

Regione Lazio

DIREZIONE EMERGENZA, PROTEZIONE CIVILE E NUE 112

Atti dirigenziali di Gestione

Determinazione 10 giugno 2024, n. G07557

Decisione di contrarre per affidamento diretto ai sensi dell'art. 50 comma, 1 lettera b) del d.lgs. 36/2023, tramite Ordine diretto d'Acquisto (OdA) sulla piattaforma MePA (www.acquistinretepa.it) della fornitura dei corsi di formazione AIB. Impegno di spesa della somma complessiva pari a 127.940,00 euro (IVA inclusa) a favore di Dream formazione e consulenza Soc. coop. (cod. cred. 250182) sul capitolo U0000E47134 - esercizio finanziario 2024. Impegno di spesa a favore dell'Autorità Nazionale Anticorruzione (cod. cred. 159683) per euro 35,00 sul capitolo U0000T19427 - esercizio finanziario 2024.

Oggetto: decisione di contrarre per affidamento diretto ai sensi dell'art. 50 comma, 1 lettera b) del d.lgs. 36/2023, tramite Ordine diretto d'Acquisto (OdA) sulla piattaforma MePA (www.acquistinretepa.it) della fornitura dei corsi di formazione AIB. Impegno di spesa della somma complessiva pari a 127.940,00 euro (IVA inclusa) a favore di *Dream formazione e consulenza Soc. coop.* (cod. cred. 250182) sul capitolo U0000E47134 - esercizio finanziario 2024. Impegno di spesa a favore dell'Autorità Nazionale Anticorruzione (cod. cred. 159683) per euro 35,00 sul capitolo U0000T19427 - esercizio finanziario 2024.

IL DIRETTORE DELLA DIREZIONE REGIONALE EMERGENZA, PROTEZIONE CIVILE E NUE 112

VISTA la Costituzione della Repubblica italiana;

VISTO lo Statuto della Regione Lazio;

VISTA la legge regionale 18 febbraio 2002, n. 6 *“Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza ed al personale regionale”*

VISTO il regolamento regionale 6 settembre 2002, n. 1 *“Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale” e successive modifiche;*

VISTA la deliberazione della Giunta regionale 26 febbraio 2024, n. 96 con la quale è stato conferito al dott. Massimo La Pietra l'incarico di Direttore della Direzione regionale *“Emergenza, Protezione Civile e Nue112”*;

VISTI:

- il decreto legislativo 23 giugno 2011, n. 118 *“Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42” e successive modifiche;*
- la Legge Regionale 12 agosto 2020, n. 11: *“Legge di contabilità regionale”*;
- il regolamento regionale 9 novembre 2017, n. 26 *“Regolamento regionale di contabilità”* che, ai sensi dell'articolo 56, comma 2, della l.r. n. 11/2020 e fino alla data di entrata in vigore del regolamento di contabilità di cui all'articolo 55 della citata l.r. n. 11/2020, continua ad applicarsi per quanto compatibile con le disposizioni di cui alla medesima l.r. n. 11/2020;
- l'articolo 30, comma 2, del regolamento regionale n. 26/2017, in riferimento alla predisposizione del piano finanziario di attuazione della spesa;
- la legge regionale 29 dicembre 2023, n. 23 *“Legge di stabilità regionale 2024”*;
- la legge regionale 29 dicembre 2023, n. 24 *“Bilancio di previsione finanziario della Regione Lazio 2024-2026”*;
- la deliberazione della Giunta regionale 28 dicembre 2023, n. 980 *“Bilancio di previsione finanziario della Regione Lazio 2024-2026. Approvazione del 'Documento tecnico di accompagnamento', ripartito in titoli, tipologie e categorie per le entrate e in missioni, programmi, titoli e macroaggregati per le spese”*;
- la deliberazione della Giunta regionale 28 dicembre 2023 n. 981 *“Bilancio di previsione finanziario della Regione Lazio 2024-2026. Approvazione del 'Bilancio finanziario gestionale', ripartito in capitoli di entrata e di spesa e assegnazione delle risorse finanziarie ai dirigenti titolari dei centri di responsabilità amministrativa”*;

- la deliberazione della Giunta regionale 14 febbraio 2024 n. 75 “*Indirizzi per la gestione del bilancio regionale 2024-2026 e approvazione del bilancio reticolare, ai sensi degli articoli 30, 31 e 32, della legge regionale 12 agosto 2020, n. 11*”;
- la deliberazione della Giunta regionale 24 aprile 2024 n. 284 “*Bilancio di previsione finanziario della Regione Lazio 2024-2026. Aggiornamento del Bilancio finanziario gestionale in relazione all’assegnazione delle risorse finanziarie ai dirigenti titolari dei centri di responsabilità amministrativa, di cui alla D.G.R. n. 981/2023, ai sensi dell’articolo 13, comma 5, della legge regionale 12 agosto 2020, n. 11*”;

VISTA la comunicazione del Direttore generale, prot. 573860 del 30/04/2024, recante “*indicazioni per l’operatività della riorganizzazione dell’apparato amministrativo disposta dal regolamento regionale 23 ottobre 2023, n. 9 e in attuazione delle direttive I, II, III, IV, V e VI di cui alle note prot. n. 1414222 del 05/12/2023, prot. n. 132306 del 30/01/2024 e prot. n. 0171408 del 06/02/202, prot. n. 0190513 del 09/02/2024, prot. n. 0231852 del 19/02/2024 e prot. n. 281552 del 28/02/2024, con decorrenza 1° maggio 2024*”;

VISTA la legge 7 agosto 1990, n. 241 “*Nuove norme sul procedimento amministrativo*” e successive modifiche, che stabilisce come “*l’attività amministrativa persegue i fini determinati dalla legge ed è retta da criteri di economicità, di efficacia, di pubblicità e di trasparenza*”;

VISTO il decreto legislativo 30 marzo 2001, n. 165 “*Norme generali sull’ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*” e successive modifiche;

VISTO il decreto legislativo 30 giugno 2003, n. 196 “*Codice in materia di protezione dei dati personali*” e successive modifiche;

VISTO il Regolamento UE 2016/679 del Parlamento e del Consiglio Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, di seguito RGPD, che garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riferimento alla riservatezza e al diritto di protezione dei dati personali;

VISTA la legge 27 dicembre 2006, n. 296 “*Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2007)*” e successive modifiche;

VISTA la legge 13 agosto 2010, n. 136 “*Piano straordinario contro le mafie, nonché delega al Governo in materia di normativa antimafia*”, segnatamente alle disposizioni in materia di tracciabilità dei flussi finanziari;

VISTO il decreto legislativo 6 settembre 2011, n. 159 “*Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, a norma degli articoli 1 e 2 della legge 13 agosto 2010, n. 136*”, come modificato dalla legge 17 ottobre 2017, n. 161 e, in particolare, l’art. 83, co. 3, lett. e), che recita “*La documentazione di cui al comma 1 non è comunque richiesta per i provvedimenti, gli atti ed i contratti il cui valore complessivo non sia superiore a 150.000,00*”;

VISTO il decreto legislativo 14 marzo 2013, n. 33 “*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*”;

VISTO il decreto legislativo 31 marzo 2023, n. 36 “*Codice dei contratti pubblici in attuazione dell’articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici*” e successive modifiche;

VISTO l’art. 1, co. 450, della legge n. 296/2006 il quale prevede, tra l’altro, che le amministrazioni pubbliche di cui all’art. 1, del d.lgs. n. 165/2001, per gli acquisti di beni e servizi di importo pari o superiore a 5.000,00 euro e di importo inferiore alla soglia di rilievo comunitario sono tenute a fare ricorso al mercato elettronico della pubblica amministrazione ovvero ad altri mercati elettronici

istituiti ai sensi del medesimo articolo 328 ovvero al sistema telematico messo a disposizione dalla centrale regionale di riferimento per lo svolgimento delle relative procedure;

TENUTO CONTO del disposto dell'art. 1, co. 1, del dl n. 95/2012, convertito con modificazioni, con legge n. 135/2012, che dispone la nullità dei contratti stipulati in violazione degli obblighi di approvvigionarsi attraverso gli strumenti di acquisto messi a disposizione da Consip S.p.A.;

CONSTATATO che non sono disponibili convenzioni Consip S.p.A. raffrontabili con quanto è oggetto di acquisto tramite la presente procedura;

VISTO il decreto legislativo 2 gennaio 2018, n. 1 "*Codice della Protezione civile*" e successive modificazioni;

VISTO il decreto legislativo 3 luglio 2017, n. 117 e successive modificazioni, che reca la nuova disciplina delle Organizzazioni di volontariato, ivi incluse quelle di protezione civile;

VISTI:

