ARSIAL
Agenzia Regionale per lo Sviluppo
e l'Innovazione dell'Agricoltura del Lazio

DELIBERAZIONE DEL CONSIGLIO DI AMMINISTRAZIONE

N. 131/RE DEL 27 OTTOBRE 2022

PROPOSTA N. 192/RE DEL 26/10/2022

STRUTTURA COMPETENTE:	**Area Affari Legali e Gestione del Contenzioso**

OGGETTO:	Approvazione del Regolamento e dei modelli Arsial per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - Attuazione delle disciplina organizzativa di Arsial delle competenze e delle responsabilità in materia di trattamento dei dati personali di cui al Modello organizzativo privacy di Arsial approvato con deliberazione del CdA n.42/RE del 09.12.2021.

Si dichiara la conformità della presente proposta di deliberazione alle vigenti norme di legge e la regolarità della documentazione.

ESTENSORE (Paola Giansanti)	RESPONSABILE P.O. (nome e cognome)	DIRIGENTE DI AREA (avv. Maria Raffaella Bellantone)	IL DIRETTORE GENERALE F.F. (Avv. Maria Raffaella Bellantone)
Firmato: Paola Giansanti		Firmato digitalmente da MARIA RAFFAELLA BELLANTONE CN = MARIA RAFFAELLA BELLANTONE O = ARSIAL AG. REG. SVIL. INNOV. AGR. LAZIO C = IT	Firmato digitalmente da MARIA RAFFAELLA BELLANTONE CN = MARIA RAFFAELLA BELLANTONE O = ARSIAL AG. REG. SVIL. INNOV. AGR. LAZIO C = IT

IL PRESIDENTE DEL CONSIGLIO DI AMMINISTRAZIONE:

Mario Ciarla
ARSIAL AG. REG. SVIL. INNOV. AGR. LAZIO
PRESIDENTE
03.11.2022 10:43:19
GMT+01:00

Approvata con Deliberazione n. 131/RE del 27 Ottobre 2022

PUBBLICAZIONE	
N. 131/RE DELL'ALBO DELL'AGENZIA	INVIATA ALL'ORGANO DI CONTROLLO IL _____ PROT. N. _____
DATA, lì 27/10/2022	ESITO _____

REGIONE LAZIO

CONSIGLIO DI AMMINISTRAZIONE

(D.P.R.L. n. T00210 del 06 Settembre 2018; D.P.R.L. n. T00164 del 01 Ottobre 2020 - D.P.R.L. n. T00120 del 07 Giugno 2021)

Estratto del verbale della seduta del giorno 27 Ottobre 2022

L'anno duemilaventidue, il giorno 27 del mese di Ottobre nella sede centrale di ARSIAL, Via Rodolfo Lanciani n. 38, Roma, alle ore 11.00, si è riunito il Consiglio di Amministrazione.

Sono presenti: (gli assenti sono indicati con *)

Ing. Mario Ciarla - Presidente

Dott. Enrico Dellapietà - Componente

Presiede il Presidente dell'Agenzia Ing. Mario Ciarla.

Partecipa l'avv. Maria Raffaella Bellantone, Direttore Generale f.f. dell'Agenzia, con funzioni di Segretario verbalizzante.

Assiste il Collegio dei Revisori dei Conti (gli assenti sono indicati con *):

Dott. Antonio Bizzarri - Presidente

Dott.ssa Monica Vecchiati – Componente (*)

Dott. Carlo Romano – Componente (*)

DELIBERAZIONE N. 131/RE

OGGETTO:	Approvazione del Regolamento e dei modelli Arsial per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - Attuazione delle disciplina organizzativa di Arsial delle competenze e delle responsabilità in materia di trattamento dei dati personali di cui al Modello organizzativo privacy di Arsial approvato con deliberazione del CdA n.42/RE del 09.12.2021.

IL CONSIGLIO DI AMMINISTRAZIONE

VISTA la Legge Regionale 10 gennaio 1995, n. 2, concernente l'Istituzione dell'Agenzia per lo Sviluppo e l'Innovazione dell'Agricoltura del Lazio (ARSIAL) e ss.mm.ii.;

VISTO il Decreto del Presidente della Regione Lazio n. T00210 del 06 Settembre 2018, con il quale è stato nominato il Consiglio di Amministrazione dell'Agenzia per lo Sviluppo e l'Innovazione dell'Agricoltura del Lazio (ARSIAL), nelle persone del Dott. Antonio Rosati, della Dott.ssa Angela Galasso e del Dott. Mauro Uniformi, ed è stato, altresì, nominato quale Presidente, con deleghe gestionali dirette, il Dott. Antonio Rosati;

VISTO il Decreto del Presidente della Regione Lazio n. T00164 del 01 Ottobre 2020, con il quale l'Ing. Mario Ciarla, è stato nominato Presidente del Consiglio di Amministrazione dell'Agenzia per lo Sviluppo e l'Innovazione dell'Agricoltura del Lazio (ARSIAL), con deleghe gestionali dirette, in sostituzione del dimissionario Dott. Antonio Rosati;

PRESO ATTO delle dimissioni presentate dal Dott. Mauro Uniformi in data 13 Maggio 2021;

VISTO il Decreto del Presidente della Regione Lazio n. T00120 del 07 Giugno 2021, con il quale il Dott. Enrico Dellapietà, è stato nominato Componente del Consiglio di Amministrazione dell'Agenzia per lo Sviluppo e l'Innovazione dell'Agricoltura del Lazio (ARSIAL), in sostituzione del dott. Mauro Uniformi, dimissionario;

VISTO il verbale del 30/06/2022, con il quale il Consiglio di Amministrazione dell'Agenzia ha preso atto che con nota prot. 6799 del 16/06/2022, la d.ssa Angela Galasso ha rassegnato le proprie dimissioni e che dette dimissioni sono state regolarmente trasmesse agli organi regionali competenti, per gli adempimenti conseguenti;

VISTA la Deliberazione del Consiglio di Amministrazione 18 luglio 2022, n. 73/RE, con la quale, in virtù dei poteri conferiti al C.d.A., è stato nominato Direttore Generale facenti funzioni di ARSIAL l'Avv. Maria Raffaella Bellantone;

VISTA la Determinazione del Direttore Generale 14 Luglio 2022, n. 568/RE, con la quale è stato prorogato, per ulteriori anni due (2), l'incarico di responsabile della direzione dell'Area Risorse Umane, Pianificazione, Formazione, Affari Generali,

conferito, con decorrenza 12 Agosto 2019, alla Dott.ssa Patrizia Bergo, giusta Determinazione del Direttore Generale 01 Agosto 2019, n. 533;

VISTA la Legge Regionale 30 Dicembre 2021, n. 21, con la quale è stato approvato il Bilancio di Previsione della Regione Lazio 2022-2024, nonché il bilancio di Previsione Finanziario esercizi 2022-2024, approvato da ARSIAL con deliberazione del Consiglio di Amministrazione n. 44/RE del 15 Dicembre 2021, avente ad oggetto: "Approvazione e adozione del Bilancio di previsione 2022-2024";

VISTA la Deliberazione del CdA 31 Gennaio 2022, n. 1/RE, con la quale è stata disposta "l'approvazione dei dati di preconsuntivo 2021. Aggiornamento del risultato presunto di amministrazione ai sensi del D.lgs. 118/2011, all. 4/2, punto 9.2 – Bilancio 2022/2024";

VISTE le Deliberazioni del CdA 24 Marzo 2022, n. 27/RE, e 06 Maggio 2022, n. 45/RE, con le quali sono stati approvati, ai sensi dell'art. n. 3, comma 4, del D.lgs. n. 118/2011 ed in ossequio al principio contabile all. 4/2 al citato decreto, punto 9.1, rispettivamente il "Riaccertamento ordinario dei residui attivi e passivi al 31.12.2021 e dei residui perenti ", e la "Integrazione al Riaccertamento ordinario dei residui attivi e passivi al 31.12.2021 e dei residui perenti ex art. 3, comma 4 del D.lgs. 118/2011 e s.m.i.";

VISTA la Deliberazione del CdA 28 Marzo 2022, n. 30/RE con la quale è stata apportata, ai sensi dell'art. 51 del D.lgs. 118/2011, nonché, dell'art. 24, comma 2°, del Regolamento Regionale di contabilità del 9 novembre 2017, n. 26, la variazione n. 1 al "Bilancio di previsione 2022-2024;

VISTA la Deliberazione del CdA 30 Maggio 2022, n. 56/RE, con la quale è stato approvato, il "Rendiconto di gestione per l'annualità 2021";

VISTA la Deliberazione del CdA 16 Settembre 2022, n. 104/RE con la quale è stata adottata la variazione n. 3 – Bilancio di previsione 2022-2024 – Assestamento generale di bilancio - Verifica salvaguardia equilibri di bilancio 2022-2024";

VISTO il D.lgs. 14 marzo 2013, n. 33, e ss.mm.ii.;

VISTI:

-il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che ha abrogato la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);

-il Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), come modificato dal Decreto legislativo 10 agosto 2018, n. 101 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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), che ha introdotto significative modifiche al vecchio Codice in materia di protezione dei dati personali;

PREMESSO che il GDPR detta un'articolata previsione normativa in materia di protezione dei dati personali, prevedendo diversi obblighi ed adempimenti a carico dei soggetti

che trattano i dati personali, ivi comprese le Pubbliche Amministrazioni, introducendo il principio della "responsabilizzazione" (*accountability)* dei soggetti stessi, ossia, l'adozione di comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento tramite una serie di attività specifiche e dimostrabili, ed in particolare, tra l'altro:

-di avere adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza corrispondente al rischio;

-di conformare i trattamenti dei dati ai principi ed alle disposizioni del GDPR medesimo;

-di predisporre ed aggiornare costantemente il registro delle attività di trattamento, contenente tutte le informazioni di cui all' art. 30 del GDPR ("*Registri delle attività di trattamento*") nonché la descrizione di tutte le misure di sicurezza, tecniche ed organizzative, adottate, da esibire, su richiesta, all' Autorità Garante;

-di tenere, ai sensi dell' art. 25 *("Protezione fin dalla progettazione e protezione dei dati per impostazione predefinita"),* un approccio basato sul rischio criteri "*data protection by default and by design",* ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "*al fine di soddisfare i requisiti*" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati:

- di sviluppare nuove politiche di gestione dei dati personali, utilizzando strategie organizzative e tecnologie orientate all'ampliamento dei diritti a favore degli interessati; un approccio alla protezione dei dati basato sul principio di responsabilizzazione di "*Protection Policy*" (un documento che indica la modalità del trattamento dei dati personali) e linee guida in merito alla revisione dei processi e dei comportamenti organizzativi nel rispetto dei principi fondamentali per tutti i trattamenti che coinvolgono dati personali;

VISTA la deliberazione del CdA n. 42/RE del 09/12/2021 avente il seguente oggetto: "*Linee di indirizzo per l'adeguamento dell'organizzazione Arsial alle norme in materia di privacy e per l'assetto dei livelli di responsabilità e contestuale definizione delle policy fondamentali in tema di trattamento dei dati personali. Individuazione e nomina Soggetto designato e individuazione Struttura interna referente privacy*", con la quale, tra l'altro, si individuavano le figure coinvolte nei trattamenti di dati personali (ciascuno con funzioni e compiti differenti), a garanzia dell'osservanza dei principi sulla protezione dei dati e del rispetto degli obblighi di trasparenza, con puntuale definizione delle responsabilità correlate, ai fini della corretta attuazione del Regolamento (UE) 2016/679 (*General Data Protection Regulation* -GDPR), della normativa privacy, conformemente alla legge istitutiva di ARSIAL n. 2 del 10/01/1995, in conformità con il modello della Regione Lazio di cui alla deliberazione della Giunta Regionale n. 733 del 27/10/2020, ed in particolare:

-Titolare del trattamento dei dati personali, ai sensi dell'articolo 4, n. 7), e dell'art. 24 ("*Responsabilità del titolare del trattamento*") del GDPR, ARSIAL: rappresentato dal Consiglio di Amministrazione (CdA) **"***cui spettano tutte le attività demandate al Titolare dal GDPR e, in particolare, l'adozione di misure tecniche e organizzative idonee a garantire, nonché a consentire di dimostrare,*

che il trattamento dei dati personali sia effettuato conformemente al GDPR medesimo (…)";

-**Soggetto Designato al trattamento dei dati personali** (anche con riferimento specifico alla previgente figura del "responsabile [interno]" del trattamento), che presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, individuato nel Direttore Genrale di Arsial, designato mediante atto di nomina, a firma del Titolare del trattamento, Arsial, rappresentata dal CdA, tramite il proprio Presidente;

- Struttura interna referente privacy individuata nell' Area Affari Legali e Gestione del Contenzioso, *"alla quale il Direttore Generale deve attribuire, con proprio atto organizzativo, gli ulteriori specifici compiti in materia di privacy, nelle more dell'adozione della riorganizzazione delle strutture di Arsial, per il necessario supporto, al Titolare e allo stesso Soggetto designato, nello svolgimento dei compiti e funzioni conferiti in materia di trattamento dei dati personali (…) in modo da garantire un presidio ed una competenza professionale adeguata per gli adempimenti continuativi, riguardanti gli aspetti normativi, organizzativi e procedurali, nonché per il costante coordinamento con le attività del DPO*";

ATTESO che nella sopracitata deliberazione si disponeva che "*il modello organizzativo, così come approvato con la presente deliberazione, sarà reso operativo, in ottemperanza alla presente Deliberazione, tramite (…) l'adozione di pedissequo ed apposito Regolamento dove verranno indicati nel dettaglio tra l'altro, gli adempimenti in materia di privacy con adozione di schemi tipo per garantire l'applicazione uniforme della disciplina in materia di privacy anche relativamente alla nomina dei soggetti sopra indicati. Tale Regolamento disciplinerà, nel dettaglio, tutte le competenze e le responsabilità in materia di trattamento dei dati personali sopra esposte e sarà vigente ed obbligatorio sia nei confronti di i dipendenti di ARSIAL sia nei confronti di tutti i soggetti passivi ed attivi che entrano in rapporto con l'Agenzia"*;

VISTA la determinazione direttoriale n. 383/RE del 20/12/2021 con la quale il Direttore Generale, nella veste di soggetto designato, attribuiva formalmente all'Area Affari Legali e Gestione del Contenzioso attribuiva, al fine di dare operatività al modello organizzativo privacy di cui alla deliberazione del CdA n. n.42/RE del 09.12.2021, la "Struttura interna referente privacy" e le ulteriori specifiche competenze in materia di privacy, ivi dettagliatamente indicate;

CONSIDERATO che, tra i compiti attribuiti alla Struttura interna referente privacy, rientra anche la predisposizione di tutti gli atti necessari (proposte regolamenti, schemi atti, comunicazioni, disciplinari, ecc.) in modo da garantire un presidio ed una competenza professionale adeguata per gli adempimenti continuativi, riguardanti gli aspetti normativi, organizzativi e procedurali, nonché per il costante coordinamento con le attività del DPO;

PREMESSO, altresì, che la Struttura Referente Privacy ha provveduto ad istruire e finalizzare la procedura per l'individuazione obbligatoria, per l' Agenzia, come Ente Pubblico, del Responsabile della protezione dei dati personali (RDP o DPO) di Arsial, provvedendo ad individuare, tramite l'elaborazione di un capitolato tecnico strutturato sulle esigenze dell' organizzazione specifica di Arsial, un

soggetto esterno a cui affidare l'incarico, formalizzato con determinazione di affidamento dell'incarico n. 556/RE del 1/07/2022 e successiva deliberazione del CdA di designazione nella veste di Titolare del Trattamento n. 87/RE del 27/07/2022 (entrambe ad istruttoria e proposta dell' Area Affari Legali), per la garanzia dell'effettivo assolvimento dei compiti all'uopo fissati dal GDPR;

VISTE:

-la Deliberazione del Consiglio di Amministrazione n. 16/RE con la quale venivano formalizzati alla Direzione Generale gli Obiettivi Strategici per l'anno 2022;

-la determinazione del Direttore Generale n. 188/RE del 16 Marzo 2022, con la quale venivano assegnati gli Obiettivi Operativi a ciascuna Area ed agli Staff dell'Agenzia;

CONSIDERATO che:

-l'obiettivo strategico n.1 assegnato all' Area Affari Legali e Gestione del Contenzioso "*Applicazione della normativa in materia di protezione dei dati personali*", ha il seguente parametro: "*Predisposizione disciplina organizzativa delle competenze e delle responsabilità di Arsial in materia di trattamento dati personali. Indicatore: Proposta di deliberazione per il Cda entro il 31/10/2022*";

- l'obiettivo strategico n.2 assegnato all'Area Affari Legali e Gestione del Contenzioso "*Applicazione della normativa in materia di protezione dei dati personali*", ha il seguente parametro: "*Predisposizione schemi ed informative per vari soggetti interni ed esterni coinvolti nella disciplina del Trattamento dei dati personali Indicatore: Proposta di deliberazione per il Cda entro il 31/10/2022*";

ATTESO che l'Area Affari Legali e Gestione del Contenzioso ha predisposto, sulla scorta del modello organizzativo e gestionale delineato con la sopracitata deliberazione n. 42/RE/2021:

- il testo del "*Regolamento Arsial per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali – attuazione della disciplina organizzativa di Arsial delle competenze e delle responsabilità in materia di trattamento dei dati personali"*, in cui sono state dettagliatamente descritte e regolamentate, in aderenza al modello Regionale di cui alla deliberazione della Giunta Regionale n. 733 del 27/10/2020 le macroaree privacy di rilievo, ed in particolare:

  -disposizioni generali in tema di trattamento dei dati personali da parte di Arsial, principi generali in tema di trattamento dei dati personali, definizioni normative e legali, presupposti e finalità del trattamento;
  -modello organizzativo, in cui sono state descritte le figure di spicco e di maggior rilievo interessate alla normativa di che trattasi (a puro titolo esemplificativo: Titolare del Trattamento, Designato al trattamento, DPO, Responsabile del Trattamento, interessati, etc…)
  -tematica della sicurezza e protezione dati;
  -organizzazione interna ed adempimenti vari in tema di privacy;

- i modelli, i disciplinari, le informative necessari all' applicazione del Regolamento di che trattasi e riferiti ai diversi soggetti interni ed esterni coinvolti

nella disciplina del trattamento dei dati personali e, in particolare dei seguenti modelli:

- Registro dei trattamenti,
- Disciplinare tecnico amministratori di sistema,
- Informativa Policy per la gestione delle istanze degli interessati,
- Addendum al contratto di lavoro e nomina soggetto designato al trattamento,
- Nomina per la persona autorizzata al trattamento,
- Nomina per l'amministratore di sistema interno,
- Informativa ai sensi dell'art. 13 del RGPD,
- Informativa per i visitatori del sito istituzionale,
- Informativa per i visitatori negli uffici di Arsial,
- nomina per il responsabile del trattamento;

ATTESO che i sopracitati documenti, elaborati dalla Struttura Referente Privacy a seguito di approfondito studio della normativa internazionale ed interna, delle pronunce del Garante Europeo ed Italiano, della prassi internazionale e nazionale e, da ultimo, delle casistiche di specie, sono stati trasmessi per la condivisione del Responsabile della protezione dei dati di Arsial (anche in tema di definizione del cd "*assessment*" dell'Agenzia, attualmente in itinere, ai fini della realizzazione del programma privacy di Arsial), che ha asseverato, con proprie osservazioni, con mail del 20 ottobre 2022;

RITENUTO di approvare i seguenti documenti, ai fini della corretta attuazione del Regolamento (UE) 2016/679 (*General Data Protection Regulation*, di seguito GDPR) della normativa privacy, in armonia con la legge istitutiva di ARSIAL n. 2 del 10/01/1995, in conformità con il modello della Regione Lazio di cui alla deliberazione della Giunta Regionale n. 733 del 27/10/2020, ed in osservanza di quanto disposto con la deliberazione del CdA n. 42/RE del 9 dicembre 2021 recante le "*Linee di indirizzo per l'adeguamento dell'organizzazione Arsial alle norme in materia di privacy e per l'assetto dei livelli di responsabilità e contestuale definizione delle policy fondamentali in tema di trattamento dei dati personali. Individuazione e nomina Soggetto designato e individuazione Struttura interna referente privacy*":

- testo del "*Regolamento Arsial per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - disciplina organizzativa di Arsial delle competenze e delle responsabilità in materia di trattamento dei dati personali*";

-modelli, disciplinari, informative necessari all' applicazione del Regolamento sopracitato ed ad esso allegati (n. 10 allegati), riferiti ai diversi soggetti interni ed esterni coinvolti nella disciplina del trattamento dei dati personali dell' Agenzia,

allegati alla presente Deliberazione e di cui ne costituiscono parte integrante, predisposti a cura ed istruttoria dell' Area Affari Legali e Gestione del Contenzioso nella veste di Struttura interna referente privacy ed asseverati e condivisi formalmente dal DPO di Arsial;

SU PROPOSTA dell'Area Affari Legali e Gestione del Contenzioso anche nella qualità di Struttura interna referente privacy;

CON VOTO Unanime;

D E L I B E R A

In conformità con le premesse che formano parte integrante e sostanziale del dispositivo della presente deliberazione,

DI APPROVARE i seguenti documenti, ai fini della corretta attuazione del Regolamento (UE) 2016/679 (*General Data Protection Regulation*, di seguito GDPR), della normativa privacy, in armonia con la legge istitutiva di ARSIAL n. 2 del 10/01/1995, in conformità con il modello della Regione Lazio di cui alla deliberazione della Giunta Regionale n. 733 del 27/10/2020, ed in osservanza di quanto disposto con la deliberazione del CdA n. 42/RE del 9 dicembre 2021 recante le "*Linee di indirizzo per l'adeguamento dell'organizzazione Arsial alle norme in materia di privacy e per l'assetto dei livelli di responsabilità e contestuale definizione delle policy fondamentali in tema di trattamento dei dati personali. Individuazione e nomina Soggetto designato e individuazione Struttura interna referente privacy*":

- testo del "*Regolamento Arsial per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - disciplina organizzativa di Arsial delle competenze e delle responsabilità in materia di trattamento dei dati personali*";

-modelli, disciplinari, informative necessari all' applicazione del Regolamento sopracitato ed ad esso allegati (tot 10 allegati), riferiti ai diversi soggetti interni ed esterni coinvolti nella disciplina del trattamento dei dati personali dell'Agenzia;

allegati alla presente Deliberazione e di cui ne costituiscono parte integrante, predisposti a cura ed istruttoria dell' Area Affari Legali e Gestione del Contenzioso nella veste di Struttura interna referente privacy ed asseverati e condivisi formalmente dal DPO di Arsial;

DI DEMANDARE al Direttore Generale, quale soggetto designato ai fini del GDPR ed alla Struttura Interna referente privacy di Arsial, il compimento di tutti gli atti conseguenti alla pubblicazione della presente deliberazione per la piena operatività delle disposizioni ivi contenute, nonché provvedere, stante la necessità e/o l'opportunità successiva, ad aggiornare il testo e i modelli approvati quali linee di indirizzo, per parti non sostanziali, o a seguito di modifiche normative cogenti.

