



Regione Lombardia
IL CONSIGLIO

DD N. 196

del 25/06/2025

UFFICIO CONTRATTI E ICT

DECRETO DIRIGENZIALE

Oggetto: SERVIZIO DI REALIZZAZIONE DELLO STUDIO "LA PARTECIPAZIONE POLITICA IN LOMBARDIA". AFFIDAMENTO DIRETTO, PREVIA ACQUISIZIONE DI PREVENTIVI, TRAMITE LA PIATTAFORMA DI NEGOZIAZIONE TELEMATICA SINTEL, AI SENSI DELL'ART. 50, COMMA 1, LETT. B) DEL D.LGS. N. 36/2023, ALLA SOCIETÀ IPSOS S.R.L. DI MILANO

IL DIRIGENTE

VISTA la legge regionale 7 luglio 2008, n. 20 *"Testo unico in materia di organizzazione e personale"*;

VISTO il regolamento contabile, approvato con deliberazione del Consiglio regionale 15 febbraio 2011, n. IX/143, e modificato con deliberazioni del Consiglio regionale 8 aprile 2014, n. X/356, e 28 luglio 2015, n. X/751;

RICHIAMATA la deliberazione dell'Ufficio di presidenza 11 novembre 2024, n. 386 *"III Provvedimento organizzativo Anno 2024: conferimento incarichi dirigenziali"*, che ha, tra l'altro, attribuito alla sottoscritta l'incarico triennale di dirigente dell'Ufficio Contratti e ICT, con decorrenza dal 1° gennaio 2025;

VISTO 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"*, così come modificato e integrato dal decreto legislativo 10 agosto 2014, n. 126;

RICHIAMATE:

- la deliberazione del Consiglio regionale 17 dicembre 2024, n. XII/662, di approvazione del bilancio di previsione finanziario per gli anni 2025-2026-2027 per il funzionamento del Consiglio regionale;
- la deliberazione dell'Ufficio di presidenza 18 dicembre 2024, n. 423, di approvazione del documento tecnico di accompagnamento e di assegnazione delle quote di bilancio al Segretario generale e al Datore di lavoro, per gli anni 2025-2026-2027;
- la deliberazione dell'Ufficio di presidenza del 3 febbraio 2025, n. 29, *"Piano Integrato di Attività e Organizzazione (PIAO) del Consiglio regionale della Lombardia, triennio 2025 - 2027 (anno 2025)"*;
- la deliberazione dell'Ufficio di presidenza 28 luglio 2021, n. 184 recante *"Aggiornamento 2021 dell'assetto organizzativo privacy - modifiche alla deliberazione 1 aprile 2019, n. 111 'Definizione dell'assetto organizzativo privacy - Articolazione delle competenze in materia di protezione dei dati personali (Regolamento UE 2016/679 e d.lgs. 196/2003)', come modificata dalla deliberazione 6 aprile 2020, n. 78"*, con cui è stata attribuita, tra l'altro, ai titolari di incarichi dirigenziali la competenza ad adottare gli atti di designazione del responsabile del trattamento di cui all'art. 28 Regolamento UE 2016/679 (RGPD) e di autorizzazione alla designazione di ulteriori sub responsabili del trattamento ai sensi dei paragrafi 2 e 4 dello stesso articolo, nell'ambito dei contratti pubblici per l'acquisizione di beni, servizi e forniture da loro stipulati per conto dell'Amministrazione;
- la deliberazione dell'Ufficio di Presidenza 24 marzo 2025, n. 100, *"Iniziative di studio e ricerca anno 2025: 'La partecipazione politica in Lombardia': determinazioni"*;

VISTO il decreto del Segretario generale 23 dicembre 2024, n. 543, di approvazione del bilancio finanziario gestionale per gli anni 2025-2026-2027 per il funzionamento del Consiglio regionale e di assegnazione delle quote ai dirigenti, che, per le procedure di affidamento ai sensi dell'articolo 50 del Codice e per le procedure di scelta del contraente ai sensi degli articoli 70 e ss. del Codice, nonché per le concessioni, ha individuato, di norma e fatte salve le diverse disposizioni di singoli atti, come

Responsabile unico del progetto (di seguito RUP) ai sensi dell'articolo 15 del Codice, il dirigente dell'ufficio contratti e ICT;

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"* (di seguito: Codice), entrato in vigore il 10 aprile 2023 con efficacia dal 1 luglio 2023 e, in particolare:

- l'articolo 15, comma 1, secondo cui nel primo atto di avvio dell'intervento pubblico da realizzare mediante un contratto, le stazioni appaltanti nominano un responsabile unico del progetto (di seguito RUP) per le fasi di programmazione, progettazione, affidamento e per l'esecuzione di ciascuna procedura soggetta al Codice;
- l'articolo 17, comma 2, ai sensi del quale le pubbliche amministrazioni, nell'atto con il quale adottano la decisione di contrarre per l'affidamento diretto, individuano l'oggetto, l'importo e il contraente, unitamente alle ragioni della sua scelta, ai requisiti di carattere generale e, se necessari, a quelli inerenti alla capacità economico-finanziaria e tecnico-professionale;
- l'articolo 21 che disciplina il ciclo di vita digitale dei contratti e gli articoli 25 e 26, che disciplinano le piattaforme di approvvigionamento digitale e le loro caratteristiche tecniche, ai fini della digitalizzazione del ciclo di vita dei contratti di cui al libro I, parte II del Codice;
- l'articolo 50, comma 1, lettera b), ai sensi del quale *"le stazioni appaltanti procedono all'affidamento dei contratti di servizi di importo inferiore a 140.000 euro, anche senza consultazione di più operatori economici, mediante affidamento diretto, assicurando che siano scelti soggetti in possesso di documentate esperienze pregresse idonee all'esecuzione delle prestazioni contrattuali, anche individuati tra gli iscritti in elenchi o albi istituiti dalla stazione appaltante"* e comma 4, che riferisce alle sole procedure negoziate i criteri di aggiudicazione;
- l'Allegato I.1 che definisce, all'articolo 3, comma 1, lettera d), l'affidamento diretto come *"l'affidamento del contratto senza una procedura di gara, nel quale, anche nel caso di previo interpello di più operatori economici, la scelta è operata discrezionalmente dalla stazione appaltante o dall'ente concedente, nel rispetto dei criteri qualitativi e quantitativi di cui all'articolo 50, comma 1 lettere a) e b), del codice e dei requisiti generali o speciali previsti dal medesimo codice"*;
- l'articolo 226, comma 5, secondo cui *"ogni richiamo in disposizioni legislative, regolamentari o amministrative vigenti al decreto legislativo 18 aprile 2016, n. 50, o al codice dei contratti pubblici vigente alla data di entrata in vigore del codice, si intende riferito alle corrispondenti disposizioni del codice o, in mancanza, ai principi desumibili dal codice stesso"*;

DATO ATTO che il Consiglio regionale ha la disponibilità e utilizza, ai sensi dell'art. 21 del Codice, per le proprie procedure di acquisto la piattaforma certificata di approvvigionamento digitale denominata "Sintel" di Regione Lombardia;

VISTO il decreto dirigenziale 8 febbraio 2024, n. 39, recante *"Linee guida per l'esecuzione dei controlli sulle dichiarazioni sostitutive di certificazione e di atto notorio ai sensi del D.P.R. 445/2000"*;

VISTA la richiesta di acquisizione (RDA) n. 13 pervenuta all'U.O. Contratti ed economato, tramite il sistema documentale EDMA, in data 15 aprile 2025, completa di

pareri, e le sue successive modifiche e integrazioni (agli atti), con la quale la Dirigente del Servizio Studi, Valutazione delle Politiche e Qualità della Normazione ha:

- espresso la necessità di acquisire, mediante affidamento diretto previa consultazione di più operatori economici, ai sensi dell'articolo 50, comma 1, lettera b) del Codice, il servizio di realizzazione dello studio "*La partecipazione politica in Lombardia*";
- individuato la finalità dell'affidamento nell'approfondimento del tema della partecipazione politica dei cittadini in Lombardia, anche per comprendere le ragioni dell'astensione dal voto, avvalendosi di apporti tecnici qualificati per assicurare rigore scientifico, secondo quanto previsto dalla Deliberazione dell'Ufficio di presidenza del 24 marzo 2025, n. 100, nell'ambito delle attività di studio, ricerca e sostegno informativo promosse per supportare i processi decisionali e le funzioni degli organi consiliari;
- precisato le modalità di svolgimento del servizio e i relativi obblighi in capo al Fornitore;
- indicato, con riferimento ai requisiti di partecipazione degli operatori economici:
 - quale requisito di idoneità professionale, l'iscrizione nel registro della camera di commercio, industria, artigianato e agricoltura con oggetto sociale pertinente a quello di affidamento,
 - quale requisito di capacità tecnica e professionale, il possesso di documentate esperienze pregresse idonee all'esecuzione delle prestazioni contrattuali, in particolare, in una o più fra le seguenti attività: ricerca, rilevazioni demoscopiche, analisi e visualizzazione dei dati, public reporting e disseminazione/comunicazione della ricerca scientifica, maturate negli ultimi dieci anni e comprovate tramite curriculum aziendale;
- indicato la durata del contratto in dodici (12) mesi dalla stipula del contratto;
- precisato che non vi sono convenzioni o accordi quadro di ARIA S.p.A. o Consip S.p.A. attive per il servizio in oggetto;
- stimato l'importo complessivo massimo per l'affidamento in euro 31.000,00 (oltre IVA al 22%), sulla base di quanto indicato nella Deliberazione dell'Ufficio di presidenza 100/2025, dei contributi di riferimento indicati nella Convenzione tra Consiglio regionale e PoliS-Lombardia per la XII legislatura (v. Deliberazione dell'ufficio di presidenza del 23 ottobre 2023 n. 269) e di precedenti attività similari;
- individuato quattro (4) operatori economici da consultare, iscritti alla piattaforma Sintel, in possesso di una o più delle seguenti caratteristiche rilevanti per la realizzazione del servizio, nel rispetto del principio di rotazione degli affidamenti di cui all'art. 49 del Codice: i) specializzazione nell'analisi dei dati e/o nelle rilevazioni demoscopiche; ii) legami con il sistema universitario e della ricerca; iii) consuetudine di rapporti con istituzioni e pubbliche amministrazioni; iv) specializzazione nel *public reporting*, visualizzazione dei dati e disseminazione della ricerca scientifica;
- stabilito di affidare il servizio sulla base di una valutazione complessiva, che tenga conto del prezzo offerto e del progetto esecutivo, e in particolare, come poi precisato nella richiesta preventivo al punto 5 "*sulla base di un giudizio complessivo, relativo alla qualità-prezzo, che tiene conto prevalentemente della proposta tecnico-qualitativa, di cui alla documentazione tecnica, e subordinatamente del prezzo offerto*";
- individuato la copertura finanziaria per l'acquisizione della fornitura in oggetto sul bilancio finanziario gestionale per gli anni 2025-2026-2027, al capitolo 11323 "*PTSI – Spese per iniziative di studio e ricerca*", codifica di V livello del piano dei conti finanziario U.1.03.02.10.003 "*Incarichi a società di studi, ricerca e consulenza*" ;

- stabilito che il pagamento avvenga mediante pagamento posticipato in più soluzioni, come di seguito precisato;
- comunicato di assumere il ruolo di direttore dell'esecuzione del contratto e individuato quale referente operativo la responsabile della U.O. Studi e Biblioteca;

ACQUISITI AGLI ATTI:

- il parere del 14 aprile 2025, con cui l'Ufficio Trasparenza, prevenzione della corruzione e Privacy ha evidenziato che:
 - stanti le informazioni disponibili, considerato che il servizio sembra poter comportare da parte del Fornitore il trattamento di dati personali quanto meno dei soggetti partecipanti all'indagine demoscopica, il Fornitore, agendo per conto del Consiglio, deve essere nominato quale responsabile del trattamento ai sensi dell'art. 28 RGPD secondo l'atto di designazione come responsabile del trattamento predisposto di cui all'allegato D del Foglio patti e condizioni;
 - tale atto potrà essere integrato sulla base della relazione illustrativa del sistema di gestione dei dati personali da trattare e del progetto di ricerca (di seguito, "Progetto esecutivo") presentati dal Fornitore, o successivamente sulla base delle ulteriori informazioni acquisite nel corso del servizio, e dovrà essere comunque sottoscritto prima dell'inizio delle attività di trattamento da parte del Responsabile;
- il parere del 9 aprile 2025, con cui l'U.O. Prevenzione, protezione e sicurezza nei luoghi di lavoro e servizi ausiliari ha rilevato che, dalla documentazione disponibile, si evince che non sussistono rischi da interferenza con le attività svolte nella sede del Consiglio regionale e che pertanto non sussiste l'obbligo di redigere il Documento Unico di Valutazione dei Rischi da Interferenze (DUVRI), come previsto dai commi 1 e 3 dell'articolo 26 del d.lgs. 81/2008;

DATO ATTO che:

- il servizio è di natura intellettuale;
- le prestazioni non rivestono interesse transfrontaliero certo, secondo quanto previsto dall'articolo 48, comma 2, del Codice e dalla giurisprudenza in materia;

RITENUTO di acquisire il servizio in argomento ai sensi dell'articolo 50, comma 1, lett. b), mediante affidamento diretto previa richiesta di preventivi tramite la piattaforma di negoziazione telematica di Regione Lombardia Sintel;

DATO ATTO che:

- in data 14 maggio 2025, tramite la piattaforma certificata di negoziazione telematica Sintel (procedura ID 201469593), è stata trasmessa la richiesta di preventivo, da presentare entro le ore 11:00 del giorno 4 giugno 2025, ai seguenti operatori economici, individuati dalla Dirigente del Servizio Studi, Valutazione delle Politiche e Qualità della Normazione:
 - Tecne S.r.l. di Roma;
 - Excellera Intelligence di Bergamo;
 - Ipsos S.r.l. di Milano;
 - Demetra opinioni.net S.r.l. di Venezia;
- entro il suddetto termine è stato richiesto agli operatori economici interessati di presentare tramite la piattaforma Sintel, oltre alla documentazione amministrativa, come precisato più nei dettagli nella richiesta di preventivo:
 - il Progetto esecutivo, con il quale l'operatore economico, sulla base delle caratteristiche minime di cui all'articolo 2, comma 2, del Foglio Patti e

condizioni, specifica obiettivi, strategia, e informazioni utili a definire operativamente le attività di ricerca, e la Relazione illustrativa del proprio sistema di gestione dei dati personali da trattare nell'ambito del servizio, in conformità al RGPD, anche in termini di adeguatezza al rispetto delle previsioni dell'allegato D al Foglio Patti e condizioni (atto di designazione come responsabile del trattamento);

- il corrispettivo complessivo offerto per il servizio;
- entro il termine ultimo sono regolarmente pervenuti i seguenti preventivi:
 - ID Sintel 1748617550843 del 30 maggio 2025, presentato da Demetra opinioni.net S.r.l. di Venezia - codice fiscale e partita IVA 03361530276;
 - ID Sintel 1748950652909 del 3 giugno 2025, presentato da Excellera Intelligence di Bergamo - codice fiscale e partita IVA 03960280166;
 - ID Sintel 1748954468829 del 3 giugno 2025, presentato da Ipsos S.r.l. di Milano - codice fiscale e partita IVA 01702460153;

DATO ATTO altresì che la sottoscritta, in qualità di RUP ha proceduto:

- in data 5 giugno 2025, tramite la piattaforma Sintel, all'apertura della busta amministrativa, alla verifica della regolarità della documentazione e delle dichiarazioni presentate e, con il supporto della dirigente della struttura richiedente, alla valutazione dell'idoneità delle esperienze pregresse dichiarate dagli operatori economici, risultati dal curriculum aziendale,
- in data 10 giugno 2025, tramite la piattaforma Sintel, all'apertura della documentazione tecnica;

DATO ATTO che la sottoscritta e la dirigente della struttura richiedente, in data 16 giugno 2025:

- hanno proceduto alla valutazione della documentazione tecnica presentata, secondo quanto previsto nella richiesta di preventivo, e all'apertura, tramite la piattaforma Sintel, delle buste economiche, riscontrando il dettaglio dei prezzi offerti dagli operatori economici;
- hanno quindi rilevato, come risulta dal verbale dalle stesse sottoscritto in data 18 giugno 2025, che il preventivo migliore sia quello presentato da Ipsos S.r.l. di Milano, in quanto, tra l'altro:
 - il progetto esecutivo, dal punto di vista qualitativo, presenta la più completa rispondenza, formale e sostanziale, al fabbisogno dell'Amministrazione come descritto nella richiesta di preventivo e nell'allegato foglio patti e condizioni;
 - la relazione illustrativa del sistema di gestione dei dati personali è ampia, tocca diversi aspetti ed è comprensiva dell'impegno al rispetto delle regole deontologiche;
 - il prezzo offerto è congruo e conveniente per i servizi richiesti e per la qualità del progetto esecutivo proposto;

RILEVATO che, in data 19 giugno 2025, è stata comunicata, tramite la Piattaforma Sintel, la proposta di aggiudicazione provvisoria del servizio, come da verbale del 18 giugno 2025, sulla in base delle valutazioni espresse in merito alla documentazione amministrativa, alla proposta tecnica e ai prezzi offerti, all'operatore economico Ipsos S.r.l. con sede in Milano, codice fiscale e partita IVA 01702460153;

ACQUISITE AGLI ATTI le dichiarazioni sull'insussistenza di situazioni, anche potenziali, di conflitto di interesse ai sensi dell'articolo 16 del Codice, dei soggetti interessati dalla procedura (prot. n. CRL.2025.0006696, CRL.2025.0006697 e CRL.2025.0006711 del 23 aprile 2025 e CRL.2025.0008501 del 5 giugno 2025);

DATO ATTO che il Fornitore procede alla fatturazione, previo ricevimento della validazione dei prodotti di cui all'articolo 6 del Foglio patti e condizioni da parte del DEC, sulla base dell'aderenza alle prescrizioni del Foglio Patti e condizioni, al Progetto esecutivo e, eventualmente, qualora l'Amministrazione accetti le modifiche proposte ai sensi dell'articolo 5, comma 2, lettera a) del Foglio patti e condizioni, al Rapporto intermedio, e previo benestare del DEC sulla regolare esecuzione per quanto riguarda la Presentazione dei risultati di cui all'articolo 5, comma 2, lettera d) del Foglio patti e condizioni, nel modo che segue:

- il 40% a seguito della validazione del Rapporto intermedio;
- il 50% a seguito della validazione del Rapporto finale e dell'Executive Summary;
- il 10% a seguito dello svolgimento della Presentazione dei risultati;

RITENUTO pertanto:

- di affidare il servizio in oggetto, come descritto nel Foglio patti e condizioni, e nella proposta tecnica (progetto esecutivo e relazione sulla gestione dei dati personali) presentata dalla società, per la durata di dodici (12) mesi a decorrere dalla data indicata nella lettera commerciale di stipulazione del contratto, a Ipsos S.r.l. con sede in Milano, codice fiscale e partita IVA 01702460153, al corrispettivo di euro 29.900,00 (oltre IVA al 22%);
- di impegnare in favore di Ipsos S.r.l. la spesa complessiva di euro 36.478,00 (IVA al 22%) sul bilancio finanziario gestionale per gli anni 2025-2026-2027, al capitolo 11323 "*PTSI – Spese per iniziative di studio e ricerca*", codifica di V livello del piano dei conti finanziario U.1.03.02.10.003 "*Incarichi a società di studi, ricerca e consulenza*" così suddivisa:
 - 2025: euro 14.591,20;
 - 2026: euro 21.886,80;

DATO ATTO altresì che:

- il pagamento del corrispettivo contrattuale è soggetto alla tracciabilità dei flussi finanziari secondo quanto previsto dall'articolo 3 della Legge 136/2010;
- trattandosi di servizi di importo inferiore a euro 40.000,00, la verifica del possesso dei requisiti dichiarati in sede di presentazione dell'offerta avverrà con le modalità di cui all'articolo 52, comma 1, del Codice e del decreto dirigenziale 39/2024, sopra richiamato, e pertanto il presente provvedimento è immediatamente efficace;
- ai sensi dell'art. 18, comma 1, secondo periodo, del Codice, trattandosi di affidamento ai sensi dell'art. 50 del Codice stesso, il contratto sarà stipulato mediante corrispondenza secondo l'uso commerciale, previa acquisizione della garanzia definitiva di cui all'articolo 18 del Foglio patti e condizioni, ai sensi dell'articolo 117 del Codice;
- come disciplinato dall'Allegato I.4 del Codice, il contratto è esente dal pagamento dell'imposta di bollo;

RITENUTO, inoltre:

- di nominare Ipsos S.r.l. quale Responsabile del trattamento dei dati ai sensi dell'articolo 28 RGPD, in conformità al parere espresso dall'Ufficio trasparenza, prevenzione della corruzione e privacy), come da atto di designazione come responsabile del trattamento di cui all'allegato D del Foglio patti e condizioni integrato sulla base della relazione illustrativa del sistema di gestione dei dati personali da trattare e del Progetto esecutivo presentati dal Fornitore ("*Allegato D, integrato sulla base della relazione illustrativa del sistema di gestione dei dati da trattare e del Progetto esecutivo presentato da Ipsos S.r.l.*"), atto che

potrà essere integrato successivamente, sulla base delle ulteriori informazioni acquisite nel corso del servizio, e in tal caso sottoscritto nuovamente prima dell'inizio delle attività di trattamento da parte del Responsabile;

- di individuare, come indicato nella sopracitata RDA, il Direttore dell'Esecuzione del Contratto nel dirigente del Servizio Studi, Valutazione delle Politiche e Qualità della Normazione, competente anche per l'eventuale modifica degli impegni di spesa, per la liquidazione delle fatture nonché per lo svincolo della garanzia definitiva al termine del contratto e quale referente operativo il Responsabile della U.O. Studi e Biblioteca;

DATO ATTO che il Fornitore deve trasmettere, prima della stipulazione del contratto:

- il nominativo e il cv professionale, firmato digitalmente dal rappresentante legale dell'operatore economico, del responsabile delle attività di ricerca, ai sensi dell'articolo 5, comma 4, del Foglio patti e condizioni e del punto 6 della richiesta di preventivo;
- il nominativo dei componenti del gruppo di ricerca, proposti in sede di procedura di affidamento, e copia dei relativi curricula professionali, firmati digitalmente dal rappresentante legale dell'operatore economico;
- individuare e comunicare al DEC i riferimenti dei referenti della privacy e del responsabile della protezione dei dati (di seguito DPO), come indicato nell'articolo 17, comma 7 del Foglio patti e condizioni;
- la garanzia definitiva di cui all'articolo 19 del Foglio patti e condizioni, ai sensi dell'articolo 117 del Codice;
- la dichiarazione relativa ai flussi finanziari di cui all'articolo 16 del Foglio patti e condizioni, completa di CIG della procedura di affidamento che l'Amministrazione comunica successivamente all'operatore economico;
- il suddetto atto di nomina e disciplina dei trattamenti, come integrato, firmato digitalmente dal rappresentante legale o da soggetto munito di idonei poteri di rappresentanza;

VERIFICATA la regolarità dell'istruttoria e della proposta di decreto, sia dal punto di vista tecnico sia sotto il profilo della legittimità;

ATTESTATA la rispondenza del contenuto del presente atto al principio della competenza finanziaria potenziata di cui al d.lgs. 118/2011, stante l'imputazione della spesa nell'esercizio finanziario nel quale l'obbligazione giuridica viene a scadenza;

VISTO il rapporto del Servizio Programmazione finanziaria e Risorse strumentali sulla disponibilità dei fondi e la prenotazione della spesa ai sensi dell'articolo 15 del regolamento contabile,

DECRETA

1. di affidare il servizio in oggetto, come descritto nel Foglio patti e condizioni, e nella proposta tecnica presentata dalla società, per la durata di dodici (12) mesi a decorrere dalla data indicata nella lettera commerciale di stipulazione del contratto a Ipsos S.r.l. con sede in Milano, codice fiscale e partita IVA 01702460153, al corrispettivo di euro 29.900,00 (oltre IVA al 22%);
2. di impegnare in favore di Ipsos S.r.l. la spesa complessiva di euro 36.478,00 (IVA al 22%) sul bilancio finanziario gestionale per gli anni 2025-2026-2027, al capitolo 11323 "*PTSI – Spese per iniziative di studio e ricerca*", codifica di V

livello del piano dei conti finanziario U.1.03.02.10.003 *"Incarichi a società di studi, ricerca e consulenza"* così suddivisa:

- 2025: euro 14.591,20;
- 2026: euro 21.886,80;

3. di annettere al presente decreto, quale parte integrante, il Foglio patti e condizioni e allegati, disciplinante il servizio, approvato dalla sottoscritta, in qualità di responsabile unico del progetto mediante sottoscrizione digitale e accettato dal Fornitore in sede di presentazione del preventivo;
4. di nominare la società Ipsos S.r.l. quale Responsabile del trattamento dei dati ai sensi dell'articolo 28 RGPD, come da atto di designazione come responsabile del trattamento di cui all'allegato D del Foglio patti e condizioni, integrato sulla base della relazione illustrativa del sistema di gestione dei dati personali da trattare e del Progetto esecutivo presentati dal Fornitore (*"Allegato D, integrato sulla base della relazione illustrativa del sistema di gestione dei dati da trattare e del Progetto esecutivo presentato da Ipsos S.r.l."*), atto che potrà essere integrato successivamente, sulla base delle ulteriori informazioni acquisite nel corso del servizio, e in tal caso sottoscritto nuovamente prima dell'inizio delle attività di trattamento da parte del Responsabile;
5. di trasmettere al Fornitore l'atto di designazione come responsabile del trattamento di cui all'allegato D del Foglio patti e condizioni integrato di cui al punto precedente (*"Allegato D, integrato sulla base della relazione illustrativa del sistema di gestione dei dati da trattare e del Progetto esecutivo presentato da Ipsos S.r.l."*), per la relativa sottoscrizione;
6. di individuare quale Direttore dell'Esecuzione del Contratto competente, anche per le attività di cui in premessa, il dirigente del Servizio Studi, Valutazione delle Politiche e Qualità della Normazione e quale referente operativo il Responsabile della U.O. Studi e Biblioteca;
7. di stipulare il contratto, ai sensi dell'articolo 18, comma 1, del Codice, mediante corrispondenza secondo l'uso commerciale, stante l'immediata efficacia del presente decreto, previa acquisizione della garanzia definitiva di cui all'articolo 19 del Foglio patti e condizioni, nonché dell'ulteriore documentazione citata nelle premesse;
8. di sottoporre il contratto alla condizione risolutiva del successivo accertamento negativo dei controlli sul possesso dei requisiti dichiarati, ferme le ulteriori conseguenze ai sensi dell'articolo 52, comma 2, del Codice.

MARA GARGATAGLI

Documento sottoscritto digitalmente, ai sensi dell'articolo 24
del d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale)

Allegato D, integrato sulla base della relazione illustrativa del sistema di gestione dei dati da trattare e del Progetto esecutivo presentato da Ipsos S.r.l.

