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
Art. 2 Principi generali e ambito di applicazione 2
Art. 3 Normativa di riferimento 3
Art. 4 Organigramma privacy 3
Art. 5 Titolare del trattamento 4
Art. 6 Compiti e funzioni dei Delegati del titolare 4
Art. 7 Compiti e funzioni del Referente privacy 5
Art. 8 Compiti e funzioni del Referente del Servizio e del Gruppo di lavoro privacy 6
Art. 9 Autorizzati al trattamento: compiti e istruzioni 7
Art. 10 Servizio sistemi informativi (IT) 8
Art. 11 Tenuta della postazione lavorativa e della scrivania 9
Art. 12 Responsabile Protezione dei Dati (R.P.D.) o Data Protection Officer (D.P.O.) 9
Art. 13 Registro delle attività di trattamento 10
Art. 14 Informazioni agli interessati 10
Art. 15 Sistemi di videosorveglianza 11
Art. 16 Valutazione d'impatto sulla protezione dei dati – DPIA 11
Art. 17 Violazione dei dati personali – *Data Breach* 12
Art. 18 Entrata in vigore del Regolamento e forme di pubblicità 12

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

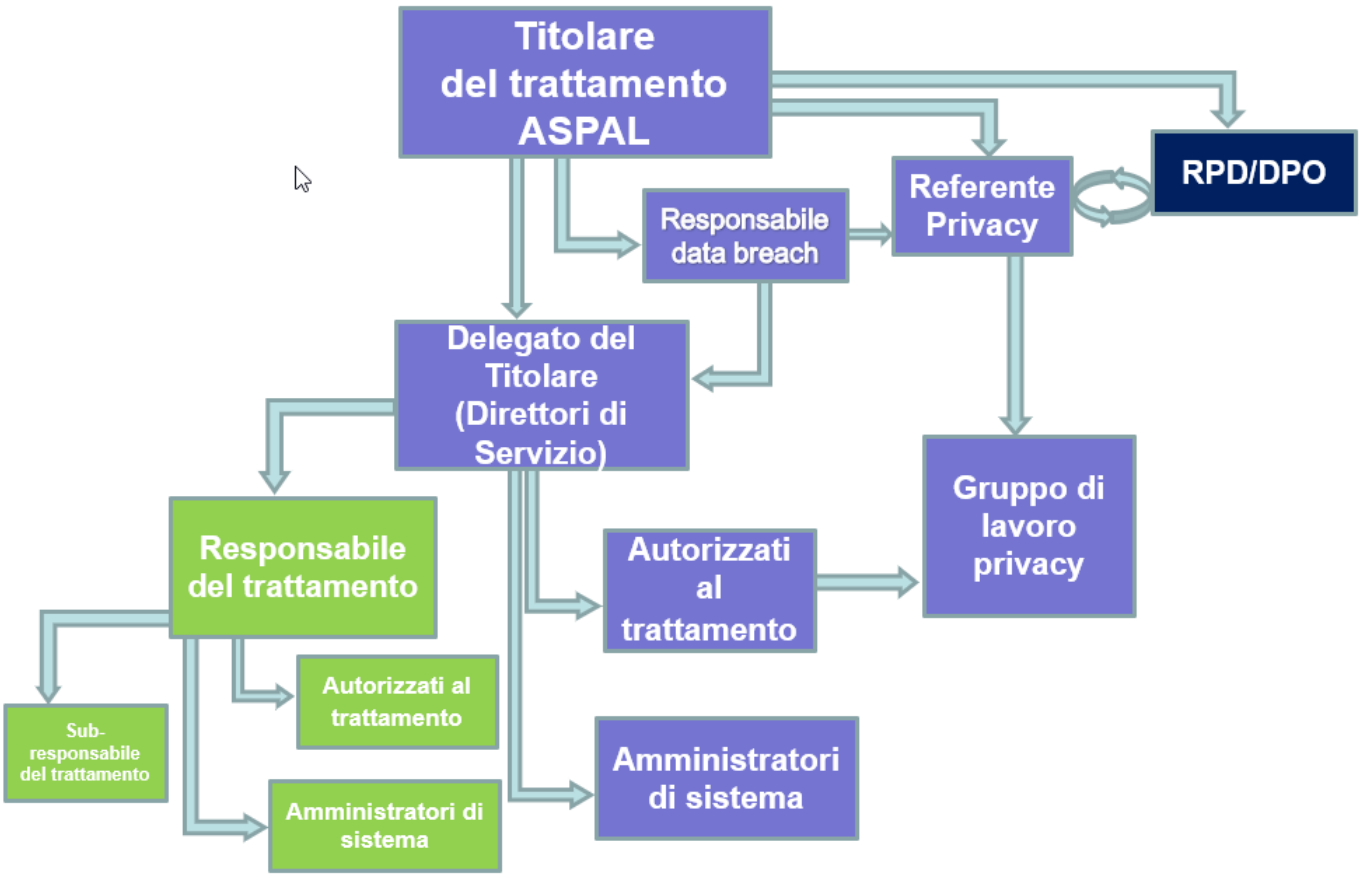
1. Il presente Regolamento interno, adottato ai sensi dello Statuto dell'ASPAL, ha per oggetto le misure organizzative e procedimentali mediante le quali l'ASPAL attua i principi e le disposizioni del Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 (di seguito indicato come 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 dipendente 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.