 2016/679, la violazione dei dati personali è "*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*." Si verifica la "distruzione" dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento; si ha la "perdita" dei dati personali quando i dati potrebbero esistere, ma il titolare del trattamento ne ha perso il controllo o l'accesso, o non ne è più in possesso; il trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati.
2. Il considerando 85 precisa che: "*una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo*."

4. Tipologie di *data breach*

1. Le violazioni possono essere classificate in base ai seguenti tre principi della sicurezza delle informazioni[1]:
    a. "**violazione della riservatezza**", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
    b. "**violazione dell'integrità**", in caso di modifica non autorizzata o accidentale dei dati personali;
    c. "**violazione della disponibilità**", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.
2. Gli eventi che determinano una violazione dei dati personali possono riguardare il trattamento di dati contenuti su supporti informatici o su supporti cartacei. Di seguito si riportano, a mero titolo esemplificativo e non esaustivo, alcuni esempi.
    a. Eventi relativi ai trattamenti **informatici**: malfunzionamento di un software, rottura di componenti hardware, esecuzione erronea di un comando o di una procedura, erronea pubblicazione di dati sui siti dell'ASPAL o su altri siti facenti capo al Sistema Regione, fornitura e comunicazione dei dati a persona diversa dall'interessato, guasti alla rete, accesso non autorizzato alla rete da soggetti esterni, perdita o furto di un dispositivo mobile o di un supporto di memorizzazione (smartphone, chiavetta USB, tablet, notebook, hard disk, etc.), rivelazione abusiva di credenziali, truffa informatica esterna o esterna (*ransomware*, *malware*, uso illegittimo delle informazioni dal personale interno e

[1] Parere 03/2014 del Gruppo di Lavoro articolo 29.

autorizzato);

b. Eventi relativi ai trattamenti **cartacei**: distruzione accidentale di documenti dovuta a incendio, allagamento o ad altri eventi o calamità naturali, smarrimento di documenti, fornitura involontaria dei dati a persona diversa dall'interessato, distruzione volontaria dei documenti da soggetti interni o esterni (es. incendio doloso o distruzione con altri mezzi), accesso non autorizzato con lettura ed eventuale estrazione di copia dei documenti da parte di personale interno non autorizzato o esterno, furto e divulgazione dei documenti.

5. Segnalazione del *data breach* da parte dei dipendenti e collaboratori

1. La segnalazione di un possibile *data breach* può provenire dall'esterno (cittadini, fornitori, enti istituzionali, etc.) o dall'interno, da parte di dipendenti e collaboratori dell'ASPAL durante lo svolgimento della propria attività lavorativa.
2. Il personale impiegato a vario titolo, i somministrati, i collaboratori e i tirocinanti, qualora rilevino personalmente una violazione di dati personali o ricevano la segnalazione dall'esterno, ossia qualora siano a conoscenza di un evento che possa costituire un potenziale *data breach*, sono tenuti a darne immediata comunicazione al Direttore del proprio Servizio e a inviare la segnalazione via e-mail all'account aspal.databreach@regione.sardegna.it utilizzando l'apposito modulo in allegato al presente documento (All. 2).
3. L'account aspal.databreach@regione.sardegna.it viene monitorato quotidianamente dal Referente data *breach* e dal Referente privacy.
4. Tutti i soggetti menzionati al comma 2 contribuiscono e partecipano, per quanto di loro conoscenza e competenza, alle valutazioni e alle analisi sulle circostanze che hanno causato un fatto o un evento che determini un'acclarata o una potenziale violazione dei dati personali.

6. Segnalazione del *data breach* da parte dei fornitori

1. I fornitori dell'ASPAL, nominati Responsabili del trattamento, qualora vengano a conoscenza di una presunta violazione di dati personali ne informano immediatamente per le vie brevi il referente (Direttore del servizio, responsabile del procedimento o comunque il dipendente ASPAL indicato nella nomina e/o nel contratto) e successivamente inviano una Pec all'indirizzo agenzialavoro@pec.regione.sardegna.it, come previsto nel documento di nomina a Responsabile del trattamento, e una mail all'indirizzo aspal.databreach@regione.sardegna.it, utilizzando il modulo allegato alla nomina a responsabile del trattamento.
2. Il fornitore garantisce assistenza, fornisce tutte le informazioni utili e svolge le dovute attività al fine di consentire che il Gruppo di gestione del *data breach* possa effettuare una corretta valutazione dell'evento e procedere con i dovuti adempimenti, quali le segnalazioni all'Autorità Garante per la protezione dei dati personali e, se del caso, all'Autorità di Pubblica Sicurezza.