- il decreto-legge 8 settembre 2021, n. 120, convertito, con modificazioni, dalla legge n. 155/2021 (*Disposizioni per il contrasto degli incendi boschivi e altre misure urgenti di protezione civile*);
- il decreto del Presidente del Consiglio dei Ministri 13 ottobre 2022 "*Riparto delle risorse del fondo per la realizzazione del piano nazionale azioni di previsione, prevenzione e lotta contro gli incendi boschivi*", che assegna alla Regione Lazio un importo complessivo pari ad euro 1.546.164,35;
- la nota protocollo regionale n. 0903915 del 11/08/2023 "*Regione Lazio. Comunicazione del Piano di impiego delle risorse previste dal Decreto Legge 120/2021. Annualità 2022*", con la quale è stato trasmesso il Piano di impiego delle risorse assegnate alla Regione Lazio per l'annualità 2022;
- la determinazione dirigenziale n. G16186 del 04/12/2023 "*Assegnazione delle risorse relative al finanziamento del "Piano Nazionale Azioni di Previsione, Prevenzione e lotta contro gli incendi boschivi". Decreto del Presidente del Consiglio dei Ministri del 13 ottobre 2022: accertamento complessivo di euro 1.546.164,35, di cui euro 130.000,00 sul capitolo di entrata E0000229181 ed euro 1.416.164,35 sul capitolo di entrata E0000439131, esercizio finanziario 2023*";

CONSIDERATO che l'amministrazione Regionale si avvale in modo continuo e costante, oltre che del proprio personale dipendente e della società partecipata LAZIOcrea S.p.A, dei volontari che operano nel Sistema Integrato di Protezione Civile Regionale per le attività di previsione, prevenzione, emergenza e superamento dell'emergenza;

RILEVATO che la legge regionale n. 2/2014 prevede all'art. 3, comma 1, lettera b) che la prevenzione dei diversi tipi di rischio si esplica in attività non strutturali concernenti l'allertamento, la pianificazione dell'emergenza, la formazione, la diffusione della conoscenza della protezione civile nonché l'informazione alla popolazione e l'applicazione della normativa tecnica;

RITENUTO indispensabile procedere alla formazione e all'aggiornamento di tutto il personale addetto alle attività Anti Incendio Boschivo (AIB);

VISTE le esigenze formative espresse nel Piano di impiego delle risorse di cui al decreto-legge 120/2021 e comunicate con la sopra citata nota n. 0903915/2023:

- corso base di formazione per volontari esperti: formazione di circa 120 volontari;
- corso di formazione sull'utilizzo del controfuoco per i Direttori delle Operazioni di Spegnimento (DOS): formazione di circa n. 120 unità di personale;
- realizzazione di n. 2 cantieri di fuoco prescritto con formazione di n. 50 unità di personale;

- corso di formazione per Responsabile di sala operativa SOUP: formazione di 15 unità di personale;
- corso di formazione “Previsori” della Sala Operativa CFR per l’attività di supporto alle decisioni della SOUP e del DOS mediante l’impiego dei modelli RISICO e PROPAGATOR: formazione di 15 unità di personale;
- corso di formazione per il personale della Sala Operativa Regionale: formazione di 40 unità di personale;

CONSIDERATO che con decreto del Presidente del Consiglio dei Ministri 13 ottobre 2022 “*Riparto delle risorse del fondo per la realizzazione del piano nazionale azioni di previsione, prevenzione e lotta contro gli incendi boschivi*”, sono stati assegnati alla Regione Lazio, tra l’altro, complessivi euro 130.000,00 per l’attività di formazione del personale AIB;

VISTO l’art. 50, comma 1, lettera b), del d.lgs. 36/2023 che prevede per importi inferiori a 140.000,00 euro al netto dell’IVA la possibilità di ricorrere all’affidamento diretto del servizio;

RITENUTO indispensabile procedere alla formazione di tutto il personale coinvolto nell’attività AIB – personale regionale, personale della società LAZIOcrea S.p.a. e volontari - mediante l’attivazione dei sopra elencati corsi;

RITENUTO opportuno affidare ad un operatore economico specializzato nella somministrazione di corsi di formazione “Antincendio” come sopra specificato;

DATO ATTO che la Scrivente Struttura ha tempestivamente effettuato una ricognizione degli operatori attivi nel settore, e che è stata individuata l’offerta presente su MePA del seguente operatore economico, società *Dream* formazione e consulenza e i relativi prodotti presenti nella vetrina MePA, alla categoria “Servizi di formazione”, CPV: 805000009;

CONSIDERATO che la *Dream* formazione e consulenza, ai fini dell’iscrizione al portale www.acquistinretepa.it nella “domanda di abilitazione”, ha autocertificato l’assenza dei motivi di esclusione previsti e il possesso dei requisiti di partecipazione previsti dal codice dei contratti pubblici;

CONSIDERATO che, il costo complessivo previsto per la fornitura pari a 127.940,00 euro IVA inclusa, è ritenuto congruo in riferimento all’offerta presente su piattaforma MePA, alle attività ivi previste e ad affidamenti similari effettuati nel corso degli anni;

RAVVISATO che ricorrono i presupposti di cui all’art. 50 comma 1, lettera b), del d.lgs. 36/2023, con riguardo ai soggetti in possesso di documentate esperienze pregresse idonee all’esecuzione delle prestazioni contrattuali per incaricare la società *Dream* formazione e consulenza all’esecuzione del servizio *de qua*;

CONSIDERATO inoltre che, trattandosi di affidamento di importo superiore a 5.000,00 euro, si necessita di fare ricorso al Mercato Elettronico, ai sensi dell’art. 1, co. 450, della legge n. 296/2006;

CONSIDERATO altresì che per l’acquisizione del servizio di formazione sarà utilizzata la piattaforma MePA (www.acquistinretepa.it), ai sensi dell’art. 25 del d.lgs. n. 36/2023, mediante l’emissione di un Ordine diretto d’Acquisto (OdA);

VISTA la delibera n. 610 del 19 dicembre 2023 dell’Autorità Nazionale Anticorruzione in materia di contribuzione per la copertura dei costi per il proprio funzionamento, ai sensi dell’art. 1, commi 65 e 67, della legge 23/12/2005, n. 266;

CONSIDERATO che, come stabilito dagli articoli 1 e 2 della citata deliberazione ANAC in cui vengono definiti i soggetti tenuti alla contribuzione e l’entità del versamento, gli importi dovuti all’Autorità, sia per la stazione appaltante (S.A.) che per gli operatori economici (O.E), sono determinati come di seguito elencato:

- quota S.A. euro 35,00, quota O.E. esente;

CONSIDERATO che occorre impegnare sul capitolo del bilancio regionale U0000T19427, es. fin. 2024, la somma di euro 35,00 all’Autorità Nazionale Anticorruzione, in ottemperanza della deliberazione su indicata;

RITENUTO pertanto, di:

- procedere all’emissione di un Ordine diretto d’Acquisto (OdA) n. 7891729 aderendo all’offerta presente sulla vetrina del mercato elettronico MePA, per l’affidamento, ai sensi dell’art. 50, co. 1, lett. b), del d.lgs. n. 36/2023, della fornitura dei corsi di formazione AIB per il personale coinvolto nell’attività AIB, alla società *Dream* formazione e consulenza per l’importo complessivo pari a 127.940,00 euro IVA inclusa;
- approvare i modelli di seguito indicati, parti integranti e sostanziali del presente atto:
 - ✓ Allegato 1 – Dichiarazione clausola *antipantouflage*;
 - ✓ Allegato II – Patto d’Integrità;
 - ✓ Allegato III – Nomina a Responsabile del trattamento dei dati personali;
- procedere all’impegno di spesa della somma complessiva pari a 127.940,00 euro IVA inclusa a favore della società *Dream* formazione e consulenza (cod. cred. 250182), sul capitolo di parte corrente U0000E47134, missione 11, programma 01, piano dei conti 1.03.02.99 - esercizio finanziario 2024;
- dover impegnare euro 35,00 a favore della Autorità Nazionale Anticorruzione (cod. cred. 159683) sul capitolo di parte corrente U0000T19427, missione 01, programma 01, piano dei conti 1.04.01.01 - esercizio finanziario 2024;

PRESO ATTO che la stazione appaltante provvederà all’acquisizione del CIG direttamente sulla piattaforma di *e-procurement* durante la fase di acquisizione del servizio così come previsto dalla delibera Anac n. 582 del 13 dicembre 2023;

RITENUTO di nominare quale Responsabile Unico del Progetto, ai sensi dell’articolo 15 del d.lgs. n. 36/2023, il dott. Massimo La Pietra, dotato di necessario livello di inquadramento giuridico e di competenze professionali adeguate in relazione ai compiti per cui è nominato;

RITENUTO di assegnare al RUP tutti i compiti relativi alle procedure di programmazione, progettazione, affidamento ed esecuzione previste dall’art. 15 del d.lgs. n. 36/2023 riguardanti il servizio in oggetto;

VISTA la dichiarazione di assenza di conflitto di interessi anche solo potenziale, ai sensi e per gli effetti dell’art. 6-*bis* della legge n. 241/1990, dell’art. 7 del d.P.R. n. 62/2013 e dell’art. 14 del medesimo d.P.R. e 16 del d.lgs. n. 36/2023, di insussistenza delle condizioni ostative ivi previste, nonché sull’insussistenza delle cause di inconfiribilità ed incompatibilità di cui al d.lgs. 8 aprile 2013, n. 39, né nelle ipotesi previste dall’art. 35-*bis* del d.lgs. 165/2001, resa dal dott. Massimo La Pietra con nota prot. n. 0698494 del 28/05/2024;

ATTESO che le obbligazioni giungeranno a scadenza entro l’esercizio finanziario 2024;

DETERMINA

per le motivazioni indicate in premessa, che si intendono integralmente riportate:

1. di procedere all’emissione di un Ordine diretto d’Acquisto n. 7891729 sulla piattaforma MePA, per l’affidamento, ai sensi dell’art. 50, co. 1, lett. b), del d.lgs. n. 36/2023, della fornitura di corsi

- di formazione del personale impiegato nelle attività AIB alla società *Dream* formazione e consulenza per l'importo complessivo pari a 127.490,00 euro IVA inclusa;
2. di approvare i modelli di seguito indicati, parti integranti e sostanziali del presente atto:
 - ✓ Allegato I – Dichiarazione clausola *antipantouflage*;
 - ✓ Allegato II – Patto d'Integrità;
 - ✓ Allegato III – Nomina a Responsabile del trattamento dei dati personali;
 3. di procedere all'impegno di spesa della somma complessiva pari a 127.490,00 euro IVA inclusa a favore della società *Dream* formazione e consulenza (cod. cred. 250182), sul capitolo di parte corrente U0000E47134, missione 11, programma 01, piano dei conti 1.03.02.99 - esercizio finanziario 2024;
 4. di impegnare euro 35,00 a favore della Autorità Nazionale Anticorruzione (cod. cred. 159683) sul capitolo di parte corrente U0000T19427, missione 01, programma 01, piano dei conti 1.04.01.01 - esercizio finanziario 2024;
 5. di dare atto che le obbligazioni giungeranno a scadenza in coerenza con quanto indicato nel piano finanziario di attuazione della spesa redatto ai sensi dell'art. 30, co. 2, del r.r. n. 26/2017;
 6. di nominare il Dott. Massimo La Pietra, in possesso di idonee capacità professionali Responsabile Unico del Progetto (RUP) di cui trattasi, ai sensi dell'art. 15 del d.lgs. n. 36/2023, nonché dell'art. 6 della Legge n. 241/1990;
 7. di dare atto che il RUP, prima di avviare la procedura di affidamento ha sottoscritto la dichiarazione di assenza di conflitto di interessi anche solo potenziale, ai sensi e per gli effetti dell'art. 6-*bis* della Legge n. 241/1990, dell'art. 7 del d.P.R. n. 62/2013 e dell'art. 14 del medesimo d.P.R. e 16 del d.lgs. n. 36/2023, nonché insussistenza delle condizioni ostative ivi previste (nota prot. n. 0698494 del 28/05/2024);
 8. di provvedere alla pubblicazione dei dati previsti dal d.lgs. n. 33/2013 nella sezione relativa alla "*Amministrazione trasparente*" del sito internet regionale (www.regione.lazio.it) e sul Bollettino Ufficiale della Regione Lazio.

Avverso la presente determinazione è ammesso ricorso giurisdizionale innanzi al Tribunale Amministrativo del Lazio nel termine di giorni 30 (trenta) dalla pubblicazione.

Il Direttore
Massimo La Pietra

CLAUSOLA PANTOUFLAGE

Il/La sottoscritto/a.....(Cod. Fiscale.....)
nato/a il.....a.....(Prov.....), in
qualità di.....
dell'Impresa con
sede a.....(Prov.....), in Via/Piazza.....
Codice Fiscale.....Partita IVA.....

DICHIARA

Ai sensi degli artt. 46 e 47 del D.P.R. n. 445 del 28/12/2000, consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere e falsità negli atti, richiamate dall'art. 76 e della conseguente decadenza dai benefici di cui all'art. 75 del citato decreto:

al fine dell'applicazione dell'art. 53, co. 16-ter, del d.lgs. n. 165/2001, introdotto dalla legge n. 190/2012 (attività successiva alla cessazione del rapporto di lavoro – **pantouflage o revolving doors**):

- di non aver concluso contratti di lavoro subordinato o autonomo e, comunque, di non aver attribuito incarichi ad ex dipendenti, che hanno esercitato poteri autoritativi o negoziali per conto delle pubbliche amministrazioni nei confronti dell'Impresa di cui sopra, nel triennio successivo alla cessazione del rapporto;
- che è consapevole che, ai sensi del predetto art. 53, co. 16-ter, i contratti conclusi e gli incarichi conferiti in violazione di tali prescrizioni sono nulli e che è fatto divieto ai soggetti privati che li hanno conclusi o conferiti di contrattare con le pubbliche amministrazioni per i successivi tre anni, con l'obbligo di restituzione dei compensi eventualmente percepiti e accertati ad essi riferiti.

Luogo e data.....

Timbro Impresa e firma del legale rappresentante*

.....

(firma per esteso e leggibile)

Ai fini della validità della presente dichiarazione deve essere allegata fotocopia, non autenticata, del documento di identità del sottoscrittore

PATTO DI INTEGRITÀ

tra

Direzione Emergenza, Protezione Civile e NUE I12 della
Regione Lazio

e

la Società.....(di seguito denominata Società),
sede legale in....., via
codice fiscale /P. IVA, rappresentata da.....
in qualità di

Nota: Il presente documento deve essere obbligatoriamente sottoscritto dal partecipante alla procedura di cui trattasi. Il mancato rispetto delle clausole contenute nel presente patto di integrità costituisce causa di esclusione dalla gara. Il presente atto costituirà parte integrante del contratto che si andrà a stipulare a conclusione della procedura.

VISTI

- la legge 6 novembre 2012 n.190, art. 1, comma 17 recante “Disposizioni per la prevenzione e la repressione della corruzione e dell’illegalità nella pubblica amministrazione”;
- il Decreto legislativo 14 marzo 2013 n.33 “Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni” e s.m.i.;
- Piano Nazionale Anticorruzione (P.N.A.), approvato dall’Autorità Nazionale Anticorruzione con delibera 11 settembre 2013, n. 72 e successivamente aggiornato con determinazione del 28 ottobre 2015 n. 12, con delibera 3 agosto 2016, n. 831, con delibera 22 novembre 2017 n. 1208, con delibera 21 novembre 2018 n. 1074 e, da ultimo, con delibera 13 novembre 2019 n. 1064;
- il Piano Triennale di Prevenzione della Corruzione (P.T.P.C.) 2022-2024 della Regione Lazio, adottato con Deliberazione del 29 marzo 2022, n. 143;
- il D.P.R. n. 62 del 16/04/2013 recante il “Regolamento recante il codice di comportamento dei dipendenti pubblici”,
- il Codice di comportamento del personale della Giunta regionale e delle Agenzie regionali, approvato con Deliberazione della Giunta della Regione Lazio 21 gennaio 2014, n. 33;

SI CONVIENE QUANTO SEGUE

Articolo I

1. Il presente Patto di integrità stabilisce la reciproca, formale obbligazione della Direzione Emergenza, Protezione Civile e NUE I12 della Regione Lazio e del partecipante alla procedura di cui trattasi, di conformare i propri comportamenti ai principi di lealtà, trasparenza e correttezza nonché l’espreso impegno anticorruzione di non offrire, accettare o richiedere somme di denaro o

qualsiasi altra ricompensa, vantaggio o beneficio, sia direttamente che indirettamente tramite intermediari, al fine dell'assegnazione del contratto e/o al fine di distorcerne la relativa corretta esecuzione.

2. La sottoscritta Società si impegna a osservare e a far osservare ai propri collaboratori a qualsiasi titolo, avuto riguardo al ruolo e all'attività svolta, gli obblighi di condotta previsti dal D.P.R. n. 62/2013 (Codice di comportamento dei dipendenti pubblici) e dal Codice di comportamento del personale della Giunta regionale e delle Agenzie regionali da intendersi qui integralmente riportato e trascritto, adottato con deliberazione della Giunta regionale n. 33 del 21/01/2014 e ss.mm.ii.. A tal fine la Società è consapevole ed accetta che, ai fini della completa e piena conoscenza dei Codici sopra citati, l'Amministrazione ha adempiuto all'obbligo di trasmissione di cui all'art.17 del D.P.R. n. 62/2013 garantendone l'accessibilità all'indirizzo web <https://www.regione.lazio.it/amministrazione-trasparente> nella sezione Amministrazione Trasparente. L'impresa si impegna a trasmettere copia dei "Codici" ai propri collaboratori a qualsiasi titolo e a fornire prova dell'avvenuta comunicazione. La violazione degli obblighi di cui al D.P.R. n. 62/2013 e al Codice di Comportamento del personale della Direzione Emergenza, Protezione Civile e NUE 112 della Regione Lazio costituisce causa di risoluzione del contratto aggiudicato, secondo la disciplina del presente atto.
3. La sottoscritta Società dichiara, ai fini dell'applicazione dell'art. 53, comma 16 ter del decreto legislativo n. 165/2001, di non aver concluso contratti di lavoro subordinato o autonomo e comunque di non aver attribuito incarichi ad ex dipendenti della Direzione Emergenza, Protezione Civile e NUE 112 della Regione Lazio, che hanno esercitato poteri autoritativi o negoziali per conto della medesima Direzione nei loro confronti, per il triennio successivo alla cessazione del rapporto. La Società dichiara, altresì, di essere consapevole che qualora emerga la predetta situazione verrà disposta l'esclusione dalla procedura di affidamento in oggetto.
4. La sottoscritta Società si impegna a segnalare alla Direzione Emergenza, Protezione Civile e NUE 112 della Regione Lazio qualsiasi tentativo di turbativa, irregolarità o distorsione nelle fasi di svolgimento della procedura di affidamento relativa al presente Patto, da parte di ogni interessato o addetto o di chiunque possa influenzare le decisioni relative alla procedura in oggetto.
5. La sottoscritta Società si impegna a riferire tempestivamente alla Direzione Emergenza, Protezione Civile e NUE 112 della Regione Lazio ogni illecita richiesta di denaro, prestazione o altra utilità, ovvero offerta di protezione, che venga avanzata nel corso dell'esecuzione dell'appalto nei confronti di un proprio rappresentante, agente o dipendente. La Società prende, altresì, atto che analogo obbligo dovrà essere assunto da ogni altro soggetto che intervenga, a qualunque titolo, nell'esecuzione dell'appalto e che tale obbligo non è in ogni caso sostitutivo dell'obbligo di denuncia all'Autorità Giudiziaria dei fatti attraverso i quali sia stata posta in essere la pressione estorsiva e ogni altra forma di illecita interferenza. La sottoscritta Società è consapevole che, nel caso in cui non comunichi i tentativi di pressione criminale, il contratto si risolverà di diritto.
6. La sottoscritta Società dichiara, altresì, che non si è accordata e non si accorderà con altri partecipanti alla procedura per limitare con mezzi illeciti la concorrenza.
7. La sottoscritta Società si impegna a rendere noti, su richiesta della Direzione Emergenza, Protezione Civile e NUE 112 della Regione Lazio, tutti i pagamenti eseguiti e riguardanti il contratto eventualmente assegnato a seguito della procedura di affidamento.