Soggetto a pubblicazione				Tabelle			Pubblicazione documento	
Norma/e	Art.	c.	l.	Tempestivo	Semestrale	Annuale	Si	No
D.lgs.33/2013	12	I		X			X	
D.lgs.33/2013	23				X		X	

REGOLAMENTO ARSIAL PER L'ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

DISCIPLINA ORGANIZZATIVA DI ARSIAL DELLE COMPETENZE E DELLE RESPONSABILITÀ IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali è effettuato da Arsial secondo le norme contenute nel 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 (Regolamento generale sulla protezione dei dati), di seguito RGPD, e nel decreto legislativo 20 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE) e successive modificazioni."

Premesso che:

-con deiberazione del CdA n. 42/RE del 09/12/2021 avente il seguente oggetto: **"***Linee di indirizzo per l'adeguamento dell'organizzazione Arsial alle norme in materia di privacy e per l'assetto dei livelli di responsabilità e contestuale definizione delle policy fondamentali in tema di trattamento dei dati personali. Individuazione e nomina Soggetto designato e individuazione Struttura interna referente privacy*", venivano fornite linee di indirizzo e istruzioni, al personale, ognuno per propri qualifica, ruolo e/o competenze ed in particolare ai soggetti designati di Arsial, finalizzate a dare formale attuazione agli obblighi introdotti dal Regolamento (UE) 2016/679 del Parlamento Europeo relativo alla *"Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati)*", provvedendo all'adeguamento formale dei propri atti organizzativi, aggiornando l'assetto dei livelli di responsabilità in materia di privacy, anche in aderenza al modello organizzativo regionale, di cui alla deliberazione della Giunta Regionale n. 733 del 27/10/2020, definendo le *policy* fondamentali di Arsial per uniformare le attività e rendere effettivo l'esercizio dei diritti degli interessati, in riferimento a tutti i trattamenti che coinvolgono dati personali, con adozione del modello citato e contestuale revoca dei pregressi provvedimenti amministrativi ed organizzativi adottati dall' Agenzia;

Ritenuto che:

- è necessario procedere all'attuazione dell' assetto organizzativo privacy dell' Agenzia, finalizzato all'adozione delle migliori strategie volte a presidiare i trattamenti effettuati, superando il previgente approccio meramente adempimentale, incentrato sulla sola adozione delle misure "minime" di sicurezza, a favore di un sistema organizzativo unitario ed omogeneo, capace di valorizzare le specificità delle diverse strutture dell'Agenzia e le differenti tipologie di trattamento dei dati, nonché identificare i distinti ruoli che dovranno presidiare le attività ed i processi organizzativi interni;

-la concreta attuazione del principio di accountability, richiede rendere prontamente operativo il nuovo assetto organizzativo privacy di Arsial, al fine di consentire a tutte le Strutture dell'Agenzia il tempestivo adeguamento e allineamento con la disciplina introdotta;

Visto il Piano Integrato di Attività e Organizzazione (PIAO) di Arsial 2022-2024;

Arsial adotta la seguente

DISCIPLINA

Capo I - Disposizioni generali

Art. 1 Oggetto

1. La presente disciplina sul modello organizzativo in materia di protezione dati personali di cui alla deliberazione CDA n. 42 del 9 dicembre 2021 regolamenta l'assetto di *governance* e le disposizioni procedimentali per l'adeguamento di Arsial (di seguito anche "Agenzia" o "Ente") al Regolamento UE del 27 aprile 2016 n. 679 relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali (di seguito anche "Regolamento 2016/679 o "RGPD") e al D.Lgs. n. 196 del 30 giugno 2003 *"Codice in materia di protezione dei dati personali"* e ss.mm.ii., nonché alle norme speciali, al fine di assicurare la migliore funzionalità ed efficacia dell'attuazione del RGPD, nonché la libera circolazione di dati personali in Arsial.
2. I dati personali sono trattati secondo quanto disposto dalla presente Disciplina.

2 Disposizioni generali in tema di trattamento dei dati personali da parte di Arsial

1. Il trattamento di dati personali da parte di Arsial è consentito esclusivamente per svolgere le funzioni istituzionali o gestionali ad esse correlate.
2. Effettuando operazioni di trattamento dei dati personali, Arsial osserva i presupposti e i limiti stabiliti dalla normativa vigente in materia della protezione dei dati personali, con particolare riferimento al "*Codice in materia di protezione dei dati personali*" di cui al Decreto Legislativo 30.06.2003, n. 196 e s.m.i., tenendo conto della diversa natura dei dati personali conferiti..
3. Il trattamento dei dati avviene nel rispetto dei diritti e delle libertà fondamentali dell'interessato ed è compiuto quando, per lo svolgimento delle finalità di interesse pubblico perseguito da Arsial, non è possibile il trattamento dei dati anonimi oppure di dati personali non sensibili o non giudiziari.
4. Il trattamento dei dati personali di cui Arsial è Titolare, avviene nel rispetto e a garanzia dei principi di cui all'art. 5 del RGPD.

Art. 3 Principi generali in tema di trattamento dei dati personali

1. Ogni trattamento di dati personali deve avvenire nel rispetto dei principi introdotti all'articolo 5 del Regolamento (UE) 2016/679 ed in particolare:
   a) liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
   b) limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità iniziali della raccolta dei dati;
   c) minimizzazione dei dati: ossia, i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
   d) esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
   e) limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
   f) integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.
2. Il Regolamento UE 2016/679, e in particolare l'articolo 5, paragrafo 2, impone al titolare di rispettare i predetti principi e di essere "*in grado di comprovarlo*", secondo il principio *responsabilizzazione* (o *accountability*) che viene poi esplicitato ulteriormente dall'articolo 24, paragrafo 1, del Regolamento, dove si afferma che "*il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento*". Si determina un approccio di responsabilizzazione sostanziale, con l'espressa indicazione di una "*Data Protection compliance*" basata su metodologie di valutazione del rischio e che deve essere integrata nei processi dell'Ente. Nella fattispecie, il presente Disciplinare realizza un "approccio preventivo, proattivo e non più reattivo", con focus su obblighi e comportamenti che

devono prevenire in modo effettivo il possibile evento di danno, configurandosi sulle specificità dei diversi trattamenti cui si riferiscono.

3. Altri principi rilevanti:
   - il principio del risk based approach: richiede in generale il prerequisito per l'individuazione delle misure tecniche e organizzative adeguate;
   - i principi di privacy by design e privacy by default (tutela dei dati personali fin dalla fase di progettazione e per impostazione predefinita) di cui all'art. 25 del Regolamento EU 2016/679: prevede che per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini;
   - principio della tutela dei diritti degli interessati di cui agli artt. da 12 a 23 del Regolamento EU 2016/679. I diritti esercitabili dall'interessato sono:
   a) diritto di ottenere informazioni dell'esistenza del trattamento e delle sue finalità;
   b) diritto di accesso;
   c) diritto di rettifica;
   d) diritto all'oblio;
   d) limitazione del trattamento;
   f) portabilità dei dati;
   g) opposizione al trattamento;
4. L'osservanza dei predetti principi è di fondamentale importanza per assicurare che le misure tecniche e organizzative siano adottate ed integrate fin dalla progettazione (ideazione) dei sistemi che ne prevendono raccolta e utilizzo, al fine di valutare i rischi di minacce che possono generare violazioni dei dati personali, per prioritizzare gli interventi, per avere la garanzia della liceità del trattamento, per monitorare costantemente le misure di sicurezza ed i trattamenti, per rendere i dipendenti e/o collaboratori consapevoli del valore del dato attraverso la formazione e la corretta applicazione di istruzioni ad hoc ed, infine, per garantire che quest'ultimi si impegnino alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza.

Art. 4 Definizioni

1. Al fine dell'applicazione della normativa vigente a tutela delle persone fisiche con riguardo ai trattamenti dei dati personali, si definisce come:

a) **dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

b) **categorie particolari di dati personali c.d. dati sensibili**: ogni informazione che concerne la sfera personale delle persone fisiche che rilevi: origine razziale o etnica; opinioni politiche; convinzioni religiose o filosofiche; appartenenza sindacale; stato di salute; vita e orientamento sessuale; dati genetici; dati biometrici intesi a identificare in modo univoco una persona fisica;

c) **trattamento dei dati**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

d) **archivio**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

e) **violazione dei dati personali c.d. data breach:** 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;

f) **titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro

organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
g) **responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
h) **soggetto designato al trattamento**: persona fisica che opera sotto la responsabilità e nell'ambito dell'assetto organizzativo del titolare del trattamento, alla quale sono attribuiti specifici compiti e funzioni connessi al trattamento di dati personali, nominata dal titolare del trattamento e che presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, mediante atto di nomina, contenente compiti e funzioni, a firma del Titolare del trattamento;
i) **responsabile della protezione dei dati personali (RPD):** soggetto interno (funzionario di Arsial) o soggetto esterno, caratterizzato da indipendenza, identificato dal Titolare, autorizzato ai seguenti compiti:
a) informare e fornire consulenza al titolare del trattamento nonché al personale in servizio presso Arsial, autorizzato, che esegue il trattamento, in merito agli obblighi derivanti dal Regolamento 2016/679, nonché da altre disposizioni di legge relative alla protezione dei dati;
b) sorvegliare l'osservanza del Regolamento 2016/679, di altre disposizioni di legge relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento 2016/679;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
j) **autorizzato al trattamento dei dati personali**: persona fisica, dipendente o collaboratore dell'Ente, che effettua materialmente le operazioni di trattamento sui dati personali sotto l'autorità del titolare del trattamento, a ciò autorizzata con specifico atto dal Titolare del trattamento o dal Soggetto designato al trattamento;
l) **struttura interna referente privacy:** struttura interna dell'Ente alla quale viene attribuita, con atto organizzativo, la funzione di supporto al Soggetto designato al trattamento nello svolgimento dei compiti e funzioni conferiti in materia di trattamento dei dati personali, al fine di assicurare un presidio ed una competenza professionale adeguata per gli adempimenti continuativi, riguardanti gli aspetti normativi, organizzativi e procedurali, nonché per il costante coordinamento con le attività del responsabile della protezione dei dati (RPD). All'interno della struttura interna referente privacy il soggetto designato individua e nomina come soggetto coordinatore il dirigente medesimo o un funzionario a tempo indeterminato dell' Agenzia, dotato di alte professionalità e competenze specialistiche, con assunzione di relative responsabilità per lo svolgimento di funzioni di coordinamento, gestione attività della struttura interna referente privacy e con elevato grado di autonomia gestionale ed organizzativa;
m) **amministratore di sistema:** figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (c.d. Enterprise resource planning) utilizzati in enti e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" (G.U. n. 300 del 24 dicembre 2008) e s.m.i.;
n) **struttura per i sistemi informativi (ICT -Information Communication Technology):** struttura competente in materia di sistemi informativi, ovvero la struttura ICT, che svolge un ruolo di supporto al Titolare e al Responsabile della protezione dei dati, in tema di risorse strumentali e di competenze in materia di patrimonio informativo ed, in particolare, in materia di gestione della sicurezza delle informazioni;
o) **interessato**: persona fisica identificata o identificabile a cui si riferiscono i dati personali;
p) **consenso dell'interessato:** qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante

dichiarazione o azione positiva inequivocabile che I dati personali che lo riguardano siano oggetto di trattamento;

q) **destinatari del trattamento:** persona fisica, giuridica, servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi, ai sensi dell'art. 51 del Regolamento 2016/679;

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

s) autorità di controllo, l'autorità pubblica indipendente istituita da uno Stato membro.

Art. 5 Presupposti di liceità del trattamento e finalità

1. I trattamenti sono effettuati dall'Ente in conformità ai principi generali di cui all'art. 5 del Regolamento 2016/679, il quale prescrive, in particolare, che i dati personali debbano essere trattati "*in modo lecito, corretto e trasparente nei confronti dell'interessato*".
   Il principio di liceità, ai sensi dell'art 6 del Regolamento 2016/679 prevede, nello specifico, che ogni trattamento deve trovare fondamento in un'idonea base giuridica.
2. In particolare il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
   a) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito l'Ente e, in particolare, nell'esercizio di funzioni amministrative per servizi di competenza regionale affidate dalla legge istitutiva di Arsial allo stesso Ente;
   b) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto l'Ente;
   c) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso interessato;
   e) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
   f) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.
3. Rientrano in questo ambito, a titolo esplicativo, ma non esaustivo, i trattamenti compiuti su:
   -dati anagrafici e di contatto degli utenti dei Sistemi Informativi di Arsial al fine di assegnare agli stessi le credenziali di accesso a detti sistemi in linea con il profilo di autorizzazione attribuito;
   -dati di navigazione degli utenti del sito istituzionale di Arsial nonché dei Siti Tematici afferenti all'Agenzia stessa (indirizzi IP, nomi a dominio dei computer e/o dei terminali utilizzati, parametri relativi al sistema operativo e/o ambiente informatico utilizzato dagli utenti, ecc.)
   -dati anagrafici, di contatto, relativi alle retribuzioni, alla salute e, più in generale, tutte le informazioni personali relative ai dipendenti di Arsial necessari per la gestione del rapporto di lavoro (ossia tutti i dati trattati per mezzo del sistema di protocollazione e/o dei sistemi utilizzati per la gestione del personale e relative retribuzioni);
   -dati anagrafici, di contatto, di fatturazione, relativi ai compensi e, più in generale, tutte le informazioni relative ai consulenti/collaboratori esterni, ai legali rappresentanti dei fornitori di Arsial e a tutti i soggetti che interagiscono a qualsiasi titolo con l'Agenzia stessa (affittuari/concessionari di immobili) necessari per la gestione dei rapporti contrattuali (ossia tutti i dati trattati per mezzo del sistema di gestione del bilancio, del sistema di protocollazione e/o dei sistemi utilizzati per la gestione della contabilità aziendale);
   -dati e informazioni afferenti a tutti coloro che operano in nome e per conto di Arsial e/o che interagiscono a qualsiasi titolo con la stessa (ossia i dati trattati per mezzo del sistema di protocollazione afferenti ai Responsabili/Referenti/Dirigenti di Arsial e/o dell'Amministrazione regionale e/o degli enti pubblici collegati alla stessa e/o all'Agenzia).
   -dati anagrafici, di contatto e informazioni varie afferenti ai produttori e/o legali rappresentanti di Aziende (ossia gli utenti dell'Agenzia) che operano nel settore Agro-Alimentare e Agricolo, ivi compresi i beneficiari di contributi, che usufruiscono delle attività e dei servizi erogati da Arsial

nell'ambito delle proprie competenze istituzionali. A titolo esemplificativo, sono trattati tutti i dati e le informazioni degli utenti di Arsial necessari ai fini dell'erogazione dei suddetti servizi da parte dell'Agenzia stessa, quindi informazioni di tipo contabile, reddituale (es per la concessione di contributi), afferenti al settore di produzione (es agricolo o Agroalimentare), afferenti all'ubicazione della specifica attività di settore (es ubicazione del terreno agricolo) e, più in generale, ogni informazione relativa ai suddetti interessati necessaria per fornire il servizio richiesto.

4. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina, dal contratto sottoscritto con l'interessato o, nel caso del trattamento basato sul consenso dell'interessato, dalla relativa informativa.

Capo II - Modello organizzativo

Art. 6 Titolare del trattamento dei dati personali (Arsial- rappresentata dal CdA)

1. Arsial è il titolare del trattamento ai sensi degli articoli 4, n. 7), e 24 del Regolamento 2016/679 ed è rappresentato secondo quanto previsto dalla legge istitutiva n. 2 del 10/01/1995, dal Consiglio di Amministrazione (CdA), al quale spettano le competenze e le responsabilità demandate al titolare dal Regolamento 2016/679 e, in particolare, l'adozione di misure tecniche e organizzative idonee a garantire, nonché a consentire di dimostrare, che il trattamento dei dati personali sia effettuato conformemente al Regolamento medesimo. In particolare, il titolare del trattamento tiene e aggiorna il registro delle attività di trattamento svolte sotto la propria responsabilità ai sensi dell'articolo 30 del Regolamento 2016/679, ed effettua una valutazione d'impatto dei trattamenti, che la richiedano, sulla protezione dei dati personali ai sensi dell'art. 35 del Regolamento. I compiti e funzioni connessi al trattamento dei dati personali possono essere demandati al Soggetto designato.
2. Spettano ad Arsial, in qualità di titolare del trattamento, tramite il CdA, i seguenti compiti:
   a) il conferimento di specifici compiti e funzioni in materia di trattamento di dati personali al soggetto designato, ai sensi dell'articolo 2-quaterdecies del d.lgs. 196/2003 e s.m.i.;
   b) l'emanazione di direttive al Soggetto designato per lo svolgimento delle attività di trattamento dei dati personali di rispettiva competenza;
   c) l'assegnazione di distinti compiti a specifiche Strutture in ragione delle peculiari competenze alle medesime attribuite con atti formali, al fine di avvalersi di particolari contributi ed apporti funzionali per il concreto e fattivo adeguamento dell'Ente al Regolamento 2016/679;
   d) la definizione degli indirizzi per l'attribuzione di specifiche competenze alla "Struttura referente privacy";
   e) la definizione delle politiche in materia di trattamento dei dati personali e, in particolare, l'adozione di disciplinari tecnici di settore specifici o trasversali, per stabilire e dettagliare le modalità per effettuare particolari trattamenti di dati personali, con riferimento alle misure di sicurezza da adottarsi nonché istruzioni operative, modelli, software necessari per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente al Regolamento 2016/679;
   f) l'allocazione di adeguate risorse economiche e strutturali al fine di un costante adeguamento alla normativa vigente in materia di trattamento dei dati personali, ivi incluso quanto necessario per la formazione dei dipendenti e dei collaboratori regionali in materia di protezione dei dati personali;
   g) la predisposizione e aggiornamento del registro delle attività di trattamento, svolte sotto la propria responsabilità, con il supporto del RPD;
   h) la predisposizione e l' aggiornamento del registro delle violazioni dei dati personali, ivi incluse le relative valutazioni di rischio;
   i) la predisposizione della valutazione d'impatto ai sensi dell'art. 35 del Regolamento 2016/679 per i trattamenti dei dati personali che la richiedono;
   j) la definizione e la sottoscrizione di un accordo di contitolarità nel caso dei trattamenti dei dati personali effettuati in associazione con altri enti;
   k) gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa, di bilancio e degli obiettivi strategici mediante analisi della situazione

in essere, tenuto conto dei costi di attuazione, della natura, dell'applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche;

l) la nomina del Responsabile della protezione dei dati (RPD);

m) la nomina dei Responsabili del trattamento ai sensi dell'art. 28 del Regolamento 2016/679.

3. Il Titolare è contitolare del trattamento, ai sensi dell'art. 26 del RGPD, nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata ad Arsial da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento.
4. Arsial valuta e favorisce, ove possibile, la propria adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del Regolamento 2016/679 e per dimostrarne il concreto rispetto della normativa in materia della protezione dei dati personali.

