Codice A2006D
D.D. 1 luglio 2025, n. 224
Museo Regionale di Scienze Naturali. Affidamento dell'incarico di esperto per l'attività di Radioprotezione e Sorveglianza Fisica (ai sensi dell'art. 128 del D.lgs. n. 101 del 31 luglio 2020) all'Azienda Ospedaliera Ordine Mauriziano di Torino. Decisione a contrarre e di affidamento. CIG B76BFB31C1. Impegno di spesa di Euro 5.124,00 (o.f.c.) sul cap 113960 annualità 2025 e 2026.

REGIONE PIEMONTE

ATTO DD 224/A2006D/2025 DEL 01/07/2025

DETERMINAZIONE DIRIGENZIALE
A2000C - CULTURA, TURISMO, SPORT E COMMERCIO
A2006D - Museo regionale di scienze naturali

OGGETTO: Museo Regionale di Scienze Naturali. Affidamento dell'incarico di esperto per l'attività di Radioprotezione e Sorveglianza Fisica (ai sensi dell'art. 128 del D.lgs. n. 101 del 31 luglio 2020) all'Azienda Ospedaliera Ordine Mauriziano di Torino. Decisione a contrarre e di affidamento. CIG B76BFB31C1. Impegno di spesa di Euro 5.124,00 (o.f.c.) sul cap 113960 annualità 2025 e 2026.

Premesso che:

• la legge regionale 29 giugno 1978, n. 37 ha istituito il Museo Regionale di Scienze Naturali (MRSN), Settore della Direzione Cultura, Turismo, Sport e Commercio della Regione Piemonte e, in particolare, il Regolamento del Museo stesso, approvato con Deliberazione del Consiglio Regionale n. 609 del 17 aprile 1980, all'articolo 9, lettera i) ha stabilito che al Direttore spetta l'attuazione dei provvedimenti di spesa necessari per lo sviluppo delle attività;

• il Settore sopra richiamato è articolato in tre Reparti: Conservazione e Ricerca, Museologia e Didattica e Informazione e Documentazione. Il primo è suddiviso in 5 Sezioni: Botanica, Entomologia, Mineralogia-Petrografia- Geologia, Paleontologia e Zoologia, che, con la sola eccezione della Botanica, hanno in comodato d'uso la gestione delle collezioni storiche dell'Università di Torino, cui dagli anni ottanta del Novecento sono andate ad unirsi le raccolte regionali, frutto di acquisizioni, donazioni, scambi e scavi. Si tratta di un patrimonio di inestimabile valore scientifico, culturale ed economico;

• presso la sede del Museo Regionale di Scienze Naturali di Torino sono conservati nelle collezioni della Sezione di Mineralogia, Petrografia e Geologia numerosi campioni di minerali e rocce radioattivi collocati in armadi schermati situati in locali posti al di fuori degli spazi adibiti a deposito in uso al personale della Sezione;

• nell'espletamento delle attività di controllo e conservazione delle collezioni il personale della

succitata Sezione può essere esposto a radiazioni ionizzanti provenienti dalle suddette sorgenti;

• ai sensi del D.Lgs n. 101 del 31 luglio 2020 e s.m.i., normativa vigente in materia di protezione contro i pericoli derivanti dall'esposizione alle radiazioni ionizzanti e in particolare ai sensi degli artt. 108 e seguenti e dell'art. 128 del D. Lgs predetto, al datore di lavoro competono compiti e adempimenti in materia di radioprotezione, fra i quali la nomina di un Esperto per l'attività di Radioprotezione, al fine di assicurare la sorveglianza fisica dei lavoratori e che effettuerà misurazioni, esami, verifiche o valutazioni di carattere fisico, tecnico o radiotossicologico;

• con DGR n. 20-1117 del 02.03.2015 il Dirigente responsabile del Settore Museo Regionale di Scienze Naturali è stato individuato, ai fini dell'applicazione del D. Lgs 81/2008, datore di lavoro del Settore stesso;

• con determinazione dirigenziale n. 216/A2006B del 20.10.2020 era stato approvato l'atto aggiuntivo rep. 212 del 30.10.2020 alla convenzione rep. 229 del 04 ottobre 2017 disciplinante i rapporti tra SCR Piemonte S.p.A. e il Settore Museo Regionale di Scienze Naturali. In particolare, il Museo aveva avuto necessità di provvedere urgentemente all'isolamento del locale ove sono custoditi i materiali radioattivi facenti parte della collezione della Sezione di Mineralogia, Geologia e Petrografia, attraverso una schermatura in lastre di piombo, al fine di migliorare ulteriormente la protezione dalle radiazioni ionizzanti, in quanto tale locale si trova nell'interrato in corrispondenza dei servizi igienici in futuro aperti al pubblico di riferimento per il Lotto XIV e nel contempo di individuare un soggetto cui affidare l'incarico di Esperto di radioprotezione per il supporto specialistico per la fase di progettazione e realizzazione delle opere di approntamento del locale di cui sopra e per tutti gli adempimenti previsti in materia dal D. Lgs 101/2020, con opzione di rinnovo al 31 dicembre 2021;

• con nota del 06.04.2021 (nostro prot. 3275/A2000A del 07.04.2021), a causa di sopraggiunte difficoltà relative al rinnovo della nomina dell'esperto di radioprotezione in carica, SCR Piemonte S.p.A. aveva comunicato di aver individuato quale nuovo professionista, nel ruolo di Esperto di radioprotezione per il Museo, il dott. Michele Stasi, Direttore della SC Fisica Sanitaria dell'Azienda Ospedaliera Ordine Mauriziano, abilitato e iscritto all'elenco nazionale Esperti di Radioprotezione di III grado (ex Esperti qualificati) col numero 30376, precisando che, essendo il dott. Stasi dipendente dell'Azienda Ospedaliera Ordine Mauriziano di Torino, i rapporti tra SCR e l'Azienda Ospedaliera erano stati regolati attraverso convenzione sottoscritta in data 2 aprile 2021;

• alla scadenza della Convenzione il Settore del Museo Regionale di Scienze Naturali ha voluto regolamentare i rapporti direttamente con l'Azienda Ospedaliera Ordine Mauriziano di Torino che mette a disposizione il professionista e procedere in autonomia all'affidamento, senza l'intervento della Società di Committenza e, pertanto, con DD n. 227/A2006C del 17.07.2024, è stato approvato dal Dirigente responsabile del Settore Museo Regionale di scienze Naturali lo schema di Convenzione, in continuità con la precedente Convenzione e fino al 31.12.2024, tra l'Azienda Ospedaliera Ordine Mauriziano di Torino e il Museo Regionale di Scienze Naturali e contestualmente affidato alla predetta Azienda il servizio professionale di un esperto per l'attività di Radioprotezione e Sorveglianza Fisica dei lavoratori e della popolazione presso il MRSN;

• in alcuni locali del Museo continua a persistere nei confronti dei conservatori della sezione di Mineralogia, Petrografia e Geologia l'esposizione a radiazioni ionizzanti, ed è, pertanto, opportuno procedere ad un nuovo affidamento per messa a disposizione di esperto di radioprotezione;

• si tratta di un incarico professionale di altissima specializzazione e non di una figura comune e facilmente rinvenibile sul mercato.

Dato inoltre atto che, in conformità a quanto previsto all'art. 49, comma 6, del D. lgs. 36/2023, " *È comunque consentito derogare all'applicazione del principio di rotazione per gli affidamenti diretti di importo inferiore a 5.000 euro",* è intenzione del Settore Museo Regionale di Scienze Naturali continuare la collaborazione con l'AO Ordine Mauriziano.

Ritenuto pertanto opportuno affidare, tramite affidamento diretto ai sensi dell'art. 50, comma 1, lettera b) del D.Lgs 36/2023 e s.m.i., l'incarico di esperto per l'attività di Radioprotezione e Sorveglianza Fisica (ai sensi dell'art. 128 del D.lgs. n. 101 del 31 luglio 2020) all'Azienda Ospedaliera Ordine Mauriziano di Torino con sede in Torino, Via Magellano 1 (C.F. 09059340019 - cod beneficiario: 106617).

Dato atto che l'Azienda Ospedaliera Ordine Mauriziano di Torino, che metterà a disposizione del MRSN la professionalità di un esperto per l'attività di Radioprotezione e Sorveglianza Fisica dei lavoratori e della popolazione e che presterà la propria attività presso il Museo Regionale di Scienze Naturali, non è iscritta come operatore economico sulle piattaforme elettroniche e che pertanto l'affidamento sopra richiamato opera in regime transitorio fuori piattaforma MEPA e Sintel come da delibera Anac n. 582 del 13.12.2023 che "*al fine di favorire le Amministrazioni nell'adeguarsi ai nuovi sistemi che prevedono l'utilizzo delle piattaforme elettroniche e garantire così un migliore passaggio verso l'amministrazione digitale, sentito il Ministero delle Infrastrutture e dei Trasporti, ha ritenuto necessario adottare un interfaccia web per gli affidamenti diretti di importo inferiore ai 5000 euro, in supporto delle amministrazioni, al fine di consentire lo svolgimento delle ordinarie attività di approvvigionamento. Tale strumento rappresenta una modalità suppletiva che può essere utilizzata in caso di impossibilità o difficoltà di ricorso alle PAD, per il primo periodo di operatività della digitalizzazione"*, regime transitorio esteso con Comunicato n. 596 del 18/12/2024 fino al 30 giugno 2025, nonché da recente comunicato del Presidente dell'Anac del 18 giugno 2025, che lo estende ulteriormente.