7. Gruppo di gestione del *data breach*

1. È costituito il "*Gruppo di gestione del data breach"* con la funzione di valutare e gestire le segnalazioni di *data breach.*
2. Il Gruppo di gestione del *data breach* è composto da:

   a) Il **Responsabile del *data breach***, nominato con determinazione del Direttore

Generale, che assume la funzione di coordinatore del Gruppo. Il Responsabile del data breach individua un sostituto con propria determinazione;

b) Il **Titolare del trattamento**, nella persona del Direttore Generale;

c) **Il Dirigente del Servizio** delegato al trattamento oggetto della violazione;

d) **Il Dirigente del Servizio Sistemi Informativi**, se la violazione concerne i sistemi informativi;

e) Il **Referente privacy,** con funzioni di supporto al Responsabile del data *breach* per tutte le attività legate all'analisi e alla gestione dell'evento;

f) Il **DPO/RPD**;

3. Possono essere coinvolti tutti i soggetti (fornitori e personale di cui all'art. 5 comma 2) che possano apportare un contributo utile alle valutazioni e alle attività.
4. Le riunioni tra i componenti del gruppo possono avvenire anche con strumenti telematici e in modalità asincrona.
5. Sono componenti necessari: il Responsabile del data *breach* o il suo delegato, il DPO o il suo delegato e il Titolare del trattamento o un suo delegato. L'individuazione dei delegati avviene con atto formale.

8. Processo di gestione del *data breach*

1. Il Gruppo è deputato allo svolgimento delle seguenti attività:
    a. analisi tecnica dell'evento;
    b. valutazione della gravità dell'evento;
    c. analisi del rischio (in caso di violazione accertata);
    d. raccomanda le misure dirette a mitigare e a contenere il danno;
    e. individuazione delle misure da adottare per porre rimedio alla violazione e per attenuarne gli effetti;
    f. altre segnalazioni dovute.
2. Il Responsabile del data breach o il Referente privacy, ricevuta la segnalazione, provvedono a darne immediata comunicazione ai componenti del gruppo (inclusi i sostituti formalmente individuati) al loro account istituzionale. La comunicazione, avente ad oggetto "Data Breach: convocazione del gruppo di gestione" deve essere inviata entro 24 ore dal momento in cui ne sono venuti a conoscenza[2]. Fin dalla prima comunicazione il Responsabile del data *breach* e il Referente privacy possono proporre l'archiviazione per le segnalazioni manifestamente infondate. Se i componenti del gruppo non si oppongono, si procede all'archiviazione con la conclusione del procedimento senza l'iscrizione dell'evento nel registro del data *breach*.
3. Salvo quanto indicato al comma 2, il Gruppo di gestione del data *breach* svolge un'analisi preliminare (comma 1 lettere a e b) al fine di verificare se i fatti per cui si procede costituiscono un mero incidente di sicurezza o se vi sia la violazione di dati personali e se questa presenti un rischio per i diritti e le libertà delle persone fisiche.
4. Qualora, a seguito della prima analisi, il Gruppo di gestione del data breach verifichi

[2] Il Gruppo si riunisce nel minor tempo possibile e comunque entro 24 ore tenendo conto che l'eventuale comunicazione al Garante Privacy deve essere effettuata entro 72 ore dal momento in cui il Titolare o il suo Delegato ne sono venuti a conoscenza, ossia quando si è ragionevolmente certi che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali (Gruppo di lavoro Articolo 29 per la protezione dei dati - Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 https://ec.europa.eu/newsroom/article29/items/612052)

l'esistenza di elementi tali da escludere la possibile violazione dei dati personali, provvede all'archiviazione. L'archiviazione determina la conclusione del procedimento, senza iscrizione dell'evento nel Registro del data *breach*.