Art. 7 Soggetto designato al trattamento dei dati (Direttore Generale)

1. Soggetto designato al trattamento dei dati personali è il soggetto che presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate, mediante atto di nomina ed è una persona fisica che opera sotto l'autorità e nell'ambito organizzativo di Arsial, caratterizzata dalla conoscenza e competenze in materia della protezione dei dati personali, alla quale vengono attribuiti specifici compiti e funzioni connessi al trattamento dei dati conferiti al Titolare, nominata dal Consiglio d'amministrazione di Arsial, tramite il proprio Presidente.
2. L'atto di nomina ("addendum al contratto di lavoro") specifica compiti e funzioni connessi al trattamento dei dati personali demandati al Soggetto designato al trattamento e può contenere delega a nominare altri soggetti designati con pari poteri o persone autorizzate alle specifiche operazioni di trattamento dei dati personali inerenti allo svolgimento delle mansioni di lavoro, nonché a ripartirgli le istruzioni relative al trattamento dei dati personali.
3. Il Soggetto designato al trattamento dei dati è individuato nel Direttore Generale di Arsial ed è supportato nello svolgimento dei propri compiti e funzioni in materia della protezione dei dati personali dalla Struttura referente privacy di cui al successivo articolo 8 e, per essa, dal soggetto coordinatore della stessa.
4. Il Soggetto designato presiede ai trattamenti di dati personali, la cui elencazione e descrizione è riportata nel registro delle attività di trattamento di cui all'articolo 30 del Regolamento 2016/679, attenendosi delle seguenti istruzioni:

a) i trattamenti devono essere svolti nel pieno rispetto delle previsioni normative vigenti in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la protezione dei dati personali (di seguito anche il "Garante");

b) la raccolta dei dati personali e la loro successiva registrazione devono avvenire per il solo perseguimento delle finalità istituzionali di Arsial e, comunque, per scopi:

1) determinati, pertanto non è consentita la raccolta come attività fine a sé stessa;

2) espliciti, quindi il soggetto interessato deve essere informato sulle finalità del trattamento;

3) legittimi, pertanto, oltre al trattamento, anche il fine della raccolta dei dati deve essere lecito;

c) i dati personali trattati devono, inoltre, essere:

1) esatti, cioè precisi e rispondenti al vero e, se necessario, aggiornati;

2) pertinenti, ovvero il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;

3) completi: idonei a contemplare specificamente il concreto interesse e diritto del soggetto interessato (da non intendersi nel senso di raccogliere il maggior numero di informazioni possibili);

4) non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;

5) conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti

amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita;

d) le operazioni di trattamento effettuate nell'ambito di ogni struttura organizzativa, devono essere organizzate in conformità con la normativa in materia di protezione dei dati personali applicabile ed in osservanza delle eventuali indicazioni scritte impartite da Arsial, assicurando l'applicazione del principio della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita di cui all'articolo 25 del GDPR, determinando i mezzi del trattamento e mettendo in atto le misure tecniche e organizzative adeguate, di cui all'articolo 32 del RGPD, prima dell'inizio delle attività. Inoltre, dovrà essere adottata ogni misura adeguata, fisica e logica, atta a garantire che i dati personali siano trattati in ossequio al principio di necessità e che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse (privacy by default);

e) il Soggetto designato collabora con il Titolare del trattamento affinché siano garantiti tutti i diritti dell'interessato di cui al Capo III del Regolamento 2016/679. In particolare, dovrà attenersi ad ogni istruzione scritta impartita al riguardo dal Titolare;

f) il Soggetto designato è tenuto a mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti previsti dalla normativa in materia di protezione dei dati personali relativamente a ogni unità organizzativa, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal Titolare stesso, dal Responsabile della protezione dei dati o da un altro soggetto;

g) il Soggetto designato è tenuto a informare il Titolare rispetto all'introduzione di eventuali nuovi trattamenti nonché rispetto alla cessazione di altri trattamenti, svolti in modalità cartacea e/o automatizzata, al fine di provvedere tempestivamente agli adempimenti previsti dalla normativa in materia della protezione dei dati personali;

h) ciascun trattamento deve avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento; deve pertanto essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi;

i) se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dalla normativa vigente in materia di protezione dei dati personali, è necessario provvedere, previa comunicazione al Responsabile della protezione dei dati alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento, fornendo, ad esempio, l'informativa omessa, ovvero provvedendo alla cancellazione dei dati se non è possibile procedere alla regolarizzazione;

5. In conformità alla normativa vigente in materia di protezione dei dati personali ed in osservanza delle eventuali indicazioni scritte impartite al riguardo dal Titolare del trattamento, il Soggetto designato dovrà:

a) individuare e, se presenti, incaricare il personale autorizzato al trattamento, che presta la propria attività lavorativa in Arsial;

b) impartire le disposizioni organizzative, operative e fornire al personale autorizzato le istruzioni per il corretto, lecito, pertinente e sicuro trattamento dei dati, eseguendo gli opportuni controlli;

c) vigilare sull'attuazione delle istruzioni impartite alla Struttura referente privacy e agli autorizzati del trattamento dei dati

d) controllare l'operato degli autorizzati al trattamento, nonché sensibilizzare gli stessi sugli aspetti normativi ed organizzativi in materia di tutela dei dati personali;

e) adottare le misure e disporre gli interventi necessari per la sicurezza del trattamento dei dati e per la correttezza dell'accesso ai dati, sulla base delle direttive e dei programmi definiti dal Titolare;

f) garantire che i profili di accesso ai sistemi informativi da parte degli autorizzati al trattamento siano configurati anteriormente all'inizio del trattamento, nonché verificare, almeno una volta l'anno, che tali profili siano conformi con le mansioni svolte. In caso di sospensione dall'attività lavorativa o revoca/esclusione dall'incarico dovrà essere comunicato alle strutture competenti la necessità di procedere alla disattivazione dell'utenza;

g) assicurare, il pieno rispetto degli adempimenti formali nei modi e nei tempi previsti dalla normativa vigente, tra i quali la predisposizione e il rilascio di informative, la corretta acquisizione del consenso degli interessati, ove previsto, e la gestione dei diritti degli interessati;

h) collaborare con il Garante in caso di ispezioni, al fine di fornire informazioni, documenti e ogni facilitazione di accesso alle banche dati inerenti all'Ufficio di competenza;

i) collaborare nelle verifiche predisposte dal Responsabile della protezione dei dati, al fine di fornire informazioni, documenti e ogni facilitazione di accesso alle banche dati;

j) informare tempestivamente il Responsabile della protezione dei dati personali di ogni questione rilevante in base alla normativa sulla protezione dei dati personali, come la presentazione di eventuali istanze inerenti all'esercizio dei diritti degli interessati ai sensi degli articoli da 15 a 22 del GDPR;
k) collaborare con il Titolare, per l'evasione di eventuali richieste dell'interessato volte all'esercizio dei diritti di cui agli artt. 15 – 22 del GDPR, nonché di richieste del Garante per la protezione dei dati personali;
l) informare tempestivamente e, in ogni caso, senza ingiustificato ritardo, dall'avvenuta conoscenza, il Responsabile della protezione dei dati personali di ogni violazione di dati personali (data breach) entro 24 ore dall'avvenuta conoscenza dell'evento. In ogni caso, la comunicazione deve essere accompagnata da ogni documentazione utile, per permettere al Titolare, ove ritenuto necessario, di notificare tale violazione al Garante e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando ne è venuto a conoscenza, ai sensi degli articoli 33 e 34 del GDPR;
m) nel caso in cui il Titolare debba fornire informazioni aggiuntive al Garante, supportare il Titolare stesso nella misura in cui le informazioni richieste e/o necessarie per il Garante siano esclusivamente in possesso del Soggetto designato;
n) collaborare, con il supporto del RPD alla redazione ed aggiornamento del Registro delle attività di trattamento di cui all'articolo 30 del GDPR, cooperando con il Titolare e con il Garante, laddove ne venga fatta richiesta ai sensi dell'articolo 30, paragrafo 4, del GDPR;
o) collaborare, unitamente al Responsabile della protezione dei dati, allo svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'articolo 35 del RGPD e nella eventuale consultazione del Garante, prevista ai sensi dell'articolo 36 del GDPR;
p) garantire che la protezione dei dati personali sia realizzata in base alle misure di sicurezza previste dall'articolo 32 del GDPR idonee a ridurre al minimo i rischi di divulgazione, distruzione, perdita o modifica anche accidentale o illegale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
q) collaborare, in caso di modifica della normativa in materia di protezione dei dati personali e nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse, con il Titolare e con il Responsabile della protezione dei dati, affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti introdotti;
r) proporre al Titolare la nomina dei Responsabili del trattamento individuati in conformità all'art. 28 del Regolamento 2016/679;
s) designare gli amministratori di sistema, nel rispetto di quanto previsto dal Provvedimento del Garante della Protezione dei dati Personali 27 novembre 2008 ("*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*) nonché degli ulteriori criteri e modalità e darne comunicazione all'Area competente in materia di sistemi informativi;
t) collaborare alla redazione del piano di formazione aziendale in ambito privacy, fornendo al Titolare il fabbisogno formativo dell'Ente e garantendo che il personale autorizzato al trattamento dei dati, che opera sotto l'autorità dell'Ente, partecipi agli eventi formativi;
u) collaborare alla mappatura dei trattamenti e al censimento delle banche dati e dei trattamenti dei dati effettuati dall'Ente in qualità del responsabile del trattamento per conto di altri titolari, al fine di redigere e tenere aggiornato il registro dei trattamenti del responsabile del trattamento.

Art. 8 Struttura interna referente privacy (Area Affari Legali e Gestione del Contenzioso)

1. La Struttura interna referente privacy è individuata nell'Area Affari Legali e Gestione del Contenzioso dell' Agenzia e supporta il Soggetto designato al trattamento nell'esecuzione dei compiti e delle funzioni di cui al precedente articolo 7, mediante provvedimento del soggetto designato di nomina e collabora con il RPD nella definizione del modello organizzativo *privacy prescelto,* fornendo linee di indirizzo, pareri, metodologia, operatività, consulenze giuridiche, per l'implementazione del medesimo modello, a supporto di una corretta e tempestiva applicazione del GDPR, al fine di garantire un presidio ed una competenza professionale elevata per gli adempimenti continuativi riguardanti gli aspetti normativi, organizzativi e procedurali, nonché per il costante coordinamento con le attività del DPO;

2. In particolare, il supporto della Struttura referente privacy al Soggetto designato consiste nel:
   a) predisporre gli atti necessari per garantire la conformità dell'attività dell'Ente alla normativa vigente in materia della protezione dei dati personali (regolamenti, atti di contitolarità, nomine e istruzioni per gli autorizzati al trattamento, nomine per responsabili del trattamento, informative, comunicazioni ecc.), in modo da garantire un presidio ed un'alta e specifica competenza professionale, adeguata per gli adempimenti continuativi riguardanti gli aspetti normativi, organizzativi e procedurali;
   b) assicurare il costante coordinamento con le attività del Responsabile della protezione dei dati;
   c) definire e implementare il modello organizzativo privacy;
   d) fornire linee di indirizzo, pareri, metodologia, operatività, consulenza per l'implementazione del medesimo modello, anche attraverso la gestione (digitalizzata) dei procedimenti, dei processi e delle attività dell'Ente,
   e) proporre le misure, anche tecniche e organizzative, finalizzate alla corretta e tempestiva applicazione del Regolamento 2016/679.
3. La Struttura Referente privacy è tenuta al segreto ed alla riservatezza in merito all'adempimento dei propri compiti e alle informazioni e dati di cui potrebbe venire a conoscenza nell'esercizio delle proprie funzioni, nonché a segnalare al Responsabile della protezione dei dati ogni possibile situazione di conflitto di interesse, anche potenziale rispetto ai propri compiti, incarichi e funzioni.
4. Le competenze della Struttura referente privacy si sostanziano nei seguenti compiti:
   a) supportare il Soggetto designato nell'adozione delle misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo, anche a seguito di analisi e approfondimenti richiesti formalmente al Responsabile della protezione dei dati;
   b) supportare il Soggetto designato nella puntuale revisione periodica delle nomine degli autorizzati del trattamento e degli amministratori di sistema nonché dei relativi compiti assegnati a quest'ultimi;
   c) supportare il Soggetto designato nell'aggiornamento del Registro dei trattamenti di dati personali effettuati, sulla base delle misure organizzative e delle risorse messe a disposizione dallo stesso;
   d) fornire supporto alle verifiche di sicurezza, svolte dalla struttura di sistemi informativi, coadiuvata dal Responsabile della protezione dei dati;
   e) supportare il Soggetto designato nella gestione delle richieste di parere al Responsabile della protezione dei dati e assicurare il coordinamento tecnico con lo stesso;
   f) costituire il riferimento principale nell'esecuzione delle attività sopraelencate, nonché per tutte le questioni che riguardano il trattamento dei dati personali;
5. All'interno della struttura interna referente privacy il soggetto designato individua e nomina come soggetto coordinatore il dirigente medesimo o un funzionario a tempo indeterminato dell' Agenzia, dotato di alte professionalità e competenze specialistiche, con relative responsabilità di prodotto e di risultato e svolgimento di funzioni di coordinamento, gestione attività della struttura referente privacy e con elevato grado di autonomia gestionale ed organizzativa.

Art. 9 Responsabile della protezione dei dati personali

1. Il Responsabile della protezione dati dell'Ente, interno o esterno all' Agenzia, è individuato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché della capacità di assolvere ai compiti di cui all'articolo 39 del Regolamento 2016/679, tramite atto negoziale di incarico a firma del Titolare del trattamento.
2. Il Responsabile della protezione dei dati svolge i seguenti compiti:
   a) informare e fornire consulenza al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento 2016/679, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
   b) sorvegliare l'osservanza del Regolamento 2016/679, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento 2016/679;
   d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 Regolamento 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

3. I compiti demandati al Responsabile della protezione dei dati sono svolte in costante monitoraggio, d'intesa e coordinamento con la Struttura interna referente privacy;
4. I compiti del Responsabile della protezione dei dati, titolo esemplificativo, ma non esaustivo, consistono in:

a) servizio di informazione e consulenza al Titolare del trattamento, al Soggetto designato e agli Autorizzati al trattamento in merito agli obblighi derivanti dal Regolamento 2016/679 e, in particolare, consulenza relativa alle attività di:

- censimento dei trattamenti dei dati personali;
- elaborazione di un parere su quanto rilevato dall'analisi del rischio di tipo tecnico/organizzativo e definire eventuali azioni da intraprendere per stabilire le opportune misure di sicurezza adeguate rispetto ai rischi eventualmente rilevati;
- verifica della tenuta del Registro delle attività di trattamento dei dati personali;
- elaborazione di procedure operative relative alla protezione dei dati personali, inclusa quella di gestione degli eventuali Data breach e la relativa gestione documentale;
- elaborazione degli atti di nomina dei responsabili del trattamento;
- elaborazione di un modello di gestione per gli accessi e l'oscuramento dei dati dell'interessato;
- elaborazione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative, al fine di garantire la sicurezza del trattamento dei dati personali;
- elaborazione di una procedura di audit periodico del mantenimento degli standard di protezione dei dati;
- valutazione e supporto alla definizione dei profili privacy riferiti alle procedure relative all'applicazione delle misure dell'amministrazione digitale;

b) servizio di consulenza finalizzato alla valutazione circa l'esistenza, completezza e correttezza degli adempimenti effettuati in materia di protezione dei dati, ivi compresi le attività previste nei regolamenti e gli aggiornamenti in materia, atti di nomina dei Responsabili del trattamento ai sensi dell'art. 28 del Regolamento 2016/679, autorizzazioni al trattamento dei dati personali agli autorizzati al trattamento, dichiarazioni di consenso al trattamento dei dati personali, tenuta e aggiornamento del Registro dei trattamenti;

c) servizio di sorveglianza sull'osservanza del Regolamento (UE) 679/2016, di altre disposizioni nazionali e/o locali relative alla protezione dei dati, delle politiche del Titolare del trattamento, anche mediante verifiche periodiche (cd. audit) a campione, fornendo un report che evidenzi il relativo grado di conformità o di parziale o totale non conformità;

d) servizio di consulenza per l'adeguamento delle informative e servizio di consulenza orale e scritta, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento affinché sia conforme a quanto prescritto dall'art. 35 del Reg. UE 679/2016;

e) servizio di messa a disposizione e l'attivazione di apposito software per la gestione degli adempimenti previsti dal Regolamento Europeo 679/2016;

f) servizio di supporto - con presenza fisica in loco - in caso di ispezioni effettuate per conto del Garante, servizio di cooperazione con l'Autorità di controllo (Garante della privacy) e Intermediazione (punto di contatto) per l'autorità di controllo per questioni connesse al trattamento per questioni connesse al trattamento (ivi compresa la consultazione preventiva qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenti un rischio elevato in assenza di misure per attenuare il rischio, ovvero la consultazione preventiva nei casi eventualmente previsti da norme di rango nazionale);

g) servizio di verifica dei requisiti dei fornitori di servizi i quali effettuano trattamento dei dati per conto del Titolare e definire e/o valutare le clausole contrattuali minime per garantire adeguata protezione dei dati;

h) servizio di consulenza relativa alle clausole contrattuali minime finalizzate a garantire adeguata protezione dei dati;

i) servizio di consulenza in merito all'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei propri dati personali ai sensi dell'articolo 5 bis, comma 2, del d.lgs. 33/2013 e successive modificazioni, nonché consulenza al responsabile della prevenzione della corruzione e della trasparenza nei casi di riesame di istanze di accesso negato o differito a tutela dell'interesse alla protezione dei dati personali;

j) attività di formazione: al Soggetto designato al trattamento dei dati personali, alla Struttura referente

privacy, agli autorizzati al trattamento dei dati personali, da fornire, in tutto o in parte, in presenza, o anche da "remoto" o con sistemi di e-learning;
k) ogni altro eventuale e ulteriore compito e attività stabiliti con successivi atti nei limiti previsti agli art. 37, 38 e 39 del Regolamento 2016/679.

5. In riferimento alle evidenze dei controlli svolti, alle eventuali segnalazioni ricevute, alla verifica di documentazione e/o ad ogni altra informazione rilevante acquisita ai fini del Regolamento 2016/679, il Responsabile della protezione dei dati può:
   a. riservarsi di chiedere approfondimenti ai soggetti competenti per i controlli;
   b. suggerire azioni idonee a favorire l'osservanza del Regolamento 2016/679 (a titolo esemplificativo, in ordine al controllo del Registro dei trattamenti);
   c. suggerire al Titolare del trattamento ulteriori controlli da effettuarsi dalla Struttura referente privacy.
6. Allo scopo di svolgere le proprie funzioni, il Responsabile della protezione dei dati può:
   a) partecipare agli incontri organizzati tra Strutture competenti, valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti. A tal fine, in osservanza al principio di privacy by design, ogni qualvolta siano in trattazione argomenti e attività che comportano trattamento di dati personali, occorre, secondo le regole organizzative dell'Ente, darne comunicazione al Responsabile della protezione dei dati, che valuterà se e come intervenire;
   b) accedere a tutta la documentazione e a tutte le sedi rilevanti dell'Ente per lo svolgimento dei propri compiti;
7. I compiti del Responsabile della protezione dei dati di cui ai commi precedenti implicano che:
   a) sia fornito supporto attivo alle sue funzioni da parte del Direttore generale e dei Dirigenti;
   b) siano assegnate adeguate risorse (finanziarie, infrastrutture - sede, attrezzature, strumentazione - e personale);
   c) sia comunicata ufficialmente la nomina del Responsabile della protezione dei dati sia esternamente (comunicazione all'Autorità Garante, informative agli interessati ex art. 13 GDPR) che a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;
   d) sia garantita la collaborazione da parte della Direzione generale e della Strutture referente privacy dell'Ente, così da fornire al Responsabile della protezione dei dati supporto, informazioni e input essenziali;
   e) sia assicurata la formazione permanente del Responsabile della protezione dei dati e dei componenti della Struttura referente privacy, in modo che possano curare il loro aggiornamento con riguardo agli sviluppi nel settore della protezione dati.
   f) sia fornito il coordinamento con la Struttura interna referente privacy e per essa al soggetto coordinatore e, se necessario, con l'Area Risorse Umane (in materia di formazione), per la programmazione e la definizione di percorsi formativi del personale di Arsial in materia di tutela della privacy.

Art. 10 Pareri del RPD

1. Il DPO esprime parere obbligatorio al Titolare o al designato in ordine alla legittimità e alla correttezza dei trattamenti di dati personali in relazione alle seguenti questioni:
   -individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che la struttura intende adottare ai fini della tutela della riservatezza, integrità e disponibilità del patrimonio informativo regionale, anche a seguito di incidenti di sicurezza o analisi dei rischi;
   -adozione di politiche specifiche in materia di protezione dei dati personali e sicurezza delle informazioni nonché redazione e aggiornamento di eventuali regolamenti tecnici con impatto sulla sicurezza delle informazioni o definizione di misure di sicurezza da adottarsi quale impostazione predefinita;
   -individuazione di misure poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;
   esiti della valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del RGPD;
   -progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;
2. Il DPO fornisce:
   -servizio di consulenza orale e scritta, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento affinché sia conforme a quanto prescritto dall'art. 35 del Reg. UE

679/2016;
- servizio di consulenza per l'adeguamento delle informative;
- servizio di supporto gestionale attraverso la messa a disposizione e l'attivazione di apposito software per la gestione degli adempimenti che Arsial deve eseguire, previsti dal Regolamento Europeo 679/2016.