Rilevato che, in data 19.06.2025, il Museo Regionale di Scienze Naturali ha acquisito con protocollo n. 6676/A2000C lo schema di Convenzione, allegato alla presente determinazione per farne parte integrante e sostanziale, con cui si intendono definire e regolamentare i rapporti di collaborazione relativi alle consulenza specialistiche da svolgersi a cura dell'AO Ordine Mauriziano presso il Museo Regionale di Scienze Naturali di Torino.

Tenuto conto che, per l'esercizio di tale attività, da svolgersi fuori orario di servizio, l'esperto di radioprotezione garantirà, come indicato nello schema di Convenzione allegato alla presente per farne parte integrante e sostanziale, un numero di sopralluoghi necessario allo svolgimento del ruolo di esperto di radioprotezione (ex D.Lgs. 101/2020) e delle attività ad esso connesse.

In particolare:

1. sorveglianza fisica delle radiazioni e radioprotezione (attività di protezione dalle radiazioni ionizzanti dei lavoratori e della popolazione, gestione della dosimetria personale e ambientale, gestione radioprotezionistica dei minerali radioattivi e valutazione dei rischi relativi);
2. protezione all'Esposizione al Radon così come previsto dal Titolo IV Capo I del D.Lgs. 101/2020; 3. gestione delle pratiche che comportano l'impiego di materiali contenenti radionunclidi di origine naturale (Capo II D.Lgs. 101/2020);
4. consulenza radioprotezionistica e monitoraggio con dosimetri ambientali.

Considerata pertanto la necessità di individuare la figura di un Esperto di radioprotezione presso l'Azienda Ospedaliera Ordine Mauriziano con sede in Torino, Via Magellano 1 (C.F. 09059340019

- cod beneficiario: 106617), abilitato e iscritto all’elenco nazionale Esperti di Radioprotezione.

Considerato che la Convenzione succitata e facente parte integrante del presente provvedimento ha decorrenza dal giorno della stipula sino al 30/06/2026.

Rilevato altresì che, come da Convenzione succitata per il servizio sopra descritto, sarà corrisposto da parte del Museo di Scienze Naturali all’AO Ordine Mauriziano di Torino un importo complessivo pari ad € 5.124,00 o.f.c..

Ritenuta dal RUP l’offerta di cui sopra economicamente conveniente e tecnicamente congrua rispetto alle esigenze del Museo Regionale di Scienze Naturali.

Considerato che ai sensi dell'Allegato I.4 al codice dei contratti pubblici, D.Lgs. 36/2023, sono esenti da imposta di bollo gli affidamenti al di sotto dei 40.000 euro e pertanto non si deve provvedere in tal senso.

Ritenuto pertanto opportuno affidare, tramite affidamento diretto, l’incarico di esperto per l’attività di Radioprotezione e Sorveglianza Fisica all’ AO Azienda Ospedaliera Ordine Mauriziano con sede in Torino, Via Magellano 1 (C.F. 09059340019 - cod beneficiario 106617) che metterà a disposizione la professionalità di un esperto per l’attività di Radioprotezione e Sorveglianza Fisica dei lavoratori e della popolazione e che presterà la propria attività presso il Museo Regionale di Scienze Naturali.

Ritenuto di impegnare a favore dell’Azienda Ospedaliera Ordine Mauriziano con sede in Torino, Via Magellano 1 (C.F. 09059340019 - cod beneficiario 106617), la somma complessiva di euro 5.124,00 (o.f.c.), di cui euro 924,00 per IVA al 22% da versare direttamente all’erario ai sensi dell’art 17 comma 2 del DPR 633/1972, la cui transazione elementare è rappresentata nell’Appendice A - parte integrante e sostanziale del presente provvedimento, così come ripartita:
• annualità 2025: impegno di spesa di euro 2.562,00 (o.f.c.), di cui euro 2.100,00 per la prestazione ed euro 462,00 per IVA soggetta a scissione dei pagamenti da versare direttamente all’erario ai sensi dell’art. 17- ter del D.P.R. 633/1972, sul Capitolo 113960, missione 5, programma 2 del Bilancio finanziario gestionale 2025-2027;
• annualità 2026: impegno di spesa di euro 2.562,00 (o.f.c.), di cui euro 2.100,00 per la prestazione ed euro 462,00 per IVA soggetta a scissione dei pagamenti da versare direttamente all’erario ai sensi dell’art. 17- ter del D.P.R. 633/1972, sul Capitolo 113960, missione 5, programma 2 del Bilancio finanziario gestionale 2025-2027;

Valutata la non presenza di rischi dati da interferenze di cui all’art. 26 comma 3) del D. Lgs. 9 Aprile 2008 n. 81, in quanto l’esperto incaricato del servizio di radioprotezione accederà esternamente al locale in cui occorre svolgere l’attività di radioprotezione.

Ritenuto inoltre di liquidare le somme sopra indicate secondo le modalità definite nella lettera a contratto da stipularsi ai sensi dell’art. 18 comma 1 del D. Lgs 36/2023 e s.m.i., parte integrante e sostanziale della presente determinazione (Allegato 2).

Dato inoltre atto che:

- alla procedura in questione è stato attribuito il seguente numero di CIG: B76BFB31C1;
- il Responsabile Unico di Progetto (RUP) è individuato nel dirigente del Settore Museo Regionale di Scienze Naturali, Ing. Marco Fino, firmatario del provvedimento;
- la scadenza dell’obbligazione ricade negli esercizi 2025 e 2026;

- sono rispettati gli obblighi in materia di trasparenza di cui al D.Lgs. 33/2013 e s.m.i.;
- per quanto riguarda le transazioni relative ai pagamenti verranno rispettate le disposizioni dell'art. 3 della Legge 136/2010 e s.m.i. in materia di tracciabilità dei flussi finanziari;
- è stata verificata la compatibilità del programma di pagamento con le regole di finanza pubblica, ai sensi dell'art. 56 del D.Lgs. n. 118/2011 e s.m.i.;
- il presente provvedimento non determina oneri impliciti per il bilancio regionale non compresi negli stanziamenti di bilancio;
- la spesa è assunta su un capitolo di spesa di natura ricorrente;
- l'impegno è registrato in competenza;
- la spesa è finanziata con risorse regionali.

Attestata:
- l'avvenuta verifica dell'insussistenza, anche potenziale, di situazioni di conflitto di interesse;
- la regolarità amministrativa del presente provvedimento ai sensi della DGR n. 8-8111 del 25 gennaio 2024 "Disciplina del sistema dei controlli e specificazione dei controlli previsti in capo alla Regione Piemonte in qualità di Soggetto Attuatore nell'ambito dell'attuazione del PNRR. Revoca delle D.G.R. 17 ottobre 2016 n. 1-4046 e 14 giugno 2021 n. 1-3361".

Tutto ciò premesso,

IL DIRIGENTE

Richiamati i seguenti riferimenti normativi:

- la Legge regionale 29 giugno 1978, n. 37 "Istituzione del Museo regionale di Scienze Naturali;
- gli artt. 4 e 17 del Decreto Legislativo n. 165 del 30 marzo 2001, "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche;
- la legge 27 dicembre 1997 n. 449 "Misure per la stabilizzazione della finanza pubblica;
- la Legge 7 agosto 1990, n. 241 (Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi) più volte integrata e modificata, nonché la corrispondente legge regionale 14 ottobre 2014, n. 14 (Norme sul procedimento amministrativo e disposizioni in materia di semplificazione);
- la Legge regionale n. 2 del 4 marzo 2003 "Legge finanziaria per l'anno 2003;
- la Legge n. 136 del 13 agosto 2010 "Piano straordinario contro le mafie, nonché delega al Governo in materia di normativa antimafia;
- il D.Lgs. n. 36/2023 "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";
- la Legge 266 del 22/11/2002 "Documento Unico di regolarità contributiva" e s.m.i..;
- il D.Lgs 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", modificato dal D.Lgs 25 maggio 2016 n. 97, e relative circolari attuative della Regione Piemonte;
- il D.Lgs 31 dicembre 2024, n. 209 "Disposizioni integrative e correttive al codice dei contratti pubblici, di cui al decreto legislativo 31 marzo 2023, n. 36";
- gli articoli 17 e 18 della legge regionale n. 23 del 28 luglio 2008, "Disciplina dell'organizzazione degli uffici regionali e disposizioni concernenti la dirigenza e il personale";