5. Una volta effettuate le analisi congiunte (comma 1 lettere c, d, e, f) e constatata la violazione dei dati personali, il Gruppo di gestione del data *breach* redige una sintetica relazione contenente le risultanze e le valutazioni svolte in merito alla necessità di procedere con la notifica della violazione al Garante e agli interessati. La relazione viene inviata al Titolare per le dovute considerazioni.
6. Il Titolare, valutata la relazione, approva le risultanze o assume differenti determinazioni, con particolare riferimento alla necessità di procedere con la notifica del *data breach* al Garante e agli interessati.
7. Il Responsabile del data breach, sulla base di quanto determinato dal Titolare, provvede a:
    a. inserire l'evento nel Registro delle violazioni (o Registro *data breach*), dando atto dell'eventuale notifica al Garante Privacy e agli interessati;
    b. notificare l'evento al Garante Privacy entro 72 ore dalla conoscenza della violazione, tenendo conto che le informazioni possono essere fornite in fasi successive, specie nei casi in cui si rendano necessari ulteriori approfondimenti e analisi di natura tecnica, anche al fine di determinare l'entità dell'evento, le sue conseguenze e il numero degli interessati. Qualora la notifica all'Autorità Garante per la protezione dei dati personali non possa essere effettuata entro le 72 ore, è corredata dei motivi del ritardo;
    c. inviare la comunicazione agli interessati, come previsto dall'art. 34 GDPR, qualora la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà delle persone.
8. Qualora, all'esito delle analisi svolte dal Gruppo, emergano degli elementi tali per cui l'incidente di sicurezza appaia collegato, connesso o dipendente a un reato, il Titolare (o un suo delegato) provvede a segnalare il fatto all'Autorità di Pubblica Sicurezza.

9. Stima della gravità del *data breach*

1. La gravità di una violazione dei dati personali è definita come la "stima dell'entità del potenziale impatto sugli individui derivante dalla violazione dei dati".
2. Al fine di valutare la gravità del data *breach* dovrà essere utilizzata la metodologia Enisa allegata al presente documento (All. 3) che fornisce al Gruppo di gestione del data *breach* una guida per una valutazione complessiva.
3. Il punteggio finale della valutazione della gravità della violazione di dati personali è dato dalla seguente formula: **Gravità = (Contesto di trattamento dati * Facilità identificazione) + Circostanze violazione.**
4. Dell'esito della decisione si informa il Titolare del trattamento che ha la facoltà, comunque, di valutare diversamente la gravità del danno.
5. Sulla base della casistica in cui si ricade, debbono essere svolte le seguenti azioni, tenendo conto del significato associato a:
    A. RISCHIO BASSO: non è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, ma l'incidente deve essere annotato all'interno del registro delle violazioni;
    B. RISCHIO MEDIO: non è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, ma devono essere adottate ulteriori misure

organizzative e tecniche al fine di migliorare la sicurezza dei dati personali e deve essere annotato l'incidente all'interno del registro delle violazioni;

C. **RISCHIO ALTO**: è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali e deve essere annotato l'incidente all'interno del registro delle violazioni

D. **RISCHIO MOLTO ALTO**: è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, annotare l'incidente all'interno del registro delle violazioni e darne comunicazione ai soggetti interessati secondo quanto disposto dal successivo articolo 10.

10. Comunicazione agli interessati

1. Come previsto dall'art. 34 del GDPR, se la violazione presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione viene effettuata, non appena ragionevolmente possibile e in collaborazione con l'Autorità Garante per la protezione dei dati personali, a cura del Referente del *data breach* con la collaborazione del Referente privacy. Qualora la portata dell'evento o il numero dei destinatari richieda una comunicazione pubblica è possibile coinvolgere il Team Comunicazione.
3. La comunicazione contiene almeno le seguenti informazioni:
    a. la descrizione della natura della violazione;
    b. i dati di contatto del RPD/DPO o di altro punto di contatto (es. Referente privacy);
    c. la descrizione delle probabili conseguenze della violazione;
    d. la descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione ed eventualmente per attenuarne i possibili effetti negativi.

11. Attività successive alla segnalazione del *data breach*

1. Il Titolare del trattamento e i Delegati del Titolare si adoperano affinché qualsiasi avvertimento, ammonimento, ingiunzione o richiesta proveniente dal Garante per la protezione dei dati personali, incluse quelle volte a soddisfare le richieste degli interessati e l'esercizio dei loro diritti, vengano eseguite tempestivamente o secondo i termini da essa indicati.
2. Il Gruppo di gestione del *data breach* dà atto, tramite verbale, di aver dato seguito alle disposizioni impartite dal Garante e lo trasmette al Titolare del trattamento.