3. Il DPO esprime pareri facoltativi alle strutture Arsial in relazione alla:
-valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei propri dati personali ai sensi dell'articolo 5 bis, comma 2, del d.lgs. 33/2013 e successive modificazioni;
-opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti; in questo caso il parere va reso entro tre giorni dalla richiesta.
4. I pareri del Responsabile della protezione dei dati sono espressi nel rispetto delle seguenti codifiche:
a) NC - non conformità, nei casi in cui siano rilevati elementi di non conformità alla normativa vigente e alle politiche regionali in materia di protezione dei dati personali;
b) OS – osservazioni, nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa vigente e alle politiche regionali in materia di protezione dei dati personali, non costituendo vincolo di attuazione;
c) PO – positivo, nei casi in cui siano prospettati elementi valutati come conformi alla normativa vigente e alle politiche regionali in materia di protezione dei dati personali.
6. Nei casi in cui il DPO esprima parere non conforme (NC) o con osservazioni (OS), il Soggetto designato, laddove ritenesse di mantenere l'originaria decisione, deve formalizzare le motivazioni che giustificano, in caso di parere NC, l'esecuzione dell'attività o l'implementazione della soluzione tecnologica in maniera non conforme alla normativa e alle politiche regionali in essere, ovvero, in caso di parere OS, in maniera difforme rispetto alle osservazioni del Responsabile della protezione dei dati.

Art. 11 Autorizzati al trattamento dei dati personali (dipendenti e collaboratori dell'Ente)

1. Il Titolare del trattamento o il Soggetto designato autorizza al trattamento dei dati tutti i dipendenti e collaboratori, che materialmente effettuano operazioni di trattamento dei dati personali sotto l'autorità diretta del Titolare del trattamento;
2. Il Soggetto designato procede all'autorizzazione di cui al precedente comma con specifico atto di nomina redatto secondo lo schema di cui all'allegato "4B". Nell'atto di nomina è individuato l'ambito del trattamento consentito, necessario per lo svolgimento delle mansioni di lavoro affidate, nonché le istruzioni operative per la protezione dei dati personali trattati;
Nelle istruzioni deve sempre essere riportato quanto segue:
-devono essere trattati solo i dati personali necessari per ogni specifica finalità del trattamento;
-non devono essere poste in atto attività non previste nelle istruzioni al fine di non pregiudicare la legittimità e correttezza dei trattamenti;
3. Le istruzioni di cui al comma 2, oltre a riguardare eventuali aspetti di dettaglio da diversificarsi in relazione alle specificità dei singoli trattamenti, devono contenere un espresso richiamo alle politiche dell'Ente in materia di sicurezza informatica e protezione dei dati personali in essere nonché alle modalità e procedure definite dall'amministrazione per l'assegnazione e l'utilizzo delle dotazioni ICT per il personale in servizio;
Nell'atto di autorizzazione i dipendenti o collaboratori sono individuati nominativamente, attraverso nome, cognome e codice fiscale, specificando, per ciascun nominativo, i trattamenti che gli stessi sono autorizzati ad effettuare, anche tramite il rinvio alle mansioni di lavoro affidate nel contratto di lavoro o altro contratto.

Art. 12 Responsabile del trattamento dei dati personali (persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto di Arsial)

1. Tutti i soggetti, pubblici o privati, che trattano dati personali per conto del Titolare del trattamento, e che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo che il trattamento soddisfi i requisiti previsti dal Regolamento 2016/679, e garantiscano la tutela dei dati dell'interessato, assumono il ruolo di Responsabili del trattamento ai sensi dell'art. 28 del Regolamento 2016/679, mediante contratto o altro atto giuridico in forma scritta, predisposto da parte del Soggetto designato al trattamento dei dati in conformità all'allegato "4G", sulla base di apposita nomina del Titolare.
2. I rapporti tra il Titolare ed i Responsabili sono disciplinati dagli atti di cui al comma 1, che specificano materia disciplinata, la durata del trattamento, la natura e la finalità del trattamento, la tipologia dei dati personali trattati, le categorie degli interessati, gli obblighi e i diritti del Titolare del trattamento.
3. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla normativa e ai compiti affidatigli dal Designato, quale delegato del Titolare.
4. Qualora l'Ente proceda alla nomina di Responsabili dovrà prevedere, in sede di contratto di servizio, che questi ultimi sviluppino il Registro dei trattamenti effettuati per conto del Titolare del trattamento in coordinazione l'Ente.

Art. 13 Amministratore di sistema
(Soggetto esterno e/o soggetto interno)

1. L/gli amministratore/i di sistema, interno o esterno, può/possono essere individuato/i anche tra i dipendenti dell'Area Servizi Informatici che per esperienza, capacità tecniche ed affidabilità forniscano idonea garanzia del pieno rispetto delle disposizioni di legge vigenti in materia, ivi compreso il profilo relativo alla sicurezza. L'atto di nomina, redatto secondo lo schema dell'allegato "4C", contiene l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
2. L'amministratore di sistema sovrintende alle risorse del sistema informativo afferenti alla struttura di appartenenza, consente agli utenti l'utilizzo delle funzioni disponibili e svolge tutte le funzioni previste dalla normativa vigente e dagli ulteriori adempimenti previsti dal Provvedimento del Garante della Protezione dei dati Personali 27 novembre 2008 e successive modificazioni, nonché dall'allegato "1".
3. Il Titolare del trattamento, anche attraverso il Soggetto designato, verifica annualmente la rispondenza dell'operato degli amministratori di sistema alla normativa vigente in materia di protezione dei dati personali.

Art. 14 Struttura per i sistemi informativi – ICT
(Staff Sistemi informativi, SIARL, SIT)

1. L'Area competente in materia di sistemi informativi, di seguito "Struttura ICT", svolge un ruolo di supporto al Titolare del trattamento, al Soggetto designato e al Responsabile della protezione dei dati in tema di risorse strumentali e di competenze, tranne per i compiti già disciplinati con convenzione ad hoc sottoscritta con Arsial.
2. La struttura ICT, in materia di gestione della sicurezza delle informazioni, svolge le seguenti funzioni:
   a) individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente; tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali sono sottoposte a parere preventivo del Responsabile della protezione dei dati personali;
   b) provvede, ogni qualvolta venga avvertito un problema di sicurezza a:
   -attivare la struttura cui sono demandati i compiti relativi alla gestione degli incidenti di sicurezza, assicurando la collaborazione con il Responsabile della protezione dei dati;
   -individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere del Responsabile della protezione dei dati;
   -segnalare al Soggetto designato e al Responsabile della protezione dei dati le violazioni dei dati personali ai fini della notifica, ai sensi dell'articolo 33 del Regolamento 2016/679, al Garante per la protezione dei dati personali;
   c) svolge verifiche sulla puntuale osservanza della normativa vigente e delle politiche dell'Ente e regionali

in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la collaborazione con il Responsabile della protezione dei dati personali, ed effettua le verifiche specifiche richieste da questi;
d) promuove la formazione di tutto il personale dell'Ente in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione coordinandosi con le azioni promosse dal Responsabile della protezione dei dati personali;
e) garantisce il rispetto delle procedure relative alle autorizzazioni per l'accesso ai varchi controllati dall'Ente, a tutela e delle persone e a protezione dei dati personali e del patrimonio informativo dell'Agenzia.

Art. 15 Diritti degli interessati

1. In conformità all'articolo 12 del Regolamento 2016/679, ai fini della corretta gestione delle richieste ricevute da parte degli interessati per l'esercizio dei diritti previsti dal Capo III del medesimo regolamento nei confronti del Titolare del trattamento, sono adottate le misure di cui all'allegato "3".

Capo III - Sicurezza e protezione dati

Art. 16 Sicurezza del trattamento

1. Il Titolare del trattamento e il responsabile del trattamento mettono in atto, per i distinti profili di responsabilità e di azione, misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
2. Costituiscono misure tecniche ed organizzative che possono essere adottate, tra le altre, i sistemi di autenticazione, autorizzazione, rilevazione di intrusione, sorveglianza; di protezione (antivirus; firewall; antintrusione); sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
3. La conformità del trattamento dei dati al Regolamento 2016/679 può essere dimostrata attraverso l'adozione delle misure disicurezza adeguate oppure con l'adesione a codici di condotta approvati ovvero a meccanismi di certificazione approvati.
4. Arsial, attraverso i ruoli individuati nel presente Regolamento, si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure anche a coloro che agiscono per suo conto ed abbiano accesso a dati personali.

Art. 17 Registro del Titolare del trattamento

1. Il Registro delle attività di trattamento svolte dall'Ente reca almeno le seguenti informazioni, come previsto dall'art. 30 del Regolamento 2016/679:
   a) il nome ed i dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del trattamento e del Responsabile della Protezione Dati;
   b) le finalità del trattamento;
   c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
   f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

2. Il Registro è conservato dalla Struttura interna referente privacy per conto del Titolare.

Art. 18 Valutazioni d'impatto sulla protezione dei dati (DPIA)

1. Il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto (DPIA) quando il trattamento medesimo, considerati la natura, l'oggetto, il contesto e le finalità dello stesso nonché l'eventuale utilizzo di nuove tecnologie, presenta un rischio elevato per i diritti e le libertà delle persone fisiche.
2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto, con il necessario supporto del Responsabile della protezione dei dati, degli elenchi delle tipologie di trattamento soggetti, o non soggetti, a valutazione come redatti e pubblicati dal Garante per la protezione dei dati personali ai sensi dell'art. 35 del RGPD.

Art. 19 Violazione dei dati personali

1. La violazione dei dati personali o "data breach" è una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Ente.
2. Il Titolare del trattamento, con ausilio del Soggetto designato e secondo le modalità individuate dal Responsabile protezione dati – RPD, deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante al fine di verificare il rispetto delle disposizioni del Regolamento 2016/679.
3. Il Titolare del trattamento senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Se la violazione comporta un rischio elevato per i diritti delle persone fisiche, il Titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.
4. Il Responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il Titolare in modo che questi possa attivarsi ad adempiere i propri obblighi previsti dalla normativa vigente in materia di protezione dei dati personali.
5. Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

Capo IV – Adempimenti, norme di rinvio, entrata in vigore

Art. 20 Adempimenti in materia di privacy. Adozione di modelli e schemi tipo

Per garantire l'applicazione uniforme della disciplina in materia di privacy da parte dell'Ente sono adottati i modelli gli schemi tipo di cui agli allegati da "1" a "4G" e, in particolare, nomine per il soggetto designato al trattamento, per gli autorizzati al trattamento, per l'amministratore di sistema interno, per i responsabili del trattamento, schema dell'informativa ai sensi dell'art. 13 del Regolamento 2016/679. Gli schemi tipo possono essere modificati e integrati dal Soggetto designato, in relazione alle specificità dei particolari settori di afferenza e dei correlati trattamenti.

Art. 21 Rinvio

Per tutto quanto non espressamente disciplinato, si applicano le disposizioni del Regolamento 2016/679 e tutte le norme vigenti in materia di protezione dei dati personali.

Art. 22 Entrata in vigore

Il presente Regolamento entra in vigore con l'adozione della Deliberazione del Titolare del trattamento, rappresentato, ai fini previsti dal Regolamento 2016/679 ed in armonia con la legge istitutiva di ARSIAL n. 2 del 10/01/1995, dal Consiglio di Amministrazione (CdA), con la quale vengono approvati il documento e gli allegati modelli allo stesso.

ALLEGATO 1

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEL TITOLARE
Art. 30, paragrafo 1 Regolamento UE 2016/679

Dati di contatto (art. 30, p. 1, lett. a) Regolamento UE 2016/679	
Titolare	ARSIAL
Dati di contatto del titolare	Indirizzo: Via Rodolfo Lanciani 38, 00162, Roma Email / PEC: arsial@pec.arsialpec.it Recapito Telefonico: 06.86.273.675/606 Sito Web: www.arsial.it
Responsabile della protezione dei dati (RPD)	Management and consulting srl- punto di contatto: dott. Luca Petrucci -

ELENCO TRATTAMENTI ATTIVI

TRATTAMENTO: ____ (denominazione e settore associato)	
Data Inizio	……..
Data Fine	……
Trattamento affidato a terzi	SI/NO
Responsabile del trattamento collegato	Eventuali soggetti che effettuano operazioni di trattamento per conto di Arsial
Tipo Finalità	Finalità perseguite dal trattamento
Categorie Interessati	Persona fisica cui si riferisce il dato trattato
Banche Dati	Eventuali banche dati su cui poggia il trattamento
Dati Trattati	Tipologia di dato trattato, in base alla seguente classifica: • personale (art. 4, punto 1) RGPD) • personali giudiziari (art. 10 del RGPD) • personali sensibili (art. 9 del RGPD)
Sintetica Descrizione del Trattamento e del Flusso Informativo	Breve descrizione dei trattamenti effettuati e indicazione se il trattamento è su larga scala.
Descrizione Misure di Sicurezza Tecniche e Organizzative Adottate per il Trattamento	Descrizione delle misure.
Modalità Cancellazione Dati	Indicare la modalità di cancellazione
Soggetti Destinatari della Comunicazione e Scopo della Comunicazione	Indicare i soggetti destinatari
Diffusione e Ambito nella Diffusione	SI/NO
Trasferimento Dati Estero	SI/NO
Adesione ai Codici di Condotta	SI/NO
Valutazione di impatto obbligatoria	SI/NO

ALLEGATO 2

DISCIPLINARE TECNICO PER AMMINISTRATORI DI SISTEMA

Premessa

Il presente disciplinare tecnico descrive le basilari regole tecniche ed organizzative che gli amministratori di sistema devono applicare per garantire la sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche in Arsial.

Tenendo conto di quanto esplicitato nel Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) pubblicato sulla G.U. n. 300 del 24.12.2008, e successive modificazioni, la definizione di "amministratori di sistema", ai fini dell'applicazione del presente disciplinare, è la seguente:

"*sono le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (quali ad es. gli amministratori di dominio e di server), nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.*"

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente «responsabili» di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti «in chiaro» le informazioni medesime.

Pertanto, considerata la delicatezza di tali peculiari mansioni e i rischi ad esse associati, la designazione di un amministratore di sistema non può prescindere da alcune considerazioni e accorgimenti:

a) valutazione delle caratteristiche soggettive: l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo allasicurezza;

b) designazioni individuali: la designazione quale amministratore di sistema deve essereindividuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

c) elenco degli amministratori di sistema: gli estremi identificativi delle persone fisicheamministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante. Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, Arsial rende nota o conoscibile l'identità degli amministratori di sistema con comunicazione effettuata nell'ambito del portale di comunicazione interna Intranet;

d) servizi in outsourcing: nel caso di servizi di amministrazione di sistema affidati in outsourcing Arsial conserva, presso la struttura competente in materia di Sistemi Informativi, ognuno per la parte di propria competenza, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;

e) verifica delle attività: l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del titolare del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti;

f) registrazione degli accessi: devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli

amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Ai fini del presente disciplinare, si intende per sistema informativo il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate all'acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni. Esempi di sistemi informativi sono server (file, database, web, mail, ecc.), applicazioni, apparati di rete (router, switch, ecc.), strumenti di sicurezza (firewall, IPS, ecc.).

Applicabilità

Le regole illustrate nel disciplinare tecnico si applicano a tutti i dipendenti appartenenti all'organicodi Arsial e a tutti coloro che a vario titolo svolgono attività, compiti, mansioni come amministratori di sistema.

Principi generali

È compito di ogni amministratore di sistema comprendere le minacce di sicurezza incombenti sui propri sistemi e adottare le contromisure di sicurezza necessarie ad assicurare confidenzialità, integrità e disponibilità dei dati e delle informazioni.

A titolo esemplificativo tali minacce possono essere:

- *minacce incombenti sui dati* (furto di dati, incluse credenziali di accesso a basi dati; distruzione anche accidentale di dati; modifica di dati, anche intenzionale, per introdurre informazioni false e fuorvianti);
- *minacce incombenti sulle applicazioni e sui sistemi operativi* (attacchi di vario tipo quali virus, spamming, SQL injection, Denial of Service; accessi non autorizzati, anche non intenzionali);
- *minacce incombenti sull'infrastruttura* (furto di apparecchiature; danneggiamento/distruzione di apparecchiature sia intenzionale che accidentale; smarrimento di apparecchiature o credenziali; reazione inadeguata ad incidenti/disastri).

Sicurezza fisica

L'accesso fisico ai locali di Arsial è regolato dall'apposito Regolamento di Arsial.

La scelta dei locali in cui installare, conservare o utilizzare sistemi informatici deve essere fatta tenendo in considerazione i potenziali rischi di sicurezza sui dati causati tanto da eventi accidentali quanto da dolo. In funzione dell'analisi dei rischi devono essere valutate e adottate idonee misure diprotezione, quali sistemi di antintrusione, sistemi antincendio, sistemi di rilevazione fumi, sistemi antiallagamento.

La scelta delle misure di sicurezza dei locali deve, in ogni caso, tenere conto dei vincoli imposti dalla normativa in materia di tutela della salute e di sicurezza dei lavoratori.

La protezione dei server e degli apparati di rete considerati critici per il funzionamento e ladisponibilità dei sistemi informativi deve prevedere sistemi di protezione elettrica quali stabilizzatori di corrente ed apparecchiature UPS e sistemi di condizionamento dell'aria nei locali per garantire il mantenimento di una costante ed adeguata temperatura di esercizio.

La scelta dei locali per gli armadi deve essere fatta individuando ambienti idonei, possibilmente dedicati e ad accesso limitato (solo agli amministratori di sistema e ad un eventuale custode autorizzato). Gli armadi medesimi devono essere chiusi a chiave e le relative chiavi devono essere in possesso dei soli amministratori di sistema (e di un eventuale custode specificatamente autorizzato). Le chiavi di accesso a locali o armadi possono essere conservate presso le portinerie di Arsial.

Controllo dell'accesso ai dati

L'accesso ai dati ed alle strumentazioni informatiche utilizzate per trattarli deve essere concesso al solo personale espressamente autorizzato (nel caso di dati personali i cosiddetti autorizzati del trattamento). L'elenco del personale autorizzato deve essere aggiornato almeno a cadenza annuale.

In nessun modo devono essere concessi permessi di accesso ai sistemi senza preventiva autorizzazione formale del responsabile funzionale o del referente regionale di progetto. Le modalità con cui viene formulata tale autorizzazione possono variare a seconda del tipo di trattamento.