- il D.Lgs 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 s.m.i.;
- la D.G.R n. 43 - 3529 del 09 luglio 2021 "Regolamento regionale di contabilità della Giunta regionale. Abrogazione del regolamento regionale 5 dicembre 2021, n. 18/R. Approvazione";
- la Legge regionale 27 febbraio 2025, n. 1 "Disposizioni per la formazione del bilancio annuale di previsione 2025-2027 (Legge di stabilità regionale 2025)";
- la Legge regionale 27 febbraio 2025, n. 2. "Bilancio di previsione finanziario 2025-2027";
- la DGR n. 12-852 del 3 marzo 2025 "Decreto legislativo n. 118/2011, articoli 11 e 39, comma 10 e 13. Legge regionale n. 2/2025 "Bilancio di previsione finanziario 2025-2027". Approvazione del Documento Tecnico di Accompagnamento e del Bilancio Finanziario Gestionale 2025-2027";
- la D.G.R. n. 11-739 del 31 Gennaio 2025 "Approvazione del Piano integrato di attività e organizzazione (PIAO) della Giunta regionale del Piemonte per gli anni 2025-2027 e della tabella di assegnazione dei pesi degli obiettivi dei Direttori del ruolo della Giunta regionale per l'anno 2025;

determina

Per le motivazioni espresse in premessa,

- di approvare lo schema di Convenzione, tra l'Azienda Ospedaliera Ordine Mauriziano e il Museo Regionale di Scienze Naturali per messa a disposizione di esperto per attività di radioprotezione e sorveglianza fisica, allegato alla presente determinazione per farne parte integrante e sostanziale;

- di affidare, ai sensi dell'art. 50 comma, comma 1, lettera b) del D. Lgs 36/2023 e s.m.i, all'Azienda Ospedaliera Ordine Mauriziano di Torino, per le motivazioni di cui in premessa, l'incarico di esperto per l'attività di Radioprotezione e Sorveglianza Fisica dei lavoratori e della popolazione, che presterà la propria attività presso il Museo Regionale di Scienze Naturali per l'importo di Euro 5.124,00 (o.f.c.), secondo lo schema di Convenzione tra l'Azienda Ospedaliera ordine Mauriziano di Torino e il Museo Regionale di Scienze Naturali;
- di impegnare a favore dell'Azienda Ospedaliera Ordine Mauriziano con sede in Torino, Via Magellano 1 (C.F. 09059340019 - cod beneficiario 106617), la somma complessiva di euro 5.124,00 (o.f.c.), di cui euro 924,00 per IVA al 22% da versare direttamente all'erario ai sensi dell'art 17 comma 2 del DPR 633/1972, la cui transazione elementare è rappresentata nell'Appendice A - parte integrante e sostanziale del presente provvedimento, così come ripartita:
  • annualità 2025: impegno di spesa di euro 2.562,00 (o.f.c.), di cui euro 2.100,00 per la prestazione ed euro 462,00 per IVA soggetta a scissione dei pagamenti da versare direttamente all'erario ai sensi dell'art. 17- ter del D.P.R. 633/1972, sul Capitolo 113960, missione 5, programma 2 del Bilancio finanziario gestionale 2025-2027;
  • annualità 2026: impegno di spesa di euro 2.562,00 (o.f.c.), di cui euro 2.100,00 per la prestazione ed euro 462,00 per IVA soggetta a scissione dei pagamenti da versare direttamente all'erario ai sensi dell'art. 17- ter del D.P.R. 633/1972, sul Capitolo 113960, missione 5, programma 2 del Bilancio finanziario gestionale 2025-2027;

- di procedere mediante stipula dello schema di Convenzione tra l'Azienda Ospedaliera Ordine Mauriziano e il Museo Regionale di Scienze Naturali, allegata alla presente determinazione per

farne parte integrante e sostanziale;

- di dare atto che la liquidazione delle somme sopra indicate avverrà secondo le modalità definite nella lettera a contratto da stipularsi ai sensi dell'art. 18 comma 1 del D. Lgs 36/2023 e s.m.i., parte integrante e sostanziale della presente determinazione (Allegato 2);
- di provvedere al pagamento nei termini previsti dal D.Lgs. 231/2002, su presentazione di fattura debitamente controllata e vistata dal RUP ai sensi del D.Lgs. 36/2023 in ordine alla regolarità e rispondenza formale e fiscale;

- di individuare quale Responsabile Unico di Progetto (RUP) il dirigente del Settore Museo Regionale di Scienze Naturali, Ing. Marco Fino.

Dati amministrazione trasparente
Direzione Cultura, Turismo, Sport e Commercio - Settore Museo Regionale di Scienze Naturali
Responsabile Unico di Progetto: Marco Fino
Beneficiario: Azienda Ospedaliera Ordine Mauriziano con sede in Torino, Via Magellano 1 (C.F. 09059340019 - cod beneficiario: 106617).
Importo: € 5.124,00 (o.f.c.)
Modalità di individuazione del beneficiario: affidamento diretto ai sensi dell'art. 50, comma 1, lettera b), del Decreto legislativo 31 marzo 2023, n. 36 e s.m.i..

La presente determinazione sarà pubblicata sul sito della Regione Piemonte nella sezione "Amministrazione trasparente", ai sensi degli articoli 23, comma 1, lettera b, e 37 del D.Lgs. 33/2013.
La presente determinazione sarà pubblicata sul Bollettino Ufficiale della Regione Piemonte ai sensi dell'art. 61 dello Statuto e dell'art. 5 della legge regionale n. 22/2010.

Avverso la presente determinazione è possibile ricorrere al TAR entro trenta giorni dalla conoscenza dell'atto, secondo quanto previsto dall'art. 120 del D.Lgs. n. 104 del 02/07/2010 (Codice del processo amministrativo).

IL DIRIGENTE (A2006D - Museo regionale di scienze naturali)
Firmato digitalmente da Marco Fino

Allegato

CONVENZIONE TRA L'AZIENDA OSPEDALIERA ORDINE MAURIZIANO DI TORINO E IL MUSEO REGIONALE DI SCIENZE NATURALI PER MESSA A DISPOSIZIONE DI ESPERTO PER ATTIVITA' DI RADIOPROTEZIONE E SORVEGLIANZA FISICA. PERIODO: DALLA DATA DI SOTTOSCRIZIONE AL 30 GIUGNO 2026.

TRA

L'Azienda Ospedaliera Ordine Mauriziano - C.F. 09059340019 - (di seguito denominata AO) con sede in Torino, Via Magellano 1, in persona del Direttore Generale e Legale Rappresentante Dott.ssa Franca DALL'OCCO, domiciliato per la carica presso la sede legale dell'Azienda.

E

Il Museo Regionale di Scienze Naturali – C.F. 80087670016 – P. Iva 02843860012 – (di seguito denominato MRSN) con sede in Torino Via Giovanni Giolitti 36, in persona del Legale Rappresentante Dr. Marco FINO, domiciliato per la carica presso la sede legale del MRSN.

SI CONVIENE E STIPULA QUANTO SEGUE

Art. 1
OGGETTO DELLA CONVENZIONE

Con la presente convenzione le Parti intendono definire e regolamentare i rapporti di collaborazione relativi all'assegnazione dell'incarico di Esperto per l'attività di Radioprotezione e Sorveglianza Fisica, al Dott. Michele Stasi – Direttore della S.C. Interaziendale Fisica Sanitaria dell'A.O..

Art. 2
RADIOPROTEZIONE

L'AO metterà a disposizione del MRSN la professionalità del dott. Michele Stasi, Direttore della S.C. Interaziendale di Fisica Sanitaria per l'attività di Radioprotezione e Sorveglianza Fisica dei lavoratori e della popolazione che presterà la propria attività presso il Museo Regionale di Scienze Naturali. Per lo svolgimento di tale attività, da svolgersi fuori orario di servizio, il Dr. Stati garantirà un numero di sopralluoghi necessario allo svolgimento delle seguenti attività:

1. Esperto di radioprotezione (ex D.Lgs. 101/2020)
2. Sorveglianza fisica delle radiazioni e radioprotezione: attività di protezione dalle radiazioni ionizzanti dei lavoratori e della popolazione, gestione della dosimetria personale e ambientale, gestione radioprotezionistica dei minerali radioattivi e valutazione dei rischi relativi.
3. Protezione all'Esposizione al Radon così come previsto dal Titolo IV Capo I del D.Lgs. 101/2020
4. Gestione delle Pratiche che comportano l'impiego di materiali contenenti radionunclidi di origine naturale (Capo II D.Lgs. 101/2020)
5. Consulenza radioprotezionistica, monitoraggio con dosimetri ambientali.

Per l'attività sopra descritta, sarà corrisposto da parte del Museo di Scienze Naturali all'AO Ordine Mauriziano di Torino un importo complessivo pari ad € 4.200,00 + IVA 22% così suddiviso:

- € 4.000,00+IVA al Dr. Stasi
- € 200,00+IVA per la copertura del costo dei dosimetri che saranno forniti dall'AO Ordine Mauriziano al Museo di Scienze Naturali attraverso la ditta che ha in appalto la fornitura della dosimetria individuale dei lavoratori dell'AO.

Art. 3
COPERTURA ASSICURATIVA

Ferme restando le coperture assicurative RCT del MRSN, la responsabilità civile personale e professionale del personale dipendente dell'AO coinvolto nella presente convenzione sarà coperta dalla polizza RCT dell'AO nei limiti e nei termini previsti dal programma assicurativo regionale.

Le prestazioni rese al di fuori dell'orario di servizio non prevedono coperture per il rischio di infortuni, compreso quello *"in itinere",* al quale dovrà eventualmente provvedere in proprio il professionista.