Al Responsabile del data breach

Al Referente privacy

aspal.databreach@regione.sardegna.it

SEGNALAZIONE DATA BREACH
DIPENDENTI E COLLABORATORI ASPAL

SEGNALANTE

Nome:
Cognome:
Servizio:
indirizzo e-mail:
telefono:

Dati identificativi di ulteriori soggetti che sono in grado di fornire maggiori informazioni sull'evento: (indicare nome, cognome, qualifica/servizio, indirizzo e-mail, telefono):

VIOLAZIONE DEI DATI PERSONALI *(che può presentare un probabile rischio per i diritti e le libertà delle persone fisiche)*

Descrizione sintetica dell'evento:

Quando si è in verificato l'incidente?

Quando ne hai avuto conoscenza?

INFORMAZIONI *sul trattamento*

Quali sono i dati personali oggetto della violazione?
Sono coinvolti anche i dati appartenenti a categorie particolari di cui agli artt. 9 e 10 del GDPR? *(origine razziale, etnica, opinioni politiche, convinzioni religiose, appartenenza ai sindacati, dati genetici, sulla salute, vita sessuale o orientamento sessuale, dati relativi a condanne penali o a reati o a misure di sicurezza)*

Qual è la categoria degli interessati coinvolti? (es. utenti del CPI, dipendenti, altro)
In via approssimativa quanti interessati sono stati coinvolti?
Uno o più interessati hanno segnalato il possibile data breach?

Gli interessati sono già stati informati del fatto che si è verificato questo incidente?

RISCHI *sul trattamento*

Sono state già intraprese delle azioni per ridurre o mitigare gli effetti della violazione dei dati sugli interessati coinvolti?

Se la risposta è affermativa, fornire brevi dettagli:

È in corso un'inchiesta interna sull'incidente?

Se la risposta è affermativa, fornire brevi dettagli:

Aggiungere qualsiasi altra informazione che possa essere utile al gruppo di gestione del data breach per valutare la violazione:

Data

Firma

METODOLOGIA VALUTAZIONE DATA BREACH

Nell'ipotesi in cui, nonostante le misure di sicurezza adottate al fine di prevenire il rischio di perdita di dati si verifichi un potenziale data breach, qui di seguito la metodologia per **la valutazione della gravità delle violazioni dei dati personali** adottata dalla Regione Sardegna. Tale metodologia è stata definita sulla base delle indicazioni fornite dall'**ENISA** (European Union Agency for Network and Information Security) all'interno del documento "*Recommendations for a methodology of the assessment of severity of personal data breaches"*.

Gli elementi chiave da tenere in considerazione in sede di valutazione della gravità risultano essere i seguenti:

- *La* natura e contesto dei dati violati **(VALUTAZIONE 1)**
- *Facilità di identificazione* dell'individuo in base ai dati violati **(VALUTAZIONE 2)**
- *Circostanze della violazione* (violazione di riservatezza, integrità e disponibilità dei dati), che hanno un'influenza aggiuntiva sulla gravità di una violazione **(VALUTAZIONE 3)**

La valutazione della gravità della violazione può essere effettuata secondo le seguenti sotto fasi:

- **Valutazione 1** analizzare la criticità dell'insieme di dati violati in un contesto di elaborazione specifico;
- **Valutazione 2:** si tratta del fattore di correzione della Valutazione 1. La criticità complessiva di un trattamento dei dati può essere ridotta in base al valore identificato.
- **Valutazione 3:** quantifica le circostanze specifiche della violazione che possono essere presenti o meno in una particolare situazione. Pertanto il fattore, laddove presente, può solo incrementare la gravità di una specifica violazione. Per questo motivo il punteggio iniziale può essere ulteriormente regolato da quest'ultima valutazione
- **Valutazione 4 - Calcolo della gravità:** calcolo della gravità della violazione sulla base dei 3 precedenti elementi.

Definizione del punteggio per la natura e contesto dei dati violati (VALUTAZIONE 1)

Il punteggio della valutazione 1 *(di seguito anche "pt.1")* è al centro della metodologia e valuta la criticità dell'insieme di dati violati in un contesto di elaborazione specifico.