Articolo 2

1. La sottoscritta Società prende nota e accetta che, nel caso di mancato rispetto degli impegni anticorruzione assunti con il presente Patto di integrità, saranno applicate, a seconda delle fasi in cui lo stesso si verifichi, le seguenti sanzioni, fatte salve le responsabilità comunque previste dalla legge:
 - a) esclusione del concorrente dalla procedura di affidamento;

- b) esclusione del concorrente dalle procedure di affidamento indette dalla Regione Lazio per i successivi 3 (tre) anni;
- c) risoluzione del contratto.

Articolo 3

Il presente Patto di integrità e le sanzioni applicabili resteranno in vigore sino alla completa esecuzione del contratto. Il presente Patto costituisce parte integrante del contratto pur se non materialmente allegato.

Articolo 4

Il presente Patto deve essere obbligatoriamente sottoscritto con firma digitale, dal legale rappresentante della Società e deve essere presentato unitamente alla documentazione di gara.

Articolo 5

Eventuali fenomeni corruttivi o altre fattispecie di illecito, fermo restando, in ogni caso, quanto previsto dagli artt. 331 e segg. del c.p.p., vanno segnalati al Responsabile Unico del Progetto e al Responsabile della prevenzione della corruzione della Regione Lazio.

Articolo 6

Ogni controversia relativa all'interpretazione, e all'esecuzione del presente Patto di integrità tra la Direzione Emergenza, Protezione Civile e NUE I 12 della Regione Lazio e gli operatori economici partecipanti alle procedure di affidamento dei contratti pubblici, sarà risolta dall'Autorità Giudiziaria competente.

_____, li _____

(Firmato digitalmente dal concorrente)

**ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI
PERSONALI**

(ove necessario **Allegato al CONTRATTO DEL XX.XX.XXXX**)

TRA

La Regione Lazio, con sede in Via R. Raimondi Garibaldi 7– 00147 Roma, nella persona del Dott.....;

E

La **<indicare ragione e denominazione sociale della Società>**, di seguito, per brevità, anche Società, con sede inin persona del legale rappresentante pro tempore Dott.;

PREMESSO CHE

la Regione Lazio, in qualità di Titolare del trattamento svolge attività che comportano il trattamento di dati personali nell'ambito dei servizi istituzionalmente affidati;

la Regione Lazio, in qualità di Titolare del trattamento è consapevole di essere tenuta a mettere in atto misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati e adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

VISTO l'articolo 474, comma 2, del r.r. 6 settembre 2002, n. 1 (Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale) e successive modificazioni, il quale prevede che il titolare del trattamento, con specifico atto negoziale di incarico ai singoli responsabili del trattamento, disciplina i trattamenti affidati al responsabile, i compiti e le istruzioni secondo quanto previsto dall'articolo 28, paragrafo 3, del RGPD e in coerenza con le indicazioni del DPO; nell'atto di incarico è, altresì, definita la possibilità di nomina di un sub-responsabile, secondo quanto previsto dall'articolo 28, paragrafi 2 e 4, del RGPD;

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 RGPD), il quale 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 alla protezione dei dati personali;

CONSIDERATO che detto Regolamento è divenuto efficace in data 25 maggio 2018, con conseguente abrogazione delle parti del decreto legislativo 30 giugno 2003 n. 196 non compatibili con il predetto Regolamento;

VISTO il decreto legislativo 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;

CONSIDERATO che le attività, erogate in esecuzione del Contratto **<indicare riferimenti del contratto>**, in essere tra Regione Lazio e **<indicare ragione e denominazione sociale della Società>**, implicano da parte di quest'ultima, il trattamento dei dati personali di cui è Titolare la Regione Lazio, ai sensi di quanto previsto dal Regolamento (UE) 2016/679;

PRESO ATTO che l'articolo 4, n. 2) del RGPD definisce «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

PRESO ATTO che l'articolo 4, n.7) del RGPD definisce "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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

PRESO ATTO che l'art. 4, n. 8) del RGPD definisce "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;

VISTO il Provvedimento del Garante per la Protezione dei Dati Personali 27/11/2008 (Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema) e successive modificazioni, pubblicato sulla Gazzetta Ufficiale n. 300 del 24/12/2008;

CONSIDERATO che il suddetto Provvedimento richiede che si proceda alla designazione individuale degli Amministratori di Sistema (System Administrator), degli Amministratori di Base Dati (Database Administrator), degli Amministratori di Rete (Network Administrator) e degli Amministratori di Software Complessi, che, nell'esercizio delle proprie funzioni, hanno accesso, anche fortuito, a dati personali;

VISTO il provvedimento dell'AgID (Misure minime di sicurezza ICT per le Pubbliche Amministrazioni), adottato in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1° agosto 2015 (di seguito per brevità "Misure minime AgID"), il quale ha dettato le regole da osservare per garantire un uso appropriato dei privilegi di Amministratore;

RITENUTO che, ai sensi dell'articolo 28, paragrafo 1 del RGPD, la Società presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento dei dati personali di cui la Regione Lazio è Titolare soddisfi i requisiti e il pieno rispetto delle disposizioni previste dal RGPD;

Quanto sopra premesso, le parti stipulano e convengono quanto segue:

Articolo I

<indicare ragione e denominazione sociale della Società>, in qualità di **RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI** in virtù del presente atto di designazione, ai sensi e per gli effetti delle vigenti disposizioni normative di cui agli articoli 4, n.8) e 28 del RGPD, con riguardo alle operazioni di trattamento connesse all'esecuzione del suddetto contratto, dichiara di essere edotta di tutti gli obblighi che incombono sul Titolare del trattamento e si impegna a

rispettarne e consentirne ogni prerogativa, obbligo, onere e diritto che discende da tale posizione giuridica, attenendosi alle disposizioni operative contenute nel presente atto.

Articolo 2

Il Responsabile del trattamento dei dati personali nell'effettuare le operazioni di trattamento connesse all'esecuzione del suddetto contratto dovrà attenersi alle seguenti disposizioni operative:

- I trattamenti dovranno essere svolti nel pieno rispetto delle previsioni legislative 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. In particolare:
 - i trattamenti sono svolti per **<indicare le finalità per cui il fornitore tratta i dati (es. ai fini di assistenza e manutenzione)>**;
 - i dati personali trattati in ragione delle attività di cui ai suddetti contratti hanno ad oggetto: dati di natura personale (articolo 4, n.1) del RGPD); dati sensibili (articolo 9 del RGPD "Categorie particolari di dati personali"; dati giudiziari (articolo 10 del RGPD); **<eliminare le eventuali tipologie di dati non oggetto di trattamento>**
 - le categorie di interessati sono **<indicare le tipologie di interessato cui i dati afferiscono>**.
- La Società è autorizzata a procedere all'organizzazione di ogni operazione di trattamento dei dati nei limiti stabiliti dai contratti in essere tra le parti e dalle vigenti disposizioni contenute nel RGPD. A tale scopo, per "trattamento" si intende ai sensi dell'articolo 4, n. 2) del RGPD, "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".
- La Società si impegna, già in fase contrattuale, al fine di garantire il rispetto del principio della "Protezione dei dati fin dalla progettazione e protezione predefinita" di cui all'articolo 25 del RGPD, a determinare i mezzi del trattamento e a mettere in atto le misure tecniche e organizzative adeguate, di cui all'articolo 32 del RGPD, prima dell'inizio delle attività.
- La Società dovrà eseguire i trattamenti funzionali alle attività ad essa attribuite e comunque non incompatibili con le finalità per cui i dati sono stati raccolti. Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, la Società dovrà informare il Titolare del trattamento ed il Responsabile della Protezione dei Dati (DPO) della Regione Lazio.
- La Società si impegna a garantire, senza ulteriori oneri per l'Amministrazione, l'esecuzione di tutti i trattamenti individuati al momento della stipula del contratto e dei quali dovesse insorgere in seguito la necessità ai fini dell'esecuzione del contratto stesso.
- La Società dovrà attivare le necessarie procedure aziendali per identificare ed istruire le persone autorizzate al trattamento dei dati personali ed organizzarne i compiti in maniera che le singole operazioni di trattamento risultino coerenti con le disposizioni di cui alla presente nomina, facendo in modo, altresì, che, sulla base delle istruzioni operative loro impartite, i trattamenti non si discostino dalle finalità istituzionali per cui i dati sono stati raccolti e trattati. La Società garantirà, inoltre, che le persone autorizzate al trattamento siano vincolate da un obbligo, legalmente assunto, di riservatezza.