Autenticazione

L'accesso ai dati trattati con strumentazioni informatiche deve essere concesso esclusivamenteprevia

opportuna autenticazione.
Gli strumenti di autenticazione devono essere progettati in funzione del valore dei dati trattati. Deve essere prevista l'ipotesi di utilizzo di sistemi di autenticazione forte ove necessario (smart card, token hardware, dispositivi one-time password, sistemi biometrici).
Devono essere previsti meccanismi di separazione dei privilegi, sia a livello di sistema operativo che a livello applicativo, per consentire l'accesso ai dati e le operazioni effettuate sugli stessi, in misura corrispondente ai diversi profili degli utenti.
Autorizzazione
È necessario introdurre dei criteri generali di definizione dei ruoli amministrativi e di gestione delle autorizzazioni, pur nel pieno rispetto dei principi di delega e di autonomia dei referenti di applicazioni e sistemi che gestiscono porzioni del sistema informativo.
Il principio generale a cui attenersi è che i ruoli amministrativi critici non si devono sovrapporre. Ad esempio, gli sviluppatori non devono essere anche sistemisti, gli amministratori della sicurezza non devono essere sistemisti o sviluppatori e così via. Qualora non fosse possibile dal punto di vista organizzativo mantenere o adottare questa separazione di ruoli, devono essere introdotti controlli compensativi che permettano di tracciare puntualmente le operazioni eseguite (ad esempio tramite l'utilizzo di strumenti evoluti di monitoraggio, audit puntuali, notifiche via e-mail).
Gestione delle credenziali
Le credenziali consentono all'utente di accedere ai dati e pertanto è necessario che la loro assegnazione segua procedure codificate e condivise. Tali procedure possono essere diverse in funzione sia del valore dei dati da trattare che dei sistemi coinvolti.
In generale, le richieste delle credenziali di autenticazione devono essere fatte dai responsabili funzionali o referenti regionali di progetto. In ogni caso, deve essere tenuta traccia della richiesta che ha generato la creazione di una credenziale di autenticazione sul sistema. Le modalità con cui sono formulate le richieste variano in funzione della criticità dei dati o dei sistemi (per esempio e- mail, lettera protocollata, determinazione).
Ogni credenziale di autenticazione deve riferirsi ad un singolo utente. Non è consentito l'utilizzo di credenziali condivise. Fanno eccezione a questa regola le credenziali amministrative di accesso ai sistemi (es. root, administrator), che devono comunque essere assegnate ad un numero limitato di autorizzati e devono essere utilizzate solo nel caso di interventi particolari sui sistemi. Ove possibile, bisogna privilegiare sempre l'utilizzo di credenziali nominative anche nel caso di operazione di amministrazione dei sistemi.
La gestione delle credenziali deve seguire le procedure documentate per i vari sistemi di autenticazione. La policy di scadenza delle credenziali non utilizzate è normalmente di 180 giorni. Fa eccezione a questa regola il dominio applicativo esterno per la peculiarità di alcune applicazioni che sono utilizzate dagli utenti con periodicità annuale: in questo caso le credenziali non utilizzate sono disabilitate dopo un anno. Le policy di gestione delle password devono essere allineate sui diversi sistemi e comunque conformi ai dettami delle norme in materia di protezione dei dati personali.
Le credenziali amministrative non nominative di gestione dei sistemi non sono vincolate alle stesse regole delle credenziali nominative, non scadono dopo un periodo di inutilizzo, non vengonobloccate dopo un certo numero di tentativi errati, non hanno la password che scade e non ne viene richiesta la modifica al primo accesso. Perciò gli amministratori dei sistemi sono tenuti ad adottare politiche manuali di modifica delle password dei loro sistemi e a monitorare gli eventuali tentativi di accesso non autorizzato. Le credenziali amministrative non nominative create al solo scopo di avviare servizi sui server non devono poter effettuare l'accesso interattivo sui sistemi stessi o, ove ciò non fosse tecnologicamente possibile, deve essere comunque monitorato il loro utilizzo per scopi diversi rispetto all'ambito per cui sono state create.
Le credenziali di autenticazione con privilegi amministrativi non devono essere inviate via e-mail: in tali casi, è necessario convocare l'utente e fornirgli le credenziali verbalmente, oppure mediante un sistema di scambio informazioni sicuro.
Gli amministratori dei sistemi sono tenuti a rispettare le procedure adottate e a non creare particolarità o eccezioni nella gestione delle credenziali utente.
La gestione delle credenziali amministrative deve seguire regole molto rigide e stringenti: devono essere identificate le persone autorizzate a richiedere l'aggiunta o la modifica di amministratori dei sistemi o delle applicazioni e deve essere previsto un sistema di notifica che avvisi gli altriamministratori del cambiamento.
In generale una procedura di gestione delle credenziali deve prevedere:
a) l'identificazione di chi può chiedere la creazione, la modifica, la disabilitazione, la cancellazione di un'utenza, le operazioni di sblocco dell'utente o il reset della password; tale identificazione, qualora avvenga

tramite telefono, deve essere fatta chiedendo alcuni dati personali al richiedente;
b) la modalità di inoltro della richiesta: alcune operazioni quali la creazione o la modifica dovranno essere fatte via e-mail o fax, altre quali il reset della password potranno anche essere fatte verbalmente dall'utente interessato tramite telefono, previa la verifica da parte degli amministratori dell'identità dell'interessato (es. tramite richiesta di alcuni dati personali);
c) l'elenco dei destinatari della richiesta: ad esempio i referenti dell'applicazione, gli amministratori dei sistemi, il servizio di help desk;
d) la tempistica di evasione della richiesta;
e) l'archiviazione e il backup delle richieste pervenute via e-mail e delle risposte relative all'attività svolta. Se la richiesta è in formato cartaceo deve essere acquisita agli atti;
f) la modalità di risposta al richiedente per comunicare l'avvenuta attivazione dell'utenza, il nome utente e la password (a tale proposito valutare se sia opportuno crittografarla, ovvero comunicarla verbalmente all'utente, ove possibile).
Le procedure di gestione delle credenziali debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti autorizzati per quanto di propria competenza.
Gestione delle password
La lunghezza minima consentita per le password deve essere impostata ad almeno otto caratteri. Ove la tecnologia non lo consenta, la lunghezza delle password deve essere impostata al massimo consentito dal sistema.
La durata della password dovrebbe essere impostata in base al grado di criticità di sistemi e basi dati. Inoltre, una eventuale password di "single sign on" è opportuno abbia una durata inferiore a quella delle password che sostituisce.
Per contrastare attacchi alle password di tipo "brute-force" i sistemi informatici devono prevedere opportuni meccanismi per la disabilitazione di un account dopo un intervallo finito di tentativi di accesso non riusciti. Devono comunque essere previsti meccanismi di difesa da attacchi di tipo *denial of service* causati dal blocco volontario di account legittimi. Un esempio di tali meccanismi di difesa è di consentire per un account un limite massimo di cinque tentativi di accesso non riusciti, prevedendo il blocco dell'account per un periodo di trenta minuti nel caso in cui tale limite venga superato.
Ove tecnologicamente possibile, deve essere data agli utenti la possibilità di modificare la propria password senza l'intervento degli amministratori.
Devono essere previsti meccanismi di implementazione dei sistemi tali da garantire all'utente la modifica della propria password al primo accesso al sistema.
Le password non devono essere conservate in chiaro, né trasmesse su canali non cifrati. Per la loro conservazione devono essere utilizzati adeguati meccanismi di cifratura anche in funzione del valore dei dati, per esempio, hash calcolati con funzioni irreversibili per la conservazione su disco; analogamente per la loro trasmissione devono essere utilizzati protocolli di comunicazione cifrati come SSL.
In caso di trattamento di dati sensibili (articolo 9 del RGPD) e/o giudiziari (articolo 10 del RGPD) o comunque di rilevanza strategica, devono essere previsti sistemi di controllo delle password per consentire il solo utilizzo di password "resistenti" ad attacchi "brute-force". Per esempio, password formate con valori alfanumerici maiuscoli e minuscoli, simboli e caratteri speciali.
Al momento dell'installazione, su tutti i sistemi, devono essere modificate le password di default utilizzate dal produttore/installatore.
Protezione dei dati
Backup
Per garantire la disponibilità dei dati devono essere previste idonee procedure di backup in funzione del valore dei dati trattati. Tali procedure devono essere formalizzate per iscritto e tenute aggiornatecon cadenza almeno annuale.
Con cadenza periodica (perlomeno annuale) devono essere effettuati controlli a campione (su un campione opportunamente numeroso: es. una copia per ogni mese) sulle copie di backup per verificarne la disponibilità e l'integrità.
A fronte di cambiamenti intervenuti nel sistema di backup o nei sistemi che devono essere archiviatidevono essere fatti dei test di backup e restore per verificare la consistenza dei dati salvati.
Tutti i test vanno documentati in un "diario" che riporti la data del test, il sistema coinvolto, la persona che ha eseguito il test e l'esito delle operazioni effettuate.
Le copie di backup devono essere conservate in locali fisicamente separati da quelli dei sistemi origine dei

dati, per garantire la disponibilità delle copie in caso di eventi accidentali quali incendi odisastri naturali. Le copie dei backup devono essere riposte, possibilmente, in casseforti le cui chiavi sono conservate da personale identificato. L'elenco del personale autorizzato deve essere regolarmente mantenuto aggiornato.
Gli amministratori devono censire e tenere aggiornate le informazioni sul backup dei sistemi da lorogestiti. In particolare, devono richiedere alla struttura competente l'attivazione del backup per i nuovi sistemi e applicazioni e devono segnalare esigenze particolari di backup che esulino dalle politiche in essere di backup centralizzato.
Gli amministratori del sistema di backup devono monitorare l'esito dei task eseguiti e, qualora rilevassero problemi, darne pronta segnalazione agli amministratori dei sistemi coinvolti.
Il sistema di backup, sia per quanto riguarda il software di base che il software applicativo, deve essere mantenuto aggiornato, in particolare relativamente alle patch/hot-fixes di sicurezza. Qualora venissero rilasciate patch/hot-fixes di sicurezza per la parte client, gli aggiornamenti sui singoli sistemi devono essere pianificati in accordo con gli amministratori degli stessi.
Le politiche di backup debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti autorizzati per quanto di propria competenza.
Procedure di dismissione dei sistemi: protezione dei dati
Ogni qualvolta si dismette un dispositivo elettronico o informatico che contiene dati personali, è necessario adottare idonei accorgimenti e misure, anche attraverso soggetti terzi, tecnicamente qualificati, che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.
Chi procede al riutilizzo di dispositivi elettronici o informatici è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo ove possibile, l'autorizzazione a cancellarli o a renderli non intellegibili.
Il processo di rimozione dei dati dai dischi dei computer è denominato *disk sanitizing*, *cleaning*, *purging*, o *wiping*. Il metodo scelto per "disinfettare" un disco dipende dalla criticità dei dati in essocontenuti.
Cancellare un file comporta in effetti la sola rimozione del puntatore al file. Esistono strumenti software in grado di recuperare file cancellati e quindi i dati in essi contenuti. Pertanto, per garantire la cancellazione sicura delle informazioni le tecniche possibili sono:

- Sovrascrittura: il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza delle informazioni di cui si vuole impedire l'indebita acquisizione) varia e incide proporzionalmente sui tempi delle procedure;
- Formattazione "a basso livello" (LLF) dei dispositivi di tipo hard disk, laddove possibile, attenendosi alle istruzioni fornite dal produttore e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;
- Smagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici, in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti sui quali potrebbero non essere applicabili le procedure di cancellazione software;
- Distruzione fisica dei dispositivi.

La sovrascrittura è in genere sufficiente a garantire che i dati prima presenti non siano più recuperabili e dunque leggibili.
Smagnetizzare o distruggere fisicamente il disco garantisce l'inutilizzabilità futura del disco medesimo e dunque previene qualsiasi tentativo di recupero dei dati.
Le procedure utilizzate in caso di reimpiego o di smaltimento dei dispositivi e degli strumenti informatici debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti autorizzati per quanto di propria competenza.

Protezione delle applicazioni
Design, sviluppo, deployment e gestione
Le applicazioni devono essere sviluppate dispiegate e gestite secondo i principi di privacy by designe privacy by default, secondo quanto definito da specifico disciplinare.

Protezione dei sistemi
È compito di ogni amministratore mantenere un elenco aggiornato e completo delle risorse gestite.L'elenco, nel caso di server, deve contenere almeno:

- i riferimenti fisici e logici del server (nome e indirizzo di rete), la sua ubicazione e i riferimenti relativi al backup;
- le versioni dell'hardware e del sistema operativo;
- le funzioni e applicazioni principali oppure il ruolo all'interno dell'infrastruttura regionale.

Precedentemente alla progettazione, implementazione, installazione o gestione di un sistema, deve essere effettuata un'analisi dei rischi per determinare le misure di sicurezza da adottare.
Tutti gli interventi tecnici che coinvolgono la creazione, modifica o eliminazione di uno dei meccanismi di sicurezza indicati nel disciplinare tecnico, devono essere opportunamentedocumentati ed autorizzati da parte del proprio referente funzionale.

Server

Gli amministratori dei sistemi server devono tener conto delle seguenti policy generali e devono documentare qualsiasi eccezione a queste regole.

Policy generale

1. Hardware, sistemi operativi, servizi ed applicazioni installati devono essere approvati dalla struttura competente in materia di Sistemi Informativi
2. Tutte le patch/hotfixes di sicurezza rilasciate dai fornitori devono essere installate nel minor tempo possibile valutando a priori, in base al rischio, la verifica in ambiente di pre-produzione. Sono ammesse eccezioni basate su specifiche esigenze di servizio di Arsial, adeguatamente giustificate, documentate e riportate dagli amministratori alla struttura competente in materia di Sistemi Informativi. I servizi non necessari devono essere rimossi/disabilitati, compatibilmente con le dipendenze del sistema in oggetto. È compito degli amministratori mantenersi costantemente aggiornati sulle patches/hotfixes da installare.
3. Servizi non sicuri devono essere sostituiti da equivalenti oggetti sicuri, ove ciò sia possibile. Per esempio, servizi con traffico in chiaro (telnet) devono essere sostituiti da servizi con traffico cifrato (SSH).
4. Relazioni di fiducia tra sistemi possono essere configurate solo per specifiche esigenze diservizio. Devono essere documentate dagli amministratori ed approvate dalla struttura competente in materia di Sistemi Informativi.
5. Qualsiasi attività di amministrazione remota deve essere effettuata utilizzando canali sicuri (es. connessioni di rete con crittografia, che utilizzino SSH o IPSEC). Qualora non sia disponibile una modalità di accesso remoto sicuro, dovrebbero essere utilizzate "one-time" password per tutti i livelli di accesso.
6. I server di produzione devono essere fisicamente localizzati in un ambiente ad accesso controllato, con un impianto di condizionamento adeguato alle esigenze, ovvero in grado di mantenere la temperatura e l'umidità entro i limiti che consentono la normale operatività dei server.
7. È vietata l'installazione di hardware e software non autorizzato. Tutte le attività di modifica di hardware o software devono essere preventivamente autorizzate, preferibilmente mediantedefinizione e schedulazione delle attività di aggiornamento (upgrade sistema operativo, modifica hardware, ecc.).
8. Tutti i server di produzione devono essere collegati ad un sistema di UPS (Uninterruptible Power Supplies) più Gruppo Elettrogeno oppure solo UPS che consenta una disconnessione (shutdown) automatica dei server prima dell'esaurimento delle batterie.

Le modalità operative di installazione, configurazione ed aggiornamento, debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet adaccesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti autorizzati per quanto di propria competenza.

Apparati di rete

Gli amministratori di rete, nell'attività di configurazione e gestione degli apparati di rete di produzione, devono basarsi sulle seguenti regole generali e documentare le eventuali deroghe o eccezioni.

Policy generale

1. Tutti i router dovrebbero usare un protocollo di accounting per autenticare gli utenti. L'accesso con account locali è consentito solo in situazioni d'emergenza ovvero quando non fosse disponibile il sistema centralizzato di autenticazione.
2. La password di enable deve essere configurata utilizzando il meccanismo di "enable secret" che ne permette la cifratura sicura.

3. Disabilitare le seguenti funzioni (alcuni termini inglesi non sono stati tradotti perché così sono conosciuti in ambito tecnico):

- IP directed broadcast;
- pacchetti in ingresso con indirizzi non validi come da RFC1918;
- TCP small services;
- UDP small services;
- tutti i source routing;
- tutti i servizi web;
- Protocollo CDP o similari.

4. Usare la community SNMP adottata da Arsial e comunque diversa da *public* o *private*, oppure limitare l'accesso agli apparati impostando opportuni filtri.
5. Le regole di accesso devono essere aggiunte o modificate aderendo alle necessità di Arsial.
6. I router devono avere un banner di login che notifichi a chi accede che l'apparato è proprietà di Arsial e che l'accesso è consentito al solo personale autorizzato.
7. Gli apparati di rete devono essere inclusi nel sistema di gestione dei sistemi di produzione adottato da Arsial e quindi censiti riportando i riferimenti dei responsabili tecnici.
8. Deve essere utilizzato il protocollo SSH per gestire i router.

Le modalità operative di installazione, configurazione ed aggiornamento, come pure gli schemi della rete debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti autorizzati per quanto di propria competenza.

Postazioni di lavoro

Gli amministratori dei client devono tener conto delle policy generali relative alle postazioni di lavoro e devono documentare qualsiasi eccezione a queste regole.

Policy generale

1. Il software utilizzato sulle postazioni di lavoro deve essere associato ad una licenza, in accordo con le specifiche del fornitore/produttore;
2. Le postazioni di lavoro assegnate al personale dell'Ente devono essere utilizzate solo per gli scopi designati;
3. E' vietato installare hardware e software addizionale senza autorizzazione della struttura competente in materia di Sistemi Informativi ed è vietato alterare o cancellare software o modificare configurazioni su una postazione di lavoro di Arsial senza autorizzazione da parte della medesima struttura.
4. Le modalità operative di installazione, configurazione ed aggiornamento, debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet adaccesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti autorizzati per quanto di propria competenza.

Dispositivi portatili

I dispositivi portatili seguono le stesse policy indicate per le postazioni di lavoro con un'attenzione maggiore alla protezione dei dati personali e alla tutela rispetto ai possibili tentativi di furto.

In caso di furto o smarrimento di un dispositivo portatile, l'amministratore di tali dispositivi deve agire tempestivamente, anche su segnalazione verbale del possessore, previa verifica dell'identità dello stesso tramite, ad esempio, la richiesta di alcuni dati identificativi personali (es. matricola, codice fiscale, ecc.).

Policy generale

Impostare la password di accesso al BIOS su tutti i dispositivi. Disabilitare, inoltre, da BIOS il boot da supporto rimovibile. Se il firmware consente di proteggere con password l'hard disk, e se lo si ritiene necessario per casi particolari e documentati, si abiliti anche questa funzionalità. La medesima password per BIOS e hard disk deve essere utilizzata su tutti i dispositivi, per accelerare gli interventi tecnici approvati.

I dispostivi portatili non devono essere lasciati in ufficio ma devono essere portati via al termine dell'orario di lavoro.

Le modalità operative di installazione, configurazione ed aggiornamento debbono esseredocumentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet adaccesso riservato per la

consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti autorizzati per quanto di propria competenza.

Gestione dei log

È compito di ogni amministratore monitorare costantemente i sistemi gestiti per prevenire e limitaregli effetti di eventuali incidenti di sicurezza. Il metodo principale per effettuare il monitoraggio è costituito dalla raccolta ed analisi dei file di log.

La definizione ed il rilevamento degli eventi di sistema deve essere effettuata in funzione del valore dei dati ed in modo tale da consentire la verifica dell'efficacia e dell'efficienza delle procedure di sicurezza. Ove possibile devono comunque essere rilevati:

- autenticazione (login e logout, riusciti e non);
- accesso ai dati classificati sensibili dal punto di vista della sicurezza (lettura e scrittura);
- modifica di funzioni amministrative (es. la disabilitazione delle funzioni di logging, la gestione dei permessi, ecc.);
- connessioni di rete (in ingresso ed in uscita).

Ove possibile ogni voce di log deve contenere:

- data/ora dell'evento;
- luogo dell'evento (macchina, indirizzo IP, ecc.);
- identità dell'utente;
- identificativo del processo che ha generato l'evento;
- connessioni di rete (in ingresso ed in uscita) relative all'evento;
- descrizione dell'evento.

In virtù del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modificazioni, i log devono essere conservati in file su cui è possibile effettuare solo la scrittura incrementale o eventualmente su supporti non riscrivibili (es. CD-R). I log, opportunamente normalizzati e filtrati devono essere conservati su host dedicati. In ogni caso, deve essere possibile poter effettuare il backup dei log secondo le normali procedure di backup previste da Arsial.

L'accesso ai log deve essere concesso al minor numero possibile di autorizzati preventivamente individuati.

La frequenza di rotazione dei log è dipendente dalla frequenza di generazione degli eventi del sistema e da eventuali vincoli tecnici o legali. In ogni caso deve essere previsto un meccanismo che,successivamente al backup, sovrascriva i log esistenti ad intervalli regolari.

Ove possibile, gli amministratori devono mantenere on line i file di log contenenti gli eventi di sicurezza per almeno 1 mese.

I log devono essere conservati per un periodo di almeno 6 mesi ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modificazioni. È opportuno che la conservazione avvenga su supporto di memorizzazione offline non accessibilein scrittura ad alcuno.

Gestione degli incidenti di sicurezza

Tutti gli amministratori devono reagire agli incidenti di sicurezza con prontezza e con spirito di cooperazione, segnalando al proprio responsabile e alla struttura competente in materia di Sistemi Informativi le violazioni di sicurezza interna o gli eventi che possono portare a credere che vi sia stata un'elusione delle misure di sicurezza previste. Gli amministratori, dopo una prima verifica dell'accaduto, devono registrare le operazioni svolte econtattare la struttura competente in materia di Sistemi Informativi.

Per gestire correttamente gli incidenti è indispensabile avere un elenco aggiornato dei beni (assets)che permetta di identificare i sistemi/applicazioni e il relativo livello di criticità.

Le macro-fasi di gestione dell'incidente sono le seguenti:

- rilevazione incidente;
- identificazione e analisi dell'incidente;
- contenimento, raccolta evidenze, rimozione e ripristino;
- chiusura dell'incidente.

Le procedure dettagliate di gestione delle violazioni di sicurezza sono oggetto di apposito disciplinare tecnico sulla gestione dei data breach.

Controlli di sicurezza

Analisi dei rischi

È obbligo di ogni amministratore valutare i potenziali rischi di sicurezza derivanti dal design, l'installazione, l'utilizzo e la gestione dei sistemi informatici di competenza.

Ogni progetto che prevede l'installazione, l'utilizzo, la modifica, l'eliminazione di uno o più sistemi informatici, deve quindi essere preceduto da un'adeguata analisi dei rischi che tenga conto del valore delle risorse da proteggere, delle potenziali minacce di sicurezza, dei meccanismi di sicurezza.

Security audit

I sistemi informatici sono periodicamente valutati ed analizzati per identificare il livello di rischio cui le risorse sono esposte.

Opportune verifiche sono regolarmente effettuate per valutare l'efficacia e l'efficienza dei meccanismi di sicurezza utilizzati.

I security audit possono essere affidati a fornitori esterni di servizi. In tal caso è necessario farsi rilasciare da questi ultimi apposita attestazione di conformità del servizio fornito ai requisiti previsti dalla normativa vigente in materia di protezione dei dati personali.