Art. 4
RISERVATEZZA E PRIVACY

L'AO e il MRSN assicurano che il personale interessato dall'attività della presente convenzione si impegna a mantenere la riservatezza sui dati e documenti dei quali abbia conoscenza, possesso e detenzione, direttamente connessi e derivanti dall'attività svolta, in ottemperanza a quanto disposto dal Codice Privacy e dal Regolamento (UE) 2016/679.
Ai sensi della normativa sopra citata, l'Azienda rende noto che i dati che verranno comunicati dal MRSN per la stipula della presente convenzione saranno trattati, anche in forma elettronica, nel rispetto della normativa vigente in materia di tutela dei dati personali e utilizzati esclusivamente per il raggiungimento delle finalità istituzionali.
La convenzione comporta il trattamento dei dati personali dei quali è Titolare il MRSN, che avvalendosi della facoltà concessa dall'art. 28 del GDPR, nomina Responsabile esterno del trattamento dei dati l'AO con cui stipula l'Accordo allegato al presente atto quale parte integrante e sostanziale. La sua sottoscrizione è condizione per la validità della presente convenzione.

Art. 5
DURATA DELLA CONVENZIONE

La presente convenzione ha decorrenza dalla data di sottoscrizione fino al 30/06/2026, dando atto che eventuali attività rese nelle more della sottoscrizione della convenzione saranno regolate ai sensi del presente disciplinare.
Non è previsto il tacito rinnovo.
Durante il periodo di vigenza della convenzione, le parti potranno comunicare formale e motivata disdetta, anche parziale, della convenzione, con preavviso di trenta giorni a mezzo posta elettronica certificata:
- per l'AO: direzionesanitaria.mauriziano@pcert.postecert.it
- per il MRSN: culturcom@cert.regione.piemonte.it

Art. 6
CLAUSOLA ARBITRALE E DISPOSIZIONI FINALI

Eventuali controversie dovessero sorgere in relazione alla presente convenzione o all'interpretazione delle disposizioni in essa contenute potranno essere devolute ad un arbitro nominato concordemente dalle parti.
L'assolvimento dell'imposta di bollo è a carico di MRSN.
La presente convenzione è soggetta a registrazione in caso d'uso, e le spese di registrazione sono a carico della parte richiedente.

Torino,

L'Azienda Ospedaliera Ordine Mauriziano
Il Direttore Generale
Dott.ssa Franca DALL'OCCO

Il MRSN
Il Direttore
Dr. Marco FINO

CONTRATTO PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 PARAGRAFO 3) DEL REGOLAMENTO UE N. 2016/679

Tra

MUSEO REGIONALE DI SCIENZE NATURALI, (C. f. 80087670016 e P. IVA: 02843860012), in persona del suo legale rappresentante pro tempore, con sede legale in Torino, via Giovanni Giolitti, 36, , in qualità di Titolare del trattamento ex artt. 4 n. 7) e 24 del Regolamento UE n. 2016/679 (GDPR) (infra "Titolare del trattamento");

e

AZIENDA OSPEDALIERA ORDINE MAURIZIANO DI TORINO, (P. IVA: 09059340019), in persona del suo legale rappresentante pro tempore, con sede legale in Torino (TO), viale Magellano, 1, in qualità di Responsabile del trattamento ex artt. 4 n. 8) e 28 del GDPR (infra "Responsabile del trattamento").

Il Titolare ed il Responsabile potranno essere denominati, di seguito, congiuntamente anche come le "Parti".

1. Premesse.

1.1. Le Parti hanno concordemente convenuto, ai sensi dell'art. 28 paragrafo 3) del GDPR, le seguenti clausole contrattuali (infra "Clausole"/"Contratto di nomina" e/o "Contratto") volte a disciplinare la nomina del MAURIZIANO quale Responsabile del trattamento, ad opera del Titolare del trattamento, a fronte dello svolgimento, da parte di quest'ultimo, di un processo preventivo di risk assessment volto a valutare e documentare, in un'ottica di accountability ex art. 5 paragrafo 2) del GDPR (e di culpa in eligendo), il grado di affidabilità e di capacità, in capo al Responsabile del trattamento qui nominato, di fornire le garanzie necessarie, idonee ed adeguate a rendere, mediante l'adozione di misure di sicurezza tecniche ed organizzative ex art. 32 del GDPR, conforme il trattamento di specie alla normativa comunitaria e nazionale sulla protezione dei dati personali, ivi incluse le pronunzie e gli atti di cd. soft law emessi sul tema.

1.2. Nel contesto della convenzione intitolata: *"Convenzione tra l'Azienda Ospedaliera Ordine Mauriziano di Torino e il Museo Regionale di Scienze Naturali per messa a disposizione di esperto per attività di radioprotezione e sorveglianza fisica. Periodo: dalla data di sottoscrizione al 30/06/2026."*, il Responsabile del trattamento provvede a svolgere, per conto del Titolare, le relative operazioni di trattamento, in conformità al Contratto di nomina ed alla normativa comunitaria e nazionale sulla protezione dei dati personali, ivi inclusa la relativa giurisprudenza, dottrina dominante ovvero normativa di secondo livello (soft law).

2. Obblighi del Responsabile del trattamento.

2.1. Fatti salvi gli altri obblighi previsti dalle disposizioni di legge applicabili, ivi inclusi gli atti di soft law ovvero i Provvedimenti ad opera delle competenti Autorità di controllo ovvero di natura giurisdizionale, il Responsabile del trattamento è obbligato a svolgere i seguenti compiti:

a. Trattare i dati personali sulla base del presente Contratto di nomina, sulla base del rapporto descritto al precedente punto 1.2) ovvero in ragione di ogni altra istruzione impartita formalmente dal Titolare del trattamento, anche in caso di trasferimento dei relativi dati personali verso un paese terzo (ossia, situato al di fuori del Spazio Economico Europeo (SEE)) o un'organizzazione internazionale, salvo che lo richieda il diritto dell'UE o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento è tenuto ad informare il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b. Garantire che le proprie persone autorizzate al trattamento ex artt. 4 n. 10), 29 e 32 n. 4) del GDPR – previamente designate per iscritto, e adeguatamente istruite circa l'ambito di attività di trattamento oggetto di tale autorizzazione – si siano impegnate alla riservatezza ovvero abbiano un adeguato obbligo legale di riservatezza;
c. Adottare le misure di sicurezza tecniche ed organizzative richieste dall'art. 32 del GDPR (meglio illustrate, seppur in via generale, al relativo allegato 3), tenuto conto dello stato dell'arte, dei costi di implementazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, così come anche il rischio di (varia) probabilità e gravità per i diritti e le libertà delle persone fisiche, onde così assicurare un livello di sicurezza adeguato al rischio associato alle attività di trattamento demandate;
d. Rispettare le condizioni di cui all'art. 28 paragrafo 2) del GDPR, al fine di ricorrere ad un altro (sub) Responsabile del trattamento, così declinate nel caso di specie: il Responsabile del trattamento ha l'autorizzazione generale del Titolare del trattamento per l'assunzione di (sub) Responsabili del trattamento indicati nell'allegato 2);
e. Rispettare le condizioni di cui all'art. 28 paragrafo 4) del GDPR, laddove il Responsabile del trattamento si avvale di un (sub) Responsabile del trattamento per lo svolgimento di specifiche attività di trattamento: a tal riguardo, il Titolare del trattamento ha la facoltà di domandare al Responsabile del trattamento di fornirgli

copia del contratto (o atto giuridico) sottoscritto tra quest'ultimo e il relativo (sub) Responsabile del trattamento nominato;

f. Tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, per quanto possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti del soggetto interessato di cui al capo III) del GDPR;
g. Assistere il Titolare del trattamento nel garantire il rispetto degli adempimenti in materia di misure di sicurezza tecniche ed organizzative di cui all'art. 32 del GDPR, così come individuate, di volta in volta, dal Titolare del trattamento, ivi incluse le seguenti: i) pseudonomizzazione e/o cifratura dei dati personali; ii) capacità di assicurare la riservatezza, l'integrità e la disponibilità dei dati e la resilienza dei sistemi e dei servizi di trattamento; iii) capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; iv) procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
h. Assistere il Titolare del trattamento nell'esecuzione dell'onere di notifica e/o di comunicazione, ai sensi degli artt. 33 e 34 del GDPR, di una violazione di dati personali (data breach) ex art. 4 n. 12) del GDPR riferita ad un attività di trattamento svolta dal Responsabile del trattamento ovvero dal nominato (sub) Responsabile del trattamento: a tal fine, il Responsabile del trattamento è tenuto ad informare il Titolare del trattamento di tale evento immediatamente o, comunque, entro il termine (inderogabile) di n. 24 (ventiquattro) ore dal momento in cui ne è venuto a conoscenza, inviando un'apposita comunicazione, cooperando, peraltro, al riguardo con il Titolare del trattamento al fine di adottare in modo immediato o, comunque, senza ritardo tutte le misure necessarie al fine di minimizzare i rischi derivanti dalla violazione per i soggetti interessati, porre rimedio al data breach e mitigarne qualsiasi ulteriore effetto negativo;
i. Al termine del rapporto descritto al precedente punto 1.2.), il Responsabile del trattamento è tenuto a restituire tutti i dati personali al Titolare del trattamento e cancellare le copie esistenti, a meno che il diritto dell'UE o dei relativi Stati membri imponga la conservazione dei dati personali in questione, da ottemperare tuttavia nel rispetto del principio di minimizzazione ex art. 5 paragrafo 1) lettera c) del GDPR;
j. Mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al GDPR ed alla connessa normativa nazionale applicabile in materia, e consentire a quest'ultimo di svolgere, ove ritenuto opportuno o necessario, un'attività di revisione nei confronti del Responsabile del trattamento, ivi incluse le ispezioni, da realizzarsi ad opera del Titolare del trattamento ovvero da parte di un altro soggetto da questi appositamente incaricato, previo congruo preavviso non inferiore a n. 10 giorni;
k. Informare, senza ritardo, il Titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR ovvero altre disposizioni normative, anche nazionali, applicabili in materia;
l. Rispettare le disposizioni di cui al capo V) del GDPR (e connesse pronunce giurisprudenziali, dottrina ed atti di soft law), in caso di trasferimento di dati personali al di fuori del SEE o verso organizzazioni internazionali, previo ottenimento dello specifico nulla osta e relative istruzioni ad opera del Titolare del trattamento; nel caso in cui il trasferimento al di fuori del SEE o verso organizzazioni internazionali sia richiesto (o comunque imposto) da una legislazione comunitaria o di uno Stato membro dell'UE, il Responsabile del trattamento è tenuto ad informare, prima di svolgere tale operazione di trattamento, il Titolare del trattamento di tale requisito legale, a meno che la disposizione normativa in questione non vieti tale tipologia di comunicazioni ai fini di interesse pubblico.