Atto di designazione come responsabile del trattamento dei dati personali e individuazione dei trattamenti consentiti, delle finalità, della tipologia dei dati personali e dei compiti del responsabile del trattamento, ai sensi dell'art. 28 del Regolamento UE 2016/679 del 27 aprile 2016, per la realizzazione dello studio 'La partecipazione politica in Lombardia'.

PREMESSA

Ai fini del presente Atto, s'intende per:

- **Titolare del trattamento**, ai sensi dell'articolo 4, n. 7, RGPD, il Consiglio regionale della Lombardia [di seguito denominato anche "Consiglio regionale" o "Titolare del trattamento"], C.F. 80053570158, nella persona del dirigente pro tempore dell'Ufficio Contratti e ICT, domiciliato per la carica presso la sede del Consiglio regionale della Lombardia in Milano, via Fabio Filzi n. 22, in conformità alla deliberazione dell'Ufficio di presidenza 1 aprile 2019, n. 111 (Definizione dell'assetto organizzativo privacy – Articolazione delle competenze in materia di protezione in materia di protezione di dati personali (Regolamento (UE) 2016/679 e d.lgs. 2003 come modificato dal d.lgs. 101/2018) e alla deliberazione dell'Ufficio di Presidenza 28 luglio 2021, n. 184 (Aggiornamento 2021 dell'assetto organizzativo privacy) e ss.mm.ii;
- **Responsabile del trattamento**, ai sensi dell'articolo 4, n. 8, RGPD, è il Fornitore, aggiudicatario del servizio, in persona del proprio Legale Rappresentante pro tempore, domiciliato presso la società che rappresenta;
- **Normativa privacy**, 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 e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), di seguito denominato RGPD, il d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, [di seguito denominato: Codice Privacy] e ogni altra disposizione di contenuto normativo sulla protezione dei dati personali applicabile sul territorio nazionale, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali;
- "sub-responsabile del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, soggetto terzo, al quale il Responsabile del trattamento abbia affidato l'esecuzione di specifiche attività di trattamento ai sensi dell'art. 28, paragrafi 2 e 4, RGPD;
- "affidamento", il Foglio Patti e condizioni/contratto definito nel decreto di aggiudicazione e/o in ogni altro atto contrattuale tra il Consiglio regionale e il Fornitore;
- per le altre definizioni si rinvia all'art. 4 RGPD.

Il presente atto è stato predisposto al fine di specificare, ai sensi dell'art. 28 del Regolamento (UE) 2016/679, i trattamenti di dati personali affidati dal Consiglio regionale al Fornitore definendo la

durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi gravanti sul Titolare e sul Responsabile del trattamento.

Il **Titolare del trattamento** e il **Responsabile del trattamento** dichiarano reciprocamente di essere informati e di acconsentire che i dati personali forniti o raccolti in conseguenza dell'affidamento sono trattati esclusivamente per le finalità ivi indicate ed in conformità a quanto previsto dalla vigente normativa in materia di protezione dei dati personali.

A tal fine il **Responsabile del trattamento** è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto dell'affidamento e si impegna ad effettuare, per conto del Titolare del trattamento, le sole operazioni di trattamento necessarie a tal fine, nei limiti delle finalità ivi specificate, nel rispetto della Normativa privacy e delle istruzioni fornite, come definitivi nell'Allegato A.1.

Le premesse e gli allegati **A.1** (Elenco dei trattamenti dei dati personali di titolarità del Consiglio regionale della Lombardia effettuati dal Fornitore in qualità di Responsabile del trattamento) e **A.2** (Elenco delle misure di sicurezza applicate dal Fornitore) costituiscono parte integrante e sostanziale del presente Atto.

Rimangono valide le prescrizioni e gli obblighi, anche relativi alle misure di sicurezza applicate, definiti nell'affidamento richiamato in premessa e negli eventuali altri atti allegati allo stesso, nonché in eventuali altri atti successivi stipulati tra le parti.

I dati economici, finanziari, patrimoniali o di qualunque altro genere, che vengano a conoscenza del Fornitore, in ragione dei servizi resi per il Consiglio regionale, sono riservati. Il Consiglio regionale s'impegna a trattare, in conformità al Codice privacy e al RGPD, i dati personali conferiti dal Fornitore per le sole finalità di definizione e gestione del servizio e dei relativi pagamenti, provvedendo alle comunicazioni e alle pubblicazioni dei dati relativi all'affidamento secondo quanto previsto dal d.lgs. 36/2023, dal d.lgs. 33/2013 e dalle altre norme in materia.

BASE GIURIDICA E PRINCIPI

Il trattamento di dati personali è effettuato in quanto indispensabile per il perseguimento delle finalità di ricerca connesse al progetto di cui all'Affidamento. La base giuridica del trattamento è il consenso dei partecipanti alla ricerca e l'esecuzione di un compito di interesse pubblico (art. 6, lett. a) ed e) RGPD).

Il trattamento dei dati personali nell'ambito dell'Affidamento deve essere effettuato in stretta aderenza ai principi di liceità, pertinenza, minimizzazione dei dati e limitazione della conservazione di cui all'art. 5 RGPD, in maniera da garantire un'adeguata sicurezza e da impedire eventuali trattamenti non autorizzati, la perdita o la modificazione accidentale dei dati stessi.

Il trattamento si conforma altresì alle disposizioni specifiche relative al trattamento per finalità di ricerca scientifica e in particolare all'art. 89 del RGPD, agli articoli 104 e seguenti del Codice Privacy e alle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018" (G.U. n. 11 del 14 gennaio 2019), denominate di seguito Regole deontologiche.

DURATA

La designazione a **Responsabile del trattamento** e le clausole del presente Atto hanno durata pari a quella dell’Affidamento.

La designazione e il presente Atto cesseranno automaticamente di avere efficacia in ipotesi di risoluzione, recesso o perdita di efficacia dell’Affidamento, salvo il tempo eventualmente necessario a consentire al Consiglio regionale di recuperare i dati personali, come contrattualmente definito. Parimenti, in caso di rinnovo, proroga e differimento a ogni titolo della durata dell’Affidamento, la designazione e il presente Atto continueranno a produrre i propri effetti senza necessità di ulteriori atti delle parti.

Il **Responsabile del trattamento** s’impegna a mantenere riservati i dati e le informazioni personali conosciute in ragione dei servizi resi e della presente designazione, anche dopo la cessazione di efficacia del presente Atto.

OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

Con riguardo alle tipologie di dati personali e categorie di interessati indicati nell’allegato A.1 del presente Atto, il Consiglio regionale verifica e garantisce, per quanto di competenza in qualità di Titolare del trattamento, la liceità del trattamento e il rispetto dei principi applicabili al trattamento di dati personali, ai sensi della Normativa Privacy, delle norme dello Statuto della Regione Lombardia, del Regolamento generale del Consiglio regionale e delle disposizioni della legge regionale e della legge statale applicabili alle diverse fattispecie e della deliberazione del Consiglio regionale 6 maggio 2014, n. X/378 (Regolamento per il trattamento dei dati personali sensibili e giudiziari di cui è Titolare il Consiglio Regionale della Lombardia (pubblicato sul BURL n. 20 serie ordinaria del 15 maggio 2014).

Il **Titolare del trattamento** s’impegna a fare un uso appropriato dei servizi forniti dal **Responsabile del trattamento** per garantire un livello di sicurezza adeguato e fare un uso responsabile delle credenziali, dei sistemi e dei dispositivi utilizzati per accedere ai servizi forniti dal **Responsabile del trattamento**.

Il **Titolare del trattamento** s’impegna a rispettare i termini per le comunicazioni, le autorizzazioni e le richieste di informazioni e di attivazione dei poteri di verifica di cui al presente Atto.

OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

Il **Responsabile del trattamento** dichiara di avere una struttura e un’organizzazione adeguata all’esecuzione dell’incarico di trattamento dei dati personali del Titolare del trattamento e s’impegna a mantenerla adeguata alla rilevanza dell’incarico stesso, garantendo il pieno rispetto per sé e per i propri dipendenti e collaboratori a qualunque titolo della Normativa Privacy e di quanto prescritto nel presente Atto.

Il **Responsabile del trattamento** esegue esclusivamente i trattamenti di cui all’Allegato A.1, richiesti dal Titolare del trattamento e indispensabili per l’esecuzione delle prestazioni contrattuali in modo lecito e secondo correttezza, per scopi legittimi e determinati assicurando l’esattezza e la

completezza dei dati e garantendo il rispetto dei principi di necessità, proporzionalità, pertinenza e non eccedenza, e garantisce lo svolgimento dei compiti sotto indicati.

In particolare, il **Responsabile del trattamento** tratterà dati personali per la realizzazione di uno studio sulla partecipazione politica finalizzato ad analizzare le dinamiche della partecipazione al voto dei cittadini della Lombardia e le ragioni dell'astensione, anche mediante una rilevazione demoscopica che fornisca informazioni statisticamente significative, indagando le caratteristiche sociodemografiche dell'elettorato lombardo partecipante e non partecipante al voto, le ragioni dell'astensione dalla partecipazione, il rapporto con le istituzioni, la politica e le relative priorità.