- La Società si attiverà per garantire l'adozione delle misure di sicurezza di cui all'articolo 32 del RGPD (come da allegato n. III dello schema G di cui al r.r. n. 2/2002, adottato con dgr n. 212/2024, allegate in calce al presente atto di nomina).
- La Società dovrà predisporre e tenere a disposizione del Titolare la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito riportate; inoltre renderà disponibili al Titolare tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dal RGPD, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal Titolare stesso o da un altro soggetto da questi incaricato.
- La Società adotterà le politiche interne e attuerà le misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (*privacy by design*); adotterà ogni misura adeguata a garantire che i dati personali siano trattati in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse (*privacy by default*).
- La Società, ai sensi dell'articolo 30 del RGPD e nei limiti di quanto in esso previsto, è tenuta a tenere un Registro delle attività di Trattamento effettuate sotto la propria responsabilità e a cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'articolo 30, paragrafo 4, del RGPD.
- La Società è tenuta ad informare di ogni violazione di dati personali (cosiddetta *data breach*) il Titolare ed il Responsabile della Protezione dei Dati (DPO) della Regione Lazio, tempestivamente e senza ingiustificato ritardo, entro 24 ore dall'avvenuta conoscenza dell'evento. Tale notifica – da effettuarsi tramite PEC da inviare all'indirizzo protocollo@regione.lazio.legalmail.it e dpo@regione.lazio.legalmail.it, deve essere accompagnata da ogni documentazione utile, ai sensi degli articoli 33 e 34 del RGPD, per permettere al Titolare, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando il Titolare ne è venuto a conoscenza. Nel caso in cui il Titolare debba fornire informazioni aggiuntive alla suddetta Autorità Garante, la Società supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità Garante siano esclusivamente in possesso del Responsabile Esterno e/o di suoi sub-Responsabili.
- La Società, su eventuale richiesta del Titolare, è tenuta inoltre ad assistere quest'ultimo nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'articolo 35 del RGPD e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'articolo 36 del RGPD.
- La Società, qualora riceva istanze degli interessati in esercizio dei loro diritti ai sensi degli articoli da 15 a 22 del RGPD, è tenuta a:
 - darne tempestiva comunicazione scritta al Titolare e al Responsabile della Protezione dei Dati (DPO) della Regione Lazio, allegando copia della richiesta;
 - valutare con il Titolare e con il DPO della Regione Lazio la legittimità delle richieste;
 - coordinarsi con il Titolare e con il DPO della Regione Lazio al fine di soddisfare le richieste ritenute legittime.
- Laddove fosse espressamente autorizzata dalla Regione Lazio la sub-fornitura / il sub-appalto, la Regione Lazio è tenuta a procedere alla designazione di detti sub-fornitori / sub-appaltatori, preventivamente autorizzati dalla Regione stessa, quali Responsabili del trattamento,

imponendogli, mediante contratto o altro atto giuridico, i medesimi obblighi in materia di protezione dei dati contenuti nella presente nomina, prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del RGPD. Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, la Società conserverà nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile ai sensi dell'articolo 28, paragrafo 4 del RGPD.

- La Società garantisce gli adempimenti e le incombenze anche formali verso l'Autorità Garante quando richiesto e nei limiti dovuti, adoperandosi per collaborare tempestivamente, per quanto di competenza, sia con il Titolare sia con l'Autorità garante per la protezione dei dati personali. In particolare:
 - fornisce informazioni sulle operazioni di trattamento svolte;
 - consente l'accesso alle banche dati oggetto delle operazioni di trattamento;
 - consente l'esecuzione di controlli;
 - compie quanto necessario per una tempestiva esecuzione dei provvedimenti inibitori, di natura temporanea.
- La Società si impegna ad adottare, su richiesta del Titolare e nel rispetto degli obblighi contrattuali assunti, nel corso dell'esecuzione dei contratti, ulteriori garanzie quali l'applicazione di un codice di condotta applicato o di un meccanismo di certificazione approvato ai sensi degli articoli 40 e 42 del RGPD, laddove adottati. Il Titolare potrà in ogni momento verificare l'adozione di tali ulteriori garanzie.
- La Società non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare.
- La Società è tenuta a comunicare al Titolare ed al DPO della Regione Lazio il nome ed i dati del proprio DPO, laddove la società stessa lo abbia designato conformemente a quanto prescritto dall'articolo 37 del RGPD. Il DPO collaborerà e si terrà in costante contatto con il DPO della Regione Lazio.

Articolo 3

(laddove le prestazioni contrattuali implicino l'erogazione di servizi di amministrazione di sistema)

In conformità a quanto prescritto dal Provvedimento del Garante del 27/11/2008 e successive modificazioni ed alle citate Misure minime AgID relativamente alle utenze Amministrative, laddove le prestazioni contrattuali implicino l'erogazione di servizi di amministrazione di sistema, la Società, in qualità di Responsabile del trattamento, si impegna a:

- individuare i soggetti ai quali affidare il ruolo di Amministratori di Sistema (System Administrator), Amministratori di Base Dati (Database Administrator), Amministratori di Rete (Network Administrator) e/o Amministratori di Software Complessi e, sulla base del successivo atto di designazione individuale, impartire le istruzioni a detti soggetti, vigilando sul relativo operato;
- assegnare ai suddetti soggetti una user id che contenga riferimenti agevolmente riconducibili all'identità degli Amministratori e che consenta di garantire il rispetto delle seguenti regole:

- divieto di assegnazione di user id generiche e già attribuite anche in tempi diversi;
- utilizzo di utenze amministrative anonime, quali “root” di Unix o “Administrator” di Windows, solo per situazioni di emergenza; le relative credenziali devono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso;
- disattivazione delle user id attribuite agli Amministratori che non necessitano più di accedere ai dati;
- associare alle user id assegnate agli Amministratori una password e garantire il rispetto delle seguenti regole:
 - utilizzare password con lunghezza minima di almeno 14 caratteri, qualora l'autenticazione a più fattori non sia supportata;
 - cambiare la password alla prima connessione e successivamente almeno ogni 30 giorni (password *again*).
 - le password devono differire dalle ultime 5 utilizzate (password *history*);
 - conservare le password in modo da garantirne disponibilità e riservatezza;
 - registrare tutte le immissioni errate di password. Ove tecnicamente possibile, gli account degli Amministratori devono essere bloccati dopo un numero massimo di tentativi falliti di login;
 - assicurare che l'archiviazione di password o codici PIN su qualsiasi supporto fisico avvenga solo in forma protetta da sistemi di cifratura;
- assicurare la completa distinzione tra utenze privilegiate e non privilegiate di amministratore, alle quali devono corrispondere credenziali diverse;
- assicurare che i profili di accesso, in particolare per le utenze con privilegi amministrativi, rispettino il principio del *need-to-know*, ovvero che non siano attribuiti diritti superiori a quelli realmente necessari per eseguire le normali attività di lavoro. Le utenze con privilegi amministrativi devono essere utilizzate per il solo svolgimento delle funzioni assegnate;
- mantenere aggiornato un inventario delle utenze privilegiate (Anagrafica AdS), anche attraverso uno strumento automatico in grado di generare un *alert* quando è aggiunta una utenza amministrativa e quando sono aumentati i diritti di una utenza amministrativa;
- adottare sistemi di registrazione degli accessi logici (log) degli Amministratori ai sistemi e conservare gli stessi per un congruo periodo non inferiore a 6 mesi. Qualora la Società utilizzi sistemi messi a disposizione dalla Regione, comunicare agli Amministratori che la Regione stessa procederà alla registrazione e conservazione dei log;
- impedire l'accesso diretto ai singoli sistemi con le utenze amministrative. In particolare, deve essere imposto l'obbligo per l'Amministratore di accedere con una utenza normale e solo successivamente dargli la possibilità di eseguire, come utente privilegiato, i singoli comandi;
- utilizzare, per le operazioni che richiedono utenze privilegiate di amministratore, macchine dedicate, collocate in una rete logicamente dedicata, isolata rispetto ad internet. Tali macchine non devono essere utilizzate per altre attività;
- comunicare al momento della sottoscrizione del presente atto, e comunque con cadenza almeno annuale ed ogni qualvolta se ne verifichi la necessità, alla Regione gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, di Base Dati, di Rete e/o di software Complessi, specificando per ciascuno di tali soggetti:
 - il nome e cognome;
 - la user id assegnata agli Amministratori;
 - il ruolo degli Amministratori (ovvero di Sistema, Base Dati, di Rete e/o di Software Complessi);
 - i sistemi che gli stessi gestiscono, specificando per ciascuno il profilo di autorizzazione assegnato;

- eseguire, con cadenza almeno annuale, le attività di verifica dell'operato degli Amministratori e consentire comunque alla Regione ove ne faccia richiesta, di eseguire in proprio dette verifiche;
- nei limiti dell'incarico affidato, mettere a disposizione del Titolare e del DPO della Regione quando formalmente richieste, le seguenti informazioni relative agli Amministratori: log in riusciti, log in falliti, log out. Tali dati dovranno essere resi disponibili per un congruo periodo non inferiore a 6 mesi;
- durante l'esecuzione dei Contratti, nell'eventualità di qualsivoglia modifica della normativa in materia di protezione dei dati personali, che generi nuovi requisiti (ivi incluse nuove misure di sicurezza di natura fisica, logica e/o organizzativa), la Società. si impegna a collaborare, nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse, con il Titolare affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti.