Nella tabella seguente sono riassunte le attività inerenti a questa fase di valutazione**:**

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
1	RPD / Gruppo di gestione data breach	Definire e Classificare i tipi di dati personali	Definisce e classifica la tipologia di dato trattato che ha subito una violazione sulla base delle seguenti quattro categorie: • dati identificativi/personali; • dati comportamentali; • dati finanziari;	Registro dei Data Breach (allegato B)

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
			• dati sensibili/particolari. Inoltre, aggiorna il Registro dei Data Breach nella sessione “Tipologia di dato trattato” (fare riferimento all’allegato B)	
2	RPD / Gruppo di gestione data breach	Attribuire il punteggio base	Attribuisce il punteggio base secondo la tabella 1 definita dalla metodologia per le categorie di natura di dato (dati identificativi/personali, dati comportamentali, dati finanziari, dati sensibili).	Tabella 1 Contesto Elaborazione Dati
3	RPD / Gruppo di gestione data breach	Aumentare o Ridurre il punteggio base secondo il contesto specifico	Aumenta o riduce il punteggio base in funzione della presenza di fattori contestuali relativi all'elaborazione dei dati (ad es. volume di dati, caratteristiche speciali dei Titolari o degli individui, inesattezza dei dati, disponibilità del dato al pubblico prima della violazione, natura del dato). Il punteggio che emerge dalla tabella 1 può variare da 1 a 4.	Tabella 1 Contesto Elaborazione Dati

Di seguito riportiamo le tabelle da utilizzare **per la determinazione del punteggio della valutazione 1:**

Tabella 1 – Natura e contesto dei dati		**Punteggio**
Dati Identificativi/ Personali	**Esempio Dati Identificativi: Data di nascita, Stato di famiglia, Studi, Lavoro, Stipendio, Inquadramento** **Esempio Dati Personali: Nome del cittadino, Numero di Telefono, Indirizzo, email, ID card, Fotografia**	
	Punteggio Base: quando la violazione riguarda "dati identificativi/personali" e il Titolare non è a conoscenza di alcun fattore aggravante.	**1**
	Il punteggio potrebbe essere **aumentato di 1**, ad esempio quando il volume di "dati identificativi/personali" e/o le caratteristiche del Titolare sono tali da consentire l'abilitazione di determinati profili o possono essere formulate assunzioni sullo stato sociale/finanziario dell'individuo.	**2**
	Il punteggio potrebbe essere **aumentato di 2**, ad esempio quando i "dati identificativi/personali" e/o le caratteristiche del Titolare possono portare a supposizioni sullo stato di salute dell'individuo, sulle preferenze sessuali, sulle convinzioni politiche o religiose.	**3**

Tabella 1 – Natura e contesto dei dati		Punteggio
	Il punteggio potrebbe essere **aumentato di 3**, ad esempio quando a causa di determinate caratteristiche dell'individuo (ad es. gruppi vulnerabili, minori), l'informazione può essere critica per la sicurezza personale o per le condizioni fisiche / psicologiche.	**4**
Dati Comportamentali	**Esempio: Abitudini, preferenze personali e interessi, vita sociale e contatti**	
	Punteggio Base: quando la violazione comporta "dati comportamentali" e il controllore non è a conoscenza di fattori aggravanti o di diminuzione.	**2**
	Il punteggio potrebbe essere **diminuito di 1**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio la combinazione di informazioni da ricerche web).	**1**
	Il punteggio può essere **aumentato di 1**, ad esempio quando il volume di "dati comportamentali" e / o le caratteristiche del controllore sono tali da consentire la creazione di un profilo dell'individuo, esponendo informazioni dettagliate sulla sua vita quotidiana e sulle sue abitudini.	**3**
	Il punteggio può essere **aumentato di 2**, ad esempio se è possibile creare un profilo basato sui dati di una persona (es. cittadini).	**4**
Dati Finanziari	**Esempio: IBAN, Numero di conto, Saldo conto, Transaction History, Informazione di base sulla carta di credito (senza CVC), Complete informazioni sulla carta di credito (con CVC), Dati sui mutui/prestiti**	
	Punteggio Base: quando la violazione riguarda "dati finanziari" e il responsabile del trattamento non è a conoscenza di fattori aggravanti o di diminuzione.	**3**
	Il punteggio potrebbe essere **diminuito di 2**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni finanziarie dell'individuo (ad esempio, il fatto che una persona sia il cliente di una determinata banca senza ulteriori dettagli).	**1**
	Il punteggio potrebbe essere **diminuito di 1**, ad esempio quando il set di dati specifici include alcune informazioni finanziarie ma non fornisce ancora informazioni significative sullo stato / sulla situazione finanziaria dell'individuo (ad esempio: i numeri di conti bancari semplici senza ulteriori dettagli).	**2**