Il **Responsabile del trattamento** si impegna a specificare in apposito progetto di ricerca la tipologia di dati personali trattati, le categorie di interessati, le fonti di acquisizione, garantendo la liceità dell'acquisizione dei dati stessi, nonché le misure di sicurezza applicate al trattamento.

Con riguardo ai dati personali e alle categorie di interessati indicati nell'allegato A.1. e raccolti direttamente dal **Responsabile del trattamento**, lo stesso verifica e garantisce, per quanto di competenza in qualità di **Responsabile del trattamento**, la liceità del trattamento e il rispetto dei principi applicabili al trattamento di dati personali, nonché delle **Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 del 19 dicembre 2018 pubblicate sulla G.U n. 11 del 14 gennaio 2019.**

Il **Responsabile del trattamento** provvede direttamente agli adempimenti privacy, compresa la redazione e consegna, previo accordo con il Titolare del trattamento, agli interessati delle informazioni di cui agli artt. 13 e 14 RGPD e delle dichiarazioni liberatorie anche per il rispetto delle previsioni in materia di diritto di cui alla l. 22 aprile 1941, n. 633, qualora necessarie, e all'acquisizione del consenso al trattamento dei dati personali.

Il **Responsabile del trattamento** può acquisire ed utilizzare, ai fini della ricerca, ulteriori dati rispetto ai dati di cui sopra, anche mediante la somministrazione di interviste (telefoniche o meno), questionari, survey e media diaries, previa acquisizione del consenso, e autorizzazione scritta del Titolare del trattamento, che costituirà un'integrazione del presente Atto.

I dati personali non devono essere oggetto di comunicazione e diffusione né di trasferimento su sistemi di soggetti terzi. Il rapporto finale della ricerca deve contenere esclusivamente dati in forma anonima e aggregata, in stretta applicazione dei criteri di minimizzazione del rischio di re-identificazione degli interessati, secondo quanto definito nelle Regole deontologiche e in considerazione di quanto espresso dal EDPB e dal gruppo di lavoro europeo Art. 29 sulle tecniche di anonimizzazione e pseudonimizzazione.

Il **Responsabile del trattamento** si attiene alle istruzioni del Titolare, tra cui rientrano anche le prescrizioni di cui al provvedimento recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni" di cui alla circolare del 18 aprile 2017, n. 2/2017, recante "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»" e, in quanto compatibili, le Linee guida sulla sicurezza nel procurement ICT (Determinazione n. 220/2020 del 17 maggio 2020 Agid), ai provvedimenti di ACN (ad es. in materia di infrastrutture e servizi cloud per le PPAA, Linee guida per la conservazione delle password, atti regolamentari della disciplina cyber).

Il **Responsabile del trattamento** deve adottare tutte le misure di sicurezza appropriate per garantire il rispetto delle citate regole deontologiche, nonché della normativa in materia di protezione dei dati personali. A tal fine è tenuto a presentare un progetto di ricerca, redatto conformemente agli standard metodologici del pertinente settore disciplinare, anche al fine di documentare che il trattamento sia effettuato per idonei ed effettivi scopi statistici o scientifici, in cui siano indicate le misure di sicurezza.

Il **Responsabile del trattamento** è autorizzato a svolgere le attività di trattamento indispensabili per lo svolgimento del servizio affidato, come descritto nell’Affidamento o concordate con il **Titolare** con altro valido atto scritto, attenendosi alla Normativa Privacy e rispettando gli obblighi di cui al presente Atto e alle istruzioni impartite dal Titolare del trattamento, in modo lecito e secondo correttezza, per scopi legittimi e determinati assicurando l’esattezza e la completezza dei dati e garantendo il rispetto dei principi di necessità, proporzionalità, pertinenza e non eccedenza.

Senza specifica autorizzazione del Titolare, il **Responsabile del trattamento** non può effettuare trattamenti di dati personali ulteriori e comunque non finalizzati all’adempimento delle prestazioni contrattuali o di obblighi di legge connessi alle prestazioni contrattuali stesse.

Il **Responsabile del trattamento** non è autorizzato a effettuare copie permanenti dei dati personali, se non su espressa autorizzazione scritta del **Titolare del trattamento** e deve in ogni caso conservare i dati personali temporaneamente acquisiti, solo per il tempo strettamente necessario alle esigenze e agli adempimenti contrattuali con il Consiglio regionale e agli altri obblighi di legge, se previsti; tali dati devono essere cancellati con modalità che ne garantiscano la certa non recuperabilità, documentando per iscritto le operazioni a tal fine eseguite entro tre mesi dalla conclusione dell’affidamento, salvo diversa richiesta del Titolare. I dati personali trattati per l’attività di ricerca verranno consegnati al Consiglio regionale previamente anonimizzati.

Le operazioni di cancellazione sicura e a norma dei dati dai supporti, sistemi e reti del **Responsabile del trattamento** devono essere documentate e in merito dell’avvenuta effettuazione e conclusione positiva delle stesse il Responsabile del trattamento deve rilasciare apposita dichiarazione ai sensi del D.P.R. 445/2000.

Il **Titolare del trattamento** può autorizzare il **Responsabile del trattamento** a copiare, duplicare, riprodurre o registrare i dati indispensabili per l’esecuzione dell’attività affidata, solo per il tempo strettamente necessario allo svolgimento della stessa e mettendo in atto le necessarie precauzioni da concordare con il Titolare del trattamento per la trasmissione/trasferimento e ogni misura di sicurezza necessaria a garantire la riservatezza dei dati tenendo conto dei rischi correlati e della natura anche sensibile dei dati stessi. In ogni caso, il **Responsabile del trattamento** garantisce che la trasmissione/trasferimento dei dati avvenga su canali sicuri o in forma criptata (per esempio, HTTPS e SSH v2; file criptati con password comunicata con altro canale), salvo che sia diversamente richiesto e autorizzato dal Titolare del trattamento.

Salvo con riguardo ai dati e ai documenti resi pubblici dal Titolare del trattamento o che siano tali per natura (per esempio provvedimenti normativi), è fatto assoluto divieto al **Responsabile del trattamento** di diffondere i dati e di comunicarli a terzi, senza previa, espressa e scritta autorizzazione del Titolare del trattamento.

Il **Responsabile del trattamento** non è autorizzato a comunicare a terzi, pubblicare, cedere, donare o altrimenti disporre dei dati personali di titolarità del Consiglio regionale, senza la preventiva ed espressa richiesta o autorizzazione dell'Amministrazione consiliare, salvo non sia richiesto da disposizioni di legge e con riguardo ai dati e ai documenti resi pubblici dal Titolare o che siano tali per natura (per esempio provvedimenti normativi).

Il **Responsabile del trattamento** informa immediatamente il **Titolare del trattamento** qualora a suo parere un'istruzione del Titolare violi la Normativa Privacy.

Personale e altri collaboratori

Il **Responsabile del trattamento** adotta le misure appropriate per garantire la conformità al presente Atto delle attività e dei comportamenti dei suoi dipendenti, altri soggetti –ricercatori, responsabili e persone autorizzate al trattamento– che fossero coinvolti nella ricerca ed eventuali appaltatori e sub-responsabili relativamente al loro ambito di prestazione. Tali soggetti devono adottare una dichiarazione di impegno a conformarsi alle regole deontologiche, al progetto di ricerca e al presente atto.

Il **Responsabile del trattamento** provvede in particolare a che gli operatori assegnati al trattamento sotto la sua autorità, compresi gli amministratori di sistema, siano autorizzati per iscritto o con modalità tracciabile agli specifici trattamenti necessari per lo svolgimento delle loro mansioni e siano adeguatamente istruiti e formati in materia di protezione dei dati personali, predisponendo e attuando un piano di formazione, nonché vincolati legalmente al rispetto degli obblighi di riservatezza di cui al presente Atto (art. 29 RGPD e art. 2-*quaterdecies* d.lgs. 196/2003) mediante la sottoscrizione di apposite dichiarazioni, le cui copie saranno messe a disposizione del Titolare del trattamento su richiesta per l'esercizio delle attività di controllo e vigilanza di propria competenza.

Il **Responsabile del trattamento** provvede altresì affinché ai dati personali accedano solo gli operatori incaricati obbligandoli a conformare il proprio comportamento alle seguenti prescrizioni: a) i dati personali possono essere utilizzati soltanto per gli scopi previsti nell'Affidamento; b) i dati personali devono essere conservati in modo da evitarne la dispersione, la sottrazione e ogni altro uso non conforme alla legge e alle istruzioni ricevute; c) i dati personali di cui si venga a conoscenza in occasione dello svolgimento della prestazione principale o di attività a essa strumentali non possono essere diffusi, né altrimenti utilizzati per interessi privati, propri o altrui; d) i comportamenti non conformi alle norme sulla protezione dei dati personali o l'eventuale smarrimento o perdita dei dati o delle credenziali di autenticazione sono immediatamente comunicati ai referenti del Titolare del trattamento. e) i dati personali sono custoditi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate; f) nel caso di comunicazioni telefoniche o vocali scambiate durante lo svolgimento delle proprie attività in merito a dati personali del Titolare i comportamenti tenuti si conformano alla necessità di garantire la riservatezza delle informazioni trattate.