3. Durata e corrispettivo.

3.1. Il presente Contratto è da considerarsi valido ed efficace a decorrere dalla data di validità e di efficacia del rapporto descritto al precedente punto 1.2.); esso, tuttavia, perderà di efficacia e di validità in caso di cessazione, per qualsivoglia motivo, del rapporto descritto al precedente punto 1.2.).

3.2. L'attività di trattamento, resa dal Responsabile del trattamento in favore del Titolare del trattamento, disciplinata dal presente Contratto di nomina, da ulteriori eventuali istruzioni, per iscritto, da parte del Titolare del trattamento nonché dalle ulteriori disposizioni normative nazionali/comunitarie applicabili è da intendersi a titolo gratuito, in deroga all'art. 1709 c.c.

4. Disposizioni finali.

4.1. L'eventuale invalidità, inapplicabilità o inefficacia di alcune delle clausole che compongono il presente Contratto non determina, di conseguenza, l'invalidità, inapplicabilità o l'inefficacia integrale del Contratto medesimo.

4.2. Le Parti concordano che eventuali controversie circa l'interpretazione della validità, applicabilità od efficacia del presente Contratto sono devolute, in via esclusiva, alla competenza giurisdizionale del Foro di Torino.

Allegato 1) al contratto per il trattamento dei dati personali ex art. 28 paragrafo 3) del Regolamento UE n. 2016/679: informazioni sulle attività di trattamento.

1.1. Natura/finalità dell'attività di trattamento.
Le operazioni di trattamento che il Responsabile del trattamento può eseguire sulle tipologie di dati personali sono connesse, anche in via indiretta, a dare esecuzione al rapporto tra le Parti descritto al punto 1.2.) del Contratto di nomina in questione.

1.2. Categoria dei soggetti interessati
Indicare quale categoria di soggetti interessati sono coinvolti nell'operazione di trattamento in questione:

- [x] Lavoratore dipendente o similare (ivi incluso, il collaboratore).
- [ ] Paziente.
- [ ] Altro soggetto: indicare .....

1.3. Categoria di dati personali.
Indicare quale categoria di dati personali sono coinvolti nell'operazione di trattamento in questione.

- [x] Dati personali ex art. 4 n. 1) del GDPR.
- [x] Dati personali cd. particolari ex art. 9 del GDPR.
- [ ] Dati personali cd. giudiziari ex art. 10 del GDPR.

Allegato 2) al contratto per il trattamento dei dati personali ex art. 28 paragrafo 3) del Regolamento UE n. 2016/679: (sub) Responsabili del trattamento autorizzati.

Ai sensi dell'art. 2.1. lettera d) del Contratto di nomina, il Titolare del trattamento autorizza il Responsabile del trattamento ad utilizzare i seguenti (sub) Responsabili del trattamento:

Denominazione	Sede	Attività di trattamento delegata

A tal riguardo, si ricorda che il Titolare del trattamento autorizza, sin dalla data di efficacia e validità del presente Contratto, il Responsabile del trattamento ad utilizzare i sopra descritti (sub) Responsabili del trattamento, i quali non possono, tuttavia, effettuare (direttamente ovvero per il tramite di un altro (sub) Responsabile del trattamento) un'attività di trattamento differente da quella sopra concordata ed autorizzata, in assenza di una specifica ed esplicita autorizzazione da parte del Titolare.

Allegato 3) al contratto per il trattamento dei dati personali ex art. 28 paragrafo 3) del Regolamento UE n. 2016/679: misure di sicurezza tecniche ed organizzative.

Il Titolare consiglia al Responsabile del trattamento di implementare le seguenti misure di sicurezza[1], in conformità con i più importanti standard (dottrina, giurisprudenza ed atti di soft law) del settore (nel caso, il Responsabile del trattamento è tenuto a far sì che le descritte misure di sicurezza vengano rispettare anche dagli eventuali (sub) Responsabili del trattamento indicati nell'allegato 2) ovvero successivamente nominati in base all'art. 2.1. lettera d) di sopra):

a. Tutto il personale – ivi inclusi, ove opportuno, i collaboratori – deve ricevere un'adeguata sensibilizzazione, istruzione, formazione, addestramento e aggiornamento periodico sulle politiche di sicurezza delle informazioni anche personali implementate, sulle procedure (e prassi) organizzative nonché sulla normativa comunitaria e nazionale sulla protezione dei dati personali ("addestramento, awareness e formazione del cd. fattore umano")[2]. Inoltre, ove ritenuto opportuno dovrebbe essere istituito un processo disciplinare, formale e comunicato, volto ad intraprendere provvedimenti nei confronti del personale che ha commesso, con dolo o colpa grave, una violazione della sicurezza delle informazioni anche personali (data breach e/o incidente di sicurezza), della normativa comunitaria e nazionale sulla protezione dei dati personali ovvero di qualsivoglia altra normativa applicabile.
b. È stata predisposta una politica che mira a disciplinare, in modo compiuto, l'ipotesi di cessazione ovvero di variazione di responsabilità, durante il rapporto di lavoro o di collaborazione, di un soggetto autorizzato al trattamento[3].
c. I dati personali, oggetto di trattamento, devono essere archiviati mediante l'utilizzo di misure idonee a proteggerli da accessi non autorizzati, alterazioni, danni o distruzioni. Inoltre, il Responsabile del trattamento è tenuto a far sì che tutto il personale (e i collaboratori, ove opportuno) è tenuto a restituire gli asset utilizzati ed in loro possesso, al termine del periodo di impiego o del contratto stipulato, fatti salvi differenti e specifici accordi.
d. Viene implementato un sistema di autorizzazione dei profili di accesso[4], in base a ruoli e responsabilità (RBAC: Role Based Access Control): i) i profili di autorizzazione devono essere definiti e configurati dall'inizio del trattamento in modo da consentire l'accesso ai dati strettamente necessari (principio del "need to know"/"least privilege")[5]; ii) i profili di autorizzazione devono essere revisionati con cadenza periodica grazie ad un'apposita politica di accessi e di autorizzazione, da aggiornare sulla base dei requisiti di business ovvero di sicurezza delle informazioni (es. processo formale di registrazione e di de-registrazione per abilitare l'assegnazione dei diritti di accesso; processo formale per l'assegnazione o la revoca dei diritti di accesso per le utenze e i sistemi e/o servizi; limitazione e controllo dell'assegnazione e uso dei diritti di accesso privilegiato; rimozione dei diritti di accesso al momento della cessazione del rapporto di lavoro/di collaborazione ovvero adozione, modifica, integrazione o revisione ad ogni variazione[6]); iii) i compiti e le aree di responsabilità in conflitto tra loro devono essere oggetto di

[1] Tali misure possono, tuttavia, essere soggette ad una revisione (o meglio, una integrazione), tenuto conto della natura, della portata, del contesto e delle finalità delle attività di trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche interessate.

[2] È necessario sensibilizzare e rendere consapevoli dei rischi tutti gli operatori che possono accedere ai dati o ad altre risorse attraverso l'uso dei vari dispositivi; in modo particolare, alcuni utenti come gli amministratori di sistema oppure i dirigenti, cioè utenti con privilegi più elevati, devono comprendere l'importanza, i rischi e le responsabilità che derivano dal loro ruolo. È di fondamentale importanza sviluppare una corretta cultura della sicurezza in tutto il personale, indipendentemente dalle sue responsabilità, per poi considerare, con particolare attenzione, i ruoli critici; tutti devono avere una consapevolezza dei rischi e della propria capacità di prevenire incidenti di sicurezza (e/o data breach) e/o di gestirli e delle insidie che sia la quotidianità sia gli eventi fuori dall'ordinario possono generare. La formazione deve essere appropriatamente progettata in base ai ruoli e alle competenze pregresse del personale, su argomenti diversificati e identificati al bisogno.