La presente nomina avrà efficacia fino al termine del suindicato contratto in essere tra Regione Lazio e la Società.

All'atto della cessazione dei contratti in essere con la Regione Lazio, la Società, sulla base delle determinazioni della Regione Lazio, restituirà i dati personali oggetto del trattamento oppure provvederà alla loro integrale distruzione, salvo che i diritti dell'Unione e degli Stati membri ne prevedano la conservazione. In entrambi i casi rilascerà un'attestazione scritta di non aver trattenuto alcuna copia dei dati.

La validità del presente atto si intende altresì estesa ad ulteriori, eventuali, proroghe contrattuali.

Titolare del Trattamento

Sottoscrivendo il presente atto, **<indicare ragione e denominazione sociale della Società>**:

- conferma di conoscere gli obblighi assunti in relazione alle disposizioni del RGPD e di possedere i requisiti di esperienza, capacità ed affidabilità idonei a garantire il rispetto di quanto disposto dal medesimo regolamento e sue eventuali modifiche ed integrazioni;
- conferma di aver compreso integralmente le istruzioni qui impartite e si dichiara competente e disponibile alla piena esecuzione di quanto affidato;
- accetta la nomina di Responsabile del trattamento dei dati personali e si impegna ad attenersi rigorosamente a quanto ivi stabilito, nonché alle eventuali successive modifiche ed integrazioni disposte dal Titolare, anche in ottemperanza alle modifiche normative in materia.

Responsabile del Trattamento

Legale Rappresentante

Allegato n. III dello schema G di cui al r.r. n. 2/2002**Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei trattamenti e dei dati****NOTA ESPLICATIVA:**

Le misure tecniche e organizzative devono essere descritte in modo concreto e non genericamente.

Si descrivono di seguito le misure di sicurezza tecniche e organizzative che il Responsabile del trattamento deve mettere in atto, (comprese le eventuali certificazioni in possesso del Responsabile del trattamento pertinenti e ove presenti), per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.

1) PRIVACY BY DESIGN E BY DEFAULT:

Il Responsabile del trattamento deve rispettare i principi di protezione dei dati fin dalla progettazione (*privacy by design*) e protezione dei dati per impostazione predefinita (*privacy by default*) di cui all'art. 25 GDPR comunicando al Titolare le soluzioni individuate ed adottate per rispettare tali principi (cfr. Considerando 78 GDPR) come meglio specificato nell'allegato VI.

2) ELENCO AGGIORNATO SUB-RESPONSABILI:

Quando il primo Responsabile del trattamento è autorizzato a ricorrere a un altro Responsabile del trattamento per l'esecuzione di specifiche attività, a prescindere dal carattere specifico o generale dell'autorizzazione preliminare scritta del Titolare del trattamento, il primo Responsabile deve tenere un elenco aggiornato degli altri (sub-)Responsabili. Su richiesta del Titolare e/o in caso di accertamenti anche da parte del Garante, il primo Responsabile del trattamento gli fornisce prontamente e non oltre 24 ore copia dell'elenco aggiornato.

3) ATTIVITA' DI REVISIONE, COMPRESSE LE ISPEZIONI:

Su richiesta del Titolare del trattamento, a intervalli annuali o se vi sono indicazioni di inosservanza, il Responsabile del trattamento consentirà e contribuirà alle attività di revisione delle attività di trattamento di cui alle presenti clausole. Nel decidere in merito a un riesame o a un'attività di revisione, il Titolare del trattamento potrà tenere conto delle pertinenti certificazioni in possesso del Responsabile del trattamento.

Il Titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del Responsabile del trattamento e, se del caso, sono effettuate con un preavviso di almeno 72 ore.

4) TRASFERIMENTO DATI EXTRA UE:

È vietato qualunque trasferimento di dati da parte del Responsabile del trattamento verso un paese terzo o un'organizzazione internazionale, ovvero a sub-Responsabili del trattamento che non rientrano nell'ambito di applicazione territoriale del GDPR, compresi trasferimenti successivi.

Il Responsabile del trattamento si assicura che anche il sub-Responsabile del trattamento non effettui trasferimenti di dati verso un paese terzo o un'organizzazione internazionale.

In presenza di una decisione di adeguatezza (cfr. <https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero>), il Responsabile del trattamento è tenuto in ogni caso a chiedere specifica autorizzazione al Titolare, in considerazione degli obblighi connessi ai trasferimenti internazionali di cui al capo V del GDPR.

In generale, il trasferimento di dati extra UE può essere effettuato soltanto su istruzione documentata del Titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il Responsabile del trattamento, e nel rispetto del capo V del GDPR.

5) AMMINISTRATORE DI SISTEMA:

Nel caso in cui il Responsabile effettua trattamenti, anche in parte, mediante strumenti elettronici, si impegna ad individuare e a designare gli Amministratori di Sistema ("AdS"), conformandosi altresì, nell'affidamento di tale incarico, a tutto quanto previsto dal provvedimento del Garante Privacy del 27 novembre 2008 [doc. web n. 1577499] (G.U. n. 300 del 24 dicembre 2008), come modificato in base al provvedimento del 25 giugno 2009.

Le persone fisiche designate AdS considerate come tali sono le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti nonché altre figure equiparabili quali gli amministratori di base dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Il Responsabile del trattamento è tenuto a dare la prova delle misure e degli accorgimenti prescritti con la designazione di Amministratore di Sistema; deve altresì conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, tenendo costantemente aggiornato tale documento interno (come da Allegato V) e in caso di accertamenti anche da parte del Garante fornire prontamente e comunque entro 24 ore il medesimo documento al Titolare.

6) MISURE MINIME E MISURE AGID:

Per il tramite degli Amministratori di Sistema designati, il Responsabile del Trattamento si impegna a garantire di default le modalità tecniche previste dall'Allegato B del Codice Privacy (Disciplinare tecnico in materia di misure di sicurezza), seppur oggi abrogato.

Il Responsabile si impegna ad installare e mantenere aggiornate, sugli strumenti elettronici oggetto del contratto, tutte le misure e gli accorgimenti eventualmente prescritti dai Provvedimenti emessi dall'Autorità Garante per la protezione dei dati personali (GPDP), dall'Agenzia per l'Italia Digitale (AGID) e dall'Agenzia per la Cybersicurezza Nazionale (ACN), applicabili al servizio commissionato, nonché le ulteriori misure di sicurezza previste nel contratto di fornitura.

Nello specifico, il Responsabile si impegna al rispetto e alla dimostrazione di quanto previsto dall'AGID con:

- le Linee guida - Sicurezza nel Procurement ICT (Pubblicato il 19/05/2020 - Aggiornato il 19/05/2020) e disponibile anche alla seguente url: https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/2013910214200__OLG_Sicurezza_Procurement_ICT_versione_finale_pub.pdf
- Linee guida per lo sviluppo del software sicuro (Ultimo aggiornamento 06-05-2020), disponibile alla seguente url: <https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro>
- le «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». (17A03060) (GU Serie Generale n.103 del 05-05-2017), disponibili anche alla seguente url: <https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict>

7) MISURE ULTERIORI

Il Responsabile del trattamento, ferma la dimostrazione della loro adozione, si impegna a mettere in atto le seguenti ulteriori misure tecniche e organizzative:

NOTA ESPLICATIVA:

(da adattare alla singola situazione - eliminare non pertinenti e non applicabili):

- misure di pseudonimizzazione e cifratura dei dati personali;
- misure per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- misure per assicurare la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
- misure di identificazione e autorizzazione dell'utente misure di protezione dei dati durante la trasmissione misure di protezione dei dati durante la conservazione
- misure per garantire la sicurezza fisica dei luoghi in cui i dati personali sono trattati misure per garantire la registrazione degli eventi
- misure per garantire la configurazione del sistema, compresa la configurazione per impostazione predefinita misure di informatica interna e di gestione e governance della sicurezza informatica
- misure di certificazione/garanzia di processi e prodotti misure per garantire la minimizzazione dei dati misure per garantire la qualità dei dati
- misure per garantire la conservazione limitata dei dati misure per garantire la Responsabilità
- misure per consentire la portabilità dei dati e garantire la cancellazione]

Il Responsabile del trattamento, ferma la dimostrazione della loro adozione, si impegna a mettere in atto le seguenti ulteriori e più specifiche misure tecniche e organizzative:

NOTA ESPLICATIVA:

(da adattare alla singola situazione - eliminare non pertinenti e non applicabili):