Il **Responsabile del trattamento** risponde per l'esatta osservanza degli obblighi di riservatezza e per l'esatta e diligente applicazione dei compiti e delle istruzioni di cui al presente atto, da parte

dei propri dipendenti o collaboratori o altre persone fisiche impegnati, su suo incarico, nell'esecuzione delle prestazioni contrattuali.

In relazione ai soggetti incaricati al trattamento che agiscono sotto la sua autorità, il **Responsabile del trattamento** è tenuto a istruirli sulla normativa privacy e sugli obblighi di cui presente Atto, predisponendo ed attuando un piano di formazione destinato ai soggetti incaricati autorizzati al trattamento.

Sistema di autenticazione per gli incaricati del Responsabile

Il **Responsabile del trattamento** è tenuto a predisporre un sistema di autenticazione per gli applicativi/postazioni di lavoro/piattaforme telematiche e analoghi strumenti che consentono l'accesso ai dati personali del **Titolare del trattamento**, che garantisca la riservatezza.

Il **Responsabile del trattamento**, con riguardo al sistema di autenticazione, è tenuto alle seguenti misure minime:

- a) prevedere profili di autorizzazione di accesso per ogni singolo soggetto incaricato/autorizzato al trattamento o gruppo omogeneo e configurarli prima dell'inizio dei trattamenti in modo adeguato alle mansioni svolte e agli ambiti di trattamento affidati;
- b) assicurarsi che a ogni soggetto incaricato/autorizzato sia assegnata una credenziale di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione del soggetto autorizzato al trattamento associato a una parola chiave (*password*) riservata e conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e a uso esclusivo dell'incaricato/autorizzato, eventualmente associato a un codice identificativo o a una parola chiave. Non è ammessa la creazione di credenziali non nominative, salvo specifica richiesta del Titolare;
- c) prescrivere necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso a uso esclusivo del soggetto incaricato/autorizzato al trattamento;
- d) assicurare che per la componente riservata della credenziale di autenticazione siano previste adeguate misure di sicurezza;
- e) richiedere al soggetto interessato di utilizzare sempre le proprie credenziali personali mantenendole riservate, evitando di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire l'individuazione dell'autore del trattamento;
- f) assicurare che la parola chiave, quando prevista sia composta da almeno quattordici (14) caratteri misti alfanumerici; essa non deve contenere riferimenti agevolmente riconducibili all'Incaricato e deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi, ove non presente un ulteriore fattore di autenticazione oltre al codice di identificazione e alla password;
- g) assicurare che l'utenza venga bloccata dopo un numero di tentativi falliti di accesso pari a tre;

- h) assicurare un sistema di reset della password che consenta l'identificazione del richiedente;
- i) assicurare che il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri incaricati, neppure in tempi diversi e assicurare che sia operata la disattivazione delle credenziali di autenticazione o delle abilitazioni di accesso del personale in caso venga a cessare la necessità di accesso da parte del soggetto incaricato autorizzato al trattamento o intervenga un'inattività per più di tre mesi;
- j) predisporre le necessarie procedure affinché, in caso di prolungata assenza o impedimento dell'incaricato/autorizzato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, si possa comunque assicurare la disponibilità di dati o strumenti elettronici;
- k) verificare a intervalli almeno annuali le autorizzazioni in essere;
- l) implementare un sistema di autenticazione a due fattori su richiesta del Titolare in base al livello di rischio dei trattamenti di dati personali e alle prescrizioni delle norme di riferimento;
- m) adottare misure per prevenire e contrastare attacchi informatici di tipo credential stuffing (testing username/password pairs obtained from the breach of another site), brute force (testing multiple passwords from dictionary or other source against a single account) e password spraying (testing a single weak password against)

È consentita l'implementazione di ulteriori o diverse misure di sicurezza rispetto a quanto sopra solo qualora le misure garantiscano un maggior livello di sicurezza, incluso un sistema di autenticazione MFA su richiesta del Titolare.

Il **Responsabile del trattamento** adotta, per la conservazione delle password degli utenti, di adeguate tecniche crittografiche quali le funzioni di derivazione di chiavi crittografiche (Key Derivation Function) che offrono garanzie in caso di loro esfiltrazione dai sistemi informatici del Produttore (cfr. OWASP Password Storage Cheat Sheet, NIST 800-63B Digital Identity Guidelines).

Amministratori di sistema

Per quanto riguarda le attività degli amministratori di sistema svolti su infrastrutture e reti proprie il **Responsabile del trattamento** deve redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche, appositamente designate, dal Responsabile stesso, che espletano nell'ambito delle attività previste dal contratto, funzioni di Amministratori di Sistema (AdS), con la definizione delle funzioni e dell'ambito operativo a ciascuno assegnato, e garantire ogni altra misura per l'assolvimento delle prescrizioni e degli obblighi di cui al provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 sugli amministratori di sistema e successive modifiche e integrazioni.

Il **Responsabile del trattamento** garantisce l'applicazione delle misure previste dal citato Provvedimento del Garante dandone conferma scritta al Titolare su richiesta.

Misure di sicurezza tecniche e organizzative

Il **Responsabile del trattamento** deve assicurare, per le componenti di sua competenza e per tutta la durata dell’Affidamento, in ogni momento, che la sicurezza fisica e logica dei dati oggetto di trattamento sia conforme alle norme vigenti. Le misure di sicurezza adottate, ai sensi dell’art. 32 del RGPD, devono in ogni situazione uniformarsi allo “standard” di maggiore sicurezza fra le disposizioni di legge e gli elementi contrattuali e/o progettuali.

Le misure di sicurezza adottate devono in ogni situazione uniformarsi allo “standard” di maggiore sicurezza fra le disposizioni di legge e gli elementi contrattuali/progettuali indicati nell’Atto di affidamento, tra cui le misure di cui al provvedimento recante “Misure minime di sicurezza ICT per le pubbliche amministrazioni” di cui alla circolare del 18 aprile 2017, n. 2/2017, recante “Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»”, alle Linee guida sulla sicurezza nel procurement ICT (Determinazione n. 220/2020 del 17 maggio 2020 Agid) e ai provvedimenti di ACN (ad es. in materia di infrastrutture e servizi cloud per le PPAA, Linee guida per la conservazione delle password, atti regolamentari della disciplina cyber) e il Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale.

Il **Responsabile del trattamento** è tenuto a implementare e mantenere efficaci le misure tecniche e organizzative, per proteggere i dati del Titolare del trattamento da distruzione, perdita, alterazione, divulgazione o accesso non autorizzati o accidentali

Il **Responsabile del trattamento** si impegna a individuare e adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenendo conto, fra l’altro, della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche nonché della tecnologia applicabile e dei costi di attuazione. Tali misure comprendono, ove opportuno:

- i) la cifratura dei dati personali;
- ii) i mezzi che permettono di garantire la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
- iii) i mezzi che permettono di ripristinare tempestivamente la disponibilità e l’accesso ai dati personali in caso d’incidente fisico o tecnico;
- iv) una procedura (messa a disposizione del titolare su richiesta) mirata a testare, verificare e valutare regolarmente l’efficacia delle misure di sicurezza tecniche e organizzative al fine di garantire la sicurezza del trattamento.

I sistemi del **Responsabile del trattamento** devono in particolare essere dotati di misure di protezione perimetrali logico-fisiche e i sistemi software, i programmi utilizzati e la protezione antivirus devono essere costantemente aggiornati sia sui server sia sulle postazioni di lavoro. L’adeguamento alle misure minime di sicurezza implica, tra l’altro, la presenza di un adeguato sistema informatico che renda possibile:

- l’accesso ai dati tramite sistema di autenticazione;
- la protezione del computer tramite programmi contro il rischio di intrusione e l’accesso abusivo in accordo ai requisiti di legge aggiornati almeno semestralmente e comunque in occasione di ogni

versione disponibile dalla casa costruttrice, anche per i sistemi non connessi in rete o che non accedono a Internet;

- la modifica e l'aggiornamento, ogni qualvolta vi sia la disponibilità e comunque entro un congruo periodo di tempo non superiore a sei mesi, dei programmi utilizzati, o almeno alla valutazione degli impatti sull'aggiornamento.

Il **Responsabile del trattamento** adotta sistemi di back up, di continuità operative e disaster recovery e s'impegna a garantire che l'accesso in rete ai dati personali avvenga su canali sicuri o in forma criptata.

Il **Responsabile del trattamento** s'impegna a garantire l'accesso in rete ai dati personali e la comunicazione degli stessi avvenga su canali sicuri o in forma criptata (per esempio. HTTPS, SSH v2), salvo che sia diversamente richiesto e autorizzato dal **Titolare del trattamento**.

Il **Responsabile del trattamento** effettua test di penetrazione con cadenza periodica (quantomeno al rilascio di ogni major release), adotta un piano di miglioramento che analizzi le vulnerabilità emerse dai VA e PT e dai bollettini di sicurezza pubblici e di fornitori terzi e ne preveda una adeguata gestione/risoluzione, svolgendo periodicamente test di vulnerabilità sugli applicativi messi a disposizione del Titolare.

Il **Responsabile del trattamento** assicura la separazione degli ambienti di test e sviluppo rispetto ad ambienti di produzione e la previsione di misure di accesso mediante credenziali e privilegi diversi in modo da ridurre al minimo i rischi.