[3] Le responsabilità e i doveri di sicurezza delle informazioni che rimangono validi dopo la cessazione o il cambio di impiego devono essere definiti, comunicati al relativo personale dipendente o al contraente, e fatti rispettare. I cambiamenti di responsabilità o di impiego dovrebbero essere gestiti come la cessazione delle responsabilità o dell'impiego attuale combinata con l'inizio di una nuova responsabilità o dell'impiego.

[4] I controlli d'accesso sono sia logici che fisici, e questi dovrebbero essere considerati insieme. Tale politica dovrebbe tener conto, inter alia, dei seguenti elementi: requisiti di sicurezza delle applicazioni aziendali; politiche per la diffusione e l'autorizzazione delle informazioni, per esempio il principio della necessità di sapere e i livelli di sicurezza delle informazioni e la loro classificazione; segregazione dei ruoli di controllo dell'accesso; requisiti per l'autorizzazione formale delle richieste di accesso, per la revisione periodica e la rimozione dei diritti di accesso; ruoli con accesso privilegiato.

[5] Le credenziali di accesso devono essere individuali per gli "user" e devono rispettare il principio di segregazione delle funzioni.

[6] Le identità digitali e le credenziali di accesso agli "user", i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza.

separazione, al fine di ridurre la possibilità di uso improprio, modifica non autorizzata o non intenzionale dei dati personali[7].

e. L'accesso ai sistemi e alle applicazioni viene controllato da procedure di log-in sicure.

f. I sistemi di gestione delle password devono essere interattivi, devono assicurare che le stesse siano di qualità (dunque siano adeguatamente complesse), e che siano opportunamente conservate e protette da accessi o utilizzi ad opera di soggetti non autorizzati.
   A tal fine, il Responsabile del trattamento deve assicurare la sussistenza dei seguenti requisiti:
   - ✓ richiesta, in via automatica, di aggiornamento periodico della password (non oltre 90 giorni) nei confronti di tutti i soggetti autorizzati al trattamento;
   - ✓ segretezza della password, la quale deve possedere, a tal fine, le seguenti caratteristiche minime:
     i. deve contenere almeno 15/12 caratteri ovvero, nel caso in cui lo strumento elettronico non lo permetta, un numero di caratteri pari al massimo consentito[8];
     ii. deve contenere lettere minuscole e maiuscole, combinate con cifre o caratteri speciali;
     iii. non deve contenere l'ID dell'utente, o comunque elemento agevolmente riconducibile a quest'ultimo;
     iv. deve essere modificata autonomamente ed obbligatoriamente dal soggetto autorizzato al primo collegamento, dopo l'eventuale re-impostazione, nel rispetto della cadenza temporale sopra descritta, nonché nel rispetto del criterio "password history" (ossia, impossibilità di riutilizzare, a breve distanza di tempo, le credenziali già precedentemente utilizzate);
     v. ove possibile, deve essere costituita dalla cd. "passphrase" (ossia, una raccolta di parole comuni casuali combinate in una frase che fornisca un'ottima combinazione di memorizzazione e sicurezza) ovvero a multi-fattori o strong authentication (MFA) (es. token; dato biometrico; informazione personale e riservata; OTP)[9].
   - ✓ la password deve essere conservata in modo sicuro, evitando la proliferazione di documenti non protetti contenenti liste di credenziali o appunti facilmente accessibili da chiunque;
   - ✓ le credenziali di autenticazione, collegate alla relativa password, devono essere disattivate se non utilizzate, in modo totale, da almeno 6 mesi o 1 anno, a seconda delle specifiche circostanze (e ad eccezione di quelle esplicitamente autorizzate)[10];
   - ✓ la password deve essere tutelata mediante impostazioni idonee a contrastare efficacemente attacchi informatici di tipo "brute force" sul sistema di autenticazione online, anche introducendo limitazioni al numero di tentativi infruttuosi di autenticazione (rate limiting)[11].

g. Viene attuata la protezione delle credenziali di autenticazione con efficaci misure di sicurezza crittografiche[12].

h. Viene assicurata la sicurezza fisica agli uffici, locali ed impianti che racchiudono dati personali, ivi inclusa la protezione da incidenti ovvero attacchi malevoli ("controllo di accesso fisico")[13].

---

[7] L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate.

[8] Cfr. punto n. 5) dell'abrogato Allegato B) del previgente Codice Privacy: "La parola chiave, quando è prevista dal sistema di autenticazione, è 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…".

[9] Cfr., in via analogica, art. 1 comma 1) lettera q-bis) del Decreto Legislativo n. 11 del 17.1.2010: "autenticazione forte del cliente": "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione" (cfr. sul punto anche: Considerando n. 6) del Regolamento UE n. 389/2018 del 27.11.2017).

[10] Cfr., sul punto, l'abrogato Allegato B) (denominato "Disciplinare tecnico in materia di misure minime di sicurezza") del previgente D.Lgs. n. 196/2003 (Codice Privacy).

[11] Il "rate limiting" è una misura di sicurezza tecnica che comporta una limitazione al numero di tentativi infruttuosi di autenticazione costituendo un'efficace protezione dagli attacchi di "denial of service" (DDOS), dai tentativi di violazione delle password con metodi "brute force" e da altri comportamenti illegali: di conseguenza, tale misura provvede a limitare o rallentare la disponibilità di una procedura di login, qualora si verifica una quantità anomala di tentativi di accesso non andati a buon fine in un intervallo di tempo relativamente ristretto, procedendo, quindi, a bloccare temporaneamente i login per l'account sotto attacco; tale misura potrebbe, altresì, prevedere un incremento delle tempistiche di blocco, qualora si riscontrassero nuovi tentativi di accesso falliti dopo lo sblocco dell'account, preferibilmente per non più di un paio d'ore, al fine di non impedire l'accesso al servizio.

[12] In merito, è opportuno che una politica sull'uso, la protezione e la durata delle chiavi crittografiche dovrebbe essere sviluppata e implementata attraverso il loro intero ciclo di vita.

i. Le apparecchiature devono essere disposte e protette al fine di ridurre i rischi derivanti dalle minacce (ivi incluso, il malfunzionamento alla rete elettrica di alimentazione) e/o da accesso non autorizzato (interno o esterno), e le stesse devono essere, altresì, correttamente manutenute.
j. I supporti fisici, al cui interno sono archiviati dati personali, devono essere protetti da idonee misure di sicurezza contro accessi non autorizzati, utilizzi impropri ovvero manomissioni[14]; inoltre, il personale dipendente e, ove opportuno, i collaboratori devono assicurare che le apparecchiature lasciate incustodite siano, comunque, adeguatamente protette.
k. Viene adottata una politica di "scrivania pulita" (clear desk) per i documenti e i supporti di memorizzazione rimovibili (es. pendrive USB), e una politica di "schermo pulito" (clear screen) per i servizi di elaborazione delle informazioni[15].
l. Vengono controllati i cambiamenti all'interno dell'organizzazione, dei processi di business, alle strutture di elaborazione delle informazioni e ai sistemi che influenzano la sicurezza delle informazioni ("gestione del cambiamento")[16].
m. E' stata predisposta una politica volta alla protezione dei dati da qualsivoglia software dannoso (virus/malware/ransomware[17]), da accessi remoti da rete pubblica da parte di sistemi non autorizzati, nonché è stato predisposto un sistema di protezione delle postazioni terminali (endpoint protection systems – EPS): i) i programmi di protezione anti virus e anti malware devono essere continuamente aggiornati; ii) gli aggiornamenti delle patch di sicurezza e le correzioni per le vulnerabilità di sistema note devono essere prontamente implementate; iii) i sistemi perimetrali, quali firewall[18], devono essere presenti, aggiornati, mantenuti, ben configurati e rivisti periodicamente.

[13] L'accesso fisico alle risorse deve essere protetto ed amministrato. Nello specifico, le relative linee guida dovrebbero prevedere, inter alia, le seguenti prescrizioni: i perimetri di sicurezza dovrebbero essere definiti, e l'ubicazione e la forza di ogni perimetro dovrebbe dipendere dai requisiti di sicurezza degli asset all'interno del perimetro e dai risultati di una valutazione dei rischi; i perimetri di un edificio o di un sito contenente strutture per l'elaborazione delle informazioni dovrebbero essere fisicamente solidi e custoditi; un'area di accoglienza presidiata o altri mezzi per controllare l'accesso fisico al sito o all'edificio dovrebbe essere in atto, e limitato solo al personale autorizzato; adeguati sistemi di rilevamento delle intrusioni dovrebbero essere installati.

[14] La documentazione deve essere custodita in un locale idoneo, appositamente individuato, che presenti un perimetro chiaramente delimitato e sia dotato di misure di protezione minime tali da consentire l'accesso alle sole persone autorizzate, ovvero in armadi di sicurezza con procedure di tracciamento delle chiavi in uso.