- a) mezzi che permettono di garantire la confidenzialità, l'integrità, la disponibilità e la resilienza costante dei sistemi e dei servizi di trattamento.
 - a.1) la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che le password relative alle utenze dei soggetti autorizzati siano di lunghezza non inferiore a otto caratteri e siano sottoposte a un controllo automatico di qualità che impedisca l'uso di password "deboli" e che le medesime password siano modificate almeno al primo utilizzo;
 - a.2) la capacità di assicurare la riservatezza dei dati trattati, facendo in modo che l'autenticazione dei soggetti autorizzati avvenga tramite un processo di autenticazione multifattoriale (MFA);
 - a.3) la capacità di contrastare efficacemente attacchi informatici di tipo brute force sul sistema di autenticazione online, anche introducendo limitazioni al numero di tentativi infruttuosi di autenticazione;
 - a.4) crittografia dei dati che i dispositivi del fornitore/Responsabile (computer, portatili, tablet, ecc.) devono rispettare;
 - a.5) l'accesso alla rete locale dell'amministrazione da parte del fornitore/Responsabile deve essere configurato con le abilitazioni strettamente necessarie alla realizzazione di quanto contrattualizzato, vale a dire consentendo l'accesso esclusivamente alle risorse necessarie. L'accesso dall'esterno mediante VPN deve essere consentito, solo se strettamente necessario, utilizzando account VPN personali configurati e abilitati opportunamente. Gli accessi dovranno poter essere tracciati per eventuali successivi audit;
 - a.6) nelle forniture di sviluppo e manutenzione, l'utilizzo dei dati dell'amministrazione per la realizzazione di quanto contrattualizzato deve essere consentito esclusivamente su server/database di sviluppo nei quali sono stati importati i dati necessari per gli scopi del progetto. Pertanto, questa misura consiste nel gestire l'accesso ai server e ai DB in modo da rispettare questa regola generale, tracciando le eventuali eccezioni che dovessero verificarsi.
- b) mezzi che permettono di ristabilire la disponibilità dei dati a carattere personale e l'accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;

- c) rilevare e detenere a norma di legge copia dei log di accesso all'applicativo e di sistema;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- e) nomina di un DPO, nei casi previsti dall'art. 37 GDPR ovvero per i soggetti privati obbligati alla sua designazione. Nel caso in cui il Responsabile del trattamento ritenesse tale nomina non obbligatoria, alla luce del principio di accountability è tenuto a dare la prova della mancanza dei criteri di nomina (cfr. Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato, punto nn. 3 e 4);
- f) poter dimostrare che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Responsabile del trattamento e non abbia ricevuto idonea formazione;
- g) una procedura per la gestione degli incidenti di sicurezza e delle violazioni di dati personali (cd. "Data Breach");
- h) sottoscrizione di polizze assicurative che tengano conto dei risarcimenti danni di cui all'art. 82 del GDPR con massimali adeguati;
- i) il Responsabile è tenuto ad effettuare preliminarmente, e indipendentemente dal Titolare del trattamento, una Valutazione del Rischio per la sicurezza dei dati che tenga in considerazione i rischi presentati dal trattamento come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati (cfr. considerando 83 GDPR). E' inteso che nel caso in cui il Responsabile, laddove la tipologia del trattamento rientri nell'elenco di cui all'ALLEGATO I AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018), è tenuto ad effettuare preliminarmente, e indipendentemente dal Titolare del trattamento, una Valutazione d'impatto sul prodotto/servizio;
- l) Sulle reti messe a disposizione dal fornitore devono essere presenti di dispositivi di sicurezza perimetrale con funzioni di sicurezza (ad esempio Firewall e sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT e in grado di gestire gli IoC (Indicator of Compromise);
- m) Il Responsabile usa protocolli cifrati e meccanismi di autenticazione nell'ambito dei servizi erogati;
- n) Qualora il Responsabile/fornitore subisca un attacco, in conseguenza del quale vengano compromessi sistemi del committente da lui gestiti, deve farsi carico delle bonifiche del caso, e riportare i sistemi in uno stato di assenza di vulnerabilità.
- o) Il Responsabile/fornitore si impegna a trattare, trasferire e conservare le eventuali repliche dei dati oggetto di fornitura, ove autorizzate dalle amministrazioni, sempre all'interno del territorio dell'UE.

7.1) Verificare la documentazione finale di progetto

NOTA ESPLICATIVA:

(da adattare alla singola situazione - eliminare non pertinenti e non applicabili):

Alla fine di ogni singolo progetto, l'amministrazione/titolare deve verificare che il fornitore/responsabile rilasci la seguente documentazione:

- documentazione finale e completa del progetto;
- manuale di installazione/configurazione;
- report degli Assessment di Sicurezza eseguiti con indicazione delle vulnerabilità riscontrate e le azioni di risoluzione/mitigazione apportate.
- "libretto di manutenzione" del prodotto (software o hardware), con l'indicazione delle attività da eseguire per mantenere un adeguato livello di sicurezza del prodotto realizzato o acquistato. In particolare, nel libretto di manutenzione deve essere indicato:

- produttore e versione dei prodotti software utilizzati (ad esempio web server, application server, CMS, DBMS), librerie, firmware;
- indicazioni per il reperimento dei Bollettini di Sicurezza dei singoli produttori di hardware/software;
- indicazioni sul processo di installazione degli aggiornamenti sicurezza;
- documento di EoL (documento che contiene indicazione dei prodotti utilizzati e relativo fine vita/rilascio aggiornamenti sicurezza).

7.2) Distruzione del contenuto logico (wiping) dei dispositivi che vengono sostituiti

Nelle acquisizioni di attività di conduzione CED o di gestione di parchi di PC (fleet management), occorre verificare che l'hardware dismesso, (sia che si tratti di server sia che si tratti di postazioni di lavoro), venga cancellato e distrutto in modo sicuro, evitando rischi che dati critici possano restare erroneamente memorizzati sull'hardware dismesso.

Nota esplicativa:

Scrivere il requisito nel capitolato non è sufficiente: va definito un processo di verifica strutturato.

Il processo può prevedere ad esempio:

- la consegna di un verbale di avvenuta distruzione da parte del fornitore,
- nel caso di sistemi critici, un'eventuale azione ispettiva che può ad esempio far parte delle attività di monitoraggio.

7.3) Manutenzione - aggiornamento dei prodotti:

Gli amministratori di sistema devono obbligatoriamente eseguire gli aggiornamenti ogni qualvolta sui siti dei produttori vengono rilasciati patch e correzioni per problemi di vulnerabilità.

7.4) Vulnerability Assessment

Il Fornitore/Responsabile deve eseguire, su beni e servizi classificati critici ed esposti sul web, un Vulnerability Assessment a cadenza almeno annuale, e ogni volta che si apportano modifiche alla configurazione software/hardware.

NOTA ESPLICATIVA:

Per i trasferimenti a (sub-)Responsabili del trattamento, descrivere anche le misure tecniche e organizzative specifiche che il (sub-)Responsabile del trattamento deve prendere per essere in grado di fornire assistenza al Titolare del trattamento.

NOTA ESPLICATIVA:

Descrivere anche le misure tecniche e organizzative specifiche che il Responsabile del trattamento deve prendere per essere in grado di fornire assistenza al Titolare del trattamento.

8) PERSONALE AUTORIZZATO:

Il Responsabile del trattamento si impegna a produrre ed aggiornare in caso di modifiche l'elenco degli operatori autorizzati singolarmente ed opportunamente formati in materia di privacy (ivi inclusi gli opportuni aggiornamenti normativi), impartendo per iscritto specifiche istruzioni per trattare i dati degli utenti nell'ambito della propria attività e con i limiti di legge, curando, in particolare, il profilo della sicurezza di accesso e dell'integrità dei dati ai sensi dell'art. 29 del GDPR. Inoltre, il Responsabile si impegna a stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli autorizzati al trattamento, avendo cura di adottare preventivamente misure organizzative adeguate al rischio per diritti e libertà delle persone fisiche. Inoltre deve garantire che le persone autorizzate

siano state istruite sulla procedura di gestione degli incidenti di sicurezza e la gestione delle violazioni di dati personali. Il Titolare può richiedere una prova documentata al fine di verificare tali adempimenti.

9) REGISTRO DEL TRATTAMENTO:

Il Responsabile del trattamento, anche laddove non rientri nelle casistiche definite dall'art. 30, parr. 2 e 5, del GDPR tiene per iscritto un Registro delle attività relative ai trattamenti svolti per conto del Titolare.

10) ASSISTENZA AL TITOLARE:

In generale, il Responsabile del trattamento è tenuto ad assistere il Titolare nel garantire il rispetto degli obblighi a cui è vincolato quest'ultimo e a rispondere prontamente e comunque non oltre 72 ore dalle richieste di informazioni del Titolare del trattamento.

Il Responsabile comunicherà ogni informazione utile al fine di assistere il Titolare nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti. Qualora il Responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti, informa senza indugio e comunque non oltre 72 ore il Titolare affinché possa garantire che i dati personali siano esatti e aggiornati.

Nel caso in cui riceva richieste degli interessati per l'esercizio dei loro diritti, il Responsabile notifica prontamente e comunque non oltre 72 ore al Titolare del trattamento qualunque richiesta ricevuta dall'interessato in quanto non è autorizzato a rispondere egli stesso alla richiesta.