Il **Responsabile del trattamento** può aggiornare o modificare le misure di sicurezza garantite al momento dell'Affidamento e/o stabilite nel decreto di incarico o atto successivo a condizione che tali aggiornamenti e modifiche non comportino il degrado della sicurezza complessiva dei servizi e dei sistemi, dandone comunicazione al **Titolare del trattamento**.

Il **Responsabile del trattamento** è tenuto, in caso di modifiche e di implementazioni di nuovi servizi o di regole afferenti ai dispositivi utilizzati nell'ambito dell'incarico richiamato nelle premesse, a condividere con il **Titolare del trattamento** le informazioni che abbiano rilievo sul trattamento dei dati personali ed è tenuto, prima di procedere alla messa in uso di tali implementazioni sui dati stessi a ottenerne l'autorizzazione scritta.

Salvo l'impegno del **Responsabile del trattamento** a fornire tutte le informazioni necessarie al **Titolare del trattamento** per rispettare la Normativa Privacy, gli interventi di modifica e le innovazioni necessarie per la sicurezza dei servizi telematici che non investono la fruizione del servizio e non modificano le modalità di trattamento dei dati né la tipologia dei dati trattati, come interventi sul codice e sulla gestione tecnica della infrastruttura, non sono soggetti a preventiva autorizzazione da parte del **Titolare del trattamento**.

Nello stesso modo, non necessitano di preventiva autorizzazione gli interventi urgenti per la sicurezza e la garanzia di continuità del servizio, per i quali il **Responsabile del trattamento** si impegna a fornire successivamente le informazioni sulle modifiche effettuate al Titolare.

Il **Responsabile del trattamento** garantisce di applicare le misure minime di sicurezza individuate nell'allegato A.2. e le altre misure di sicurezza definite nell'Affidamento. Tra queste rientrano anche le misure di sicurezza definite nel progetto di ricerca.

Il **Responsabile del trattamento** deve descrivere nella relazione in cui descrive il proprio sistema di gestione dei dati personali in conformità al RGPD come le misure tecniche e di sicurezza implementate siano adeguate a garantire che il progetto di ricerca rispetti la normativa privacy, anche documentando esperienze pregresse simili.

Il Titolare, qualora ritenga che le misure ivi indicate non siano sufficienti rispetto al livello di rischio, potrà richiedere l'implementazione di ulteriori misure di sicurezza.

Il **Responsabile del trattamento** è tenuto a fornire, su richiesta del **Titolare del trattamento**, informazioni di dettaglio sulle misure di sicurezza adottate in relazione al trattamento dei dati personali, secondo quanto previsto dal presente atto e dall'art. 32 del RGDP, nonché a documentare l'adozione delle stesse e la valutazione della loro idoneità ai sensi del già menzionato articolo e, in genere, della normativa Privacy.

Il **Responsabile del trattamento** è tenuto a predisporre e mettere a disposizione la documentazione degli strumenti utilizzati per trattare i dati (indicazione del DB utilizzato, strumento di scrittura del codice, sistema di conservazione dei documenti prodotti), definendo le misure di sicurezza poste a tutela dei dati (profili di accesso al DB, crittografia del DB, dialogo tra applicazione e DB e protezione delle password, ecc.).

Il **Responsabile del trattamento** è tenuto altresì a informare immediatamente il **Titolare del trattamento**, nel caso in cui riscontri carenze in relazione alla sicurezza del trattamento, nell'ambito delle verifiche sulle misure di sicurezza adottate nel trattamento dei dati personali, che il **Responsabile del trattamento** è tenuto a effettuare regolarmente.

Con riguardo ai trattamenti di dati personali svolti occasionalmente senza ausilio di strumenti elettronici e informatici, il **Responsabile del trattamento** se nel caso deve provvedere a che gli archivi fisici siano adeguatamente custoditi e l'accesso sia riservato solo ai soggetti autorizzati. Devono essere definite le procedure di deposito, custodia, consegna, restituzione e compartimentazione dei documenti contenenti dati personali e, in ragione della particolare natura dei dati personali, predisposti contenitori separati e serrati con appositi strumenti e definita una procedura di gestione delle chiavi.

Operazioni da eseguire sui dati personali al termine dell'affidamento, anche anticipato

In caso di revoca della designazione come **Responsabile del trattamento** oppure al termine dell'affidamento, anche anticipato per recesso o risoluzione, il **Responsabile del trattamento**, in accordo con il Titolare, è tenuto:

- alla restituzione completa dei dati personali di titolarità del Consiglio regionale, di cui abbia disponibilità, previa anonimizzazione;
- alla distruzione di eventuale documentazione contenente i dati personali di cui all'allegato A.1, salvo sia obbligatorio conservare alcuni documenti in ragione degli adempimenti amministrativi e contabili stabiliti dalla legge o di specifica richiesta da parte del Titolare del trattamento o anonimizzazione;
- alle altre operazioni richieste dal Titolare del trattamento stesso o previste dall'Affidamento, compresa la cancellazione dei dati personali di cui all'allegato A.1. dai supporti elettronici e

informatici utilizzati con modalità che non ne consentano il recupero, in conformità al provvedimento del Garante per la protezione dei dati personali 13 ottobre 2008 in materia di rifiuti di apparecchiature elettriche ed elettroniche (RAEE) e misure di sicurezza dei dati personali, salvo anonimizzazione.

In questo ambito risulta necessario procedere a: a) emanare adeguate istruzioni di comportamento a tutti i soggetti incaricati autorizzati al trattamento; b) effettuare una ricognizione completa di tutti i supporti di memoria che possano essere riutilizzabili (sia su parti di tipo asportabile sia di quelli presenti in aree di memoria interne al sistema operativo od in programmi), ove possano trovarsi dati; c) esaminare tutti i nuovi supporti, sistema operativo e programmi, che vengono inseriti nel sistema di trattamento dei dati, analizzando i possibili rischi ed impartendo specifiche istruzioni ai soggetti incaricati autorizzati al trattamento.

In caso di occasionali trattamenti svolti senza ausilio di strumenti elettronici e informatici, è necessario procedere con la triturazione del supporto al fine di non consentire l'identificazione degli interessati.

Delle operazioni di cancellazione compiute e degli obblighi di conservazione ulteriori, il **Responsabile del trattamento** è tenuto a rilasciare apposita dichiarazione scritta e firmata dal legale rappresentante al **Titolare del trattamento**.

Rimangono ferme le eventuali specificazioni definite nell'Affidamento.

Obblighi di informazione e collaborazione

Il **Responsabile del trattamento** deve fornire la documentazione e le informazioni necessarie in relazione ai servizi svolti e alle misure di sicurezza applicate e dare l'assistenza necessaria per garantire il rispetto della Normativa privacy.

In particolare, il **Responsabile del trattamento** deve dare assistenza e collaborare, fornendo la documentazione e le informazioni necessarie anche con riguardo alle misure di sicurezza, nello svolgimento e nella redazione dei documenti relativi all'analisi del rischio per la protezione dei dati personali e alla valutazione di impatto sulla protezione dei dati personali (art. 32 e 35 RGPD), secondo le procedure di cui alla deliberazione dell'Ufficio di Presidenza 4.11.2019, n. 423 recante "Metodologia per l'analisi del rischio e la valutazione di impatto per la protezione dei dati personali da applicare ai trattamenti di dati personali del Consiglio regionale della Lombardia" e ss.mm.ii.

Il **Responsabile del trattamento**, ai sensi dell'art. 30, paragrafo 2, del RGPD, salva la deroga di cui al medesimo articolo, tiene il registro delle attività relative al trattamento dei dati personali effettuate per conto del Titolare e, su richiesta, mette tale registro a disposizione del Titolare e/o del Garante per la protezione dei dati personali.

Il **Responsabile del trattamento** è comunque tenuto a fornire al Titolare le informazioni necessarie alla compilazione del "Registro delle attività di trattamento" e delle informative sul trattamento dei dati personali per gli interessati, come previsto dalla Normativa privacy, anche curando ogni necessario rapporto con gli eventuali sub responsabili e a mettere a disposizione del **Titolare del trattamento** le informazioni necessarie all'espletamento delle attività di revisione, comprese le ispezioni richieste dallo stesso **Titolare del trattamento** o da altro soggetto da esso autorizzato, al

fine di rilevare il rispetto degli obblighi previsti dalla Normativa privacy e dal contenuto specifico dell’Affidamento del servizio richiamato nel presente Atto.

Il **Responsabile del trattamento** deve evadere tempestivamente le richieste del Titolare e impegnarsi alla collaborazione necessaria in modo da consentire l’esercizio dei diritti da parte degli interessati, richiamati dalla Normativa privacy. Nel caso in cui il **Responsabile del trattamento** riceva, da parte dell’interessato, un’istanza per l’esercizio dei suoi diritti ai sensi degli artt. da 15 a 22 RGPD è tenuto ad evaderla, informando prontamente il **Titolare del trattamento**.