Documentazione tecnica

Gli amministratori di sistema hanno il compito di provvedere alla documentazione e al tempestivo aggiornamento della stessa, in relazione a tutti i sistemi, banche dati, apparati di rete e sicurezza, applicazioni software di qualunque natura e complessità, nonché alle procedure operative di installazione, configurazione ed aggiornamento delle strumentazioni informatiche e telematiche di competenza. Tale documentazione deve essere messa a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti autorizzati per quanto di propria competenza.

ALLEGATO 3

POLICY PER LA GESTIONE DELLE ISTANZE DEGLI INTERESSATI

1. **Premessa**

Il Regolamento Generale sulla protezione dei dati delle persone fisiche (Regolamento UE 679/2016) - RGPD - ha stabilito nuove ed uniformi norme all'interno dell'Unione Europea con riferimento alla protezione dei dati personali delle persone fisiche ivi residenti. Esso garantisce diritti specifici agli interessati nei confronti del titolare del trattamento con riferimento alla possibilità di accesso, verifica e controllo, cancellazione dei propri dati personali.

1.1 Obiettivo

Finalità del presente documento è definire le attività, i ruoli e le responsabilità che l'Arsial (di seguito anche "Agenzia"), in qualità di Titolare dei dati trattati, pone in essere per la gestione delle richieste ricevute da parte degli interessati per l'esercizio dei propri diritti, così come previsto dall'articolo 12 del RGPD, fermo restando che, per quanto qui non riportato, si applicano le disposizioni previste nel suddetto regolamento.

1.2 Soggetti destinatari

I soggetti ai quali si rivolge il contenuto del presente documento sono:

- il Titolare;
- il Soggetto designato al trattamento dal titolare, ovvero il Direttore Generale.

2. **Ambito di applicazione**

Ambito di riferimento del presente documento sono i processi di conformità che devono essere rispettati con riferimento all'evasione delle richieste degli interessati.
Tali richieste rientrano nell'ambito dell'esercizio dei diritti di quest'ultimi, ai sensi degli articoli da 15 a 22 del RGPD (ferme restando le limitazioni di cui all'articolo 23 del RGPD), ossia diritti di:

a) accesso ai dati (art. 15 del RGPD);
b) rettifica dei dati (art. 16 del RGPD) ed eventuale notifica ai destinatari dei dati (art. 19 delRGPD);
c) cancellazione dei dati (diritto all'oblio, art. 17 del RGPD) ed eventuale notifica aidestinatari dei dati (art. 19 del RGPD);
d) limitazione del trattamento (art. 18 del RGPD) ed eventuale notifica ai destinatari dei dati(art. 19 del RGPD);
e) portabilità dei dati (art. 20 del RGPD);
f) opposizione (art. 21 del RGPD);
g) diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22 del RGPD).

L'informazione sull'esercizio di tali diritti è inclusa all'interno dell'informativa resa al soggetto interessato.

2.1. Diritto di accesso

L'interessato ha il diritto di richiedere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in caso affermativo, di ottenere l'accesso agli stessi e alle informazioni indicate dall'articolo 15 del RGPD (quali, ad esempio, le finalità del trattamento e le categorie di dati trattati).
Tale accesso non deve ledere i diritti e le libertà altrui; qualora i dati richiesti contengano anche riferimenti a soggetti terzi rispetto all'interessato, il titolare del trattamento deve valutare se la comunicazione di tali dati possa ledere i diritti di libertà dei soggetti terzi. In caso affermativo, occorre applicare una soluzione operativa, quale quella di oscurare i dati relativi a terzi.
In base al Considerando 63 del RGPD, nel caso in cui l'interessato effettui una richiesta di accesso troppo generica, non chiarendo a quali dati si riferisce, si può chiedere un'ulteriore specificazione,in ragione del fatto che l'Agenzia tratta una notevole quantità di informazioni potenzialmente riferibili all'interessato.

2.2. Diritto di rettifica

L'interessato ha il diritto di richiedere la rettifica dei dati personali inesatti che lo riguardano e/o l'integrazione dei dati personali incompleti. La rettifica e/o l'integrazione devono avvenire senza ingiustificato ritardo.

2.3. Diritto all'oblio

L'interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo. La richiesta del soggetto interessato può essere effettuata solo per uno dei seguenti motivi che il Soggetto designato o la persona autorizzata al trattamento hanno l'onere di verificare:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1 del RGPD e nonsussiste alcun motivo legittimo prevalente per procedere al trattamento;

c) i dati personali sono stati trattati illecitamente;

d) i dati personali devono essere cancellati per adempiere un obbligo legale.

Il Diritto all'oblio non può essere esercitato se il trattamento è necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito l'Ente;

c) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, del RGPD, nella misura in cui il diritto di cui all'articolo 17, paragrafo 1, rischi di rendere impossibile o di pregiudicare gravementeil conseguimento degli obiettivi di tale trattamento;

d) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Quando la richiesta dell'interessato, a seguito di valutazione, è ritenuta fondata, occorre altresì verificare se i dati di cui si chiede la cancellazione siano stati indicizzati, nel qual caso occorre chiedere ai motori di ricerca (ad esempio Google, Bing, Yahoo, ecc.) la deindicizzazione dei contenuti relativi ai dati personali riferiti all'interessato.

2.4. Diritto di limitazione del trattamento

L'interessato può richiedere la temporanea esecuzione della sola operazione di conservazione dei dati personali trattati dall'Agenzia, con conseguente inutilizzabilità e inaccessibilità dei dati per tutto il periodo di limitazione, nei casi di seguito indicati:

a) quando sia contestata l'esattezza dei dati personali che lo riguardano, eventualmente esercitando il diritto di rettifica di cui all'articolo 16 RGPD; in tali casi la limitazione di trattamento potrà durare per il periodo di tempo necessario a procedere alla verifica dei dati dicui l'Agenzia è in possesso;

b) quando l'interessato sostiene che il trattamento dei dati personali è illecito, ma si oppone alla cancellazione dei propri dati personali e chiede che ne sia limitato l'utilizzo;

c) qualora i dati personali siano necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, seppure non più utili all'Agenzia;

d) nel caso in cui l'interessato si sia opposto al trattamento dei dati ai sensi dell'articolo 21 delRGPD.

Nonostante sia stata disposta la limitazione di trattamento, i dati personali possono essere eccezionalmente trattati nei seguenti casi:

a) il trattamento sia necessario per l'accertamento, l'esercizio o la difesa di un diritto dell'Agenzia in sede giudiziaria;

b) per tutelare i diritti di una persona fisica o giuridica diversa dall'interessato istante;

c) per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

A titolo esemplificativo, si rappresentano le modalità attraverso le quali dare seguito a tale richiesta:

- trasferire temporaneamente i dati personali contrassegnati verso un altro sistema ditrattamento;
- contrassegnare i dati personali come inaccessibili agli utenti del sistema di trattamento deidati;

- rimuovere temporaneamente i dati contrassegnati dal sito web istituzionale.

2.5 Diritto di portabilità dei dati

L'interessato ha il diritto di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano, forniti a un Titolare del trattamento, e di trasmetterli a un altro Titolare del trattamento, senza impedimenti da parte del Titolare del trattamento cui li ha forniti, qualora siano verificate entrambe le seguenti condizioni:

a) il trattamento si basi sul consenso dell'interessato al trattamento dei propri dati personali per una o più finalità specifiche, salvo il caso in cui il diritto dell'Unione o degli Stati membri disponga che l'interessato non possa revocare il divieto di trattare categorie particolari di dati ai sensi dell'articolo 9, paragrafo 1, del RGPD ovvero il trattamento sia necessario per l'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
b) trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento ad un altro, laddove risulti essere tecnicamente fattibile.
Il diritto alla portabilità dei dati non pregiudica il diritto di cancellazione. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di autorità pubbliche attribuite al Titolare.
Il diritto alla portabilità dei dati non pregiudica i diritti e le libertà altrui.

2.6. Diritto di opposizione al trattamento

Ai sensi dell'articolo 21 del RGPD l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), del RGPD, compresa la profilazione.
Tale opposizione è volta ad inibire unicamente un determinato utilizzo dei dati personali dell'interessato.
Il Soggetto designato e le persone autorizzate al trattamento possono continuare a trattare, a seguito di propria valutazione, i dati al cui trattamento l'interessato si è opposto, rappresentando allo stesso interessato l'esistenza di motivi legittimi cogenti per procedere al trattamento, che prevalgono sugli interessi o sui diritti e sulle libertà fondamentali che lo riguardano.

2.7. Limitazioni ai diritti dell'interessato

È possibile che i diritti dell'interessato di cui ai punti da 2.1 a 2.6 siano limitati da particolari interessi pubblici o di altri privati. In particolare, nell'ambito del bilanciamento tra i diritti riconosciuti all'interessato ai sensi degli articoli da 15 a 22 del RGPD e determinate ipotesi concrete in cui possa ricorrere l'esercizio degli stessi, il legislatore italiano individua specifici ambiti e materie privilegiate la cui tutela, in certe ipotesi, può determinare una compressione dei diritti dell'interessato.
Con riferimento ai limiti all'esercizio dei diritti previsti dagli articoli da 15 a 22 del RGPD, si applicano, in particolare, gli articoli 2-undecies (limitazioni ai diritti dell'interessato), 2-duodecies(limitazioni per ragioni di giustizia) e 2-terdecies (diritti riguardanti le persone decedute) del d.lgs. 196/2003 e successive modificazioni.
In particolare, ai sensi dell'articolo 2-undecies del suddetto decreto legislativo, i diritti non possono essere esercitati in ragione della possibilità che possa derivare un pregiudizio effettivo e concreto:

a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;
b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;
c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in basead una espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla

tutela della loro stabilità;

e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;

f) alla riservatezza dell'identità del dipendente che segnala, ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio;

g) agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale.

3. **Esercizio dei diritti degli interessati**

Gli interessati che vogliano esercitare uno o più dei diritti ad essi spettanti, devono presentare la relativa domanda alla Struttura interna referente privacy al contatto strutturainternareferenteprivacy@arsial.it che la inoltra al Soggetto designato dal Titolare e tiene traccia delle domande stesse, nonché dei rispettivi riscontri. Il Soggetto designato dal Titolare valuta le domande e provvede al soddisfacimento delle stesse, tenendo traccia di tutti i passaggi del procedimento relativo a ciascuna di esse.

3.1. Modalità di presentazione delle istanze

Le istanze devono essere formulate in modo che sia possibile un'identificazione certa dell'interessato richiedente. In particolare:

a) qualora la richiesta provenga direttamente dall'interessato, dovranno essere richiesti gli estremi del documento di identità in corso di validità;

b) qualora la richiesta provenga da parte di un terzo a ciò delegato, incluso un familiare, dovranno essere richiesti gli estremi del documento di identità in corso di validità di chi presenta la richiesta, gli estremi del documento di identità (fotocopia) in corso di validità dell'interessato, la delega scritta e firmata dell'interessato (non necessaria, invece, in caso di genitore che esercita la potestà genitoriale su un minore; in tal caso è richiesta la documentazione che attesti il legame di parentela);

c) qualora la richiesta provenga da parte di un legale dovranno essere richiesti gli estremi del documento di identità (fotocopia) in corso di validità dell'interessato, la richiesta su carta intestata del legale recante gli estremi necessari per la verifica dell'iscrizione all'albo, il mandato conferito nell'ambito della propria professione o la delega scritta e firmata dell'interessato.

Nei casi di istanze presentate telematicamente, ai fini della verifica dell'identità dell'istante, si richiama quanto disposto dall'articolo 65 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) e successive modificazioni.

Le istanze per l'esercizio dei diritti sopra citati sono trasmesse dai richiedenti direttamente alla Struttura interna referente privacy con una delle modalità previste dalla normativa vigente.

Per tutte le istanze pervenute la Struttura interna referente privacy comunica al richiedente, nella stessa forma in cui avviene la richiesta, se le informazioni date sono complete, e provvede a dare evidenza dell'avvenuta presa in carico.

La Struttura interna referente privacy in particolare:

a) inoltra le domande al Soggetto designato dal Titolare;
b) invita gli interessati a formulare le richieste a mezzo di apposito modulo messo a disposizione dall'Agenzia sul proprio sito istituzionale e presso la sede della Struttura interna referente privacy;
c) tiene un registro di tutte le richieste e dei riscontri forniti dal Soggetto designato dal Titolare.

Nel caso in cui, per errore, il Soggetto designato dal Titolare, il RPD o altro organo regionale riceva direttamente un'istanza, dovrà inoltrare la stessa Struttura interna referente privacy per l'avvio della procedura.

3.2 Valutazione e classificazione della richiesta

A seguito della ricezione della richiesta, il Soggetto designato dal Titolare individua il trattamento cui la stessa si riferisce e procedono alla verifica della sua legittimità, nonché della veridicità e completezza delle informazioni ricevute. Solo nei casi particolarmente complessi lo stesso può richiedere il supporto del RPD.

La richiesta viene valutata sulla base dei seguenti aspetti:

a) legittimità: valutazione della presenza di eventuali condizioni ostative all'evasione della richiesta

(es. impossibilità di cancellazione dei dati per motivi di ordine superiore, quali salute o sicurezza pubblica, etc.);

b) veridicità: valutazione dell'esistenza dei dati che riguardano l'interessato;

c) completezza: verifica che i dati ricevuti siano completi al fine di evadere la richiesta e valutazione dell'identificabilità del richiedente.

A seconda dell'esito della valutazione, la richiesta viene classificata in:

- Evadibile: la richiesta è legittima, completa e non ci sono elementi ostativi alla richiesta. Lemodalità di gestione della richiesta sono descritte nei paragrafi successivi;
- Rigettata: la richiesta non è legittima e sussistono motivazioni per il rigetto da parte del Soggetto designato dal Titolare, i quali ne danno informazione alla Struttura interna referente privacy che provvede al riscontro formale all'interessato;
- Con informazioni mancanti: il Soggetto designato dal Titolare comunica alla Struttura interna referente privacy la mancanza di informazioni, e la Struttura interna referente privacy procede formalmente con la richiesta delle informazioni stesse all'interessato;

3.3. Termini per il riscontro

Il Soggetto designato dal Titolare è tenuto a rispondere, tramite la Struttura interna referente privacy alle richieste dell'interessato senza ingiustificato ritardo e al massimo entro un mese.
Il termine decorre dal ricevimento della richiesta che consenta un'identificazione dell'interessato da parte della Struttura interna referente privacy .Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.. La Struttura interna referente privacy informa l'interessato di tale proroga, nonché dei motivi del ritardo, entro un mese dal ricevimento della richiesta (articolo 12 del RGPD).

3.4. Modalità del riscontro

Il Soggetto designato dal Titolare, eventualmente con il supporto della struttura ICT e del partner tecnologico coinvolto, comunicano alla Struttura interna referente privacy l'esito della richiesta.
L'interessato ha il diritto di ottenere una copia dei dati personali oggetto di trattamento.
I dati e le informazioni richieste sono forniti dalla Struttura interna referente privacy per iscritto o con altri mezzi, anche elettronici, (in particolare se la richiesta è presentata con mezzi elettronici e in un formato elettronico di uso comune), salvo diversa indicazione da parte dell'interessato.
Il riscontro deve essere fornito in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice, chiaro e comprensibile. Se richiesto dall'interessato, le informazioni possono essere anche fornite oralmente.
Qualora la richiesta riguardi la portabilità dei dati, il Soggetto designato dal Titolare, eventualmente con il supporto della struttura ICT e del partner tecnologico coinvolto, compila un modulo interoperabile per trasmettere i dati alla parte terza e la Struttura interna referente privacy comunica all'interessato l'avvenuto trasferimento.

3.5. Mancato accoglimento

Il mancato accoglimento della richiesta deve essere motivato compiutamente e reso per iscritto, o con altri mezzi, anche elettronici, dalla Struttura interna referente privacy fornendo l'informazione relativa alla possibilità di proporre reclamo al Garante per la protezione dei dati personali e ricorso giurisdizionale.
Se le richieste dell'interessato sono manifestamente infondate o eccessive, la Struttura interna referente privacy e il Soggetto designato dal Titolare possono rifiutare di soddisfare la richiesta, dimostrando, con adeguata motivazione, il carattere manifestamente infondato o eccessivo della richiesta.

3.6 Tracciamento del processo

Il Soggetto designato dal Titolare ha l'obbligo di tenere traccia e conservare tutta la documentazione relativa

alle richieste raccolte ed evase e di darne comunicazione semestrale al Responsabile Protezione dei Dati (RPD).

La comunicazione deve essere effettuata fornendo almeno le seguenti informazioni:

-numero di protocollo e data di ricezione della richiesta;

-oggetto della richiesta;

-dati identificativi del soggetto interessato richiedente;

-dati identificativi del soggetto eventualmente delegato dall'interessato;

-esito della richiesta;

-data di evasione della richiesta.

ALLEGATO 4a

"ADDENDUM AL CONTRATTO DI LAVORO"

CONFERIMENTO DI COMPITI E FUNZIONI IN QUALITA' DI SOGGETTO DESIGNATO AI SENSI DELL'ARTICOLO 2 QUATERDECIES D.LGS. 196/2003

(Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.) e successive modificazioni.

ISTRUZIONI PER L'ESERCIZIO DELLE FUNZIONI CONFERITE

PREMESSO CHE

-con Deliberazione n. 42/RE del 9 dicembre 2021 avente il seguente oggetto: "*Linee di indirizzo per l'adeguamento dell'organizzazione Arsial alle norme in materia di privacy e per l'assetto dei livelli di responsabilità e contestuale definizione delle policy fondamentali in tema di trattamento dei dati personali. Individuazione e nomina Soggetto designato e individuazione Struttura interna referente privacy"* è stato stabilito e disposto, da parte del Titolare del Trattamento dei dati personali, ARSIAL, rappresentata, ai fini previsti dal GDPR, della normativa privacy ed in armonia con la legge istitutiva di ARSIAL n. 2 del 10/01/1995, dal Consiglio di Amministrazione (CdA), ai sensi dell'articolo 4, n. 7), e dell'art. 24 del GDPR ("*Responsabilità del titolare del trattamento*"), tra l'altro, quanto segue:

"DI FORNIRE linee di indirizzo, ovvero istruzioni, al personale, ognuno per propri qualifica, ruolo e/o competenze ed in particolare ai soggetti designati di Arsial, finalizzate a dare formale attuazione agli obblighi introdotti dal Regolamento (UE) 2016/679 del Parlamento Europeo relativo alla "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati)" provvedendo con il presente provvedimento all'adeguamento formale dei propri atti organizzativi, aggiornando l'assetto dei livelli di responsabilità in materia di privacy, anche in aderenza al modello organizzativo regionale, di cui alla deliberazione della Giunta Regionale n. 733 del 27/10/2020, definendo le policy fondamentali di Arsial per uniformare le attività e rendere effettivo l'esercizio dei diritti degli interessati, in riferimento a tutti i trattamenti che coinvolgono dati personali, con adozione del modello sopra esposto e contestuale revoca dei pregressi provvedimenti amministrativi ed organizzativi adottati dall' Agenzia;
DI INDIVIDUARE quale "Soggetto Designato", al trattamento dei dati personali di cui alla vigente normativa in tema di tutela dei dati personali, che opera sotto la propria autorità, il Direttore Generale di Arsial;
DI APPROVARE l'atto individuale di nomina quale "Soggetto Designato" al trattamento dei dati personali, Allegato sub A, "ADDENDUM AL CONTRATTO DI LAVORO" al presente provvedimento, contenente le istruzioni per l'esercizio delle funzioni conferite;

DI DARE ATTO che la designazione quale Soggetto Designato di cui al presente provvedimento nei confronti, avrà validità fino al mantenimento della titolarità dell'incarico attualmente rivestito dallo stesso di Direttore generale di Arsial e terminerà, di diritto, con la cessazione dell'incarico medesimo, fermo restando in ogni caso la facoltà del CdA, in qualità di Titolare del Trattamento di ritirarla in caso di inadempimento o di sopraggiunte cause di conflitto o di opportunità;"

VISTO l'articolo 2-quaterdecies del D. lgs. N. 196/2003 e successive modificazioni, il quale dispone che *"il Titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*";

VISTO il decreto legislativo 30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche) e successive modificazioni;

VISTO il 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 GDPR), che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento al diritto di protezione dei dati personali;

TENUTO CONTO che, ai sensi dell'articolo 24 del GDPR, il Titolare del trattamento è tenuto a mettere in atto le misure, tecniche ed organizzative, adeguare per garantire ed essere in grado di dimostrare che il trattamento sia effettuato conformemente al GDPR;

TENUTO CONTO che l'articolo 29 del GDPR stabilisce la regola generale per cui "*chiunque agisca sotto l'autorità del responsabile del trattamento o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*";

DATO ATTO che il <**indicare nome e cognome**> in qualità di Direttore generale di Arsial è soggetto designato al trattamento dei dati ai sensi e per gli effetti di cui all'articolo 2 quaterdecies del d.lgs. 196/2003 e successive modificazioni;

RITENUTO che il <**indicare nome e cognome**> in qualità di Direttore di Arsial, per l'ambito di attribuzioni, funzionie competenze conferite, abbia le garanzie sufficienti per mettere in atto tutte le misure tecniche ed organizzative adeguate a soddisfare i requisiti del RGPD e garantire la tutela dei diritti degli interessati;

Tutto ciò premesso

SI CONVIENE QUANTO SEGUE

Art. 1 (Obblighi del Soggetto designato)

Il ***<indicare nome e cognome>***, quale Soggetto designato al trattamento dei dati ai sensi dell'articolo 2 *quaterdecies* del d.lgs. 196/2003 e successive modificazioni, svolge i compiti e assume le responsabilità previste dalle disposizioni vigenti in materia di trattamento di dati personali e osserva scrupolosamente quanto in esse previsto, nonché le seguenti istruzioni.