[15] La politica di clear desk/clear screen dovrebbe, inter alia, considerare i seguenti aspetti: le informazioni aziendali sensibili o critiche dovrebbero essere chiuse a chiave quando non sono necessarie, specialmente quando l'ufficio è lasciato libero; i computer e i terminali dovrebbero essere lasciati scollegati o protetti con un meccanismo di blocco dello schermo e della tastiera controllato da una password, un token o un meccanismo simile di autenticazione dell'utente quando non sono sorvegliati, e dovrebbero essere protetti da password o altri controlli quando non sono in uso. Una politica di clear desk/clear screen riduce i rischi di accesso non autorizzato, perdita e danno alle informazioni durante e al di fuori del normale orario di lavoro; invece, casseforti o altre forme di archiviazione sicura potrebbero anche proteggere le informazioni ivi conservate da disastri come un incendio, un terremoto, un'inondazione o un'esplosione.

[16] I cambiamenti nell'organizzazione, nei processi di business, nelle strutture di elaborazione delle informazioni e nei sistemi che influiscono sulla sicurezza delle informazioni devono essere controllati. In particolare, devono essere considerati i seguenti elementi: identificazione e registrazione dei cambiamenti significativi; valutazione degli impatti potenziali, compresi gli impatti sulla sicurezza delle informazioni anche personali, di tali cambiamenti; verifica che i requisiti di sicurezza delle informazioni siano stati soddisfatti; comunicazione dei dettagli del cambiamento a tutte le persone interessate; procedure di fall back.

[17] Si definisce "malware" qualsiasi software che, una volta eseguito su un sistema informatico, possa apportare modifiche indesiderate o danni al sistema stesso e ai suoi utenti; i malware possono effettuare le azioni più diverse sul sistema "vittima", quali ad esempio: possono sottrarre le informazioni memorizzate, danneggiarle o modificarle in maniera ponderata; catturare schermate del dispositivo "vittima" violando la privacy dei suoi utenti; rubare le credenziali degli utenti che usano il sistema. Invece, i "ransomware" rappresentano una tipologia specifica di malware il cui obiettivo è quello di impedire alla vittima l'accesso e l'uso di documenti e dispositivi.
La politica contro il malware dovrebbe essere basata sul software di rilevamento e riparazione del malware, sulla consapevolezza della sicurezza delle informazioni e su controlli appropriati dell'accesso al sistema e della gestione dei cambiamenti. La relativa guida dovrebbe almeno: stabilire una politica formale che proibisca l'uso di software non autorizzato; implementazione di controlli che impediscano o rilevino l'uso di un software non autorizzato; implementare controlli che impediscano o rilevino l'uso di siti web maligni noti o sospetti; condurre revisioni regolari del contenuto del software e dei dati dei sistemi che supportano i processi aziendali critici: la presenza di qualsiasi file non approvato o modifiche non autorizzate dovrebbe essere formalmente indagata.

[18] Il "firewall" è un componente che si interpone tra due reti, e permette di imporre regole sul transito di informazioni tra queste.

n. E' stata predisposta una procedura di backup[19] (crittografato, ove possibile) volta a garantire il recupero dei dati e il ripristino dei sistemi in caso di incidenti di sicurezza, data breach, anomalie o altri eventi dannosi: i) la copia dei dati e delle configurazioni dei sistemi deve essere eseguita almeno su base giornaliera ove possibile; ii) la retention di tali copie deve essere pari ad almeno una settimana, salvo richieste differenti che potranno essere concordate nella fase contrattuale o nel corso dell'esecuzione del servizio di cui al punto 1.2.) del Contratto; iii) le copie dei dati devono essere protette da accessi non autorizzati e conservate in un luogo sicuro, preferibilmente offline; iv) deve essere garantita l'integrità delle copie dei dati e il funzionamento delle procedure di restore da testare con regolarità.

o. Le attività degli Amministratori di Sistema (AdS)[20] vengono sottoposte ad audit log[21], conservati, protetti e riesaminati in modo periodico, nel rispetto del Provvedimento del 27.11.2008 del Garante Privacy, così come modificato in base al successivo Provvedimento del 25.6.2009.

p. Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere valutata, e appropriate misure devono essere intraprese per affrontare i rischi relativi (cd. gestione delle vulnerabilità tecniche).

q. Le reti devono essere gestite e controllate al fine di proteggere le informazioni nei sistemi informativi e nelle applicazioni software.

r. Le informazioni trasmesse attraverso messaggistica elettronica devono essere protette in modo appropriato (es. antispam; mail filter[22]).

s. È stata stabilita la responsabilità e la procedura di gestione volta ad assicurare una risposta rapida, efficace ed ordinata agli incidenti di sicurezza e/o agli incidenti relativi alla sicurezza delle informazioni personali: tali eventi devono essere segnalati il più velocemente possibile, tramite appropriati canali gestionali. A tal fine, il personale dipendente e, ove opportuno, i collaboratori che utilizzano i sistemi informativi e i servizi dell'organizzazione devono essere tenuti a registrare e a segnalare ogni punto di debolezza relativo alla sicurezza delle informazioni che sia stato osservato o sospettato nei sistemi o nei servizi.

t. I piani di ripristino (recovery plan)[23], la conoscenza acquisita dall'analisi e dalla soluzione degli incidenti costituenti la violazione di dati personali (data breach) o della sicurezza delle informazioni deve essere utilizzata per ridurre la verosimiglianza o l'impatto di incidenti futuri ("lesson learned").

u. E' stata predisposta una procedura di risposta (Incident Response e Business Continuity, nel rispetto della ISO/IEC 22301:2014) e di recupero (Incident Recovery e Disaster Recovery[24]), al fine di fronteggiare un incidente, un evento imprevisto o di forza maggiore ovvero un disastro[25]; le descritte procedure devono

---

[19] Quando si progetta un piano di back up, almeno i seguenti elementi dovrebbero essere presi in considerazione: devono essere prodotte registrazioni accurate e complete delle copie di back up e delle procedure di ripristino documentate; i back up dovrebbero essere conservati in un luogo remoto, ad una distanza sufficiente per sfuggire a qualsiasi danno di un disastro nel sito principale; le informazioni di back up dovrebbero ricevere un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati al sito principale; i supporti di back up dovrebbero essere testati regolarmente, al fine di garantire che si possa fare affidamento su di essi quando necessario; nelle situazioni in cui la riservatezza è importante, i back up dovrebbero essere protetti con mezzi di crittografia.

[20] Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate a: gestione e manutenzione di un impianto di elaborazione o di sue compenti (es. salvataggio dei dati; organizzazione dei flussi di rete; gestione dei supporti di memorizzazione; manutenzione degli hardware) (cd. AdS di una infrastruttura informatica); gestione e manutenzione di un sistema operativo; gestione e manutenzione di uno o più applicativi (es. data base; antivirus) (cd. AdS degli applicativi). Inoltre, si ricorda che, nel rispetto del citato Provvedimento del Garante Privacy italiano, gli estremi identificativi delle persone fisiche qualificate come "amministratori di sistema" devono essere riportati in un documento interno da mantenere aggiornato.

[21] Audit log: consiste nel log sulle attività svolte all'interno di uno specifico sistema/apparato informativo; esso si differenzia dall'"access log", il quale riguarda, invece, i log di entrata e di uscita da un determinato sistema informativo.

[22] È un componente che intercetta ogni mail in transito verso l'azienda, al fine di identificare e bloccare tempestivamente possibili minacce.

[23] I processi e le procedure di ripristino devono essere eseguiti e mantenuti al fine di assicurare un recupero dei sistemi o asset coinvolti da un incidente di sicurezza e/o da una violazione dei dati personali (data breach).

[24] Cfr., in via analogica, il Provvedimento n. 333 del 4.7.2013 a firma del Garante Privacy italiano: "...con il termine "disaster" si intende, ai fini del provvedimento in esame, "l'effetto di un evento improvviso che ha come impatto gravi e prolungati danni e/o perdite per l'organizzazione", laddove la nozione di DR configura invece "l'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro di elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare indisponibilità prolungate". Il DR comprende quindi le attività necessarie per ripristinare – in tutto o in parte – le funzionalità del sistema informatico inteso come complesso di strutture hardware, software e di servizi di comunicazione".

[25] A tal fine, deve sussistere un documento aggiornato di dettaglio contenente i piani di continuità operativa/disaster recovery, nonché quelli di risposta e di recupero in caso di incidenti, che comprende almeno: le politiche e i processi impiegati per

essere, altresì, verificate ad intervalli di tempo regolari, al fine così di assicurare che siano sempre valide ed efficaci durante il verificarsi di una situazione avversa, di crisi o comunque imprevista.

v. I dati personali, oggetto dell'attività di trattamento demandata dal Titolare al Responsabile, vengono distrutti, cancellati, sovrascritti o comunque resi inutilizzabili (o in alcun modo ricostruibili) in modo irreversibile, in caso di sostituzione di un hardware/software o in caso di riutilizzo, per differenti finalità di trattamento, dell'hardware/software medesimo.
w. È stato predisposto un sistema di prevenzione delle intrusioni (intrusion prevention systems[26] – IPS), da tenere aggiornato, mantenuto, ben configurato e rivisto periodicamente.
x. Viene svolto, con cadenza periodica, il monitoraggio della rete informatica al fine di rilevare potenziali eventi di cybersecurity[27].
y. Viene attuata la protezione delle comunicazioni di dati in transito (data in transit) con tecniche crittografiche allo stato dell'arte.
z. Vengono effettuate delle sessioni di vulnerability assessment e penetration test (VAPT) sui sistemi/applicativi coinvolti nell'esecuzione delle attività di trattamento di cui al Contratto, da eseguirsi con cadenza regolare e periodica, anche ad opera, ove necessario, di terze parti indipendenti.