Tabella 1 – Natura e contesto dei dati		Punteggio
	Il punteggio potrebbe essere **aumentato di 1**, ad esempio quando a causa della natura e / o del volume dell'insieme di dati specifici, vengono divulgate informazioni complete finanziarie (ad esempio: informazioni complete sulla carta di credito con il codice cvc)	**4**
Dati Sensibili/Particolari	**Esempio: Dati Sanitari, Razza / origine etnica, Orientamento politico e religioso, Orientamenti sessuali, Procedimento penale / condanna, Dati biometrici, Dati genetici**	
	Punteggio Base: quando la violazione riguarda "dati sensibili" e il controllore non è a conoscenza di alcun fattore di diminuzione.	**4**
	Il punteggio potrebbe essere **diminuito di 3**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni sui dati sensibili o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio la combinazione di informazioni da ricerche web).	**1**
	Il punteggio potrebbe essere **diminuito di 2**, ad esempio quando la natura dei dati può portare a ipotesi generali.	**2**
	Il punteggio potrebbe essere **diminuito di 1**, ad esempio quando la natura dei dati può portare a supposizioni su informazioni sensibili.	**3**

Si specifica che l'elenco dei tipi di dati descritti nelle quattro categorie non è esaustivo; tuttavia, la maggior parte dei dati coinvolti in casi reali può essere abbinata ad almeno una delle categorie.

La definizione dell'indicatore per la natura e contesto dei dati violati è il punteggio più alto raggiunto. Se i dati corrispondono a più di una categoria, è necessario seguire i passaggi sopra indicati per ogni categoria applicabile e in questi casi il valore da prendere in considerazione è il punteggio della categoria a cui è stato attribuito il valore più alto. Esempio:

- se la violazione riguarda "dati identificativi/personali" e il Titolare non è a conoscenza di alcun fattore aggravante, il punteggio da attribuire è 1;
- se la violazione riguarda anche dati comportamentali" e il Titolare non è a conoscenza di fattori aggravanti o di diminuzione, il punteggio è 2;

Pertanto, ai fini del calcolo del punteggio per la natura e contesto dei dati violati (VALUTAZIONE 1), occorre prendere in considerazione il valore 2.

<u>Definizione del punteggio per la facilità di identificazione (Valutazione 2)</u>

Il punteggio della 2^ valutazione *(di seguito anche "pt.2")* è il fattore di correzione della Valutazione 1 che tiene in considerazione la facilità di identificazione dell'individuo in base ai dati violati.

Nella tabella seguente sono riassunte le attività inerenti alla **valutazione 2:**

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
4	RPD	Valutare la facilità di identificazione dell'individuo e determinare il pt.2	Valuta la **facilità di identificazione** dell'individuo ed attribuisce un punteggio secondo la tabella 2 definita dalla metodologia secondo i seguenti quattro livelli: • trascurabile (0,25); • limitato (0,5); • significativo (0,75); • massimo (1). Il fattore di correzione pt.2 può essere 0,25 / 0,5/ 0,75 o 1. Il punteggio più basso viene attribuito quando la possibilità di identificare l'individuo è trascurabile, il che significa che è estremamente difficile abbinare i dati a una determinata persona, ma comunque potrebbe essere possibile con determinate condizioni. Al contrario, il punteggio più alto viene attribuito quando l'identificazione è possibile direttamente dai dati violati, senza alcuna ricerca specifica per determinare l'identità dell'individuo.	Tabella 2 Facilità di identificazione
5	RPD	Correggere il valore identificato in fase 1 moltiplicando con il fattore di valutazione 2	Una volta individuato il fattore di correzione, esso viene moltiplicato per il valore 1, al fine di determinare il punteggio iniziale della gravità della violazione dei dati.	Tabella 2 Facilità di identificazione

Di seguito riportiamo le tabelle da utilizzare **per la valutazione del secondo valore (valutazione 2):**

Tabella 2 - Facilità di identificazione		**Punteggio**	**Livello**
	Definizione: Facilità con cui possono essere identificati gli interessati (FI)		