Inoltre, il Responsabile del trattamento assiste il Titolare nel garantire il rispetto degli obblighi imposti a quest'ultimo ai sensi dell'articolo 32 del GDPR, fornendogli, tra l'altro, le informazioni riguardanti le misure tecniche e organizzative da questi adottate in conformità all'articolo 32 medesimo, unitamente a tutte le altre informazioni necessarie al Titolare del trattamento per conformarsi agli obblighi a lui imposti per garantire un livello di sicurezza adeguato al rischio.

Il Responsabile si impegna a predisporre, condividere e aggiornare periodicamente la valutazione del rischio per la sicurezza dei dati e la valutazione di impatto sulla protezione dei dati e, comunque, a redigere uno o più atti di documentazione delle scelte, dando atto della conformità alla normativa sulla protezione delle persone con riguardo al trattamento dei dati e alla circolazione dei dati, ovvero indicando che il trattamento presenterebbe un rischio elevato.

Laddove la valutazione di impatto sulla protezione dei dati presentasse un rischio elevato, anche in fase di consultazione con la/le autorità di controllo competenti, il Responsabile assisterà il Titolare del trattamento per adottare le misure adeguate per attenuare il rischio.

Il Responsabile si impegna ad adibire apposito ufficio/referente, segnalando un punto di contatto diretto al Titolare del trattamento, alle incombenze relative alla notificazione e comunicazioni previste dal GDPR.

11) COMUNICAZIONE E REGISTRO DI INCIDENTI DI SICUREZZA E DI VIOLAZIONI DI DATI PERSONALI:

In caso di incidente di sicurezza e/o di violazione dei dati personali (cd. Data Breach), senza indugio il Responsabile del trattamento coopera con il Titolare e lo assiste nell'adempimento degli obblighi, ai sensi degli artt. 33 e 34 GDPR.

Nel caso di incidente di sicurezza e/o di una violazione dei dati personali trattati dal Responsabile del trattamento, quest'ultimo ne dà comunicazione al Titolare senza ingiustificato ritardo e comunque non oltre 24 ore dopo esserne venuto a conoscenza. La comunicazione iniziale contiene le informazioni disponibili in quel momento e le altre informazioni sono fornite non appena disponibili, senza ingiustificato ritardo. Il Responsabile documenta qualsiasi incidente di sicurezza e/o

di violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Il Responsabile deve mantenere un Registro degli incidenti di sicurezza, anche qualora non vi siano delle violazioni dei dati personali, per coadiuvare il Titolare nel suo obbligo relativo al paragrafo 5 dell'art. 33 del GDPR.

A seguito del verificarsi di detti incidenti il Titolare potrà:

- effettuare le succitate attività di revisione, comprese le ispezioni (v. misura n. 3);
- prescrivere l'adozione di misure di sicurezza aggiornate e/o ulteriori anche rispetto a quelle previste dal presente accordo;
- attivare azioni di rivalsa nei confronti del Responsabile;
- applicare le penali contrattuali;
- risolvere il contratto (cfr. la succitata Clausola 10).

Il Responsabile deve adottare procedure tecniche e organizzative volte alla gestione di eventuali incidenti di sicurezza e di violazioni di dati personali; deve disporre altresì di una struttura per la prevenzione e gestione degli incidenti informatici e delle violazioni di dati personali con il compito d'interfacciarsi con le analoghe strutture del Titolare.

12) LINEE GUIDA E PROVVEDIMENTI DELL'AUTORITA' GARANTE PRIVACY:

Il Responsabile del trattamento s'impegna a mettere in atto le misure tecniche e organizzative previste da Linee Guida e provvedimenti adottati dalle Autorità europee in materia di protezione dei dati personali, con particolare riferimento a quelli adottati dal Garante Privacy quali a titolo esemplificativo:

NOTA ESPLICATIVA: i provvedimenti elencati sono un elenco non esaustivo da adattare alla singola situazione, da eliminare non pertinenti e non applicabili e da aggiungere eventuali provvedimenti attinenti e sopraggiunti:

- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015 ((Pubblicato sulla Gazzetta Ufficiale n. 179 del 4 agosto 2015);
- Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali - 13 ottobre 2008 (G.U. n. 287 del 9 dicembre 2008);
- Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali - 27 novembre 2008 (G.U. n. 287 del 9 dicembre 2008);
- Posta elettronica e internet – provvedimento 1° marzo 2007.

I provvedimenti e le linee guida specifiche in materia di Privacy applicabili al Responsabile sono:

- Linee guida in materia di conservazione delle password (ACN & GPDP, Provvedimento n. 594 del 7 dicembre 2023)
- Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021
- Provvedimento in materia di videosorveglianza - 8 aprile 2010;
- Adempimenti semplificati per il customer care (inbound) - 15 novembre 2007
- RFID Etichette intelligenti: prescrizioni - 9 marzo 2005;
- Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014;
- Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro - 4 ottobre 2011;
- Sistemi di videosorveglianza per il controllo della procedura di raccolta del campione urinario a fini certificatori o di cura della salute 15 maggio 2013;
- Trattamento di dati personali per profilazione on line - 19 marzo 2015;

- Provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di mobile remote payment – 22 maggio 2014 (Pubblicato sulla Gazzetta Ufficiale n. 137 del 16 giugno 2014)
- Trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati – 15 maggio 2014;
- Dossier sanitario - 4 giugno 2015
- Svolgimento di indagini di customer satisfaction in ambito sanitario - 5 maggio 2011;
- Le norme del Codice Privacy non in contrasto con il Regolamento Europeo e non oggetto di abrogazione/modifica
- per i trattamenti di dati sensibili svolti dai soggetti pubblici (quelli di cui all'art. 6.1.c) ed e) del GDPR), in considerazione dell'art. 6.2 del GDPR saranno valutate le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 del Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.
- Le buone prassi in materia di sicurezza o Privacy proposte da ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione);
- Le buone prassi in materia di sicurezza o Privacy proposte da associazioni, a titolo esemplificativo: Center for Internet Security; Critical Security Controls for Effective Cyber Defense; CIS Benchmarks.

13) CERTIFICAZIONI

NOTA ESPLICATIVA: eliminare quelle non pertinenti e aggiungere quelle mancanti:

Per attestare l'adeguatezza delle misure di sicurezza adottate (cfr. art. 28.5 del GDPR), il Responsabile del trattamento aderisce a specifici codici di condotta o a schemi di certificazione come di seguito:

a) visto l'art. 43.1.b) del GDPR, che prevede una certificazione accreditata ISO 17065, il Responsabile del trattamento ha ottenuto il rilascio delle seguenti certificazioni:

- ISDP©10003 (ITA);
- Carpa (LU);
- Europrivacy (LU);
- Europrice (D);
- altra certificazione accreditata ISO 17065 in materia di protezione dei dati personali;

b) analizzato l'art. 32 (nonché l'art. 25) del GDPR; considerato che la norma di accreditamento ISO 17021-I non è da considerarsi valida ai fini del GDPR, pur tuttavia molti argomenti trattati hanno riscontro in specifici requisiti di legge europei e nazionali, il Responsabile del trattamento possiede le seguenti certificazioni:

- ISO/IEC 27001;
- ISO/IEC 22301;
- ISO/IEC 20000-1;
- ISO/IEC 27701;
- ISO/IEC 27017 e ISO/IEC 27018, integrate, come addendum alla Norma ISO/IEC 27001;
- altra certificazione accreditata (e/o integrata) come addendum alla Norma ISO/IEC 27001;
- altra certificazione accreditata in materia di privacy e gestione della sicurezza delle informazioni;

c) il Responsabile del trattamento ha ottenuto inoltre le seguenti certificazioni:

- ISO 9001;
- ISO 13485;
- altra certificazione accreditata in materia di gestione della qualità;
- ALTRO.....

14) INFORMAZIONI SUL TRATTAMENTO E CONSENSO DELL'INTERESSATO:

Informazioni sul trattamento

L'informativa resa dal titolare per i trattamenti di cui all'allegato II, elaborata dal Titolare del trattamento, deve essere:

NOTA ESPLICATIVA: individuare la fattispecie pertinenti e, eventualmente, aggiungere quelle mancanti:

- Consegnata a mano all'interessato;
- Pubblicata online sul sito XXXX;
- Non applicabile;
- L'informativa redatta e consegnata dal Titolare stesso;
- Altro (specificare nello spazio sottostante).

Gestione del consenso.

Nell'eventualità in cui il trattamento fosse fondato sulla base giuridica del consenso "libero" dell'interessato, a quest'ultimo sarà fornita una specifica ed ulteriore nota di informazioni e gli sarà richiesto l'apposito consenso, in mancanza del quale non si procederà al relativo trattamento. Il trattamento prevede la raccolta e registrazione del consenso tramite:

NOTA ESPLICATIVA: individuare la fattispecie pertinenti e, eventualmente, aggiungere quelle mancanti:

- Informativa e modulo raccolta consenso cartaceo redatto, reso e raccolto a cura del Titolare del trattamento;
- Informativa e modulo raccolta consenso cartaceo redatto a cura del Titolare e reso/raccolto da XXXX che dovrà consegnare la modulistica firmata al Titolare del trattamento;
- Raccolta e registrazione del consenso tramite sistema XXXX;
- Altro;
- Non applicabile.