Art. 2 (Istruzioni per il trattamento dei dati personali)

Il ***<indicare nome e cognome>***, Soggetto designato, nell'ambito delle sue funzioni, presiede ai trattamenti di dati personali di competenza di Arsial, la cui elencazione e descrizione è riportata nel "Registro delle attività di trattamento" di cui all'articolo 30 del RGPD, attenendosi al rispetto delle seguenti **istruzioni**:

a) i trattamenti devono essere svolti nel pieno rispetto delle previsioni normative vigenti in materia di protezione dei dati personali, nonché tenendo conto dei provvedimenti e dei comunicati ufficiali emessi dall'Autorità Garante per la Protezione dei Dati Personali, di seguito denominata Garante;

b) la raccolta dei dati personali e la loro successiva registrazione devono avvenire per il solo perseguimento delle finalità istituzionali di ARSIAL e, comunque, per scopi:

1) determinati, pertanto non è consentita la raccolta come attività fine a sé stessa;
2) espliciti, quindi il soggetto interessato deve essere informato sulle finalità del trattamento;
3) legittimi, pertanto, oltre al trattamento, anche il fine della raccolta dei dati deve essere lecito;

c) i dati personali trattati sono: dati genericamente di natura personale (articolo 4, n. 1), del GDPR); dati sensibili (articolo 9 del GDPR "*Categorie particolari di dati personali*"); dati giudiziari (articolo 10 del GDPR);

d) le categorie di interessati sono quelle identificate nelle parti di competenza di Arsial del "Registro delle attività di Trattamento" di cui all'articolo 30 del GDPR;

e) le operazioni di trattamento nell'ambito della struttura di competenza, dovranno essere organizzate in conformità con la normativa in materia di protezione dei dati personali applicabile ed in osservanza delle eventuali indicazioni scritte impartite da Arsial, assicurando l'applicazione del principio della protezione dei dati fin dalla progettazione e protezione predefinita di cui all'articolo 25 del GDPR, determinando i mezzi del trattamento e mettendo in atto le misure tecniche e organizzative adeguate, di cui all'articolo 32 del RGPD, prima dell'inizio delle attività. Inoltre, dovrà essere adottata ogni misura adeguata, fisica e logica, atta a garantire che i dati personali siano trattati in ossequio al principio di necessità e che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse (privacy by default);

f) in veste di Soggetto designato al trattamento dei dati personali, dovrà collaborare con il Titolare del trattamento affinché siano garantiti tutti i diritti dell'interessato di cui al Capo III del RGPD. In particolare, dovrà attenersi ad ogni istruzione scritta impartita al riguardo dal Titolare;

g) dovranno essere rese disponibili al Titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti previsti dalla normativa in materia di protezione dei dati personali relativamente alla struttura di competenza, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal Titolare stesso, dal Responsabile della Protezione dei Dati o da un altro soggetto incaricato;

h) informare il Titolare del trattamento ed il Responsabile della Protezione dei Dati personali, qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti;

i) i dati devono, inoltre, essere:

1) esatti, cioè precisi e rispondenti al vero e, se necessario, aggiornati;
2) pertinenti, ovvero il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
3) completi: idonei a contemplare specificamente il concreto interesse e diritto del soggetto interessato (da non intendersi nel senso di raccogliere il maggior numero di informazioni possibili);

4) non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;

5) conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita;

l) ciascun trattamento deve avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento; deve pertanto essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi;

m) se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dalla normativa vigente in materia di protezione dei dati personali, è necessario provvedere, previa comunicazione al Responsabile della Protezione dei Dati (DPO) della Regione, al blocco dei dati stessi, ossia alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento, fornendo, ad esempio, l'informativa omessa, ovvero provvedendo alla cancellazione dei dati se non è possibile procedere alla regolarizzazione.

2. In conformità alla normativa vigente in materia di protezione dei dati personali ed in osservanza delle eventuali indicazioni scritte impartite al riguardo dal Titolare del trattamento, dovrà:

a) individuare e, se presenti, designare le persone autorizzate al trattamento, detti incaricati, che prestano la propria attività in Arsial nonché un referente privacy per il supporto nello svolgimento dei compiti e funzioni conferiti dal Titolare in materia di trattamento dei dati personali;

b) controllare l'operato degli incaricati al trattamento, nonché sensibilizzare gli stessi sugli aspetti normativi ed organizzativi in materia di tutela dei dati personali;

c) garantire che i profili di accesso ai sistemi informativi da parte degli incaricati al trattamento siano configurati anteriormente all'inizio del trattamento, nonché verificare, almeno una volta l'anno, che tali profili siano conformi con le mansioni svolte. In caso di sospensione dall'attività lavorativa o revoca/esclusione dall'incarico dovrà essere comunicato alle strutture competenti la necessità di procedere alla disattivazione dell'utenza;

d) assicurare, il pieno rispetto degli adempimenti formali nei modi e nei tempi previsti dalla normativa vigente, tra i quali la predisposizione e il rilascio di informative e la gestione dei diritti degli interessati;

e) collaborare con il Garante in caso di ispezioni, al fine di fornire informazioni, documenti e ogni facilitazione di accesso alle banche dati inerenti all'Ufficio di competenza;

f) collaborare nelle verifiche predisposte dal DPO, al fine di fornire informazioni, documenti e ogni facilitazione di accesso alle banche dati;

g) informare prontamente il DPO di ogni questione rilevante in base alla normativa sulla protezione dei dati personali, come la presentazione di eventuali istanze inerenti all'esercizio dei diritti degli interessati ai sensi degli articoli da 15 a 22 del GDPR;

h) informare tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il DPO di ogni violazione di dati personali (cosiddetto data breach) entro 24 ore dall'avvenuta conoscenza dell'evento. In ogni caso, l'informativa deve essere accompagnata da ogni documentazione utile, per permettere al Titolare, ove ritenuto necessario, di notificare tale violazione al Garante e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando ne è venuto a conoscenza, ai sensi degli articoli 33 e 34 del GDPR;

i) nel caso in cui il Titolare debba fornire informazioni aggiuntive al Garante, supportare il Titolare stesso nella misura in cui le informazioni richieste e/o necessarie per il Garante siano esclusivamente in possesso del Soggetto designato;

l) collaborare, alla redazione ed aggiornamento del Registro delle attività di trattamento di cui all'articolo 30 del GDPR, cooperando con il Titolare e con il Garante, laddove ne venga fatta richiesta ai sensi dell'articolo 30, paragrafo 4, del GDPR;
l'informativa omessa, ovvero provvedendo alla cancellazione dei dati se non è possibile procedere alla regolarizzazione.
2. In conformità alla normativa vigente in materia di protezione dei dati personali ed in osservanza delle eventuali indicazioni scritte impartite al riguardo dal Titolare del trattamento, dovrà:
a) individuare e, se presenti, designare le persone autorizzate al trattamento, detti incaricati, che prestano la propria attività in Arsial nonché un referente privacy per il supporto nello svolgimento dei compiti e funzioni conferiti dal Titolare in materia di trattamento dei dati personali;
b) controllare l'operato degli incaricati al trattamento, nonché sensibilizzare gli stessi sugli aspetti normativi ed organizzativi in materia di tutela dei dati personali;
c) garantire che i profili di accesso ai sistemi informativi da parte degli incaricati al trattamento siano configurati anteriormente all'inizio del trattamento, nonché verificare, almeno una volta l'anno, che tali profili siano conformi con le mansioni svolte. In caso di sospensione dall'attività lavorativa o revoca/esclusione dall'incarico dovrà essere comunicato alle strutture competenti la necessità di procedere alla disattivazione dell'utenza;
d) assicurare, il pieno rispetto degli adempimenti formali nei modi e nei tempi previsti dalla normativa vigente, tra i quali la predisposizione e il rilascio di informative e la gestione dei diritti degli interessati;
e) collaborare con il Garante in caso di ispezioni, al fine di fornire informazioni, documenti e ogni facilitazione di accesso alle banche dati inerenti all'Ufficio di competenza;
f) collaborare nelle verifiche predisposte dal DPO, al fine di fornire informazioni, documenti e ogni facilitazione di accesso alle banche dati;
g) informare prontamente il DPO di ogni questione rilevante in base alla normativa sulla protezione dei dati personali, come la presentazione di eventuali istanze inerenti all'esercizio dei diritti degli interessati ai sensi degli articoli da 15 a 22 del GDPR;
h) informare tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il DPO di ogni violazione di dati personali (cosiddetto data breach) entro 24 ore dall'avvenuta conoscenza dell'evento. In ogni caso, l'informativa deve essere accompagnata da ogni documentazione utile, per permettere al Titolare, ove ritenuto necessario, di notificare tale violazione al Garante e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando ne è venuto a conoscenza, ai sensi degli articoli 33 e 34 del GDPR;
i) nel caso in cui il Titolare debba fornire informazioni aggiuntive al Garante, supportare il Titolare stesso nella misura in cui le informazioni richieste e/o necessarie per il Garante siano esclusivamente in possesso del Soggetto designato;
l) collaborare, alla redazione ed aggiornamento del Registro delle attività di trattamento di cui all'articolo 30 del GDPR, cooperando con il Titolare e con il Garante, laddove ne venga fatta richiesta ai sensi dell'articolo 30, paragrafo 4, del GDPR;
m) collaborare, unitamente al DPO, allo svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'articolo 35 del RGPD e nella eventuale consultazione del Garante, prevista ai sensi dell'articolo 36 del GDPR;
n) garantire che la protezione dei dati personali sia realizzata in base alle misure di sicurezza previste dall'articolo 32 del GDPR idonee a ridurre al minimo i rischi di divulgazione, distruzione, perdita o modifica anche accidentale o illegale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
o) collaborare, in caso di modifica della normativa in materia di protezione dei dati personali e nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse, con il Titolare e con il

DPO, affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti introdotti;
p) proporre al Titolare la designazione di eventuali ulteriori Responsabili del trattamento individuati in conformità alle relative disposizioni del GDPR;
q) designare gli amministratori di sistema, nel rispetto di quanto previsto dal Provvedimento del Garante della Protezione dei dati Personali 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) nonché degli ulteriori criteri e modalità e darne comunicazione all' Area competente in materia di sistemi informativi.
3. In particolare il Soggetto Designato al trattamento, dott. agr. Fabio Genchi, nell'ambito di compiti e responsabilità assegnati, dovrà:
- verificare e controllare che il trattamento dei dati sia effettuato in conformità al GDPR;
- individuare, nominare e designare per iscritto il personale autorizzato al trattamento dei dati;
- collaborare alla redazione del piano di formazione aziendale in ambito privacy, fornendo al Titolare il fabbisogno formativo di Arsial e garantendo che il personale addetto al trattamento dei dati, che agisce sotto la propria autorità, partecipi agli eventi formativi organizzati dall'Ente;
impartire le disposizioni organizzative, operative e fornire al personale autorizzato (incaricati) le istruzioni per il corretto, lecito, pertinente e sicuro trattamento dei dati, eseguendo gli opportuni controlli;
- sovrintendere e vigilare sui corretti comportamenti e sull'attuazione delle istruzioni impartite ai referenti privacy e agli incaricati del trattamento dei dati;
- adottare le misure e disporre gli interventi necessari per la sicurezza del trattamento dei dati e per la correttezza dell'accesso ai dati, sulla base delle direttive e dei programmi definiti dal Titolare;
- assicurare e curare, ai sensi degli artt. 13 e 14 del Reg. UE 679/2016, mediante l'utilizzo della modulistica di sistema predisposta e/o altre forme idonee di informazione la corretta raccolta dei dati come da informativa resa agli interessati, l'acquisizione del consenso degli interessati, laddove previsto;
- collaborare con il Titolare, per l'evasione di eventuali richieste dello interessato, ai fini dell'esercizio dei diritti dello stesso, ai sensi degli artt. 15 – 22 del GDPR;
- collaborare con il Titolare per l'evasione delle richieste degli interessati ai sensi del GDPR e delle istanze del Garante per la protezione dei dati personali;
- collaborare per la mappatura dei trattamenti, per il censimento delle banche dati e dei trattamenti dei dati svolti per conto del titolare da responsabili del trattamento esterni, ai fini della redazione e aggiornamento del registro dei trattamenti;
- informare il Titolare rispetto all'introduzione di eventuali nuovi trattamenti nonché rispetto alla cessazione di altri trattamenti, svolti in modalità cartacea e/o automatizzata;
- proporre al Titolare del trattamento dei dati la nomina di soggetti esterni quali Responsabili del trattamento dati in relazione all'affidamento agli stessi di determinate attività, nell'ambito dei compiti istituzionali dell'Amministrazione;
- sovrintendere ai procedimenti di comunicazione, diffusione, trasformazione, blocco, aggiornamento, rettificazione e integrazione dei dati;
- collaborare con il Titolare all'attuazione e all'adempimento degli obblighi previsti dal GDPR e segnalare eventuali problemi applicativi e/o violazioni dei dati personali verificatesi, al DPO nominato, per consentirne la valutazione e l'eventuale comunicazione all'Autorità Garante e agli interessati in conformità con le procedure di Arsial che disciplinano la materia.
4) Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Luogo e data:

IL TITOLARE DEL TRATTAMENTO

Per il Cda: Il Presidente _____

Per accettazione

Luogo e data

Il SOGGETTO DESIGNATO_____

ALLEGATO 4b

LETTERA DI INCARICO PER LA PERSONA AUTORIZZATA AL TRATTAMENTO

Premesso che

per effetto del Regolamento Europeo n. 2016/679 il Titolare del Trattamento ha l'obbligo di adottare specifiche misure organizzative e di impartire istruzioni a tutti coloro che sono stati autorizzati al trattamento dei dati personali (artt. 5, 24, 29 e 32).

_____ in qualità di legale rappresentante di Arsial, titolare del trattamento
(o per suo conto il Soggetto Designato al trattamento) _____

NOMINA

NOME e COGNOME, CODICE FISCALE

Persona Autorizzata al Trattamento delle sottoelencate banche dati elettroniche e cartacee:

Informazioni

Al fine di adempiere alle attività di trattamento dei dati personali che rientrano nell'ambito della propria mansione, si forniscono le seguenti istruzioni.

ISTRUZIONI:

Per i trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici, le Persone Autorizzate al Trattamento dei dati personali devono osservare le seguenti disposizioni:

- Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità dichiarate dall'Agenzia nel registro dei trattamenti e, pertanto, in conformità alle informazioni che l'Agenzia comunica agli interessati. L'eventuale raccolta di dati dovrà avvenire nel rispetto delle procedure e dei modelli di informativa messi a disposizione dell'Agenzia;
- La Persona Autorizzata al Trattamento deve prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi;
- La Persona Autorizzata al Trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente.
- Ogni Persona Autorizzata al Trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta, così come risulta dalla prassi dell'Agenzia;
- La Persona Autorizzata al Trattamento dei dati personali che ha ricevuto le credenziali di autenticazione per il trattamento dei dati personali, deve conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo;
- La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;

- La componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili alla Persona Autorizzata al Trattamento;
- Le credenziali devono essere modificate alla scadenza;
- La Persona Autorizzata al Trattamento non deve in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici le Persone Autorizzata al Trattamento dei dati personali debbono osservare le seguenti disposizioni:

- Ove per ragioni connesse all'attività dell'Ufficio si disponesse di dati sensibili le relative pratiche devono essere trattate con assoluta riservatezza sia con riferimento al supporto cartaceo che al supporto informatico, e devono essere conservati in cassetti o armadi chiusi a chiave;
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dell'Ufficio se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;
- Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, la Persona Autorizzata al Trattamento non dovrà lasciarli mai incustoditi;
- Al termine dell'orario di lavoro la Persona Autorizzata al Trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione;
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro se l'ufficio è aperto al pubblico;
- Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici;
- Per evitare il rischio di diffusione dei dati personali si deve limitare l'utilizzo di copie fotostatiche;
- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura;
- È tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti;
- Quando i documenti devono essere trasportati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, la Persona Autorizzata al Trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti;
- È proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia una Persona Autorizzata al Trattamento a potere trattare i dati in questione;
- Si raccomanda vivamente non parlare mai ad alta voce, trattando dati personali per telefono in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.

Le istruzioni sopra descritte fanno parte integrante della prestazione lavorativa e pertanto sono a lei dovuti in base al vigente contratto di lavoro.

Nel caso di inadempimento si applicheranno le sanzioni disciplinari previste dal vigente contratto di lavoro.

La presente lettera di incarico si intenderà revocata in qualsiasi momento, con effetto immediato e senza obbligo di preavviso o di diritto alla scadenza del rapporto o alla risoluzione, per qualsiasi causa, dello stesso.

Persona autorizzata al trattamento (*Per presa visione dell'incarico)*	**Titolare del trattamento Arsial o per suo conto il Soggetto Designato al trattamento**
_____	_____

ALLEGATO 4c

NOMINA AMMINISTRATORE DI SISTEMA INTERNO

Tenuto conto delle mansioni svolte alle dipendenze di Arsial;

Considerato che per preparazione ed esperienza Lei fornisce idonea garanzia del pieno rispetto della normativa in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza informatica;

Arsial, rappresentato dal Consiglio di amministrazione, nomina quale **Amministratore Di Sistema**:

Cognome e Nome:_____
Codice fiscale: _____
Data e Luogo di Nascita: _____
Residenza: _____
Recapiti telefonici (per emergenze): _____

Per i seguenti ambiti

Banca Dati	**Descrizione Attività Da Svolgere**
Specificare	Specificare

Per le tipologie e i profili di autorizzazione di seguito descritti

Abilitazione	**Tipologia Amministratore**	**Profilo di Autorizzazione**
SI/NO	***Enterprise Administrator***	• Accesso completo a tutti i dati e a tutte le macchine appartenenti a tutti i domini della rete (a meno di diversa ed esplicita configurazione); • Creazione degli account ed abilitazione degli accessi agli Amministratori di livello 0, 1 e 2 di tutti i domini; • Analisi e controllo dei log di tutte le macchine appartenenti a tutti i domini e dei dispositivi di tutta la rete.
SI/NO	***Domain Administrator***	• Accesso completo a tutti i dati ed a tutte le macchine appartenenti ad un singolo dominio della rete (a meno di diversa ed esplicita configurazione); • Creazione degli account e all'abilitazione degli accessi agli Administrator di livello 0, 1 e 2 del solo dominio di appartenenza; • Analisi e controllo dei log di tutte le macchine appartenenti al solo dominio di appartenenza e dei dispositivi della porzione di rete gestita.
SI/NO	***Server Administrator***	• Accesso completo al sistema ed ai dati contenuti nel server (a meno di diversa ed esplicita configurazione: es. escluso data base); • A compiere qualsiasi operazione sistemistica e di modifica della configurazione del server; • Analisi e controllo dei log.
SI/NO	***Account Administrator***	• Creazione/disabilitazione degli account utente; • Assegnazione del profilo di autorizzazione all'account utente.
SI/NO	***Network Administrator***	• Accesso completo ai dispositivi di comunicazione (es. router, switch, hub, centrale telefonica) ed alle linee di comunicazione; • Compiere qualsiasi operazione di modifica della configurazione

		dei dispositivi di comunicazione; • Analisi e controllo dei log, del traffico dati e telefonico.
SI/NO	***Security Administrator***	• Accesso completo ai dispositivi di sicurezza (es. Firewall, Antivirus, Log Management, Traffic analyzer); • Compiere qualsiasi operazione di modifica della configurazione dei dispositivi di sicurezza; • Analisi e controllo dei log.
SI/NO	***Database Administrator***	• Accesso completo al motore del database ed ai dati memorizzati; in casi particolari è possibile autorizzare anche la singola istanza di database; • A compiere qualsiasi operazione di modifica della configurazione e degli schemi dei database; • Analisi e controllo dei log.
SI/NO	***Backup Administrator***	• Accesso (almeno in lettura): - Dei dump dei database (o direttamente delle istanze in caso di utilizzo di agent); - Delle share di rete; - Dei system state e degli snapshot delle macchine; - Delle configurazioni (che necessitano di backup); - Degli export di specifici servizi; - Dei log di tutte le macchine della rete.
SI/NO	***Service / Application Administrator***	• Gestione, modifica delle configurazione, stop/start del singolo servizio o applicazione; • Analisi e controllo dei log specifici del servizio o applicazione.
SI/NO	***Local Administrator - Technical Support***	• Accesso completo ad un insieme specificato nella nomina di sistemi client ed ai dati contenuti nei dispositivi di memorizzazione (a meno di diversa ed esplicita configurazione); • Analisi e controllo dei log locali.