Descrizioni (a titolo esemplificativo)	L'aggressione riguarda dati identificativi o dati personali **non direttamente identificabili (ad esempio: nome/cognome molto diffuso in un paese)**	**0,25**	Trascurabile
	L'aggressione riguarda i dati identificativi **di un individuo ma non facilmente identificabile (ad esempio: nome/cognome condiviso da poche persone in un intero paese)**	**0,5**	Limitata
	L'aggressione riguarda dati identificativi e **rivela ulteriori informazioni di identificazione dell'individuazione (ad esempio: nome completo con l'indicazione dell'indirizzo email di questa persona)**	**0,75**	Significativo
	L'aggressione riguarda dati identificativi o dati personali **direttamente identificativi (ad esempio: nome completo con l'indicazione della data di nascita e l'indirizzo email di questa persona)**	**1**	Massimo

La definizione del punteggio per la facilità di identificazione (Valutazione 2) è il punteggio più alto raggiunto. Se i dati corrispondono a più di una categoria, è necessario prendere in considerazione il punteggio della categoria a cui è stato attribuito il valore più alto.

Definizione del punteggio per le Circostanze della violazione (Valutazione 3)

Il punteggio della valutazione 3 quantifica le **circostanze specifiche della violazione** che possono essere presenti o meno in una particolare situazione.

Nella tabella seguente sono riassunte le attività inerenti alla **Valutazione 3 :**

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
6	RPD	Quantificare le circostanze specifiche della violazione	Attribuisce il punteggio relativo **alle circostanze della violazione** classificate secondo le seguenti macro categorie: • violazione di riservatezza; • violazione di disponibilità; • violazione di integrità dei dati; • eventuali intenzioni malevole.	Tabella 3

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
			Le circostanze possono avere solo un'influenza aggiuntiva sulla gravità di una violazione. Il pt.3 può incrementare il punteggio iniziale delle gravità di 0,25 o 0,5 a seconda dei casi.	

Di seguito riportiamo la tabella da utilizzare **per la valutazione del terzo punteggio (*di seguito "pt.3"):***

Tabella 3 - Circostanze della violazione		**Punteggio**
Violazione di riservatezza	**Definizione:** La perdita di riservatezza si verifica quando le informazioni s**ono accessibili da parti che non sono autorizzate o che non hanno uno scopo legittimo** di accedervi. L'entità della perdita di riservatezza varia a seconda della portata della divulgazione, ovvero il numero potenziale e il tipo di parti che possono avere accesso illecito all'informazione.	
	Esempi di dati esposti a rischi di riservatezza **senza prove che l'elaborazione illegale si è verificata:** - Un file cartaceo o un laptop si perde durante il transito; - L'attrezzatura è stata smaltita senza distruzione dei dati personali.	**0**
	Esempi di dati trasmessi verso un certo numero **di destinatari conosciuti:** - Un'e-mail con dati personali è stata inviata erroneamente a un certo numero di destinatari conosciuti; - Alcuni soggetti esterni (es. cittadini, rappresentanti legali di un ente) possono accedere agli account di altri in un servizio online.	**0,25**
	Esempi di dati trasmessi verso un certo numero **di destinatari sconosciuti:** - I dati sono pubblicati su una bacheca internet; - I dati vengono caricati su un sito P2P; - Un dipendente vende un CD ROM con i dati del cittadino; - Un sito Web configurato in modo errato rende accessibili pubblicamente i dati Internet dagli utenti interni.	**0,5**
Violazione di integrità	**Definizione:** La perdita di integrità si verifica **quando le informazioni originali vengono alterate** e la sostituzione dei dati può essere pregiudizievole per l'individuo. La situazione più grave si verifica quando esistono gravi possibilità che i dati modificati siano stati utilizzati in un modo che potrebbe danneggiare l'individuo.	
	Esempi di **dati modificati** ma **senza alcun uso errato o illegale** identificato: - Le registrazioni di un database con dati personali sono state	**0**