Torino, lì ……

AZIENDA OSPEDALIERA ORDINE MAURIZIANO DI TORINO
(in persona del suo legale rappresentante pro tempore)

Dott.ssa Franca Dall'Occo

MUSEO REGIONALE DI SCIENZE NATURALI
(in persona del suo legale rappresentante pro tempore)

……

identificare le priorità degli eventi; le fasi di attuazione dei piani; i ruoli e le responsabilità del personale; i flussi di comunicazione e reportistica.

[26] È un componente che controlla in modo continuo il traffico e le attività in essere nella rete aziendale per identificare e, laddove possibile, prevenire possibili intrusioni non autorizzate.

[27] Il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali sono monitorati e correlati al fine di identificare eventi di cybersecurity.

REGIONE PIEMONTE

Direzione Cultura, Turismo, Sport e Commercio
Settore Museo Regionale di Scienze Naturali
marco.fino@regione.piemonte.it - culturcom@cert.regione.piemonte.it

Data (*)

Protocollo (*) */ A2006D*

Classificazione 2.80 F 3/2025A

Spett.le
A.O. Ordine Mauriziano
Via Magellano 1
Torino

pec
direzionesanitaria.mauriziano@pcert.postecert.it
gmarruso@mauriziano.it

* *Segnatura di protocollo riportata nei metadati di DOQUI ACTA*

OGGETTO: Museo Regionale di Scienze Naturali. Affidamento di incarico di messa a disposizione di esperto per l'attività di Radioprotezione e Sorveglianza Fisica (ai sensi dell'art. 128 del Dlgs. n. 101 del 31 luglio 2020) all'Azienda Ospedaliera Ordine Mauriziano di Torino. Stipula Convenzione tra l'A.O.O Mauriziano di Torino e il Museo Regionale di Scienze Naturali.
CIG: B76BFB31C1

Si comunica che con determinazione n. XXX/ A2000D del XX/XX/2025 è stata affidato a codesto Ente l'incarico di messa a disposizione di esperto per l'attività di Radioprotezione e Sorveglianza Fisica (ai sensi dell'art. 128 del Dlgs. n. 101 del 31 luglio 2020) all'Azienda Ospedaliera Ordine Mauriziano di Torino Istituzione la fornitura dei documenti digitali in oggetto per l'importo complessivo di € **5.124,00 (o.f.c.)**

La Stazione appaltante è la Regione Piemonte, Direzione Cultura, Turismo, Sport e Commercio, Settore Museo Regionale di Scienze Naturali, Via Giolitti, 36 - 10123 Torino, tel. 011 4325616
Responsabile del procedimento: Marco Fino,
E-mail: *marco.fino@regione.piemonte.it.*

La prestazione, come meglio indicata nella Convenzione tra l'A. O. Mauriziano e il Museo Regionale di Scienze Naturali consiste nella:

1. sorveglianza fisica delle radiazioni e radioprotezione (attività di protezione dalle radiazioni ionizzanti dei lavoratori e della popolazione, gestione della dosimetria personale e ambientale, gestione radioprotezionistica dei minerali radioattivi e valutazione dei rischi relativi);

2. protezione all'Esposizione al Radon così come previsto dal Titolo IV Capo I del D.Lgs. 101/2020; 3. gestione delle pratiche che comportano l'impiego di materiali contenenti radionunclidi di origine naturale (Capo II D.Lgs. 101/2020);

4. consulenza radioprotezionistica e monitoraggio con dosimetri ambientali.

La prestazione verrà svolta sulla base di quanto previsto dalla Convenzione medesima e non oltre il 30 giugno 2026.

I pagamenti saranno disposti alle seguenti scadenze:
- rata pari al 50% dell'importo contrattuale dopo sei mesi dall'inizio della prestazione;
- rata a saldo pari al 50% dell'importo contrattuale al completamento delle prestazioni e previa presentazione di relazione sulle prestazioni eseguite, a seguito di emissione di fattura da parte dell'A.O. Ordine Mauriziano, il cui pagamento avverrà entro 30 giorni dalla data di ricevimento delle medesime e, comunque, a condizione dell'esito favorevole del parere di conformità delle attività svolte alle caratteristiche tecniche richieste e previo accertamento della regolarità contributiva ai sensi della vigente normativa.

Le fatture in formato elettronico dovranno pervenire a: Regione Piemonte, Direzione Cultura e Commercio/Settore Museo Regionale di Scienze Naturali (**codice univoco YVDPFP)**, Via Giolitti, 36 - 10123 Torino (P.IVA 02843860012 - C.F. 80087670016) corredate delle indicazioni del c/c dedicato e delle coordinate bancarie (codice Iban), ai sensi dell'art. 25 del decreto legge 66/2014, come convertito nella legge 89/2014.

Ai sensi dell'articolo 25 del D.L. n. 66/2014, convertito con legge n. 89/2014, nella fattura dovrà essere indicato, pena l'impossibilità di procedere al pagamento delle medesime, il CIG B75410FDE4 e, nella causale, gli estremi della determinazione dirigenziale di affidamento (DD n. xx/A2006D del xx/06/2025).

Il pagamento è subordinato
- all'accertamento, da parte della Stazione Appaltante della prestazione effettuata, in termini di quantità e qualità, rispetto alle prescrizioni previste nei documenti contrattuali e pertanto all'accertamento della regolare esecuzione delle prestazioni da parte del Rup del Settore Museo Regionale di Scienze Naturali. Dal corrispettivo saranno dedotti gli importi relativi alle mancate prestazioni. Dal corrispettivo saranno dedotte le eventuali penali applicate.

Specifiche dell'affidamento:
1. l'esecutore assume tutti gli obblighi di tracciabilità dei flussi finanziari di cui alla legge 13 agosto 2010, n. 136 ("Piano straordinario contro le mafie, nonché delega al Governo in materia di antimafia") e s.m.i.;
2. l'esecutore deve comunicare alla Regione Piemonte gli estremi identificativi dei conti correnti dedicati di cui all'art. 3, comma 1, della legge 136/2010, entro sette giorni dalla loro accensione o, nel caso di conti correnti già esistenti, dalla loro prima utilizzazione in operazioni finanziarie relative ad una commessa pubblica, nonché, nello stesso termine, e generalità e il codice fiscale delle persone delegate ad operare su di essi. In caso di successive variazioni, le generalità e il codice fiscale delle nuove persone delegate, così come le generalità di quelle cessate dalla delega sono comunicate entro sette giorni da quello in cui la variazione è intervenuta. Tutte le comunicazioni previste nel presente comma sono fatte mediante dichiarazione sostitutiva dell'atto di notorietà ai sensi dell'art. 21 del D.P.R. 28 dicembre 2000, n. 445;

3. la Regione Piemonte non esegue alcun pagamento all'esecutore in pendenza delle comunicazione dei dati di cui al comma precedente, di conseguenza, i termini di pagamento s'intendono sospesi;
4. la Regione Piemonte risolve la collaborazione in presenza anche di una sola transazione eseguita senza avvalersi di bonifico bancario o postale ovvero di altri strumenti idonei a consentire la piena tracciabilità delle operazioni, secondo quanto stabilito all'art. 3, comma 1, della legge 136/2010;
5. nel rispetto del Piano Triennale per la Prevenzione della Corruzione e della Trasparenza 2025-2027" approvato con DGR. n. 11-739 del 31 Gennaio 2025, in attuazione della Legge 190/2012 della Regione Piemonte, l'esecutore non deve concludere contratti di lavoro subordinato o autonomo, e non attribuire incarichi ad ex dipendenti che hanno esercitato nei loro confronti poteri autoritativi o propedeutici alle attività negoziali per conto della Regione Piemonte, nei tre anni successivi alla cessazione del rapporto di lavoro;
6. l'esecutore della fornitura si impegna a rispettare gli obblighi di condotta delineati dal Codice di comportamento dei dipendenti della Giunta regionale (pubblicato sul sito Web della Regione Piemonte, Sezione amministrazione trasparente, Disposizioni generali, Atti generali), per quanto compatibili con il servizio affidato;
7. nel rispetto del Piano Triennale per la Prevenzione della Corruzione e della Trasparenza 2025-2027 della Regione Piemonte, l'esecutore si impegna a rispettare i Protocolli di legalità o Patti di integrità previsti nella presente lettera di affidamento, con la clausola di salvaguardia che il mancato rispetto di tali protocolli/patti darà luogo alla risoluzione della collaborazione.

Per tutto quanto non espressamente previsto nella presente lettera contratto, si rinvia alle disposizioni del D. Lgs 36/2023 e s.m.i..

La presente dovrà essere restituita firmata dal Vs. legale rappresentante per accettazione delle clausole su citate.

Marco Fino
Il presente documento è sottoscritto con firma digitale ai sensi dell'art. 21 del d.lgs. 82/2005

Per accettazione
(data e firma digitale del legale rappresentante)

……