ISTRUZIONI

L'Amministratore di Sistema è tenuto:

- ad informare prontamente il Responsabile Della Protezione Dei Dati personali ed il Titolare del Trattamento in caso di violazione dei dati personali, al fine di consentire l'attivazione della procedura prevista dalla norma quando ricorre tale situazione (data breach);
- ad osservare la massima riservatezza in merito alle informazioni ottenute nello svolgimento dell'attività, incluse le informazioni relative alla situazione di sicurezza dell'organizzazione, come sistemi operativi, applicativi software, documentazione, architettura e connessioni di rete;
- a predisporre un sistema di registrazione dei suoi accessi logici ai sistemi informatici, che consentano di risalire al tempo e alle modalità di accesso;
- ad attuare le misure di sicurezza indicate nella circolare Agid n. 2 del 28.4.2017;
- ad implementare e a tenere aggiornate le misure di sicurezza informatiche così come previsto dalle procedure dell'Ente (antispam, antivirus, firewall, ecc).
- ad impostare e gestire un sistema di autenticazione informatica così come previsto dalle procedure dell'Ente;
- alla gestione del salvataggio dei dati così come previsto dalle procedure dell'Ente;
- ad adottare le procedure, per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi e organizzare il salvataggio dei dati, così come previsto dalle procedure dell'Ente;
- a sottoporre all'attenzione del Titolare Del Trattamento le situazioni di rischio informatico considerate non accettabili;
- ad aggiornare l'inventario delle risorse informatiche quando nuovi dispositivi approvati vengono collegati in rete;

- a gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP o quanto indicato dalle procedure dell'Ente;
- a stilare un elenco dei software autorizzati e relative versioni necessario per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi;
- a verificare che sui sistemi presenti in azienda non vi siano software non autorizzati;
- ad utilizzare configurazioni sicure standard per la protezione dei sistemi operativi;
- a conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza;
- ad utilizzare credenziali amministrative riconducibili ad una sola persona;
- a sostituire le utenze amministrative con sufficiente frequenza (password aging);
- a suggerire al Titolare Del Trattamento l'adozione e l'aggiornamento delle più ampie misure di sicurezza, anche tenendo conto dello stato dell'arte e dei costi di attuazione, atte a realizzare quanto previsto dalla normativa privacy in materia di sicurezza del trattamento;
- a collaborare attivamente con il Titolare Del Trattamento, con il Responsabile Del Trattamento e con il Responsabile Della Protezione Dei Dati per assicurare che il trattamento sia conforme a quanto previsto dalla normativa e dalle procedure adottate dall'Ente;
- a collaborare con i soggetti incaricati dall'Ente per la redazione della valutazione d'impatto sulla protezione dei dati.

La presente lettera di incarico si intenderà revocata di diritto alla scadenza del rapporto o alla risoluzione, per qualsiasi causa, dello stesso.

Luogo, data

L'Amministratore Di Sistema	**Il Titolare Del Trattamento o per suo conto il Soggetto Designato al trattamento**
(*Per accettazione dell'incarico*)	
_____	_____

ALLEGATO 4d

INFORMATIVA AI SENSI DELL'ARTICOLO 13 DEL REGOLAMENTO EUROPEO N. 2016/679

Si forniscono le seguenti informazioni relative al trattamento dei dati personali.

Nota: Gli articoli citati si riferiscono al Regolamento Europeo n. 2016/679

Titolare del trattamento	Denominazione: …….. Indirizzo postale:…….. Indirizzo di posta elettronica: …… Numero di telefono: …….
Responsabile della protezione dati	Indirizzo di posta elettronica presso l'Ente del RPD: … Indirizzo postale: …….
Finalità	Finalità perseguite dal trattamento
Base giuridica	• Art. 6 GDPR (Liceità del trattamento) • Art. 9 GDPR (Trattamento di categorie particolari di dati) Specificare:……
Destinatari dei dati personali	Indicare i destinatari ……..
Trasferimento dei dati personali a un Paese terzo o a un'organizzazione internazionale	SI/NO
Periodo/criteri di conservazione	Indicare periodo e/o criteri di conservazione
Diritti dell'Interessato	Lei potrà, in qualsiasi momento, esercitare i diritti: • di richiedere maggiori informazioni in relazione ai contenuti della presente informativa • di accesso ai dati personali; • di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano (nei casi previsti dalla normativa); • di opporsi al trattamento (nei casi previsti dalla normativa); • alla portabilità dei dati (nei casi previsti dalla normativa); • di revocare il consenso, ove previsto; la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso conferito prima della revoca; • di proporre reclamo all'autorità di controllo (Garante Privacy); • di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro per l'esercizio dei suoi diritti; • di richiedere il risarcimento dei danni conseguenti alla violazione della normativa.
Obbligatorietà della fornitura dei dati personali e le possibili conseguenze della mancata comunicazione di tali dati	Indicare se e per quale motivo……
ART: 13-14 Esistenza di un processo decisionale automatizzato, compresa la profilazione	SI/NO

ALLEGATO 4e

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI
degli utenti che consultano i siti web di ARSIAL
ai sensi dell'articolo 13 del Regolamento (UE) 2016/679

Gentile Utente,

in questa pagina sono descritte le modalità di gestione del portale dell'Agenzia regionale per lo sviluppo e l'innovazione dell'agricoltura del Lazio (di seguito "Arsial" o "Ente") relativamente al trattamento dei dati personali degli utenti che lo consultano.
Si tratta di un'informativa resa ai sensi dell'art. 13 del Regolamento UE n. 2016/679 "Regolamento Generale sulla protezione dei dati" (di seguito "RGPD" o "Regolamento") agli utenti che interagiscono con il sito istituzionale di Arsial a partire dall'indirizzo www.arsial.it, e non con altri domini web esterni ed eventualmente collegati a questo tramite link.
A seguito della consultazione dei siti sopra elencati possono essere trattati dati relativi a persone fisiche identificate o identificabili.

1. TITOLARE DEL TRATTAMENTO

Titolare del trattamento è A.R.S.I.A.L., l'Agenzia regionale per lo sviluppo e l'innovazione dell'agricoltura del Lazio, con sede in Via Rodolfo Lanciani, 38, 00162 Roma, e-mail: strutturainternareferenteprivacy@arsial.it PEC: arsial@pec.arsialpec.it.

2. RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati personali (o DPO) è Management and Consulting S.r.l., con sede in via Vespasiano, 12, 00192 Roma.
Il punto di contatto per il Responsabile della protezione dei dati è: Dott. Luca Petrucci
e-mail: privacy@mandc.it
PEC: mac-srl@pec.it.

3. BASE GIURIDICA DEL TRATTAMENTO

I dati personali indicati in questa pagina sono trattati dall'Agenzia regionale per lo sviluppo e l'innovazione dell'agricoltura del Lazio nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri ai sensi dell'art. 6, paragrafo 1, lett. e) del Regolamento UE n. 2016/679.

4. TIPI DI DATI TRATTATI E FINALITÀ DEL TRATTAMENTO

Dati di navigazione
I sistemi informatici e le procedure software preposte al funzionamento di questo sito acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer e dei terminali utilizzati dagli utenti, gli indirizzi in notazione URI/URL (Uniform Resource Identifier/Locator) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Tali dati, necessari per la fruizione dei servizi web, vengono anche trattati allo scopo di:
• ottenere informazioni statistiche sull'uso dei servizi (pagine più visitate, numero di visitatori per fascia oraria o giornaliera, aree geografiche di provenienza, ecc.);

• controllare il corretto funzionamento dei servizi offerti.

Dati personali comunicati dall'utente
L'invio facoltativo, esplicito e volontario di messaggi agli indirizzi di contatto di Arsial pubblicati sul portale istituzionale, di messaggi inviati dagli utenti ai profili/alle pagine istituzionali sui social media, nonché la compilazione e l'inoltro dei moduli presenti sui siti dell'Ente, al fine di ottenere notizie e informazioni sui servizi offerti dallo stesso, comportano l'acquisizione dei dati di contatto del mittente (nome, cognome, email, ecc.), necessari a rispondere, nonché di tutti i dati personali inclusi nelle comunicazioni.

I dati personali forniti dagli utenti che inoltrano richieste sono utilizzati al solo fine di dare esecuzione alla richiesta di volta in volta inoltrata.
Specifiche informative verranno pubblicate nelle pagine dei siti dell'Ente predisposte per l'erogazione di determinati servizi, ove presenti.

5. DESTINATARI DEI DATI
I dati personali degli utenti di cui al punto 4 della presente informativa, raccolti a seguito della consultazione del sito istituzionale di Arsial, possono essere comunicati ai soggetti designati dall'Ente ai sensi dell'art. 28 del Regolamento n. 2016/679, quali responsabili del trattamento.
In particolare, tali dati possono essere comunicati a LAZIOcrea S.p.A., quale fornitore dei servizi di sviluppo, assistenza tecnica e manutenzione adeguativa, evolutiva e correttiva del sito istituzionale dell'Ente e del portale web.
Sui responsabili del trattamento sono imposti, da parte di Arsial, mediante contratto o altro atto giuridico a norma del diritto dell'UE o degli Stati membri, opportuni obblighi in materia di protezione dei dati personali attraverso istruzioni operative, con particolare riferimento all'adozione di misure tecniche ed organizzative adeguate, al fine di poter garantire la riservatezza e la sicurezza dei dati ai sensi dell'art. 32 del Regolamento UE n. 2016/679.
I dati personali raccolti sono altresì trattati dal personale dell'Ente autorizzato che agisce sulla base di specifiche istruzioni fornite in ordine a finalità e modalità del trattamento, solo qualora il trattamento sia necessario allo svolgimento delle mansioni assegnate.
Al di fuori di queste ipotesi i dati non saranno comunicati a terzi né diffusi, se non nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

6. TRASFERIMENTO DEI DATI PERSONALI VERSO PAESI NON APPARTENENTI ALL'UNIONE EUROPEA

I dati personali raccolti non vengono trasferiti a paesi terzi al di fuori dello Spazio Economico Europeo.

7. LINK A SITI ESTERNI

Questo sito internet contiene collegamenti ipertestuali detti "link" (ossia strumenti che consentono il collegamento ad una pagina web di un altro sito): i siti esterni raggiungibili tramite link attraverso il portale di Arsial sono sviluppati e gestiti da soggetti sui quali l'Ente non ha alcuna titolarità né controllo e non è in alcun modo responsabile circa contenuti, qualità, accuratezza e servizi offerti. La visita e l'utilizzo dei siti consultati dall'utente dal presente sito tramite link, quindi, è rimessa esclusivamente alla discrezionalità e responsabilità dell'utente. La presente informativa, pertanto, è resa solo per i siti di Arsial e non anche per altri siti web eventualmente consultati dall'utente tramite link.

8. CONFERIMENTO FACOLTATIVO DEI DATI
Fatto salvo quanto specificato per i dati di navigazione, l'utente è libero di fornire i dati personali richiesti dalla modulistica da inoltrare all'Ente. Il mancato conferimento di determinati dati personali, nei moduli e nelle comunicazioni di richiesta di informazioni, può comportare esclusivamente l'impossibilità di ottenere una risposta.

9. DURATA DI CONSERVAZIONE

I dati personali saranno conservati per un periodo di tempo non superiore al conseguimento delle finalità per

cui sono stati raccolti, in conformità al principio di limitazione della conservazione di cui all'art. 5 del Regolamento UE n. 2016/679 o in base alle scadenze previste dalle norme di legge. I dati di navigazione non persistono per più di sette giorni e vengono cancellati immediatamente dopo la loro aggregazione, salve eventuali necessità di accertamento di reati da parte dell'Autorità giudiziaria.

10. DIRITTI DEGLI INTERESSATI

Gli interessati hanno facoltà di esercitare, in ogni momento, i diritti previsti dagli artt. 15 e ss. del Regolamento UE n. 2016/679, ove applicabili. Fra questi si segnalano, in conformità a quanto previsto dall'art. 13, comma 2, lett. b) del Regolamento: il diritto di chiedere l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o di opporsi al loro trattamento, oltre il diritto alla portabilità dei dati, nei casi previsti.

Al fine di esercitare i propri diritti, gli interessati possono presentare le relative richieste ad Arsial, in qualità di titolare del trattamento, al seguente indirizzo strutturainternareferenteprivacy@arsial.it PEC: arsial@pec.arsialpec.it.

11. DIRITTO DI RECLAMO

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti effettuato attraverso questo sito avvenga in violazione di quanto previsto dal RGPD hanno il diritto di proporre reclamo al Garante per la protezione dei dati personali, come previsto dall'art. 77 del Regolamento UE n. 2016/679, seguendo le procedure e le indicazioni pubblicate sul sito web ufficiale dell'Autorità su www.garanteprivacy.it., o di adire le opportune sedi giudiziarie ai sensi dell'art. 79 del Regolamento.

12. PROFILAZIONE

Non sono svolti processi decisionali automatizzati sui dati personali raccolti, non si profilano gli utenti del portale www.arsial.it.

ALLEGATO 4f

INFORMATIVA AI SENSI DELL'ARTICOLO 13 DEL REGOLAMENTO EUROPEO N. 2016/679

Si forniscono le seguenti informazioni relative al trattamento dei dati personali: "***registrazione e archiviazione delle presenze dei visitatori negli uffici di Arsial***"

Nota: Gli articoli citati si riferiscono al Regolamento Europeo n. 2016/679

Titolare del trattamento	Denominazione: ARSIAL Indirizzo postale: via Rodolfo Lanciani 38, 00162 Roma (RM) Email / PEC: arsial@pec.arsialpec.it Recapito telefonico: 06.86.273.675/606 Sito web: www.arsial.it
Responsabile della protezione dati	Denominazione: Management and Consulting S.r.l. Indirizzo di posta: privacy@mandc.it PEC mac-srl@mandc.it Indirizzo postale: via Vespasiano, 12, 00192 Roma (RM)
Finalità	Acceso fisico agli uffici di Arsial
Base giuridica	• Art. 6, paragrafo 1, lett. e): il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri
Destinatari dei dati personali	Responsabili del trattamento:…….. Persone autorizzate al trattamento dei dati che La riguarda/interessa:…….
Trasferimento dei dati personali a un Paese terzo o a un'organizzazione internazionale	NO
Periodo/criteri di conservazione	I documenti d'identità saranno conservati per il periodo di permanenza del visitatore nei locali di Arsial. I dati personali saranno conservati per il tempo strettamente necessario al perseguimento delle finalità per cui sono trattati, nei limiti stabiliti dalla normativa vigente e, comunque, non oltre il termine di 3 mesi dall'ultimo accesso alle sedi di Arsial.
Diritti dell'Interessato	Lei potrà, in qualsiasi momento, esercitare i diritti: • di richiedere maggiori informazioni in relazione ai contenuti della presente informativa; • di accesso ai dati personali; • di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano (nei casi previsti dalla normativa); • di opporsi al trattamento (nei casi previsti dalla normativa); • alla portabilità dei dati (nei casi previsti dalla normativa); • di revocare il consenso, ove previsto; la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso conferito prima della revoca; • di proporre reclamo all'autorità di controllo (Garante per la protezione dei dati personali); • di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro per l'esercizio dei suoi diritti;

	• di richiedere il risarcimento dei danni conseguenti alla violazione della normativa.
Obbligatorietà della fornitura dei dati personali e le possibili conseguenze della mancata comunicazione di tali dati	Il conferimento dei dati personali è facoltativo; resta inteso che l'eventuale rifiuto a fornire tali dati comporterà l'impossibilità di accesso negli uffici di Arsial.
ART: 13-14 Esistenza di un processo decisionale automatizzato, compresa la profilazione	NO

ALLEGATO 4g

RESPONSABILE DEL TRATTAMENTO, AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679
ADDENDUM CONTRATTUALE

"_____" in qualità di legale rappresentante di Arsial, titolare del trattamento da una parte, e

"_____" con sede in _____ P.IVA: _____ (qui di seguito "il Responsabile del trattamento")

Si conviene e stipula quanto di seguito riportato, quale addendum al contratto _____

Oggetto:

Oggetto del presente addendum contrattuale è definire le modalità attraverso le quali il Responsabile del trattamento si impegna a effettuare per conto del Titolare, le operazioni di trattamento dei dati personali definiti di seguito.
In particolare, i trattamenti del presente contratto sono:

_____

Il responsabile del trattamento è vincolato al rispetto di quanto di seguito previsto:

• **Informazioni**	
Trattamento	Inserire denominazione
Tipo Finalità	Finalità perseguite dal trattamento
Natura del trattamento	Se il trattamento potrà essere svolto sia in forma automatizzata che in forma non automatizzata
Durata del Trattamento	Di solito equivale alla durata del rapporto contrattuale sottostante
Dati Trattati	Tipologia di dato trattato, in base alla seguente classifica: • personale (art. 4, punto 1) RGPD) • personali giudiziari (art. 10 del RGPD) • personali sensibili (art. 9 del RGPD)
Categoria Interessati	Persona fisica cui si riferisce il dato trattato.

Il **Responsabile Del Trattamento** si impegna a:

a) Trattare i dati solo per la finalità o le finalità sopra specificate e per l'esecuzione delle prestazioni contrattuali;
b) mettere in atto misure tecniche e organizzative coerenti con i principi del Regolamento UE 2016/679 (GDPR). Inoltre, se il Responsabile del trattamento è tenuto a procedere ad un trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione o delle leggi dello stato membro alle quali è sottoposto, deve informare il Titolare del trattamento di questo

obbligo giuridico prima del trattamento, a meno che le leggi interessate proibiscano tale informazione per rilevanti motivi di interesse pubblico;

c) all'annotazione del trattamento nel registro dei trattamenti cosi come previsto dall'art.28 del Regolamento UE 2016/679;
d) a non ricorrere ad altro responsabile senza previa autorizzazione scritta, specifica o generale, dell'Ente;
e) a garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o hanno assunto un adeguato obbligo legale di riservatezza;
f) ad adottare tutte le misure di sicurezza adeguate al trattamento così come previsto dall'art. 32 del Regolamento UE 2016/679;
g) ad assistere Arsial con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
h) ad assistere Arsial nel garantire il rispetto degli obblighi in materia di sicurezza del trattamento, comunicazione di una violazione dei dati, valutazione d'impatto e consultazione preventiva del Garante tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile;
i) a cancellare o restituire tutti i dati personali su richiesta scritta di Arsial e a cancellare le copie esistenti, salvo l'obbligo normativo di conservare i dati;
j) a mettere a disposizione di Arsial tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che derivano dal presente atto;
k) a rispettare il diritto di informazione degli interessati;
l) a esercitare i diritti degli interessati.
   Per quanto possibile, il Responsabile del trattamento deve coadiuvare il Titolare del trattamento nell'adempimento dei propri obblighi di far seguito alle domande di esercizio dei diritti degli interessati: diritto di accesso, di rettifica, di cancellazione e di opposizione, diritto alla limitazione del trattamento.
   Opzione A - Qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento presentando la relativa richiesta, il Responsabile del trattamento deve inoltrare tale richiesta al Titolare del trattamento.
m) a notificare le violazioni dei dati personali. Il Responsabile del trattamento notifica tempestivamente al Titolare del trattamento ogni violazione di dati personali dopo esserne venuto a conoscenza. Tale notifica è accompagnata da ogni documentazione necessaria da poter permettere al Titolare del trattamento, se necessario, di notificare tale violazione all'autorità Garante per la protezione dei dati personali;
n) al termine della prestazione dei servizi relativi al trattamento di questi dati, il Responsabile del trattamento si impegna a:
   A scelta delle parti:
   -Rimandare tutti i dati a carattere personale al Titolare del trattamento
   Il rinvio deve essere accompagnato dalla distruzione di tutte le copie esistenti nei sistemi di informazione del Responsabile del trattamento. Una volta distrutte, il Responsabile del trattamento deve documentare per iscritto l'avvenuta distruzione;
o) a comunicare al Titolare del trattamento il nome ed i dati del proprio Responsabile della protezione dei dati (DPO), qualora ne abbia designato uno conformemente all'articolo 37 del Regolamento Europeo (GDPR);
p) a mettere a disposizione del Titolare del trattamento la documentazione necessaria volta a dimostrare il rispetto di tutti gli obblighi e per permettere la realizzazione di revisioni, comprese le ispezioni, da parte del Titolare del trattamento o di un altro revisore che lui ha incaricato.

Il Responsabile del trattamento acconsente e contribuisce alle attività di revisione, comprese le ispezioni, realizzati da Arsial o da un altro soggetto da questo incaricato.

Il presente incarico avrà la medesima durata del Contratto e, quindi, cesserà con il venire meno di quest'ultimo per qualsivoglia ragione, senza alcuna necessità di atti di revoca o di altra comunicazione in merito.

Con la sottoscrizione del presente atto, _____, in persona del legale rappresentante pro tempore, accetta la nomina, confermando la propria esperienza e capacità nella materia, nonché la conoscenza puntuale delle prescrizioni di Legge, e si impegna a procedere al trattamento dei dati personali attenendosi alle prescrizioni di legge ed alle su esposte istruzioni.

Responsabile Del Trattamento (*Per accettazione dell'incarico*)	**Titolare Del Trattamento** Arsial
_____	_____