Tabella 3 - Circostanze della violazione		Punteggio
	erroneamente aggiornate ma è stata effettuata una copia dell'originale prima del verificarsi della modifica.	
	Esempi di dati modificati ed **eventualmente usati in modo errato o illegale ma con possibilità di recupero**: - Un dato necessario per la fornitura di un servizio online è stato modificato e l'individuo deve richiedere il servizio in modalità offline. - È stato modificato un dato importante per l'accuratezza del file di un individuo in un servizio medico online.	**0,25**
	Esempi di dati modificati ed **eventualmente usati in modo errato o illegale senza possibilità di recupero**: - Valgono gli esempi precedenti con l'aggravante che i dati originali non possono essere recuperati.	**0,5**
Violazione di disponibilità	**Definizione:** La **perdita di disponibilità** si verifica quando non è possibile accedere ai dati originali quando ce n'è bisogno. Può essere temporaneo (i dati sono recuperabili ma richiederà un periodo di tempo e questo può essere dannoso per l'individuo) o permanente (i dati non possono essere recuperati).	
	Esempi di dati che **possono essere recuperati senza difficoltà**: - Una copia del file è persa ma sono disponibili altre copie. - Un database è danneggiato ma può essere facilmente ricostruito da altri database.	**0**
	Esempi di **indisponibilità temporale**: - Un database è corrotto ma può essere ricostruito da altri database, sebbene sia richiesta qualche elaborazione. - Un file è perso ma l'informazione può essere fornita di nuovo dall'individuo	**0,25**
	Esempi di **indisponibilità totale** (i dati non possono essere recuperati dal controllore o dai singoli): - Un file è perso / database danneggiato, non c'è il backup di queste informazioni e non può essere fornito dall'individuo.	**0,5**
Intenzioni malevole	**Definizione:** La violazione è **dovuta a un'azione intenzionale malevola**, ad esempio al fine di causare problemi al Titolare o danneggiare gli interessati.	
	Esempi di violazione dovuta a un'azione intenzionale: - Un dipendente condivide intenzionalmente dati privati dai cittadini in un sito pubblico di social media. - Un dipendente vende dati privati dei cittadini a una società. - Un membro di un social network invia intenzionalmente delle	**0,5**

Tabella 3 - Circostanze della violazione		Punteggio
	informazioni sugli altri membri ai propri familiari al fine di danneggiarli.	

La definizione del punteggio per le Circostanze della violazione (Valutazione 3) è data dalla somma dei punteggi ottenuti per ciascuna tipologia di circostanza.

> Esempio: se è stato quantificato un punteggio di 0,5 per la violazione di riservatezza, di 0,5 per la violazione di integrità, di 0,5 per la violazione di disponibilità, di 0,5 per la violazione di intenzioni malevole, il punteggio da tenere in conto per le Circostanza della violazione (Valutazione 3) è 2.

Calcolo della gravità (Valutazione 4)

Il punteggio finale mostra il livello di gravità di una determinata violazione, tenendo conto dell'impatto sui diritti e libertà delle persone fisiche.

Nella tabella seguente sono riassunte le attività inerenti alla **fase di Calcolo della gravità (CG):**

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
7	Gruppo di gestione data breach / RPD	Procedere al Calcolo della ***Gravità = pt.1* pt.2 + pt.3***	Calcola la gravità della violazione applicando la formula definita dalla metodologia	Formula
8	RPD	Definire il livello di gravità della violazione	Definisce il livello di gravità (basso, medio, alto e molto alto) secondo il risultato finale della valutazione. Il risultato viene classificato secondo quattro livelli di gravità: • Basso (punteggio finale è inferiore a 2) • Medio (punteggio finale è tra 2 e 3) • Alto (punteggio finale è tra 3 e 4) • Molto alto (punteggio finale è superiore a 4)	Tabella livello gravità della violazione

Di seguito riportiamo le tabelle da utilizzare **per la valutazione del livello di gravità:**

Punteggio	Livello	Descrizione	Esito valutazione
Gravità < 2	**Basso**	Gli individui non saranno interessati dalla violazione o potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema (tempo trascorso a reinserire informazioni, fastidi, etc.).	Non è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, ma l'incidente deve essere annotato all'interno del registro delle violazioni.
2 ≤ Gravità < 3	**Medio**	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi dell'ente, paura, mancanza di comprensione, stress, disturbi fisici minori, etc.).	Non è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, ma devono essere adottate ulteriori misure organizzative e tecniche al fine di migliorare la sicurezza dei dati personali e deve essere annotato l'incidente all'interno del registro delle violazioni.
3 ≤ Gravità < 4	**Alto**	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, etc.).	È necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali e deve essere annotato l'incidente all'interno del registro delle violazioni.
4 ≤ Gravità	**Molto Alto**	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, etc.).	È necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, darne comunicazione ai soggetti interessati e annotare l'incidente all'interno del registro delle violazioni.