Il **Responsabile del trattamento** deve collaborare attivamente con l’Autorità Garante per la Protezione dei dati personali e le Autorità Pubbliche, per consentire a queste ultime l’esercizio delle proprie attività istituzionali, quali richieste di informazioni, attività di controllo mediante accessi e ispezioni, relativamente ai trattamenti oggetto del presente Atto, informando immediatamente il Titolare di qualsiasi richiesta e/o comunicazione relativa ai dati personali pervenutagli dal Garante e da qualsiasi Autorità.

Qualora il **Titolare** debba svolgere una revisione della valutazione del rischio ai sensi degli articoli 32 e 35 RGPD, il **Responsabile del trattamento** si impegna a fornire le informazioni necessarie anche in merito alle misure di sicurezza applicate.

Designazione di sub–responsabili (art. 28, paragrafi 2 e 4, RGPD)

Il **Responsabile del trattamento** ha la facoltà di ricorrere ad altri responsabili del trattamento di dati personali (sub - responsabili del trattamento) nell’ambito delle attività di trattamento di dati personali per conto del Consiglio regionale della Lombardia. Ai sensi dell’art. 28, paragrafo 2, del RGPD, tale facoltà è da intendersi quale autorizzazione scritta generale da parte del Consiglio regionale della Lombardia, **Titolare del trattamento**, nei confronti del **Responsabile del trattamento** per le attività sopra menzionate, salvo l’obbligo di comunicazione nei termini sotto specificati.

Il **Responsabile del trattamento**, in sede di designazione di sub-Responsabili, deve informare il **Titolare del trattamento**, al fine di consentire, come previsto dall’art. 28 paragrafo 2 RGPD, di poter manifestare eventuale formale opposizione a tale designazione entro e non oltre il termine di quindici giorni dalla ricezione della comunicazione; decorso il termine quest’ultima potrà procedere all’effettuazione delle designazioni nei confronti dei sub-responsabili del trattamento individuati.

In ogni caso, la designazione di un sub-responsabile del trattamento da parte del **Responsabile del trattamento** è possibile a condizione che su tale soggetto siano imposti gli stessi obblighi in materia di protezione dei dati contenuti nel presente Atto, incluse garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti richiesti dalla Normativa privacy e dal rischio correlato al trattamento e che sia la garanzia che il trattamento sia svolto nel territorio dell’Unione Europea o nel territorio di Paesi non appartenenti allo Spazio Economico Europeo ritenuti adeguati tramite decisione della Commissione europea ai sensi degli art. 45 e 46 del Regolamento UE 2016/679.

Il **Responsabile del trattamento** deve inviare al **Titolare del trattamento**, su richiesta di quest'ultimo, la documentazione relativa alla designazione del sub-responsabile del trattamento per l'esercizio delle prerogative stabilite dall'art. 28 RGPD.

Il **Responsabile del trattamento** rimane comunque interamente responsabile nei confronti del Consiglio regionale della Lombardia con riguardo all'adempimento degli obblighi in materia di protezione dei dati da parte del sub-responsabile del trattamento, ai sensi dell'art. 28, paragrafo 4, RGPD ed è tenuto alla gestione di ogni rapporto con tale soggetto a garanzia della protezione dei dati personali di titolarità del Consiglio regionale e al rispetto della Normativa Privacy.

Il **Titolare del trattamento** può in qualsiasi momento verificare le garanzie e le misure tecniche e organizzative del sub-responsabile del trattamento, tramite audit e ispezioni, anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inidonee, il Titolare del trattamento può chiedere la presentazione di garanzie sufficienti entro un termine congruo.

Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del RGPD o risulti che il sub-responsabile agisca in modo difforme o contrario alle istruzioni fornite dal Titolare del trattamento, quest'ultimo applicherà al **Responsabile del trattamento** le penali e le ulteriori conseguenze sul contratto previste nell'Affidamento e diffiderà lo stesso a far adottare al sub-responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato.

Il **Responsabile del trattamento** garantisce che i dati personali non siano utilizzati dagli altri sub – responsabili per finalità non connesse allo svolgimento delle prestazioni di cui all'Affidamento, salvo che l'interessato non esprima, in autonomia e in aggiunta a quanto previsto nel presente Atto, valido consenso agli ulteriori trattamenti nel rispetto della Normativa privacy e previa informativa.

Gestione degli incidenti di sicurezza informatica e violazioni di dati personali (*data breach*)

Il **Responsabile del trattamento** è tenuto ad adottare un piano di gestione degli incidenti di sicurezza, conforme alla Normativa Privacy e ai provvedimenti del Garante per la protezione dei dati personali.

Fermo quanto previsto nell'Affidamento, il **Responsabile del trattamento** è tenuto a comunicare al Titolare, senza ingiustificato ritardo, ogni violazione dei dati o di incidenti informatici o altro accadimento che possa aver comportato un impatto sui dati personali del Consiglio regionale della Lombardia, **Titolare del trattamento**, violandone la riservatezza, integrità, disponibilità o comunque esponendoli a rischio, secondo quanto richiesto dalla Normativa privacy vigente.

Il **Responsabile del trattamento** è dotato di un modello di comunicazione al **Titolare del trattamento** per i casi di violazione dei dati personali conforme alla Normativa Privacy e ai provvedimenti del Garante per la protezione dei dati personali.

La comunicazione deve contenere almeno le seguenti informazioni:

- i) la descrizione della natura del *data breach* compresi, ove possibile, le categorie e il numero approssimativo d'interessati colpiti dalla violazione nonché le categorie e il numero approssimativo di registrazioni dei dati personali oggetto della violazione;

- ii) il nome e i dati di contatto del responsabile per la protezione dei dati o di altro punto di contatto del responsabile, presso cui ottenere informazioni ulteriori;
- iii) la descrizione delle probabili conseguenze del *data breach*;
- iv) se del caso, tenendo conto della natura del trattamento, dei servizi e del contratto, la descrizione delle misure adottate dal responsabile o di quelle di cui propone l'adozione per porre rimedio al *data breach* ovvero attenuarne i possibili effetti negativi.

La comunicazione deve avvenire anche qualora la violazione sia solo presunta o esista un sospetto, pur in assenza di certezze.

La comunicazione deve essere rivolta al Dirigente dell'Ufficio Contratti e ICT all'indirizzo: protocollo.generale@pec.consiglio.regione.lombardia.it e sistema.informativo@consiglio.regione.lombardia.it, nonché per conoscenza all'indirizzo rpd@consiglio.regione.lombardia.it.

Eventuali modifiche o precisazioni sulla procedura possono essere oggetto di separato accordo con il Titolare del trattamento.

Le informazioni e i dati relativi alla violazione sono mantenuti riservati, fermi restando gli obblighi di notifica e comunicazione previsti dagli articoli 33 e 34 RGPD.

Luogo di trattamento e trasferimento di dati personali

I dati personali trattati dal **Responsabile del trattamento** per l'erogazione dei servizi, di cui all'Affidamento, sono ubicati in architetture e storage dedicati o logicamente separati.

Il **Responsabile del trattamento** assicura che la porzione dedicata ai dati del Titolare del trattamento è ubicata nel territorio dell'Unione Europea o nel territorio di Paesi non appartenenti allo Spazio Economico Europeo ritenuti adeguati tramite decisione della Commissione europea ai sensi degli art. 45 e 46 del Regolamento UE 2016/679 presso data center in cui, compatibilmente alla tipologia, vengono eseguite le procedure automatizzate per l'eventuale conservazione, duplicazione, backup e ripristino dei dati.

Il **Responsabile del trattamento** assicura che il trasferimento dei dati personali trattati avvenga su canali sicuri o in forma criptata (per esempio: HTTPS, SSH v2).

Il **Responsabile del trattamento**, in assenza di una decisione della Commissione europea o di garanzie adeguate ai sensi degli artt. 45 e 46 del Regolamento UE 2016/679, non può:

- 1) trasferire i dati personali a un titolare del trattamento o a un responsabile del trattamento in un paese terzo o in un'organizzazione internazionale situati fuori dall'Unione europea;
- 2) trasferire il trattamento di dati personali a un sub - responsabile del trattamento in un paese terzo situato fuori dall'Unione europea;
- 3) far elaborare i dati personali dal responsabile del trattamento in un paese terzo situato fuori dall'Unione europea.

Obblighi del responsabile relativi all'infrastruttura cloud utilizzata per l'erogazione del servizio

In caso di utilizzo di cloud per l'erogazione del servizio, il **Responsabile del trattamento** garantisce di utilizzare un'infrastruttura cloud conforme alle «best-practice» del settore e si impegna a

adeguarla ovvero a mantenerla adeguata alle necessità dell'incarico stesso, garantendo il pieno rispetto degli obblighi e adempimenti previsti dalla normativa europea e italiana in materia.

Il **Responsabile del trattamento** garantisce in particolare di utilizzare un'infrastruttura cloud conforme ai requisiti minimi previsti dai provvedimenti di ACN vigenti, da ultimo dal Regolamento unico per le infrastrutture e i servizi cloud di ACN (Decreto Direttoriale n. 21007/24 del 27 giugno 2024) e ss.mm.ii.

ATTIVITÀ DI VIGILANZA E VERIFICA DEL TRATTAMENTO

Per sorvegliare l'osservanza del presente Atto, il **Titolare del trattamento** può effettuare periodiche azioni di verifica. Tali verifiche possono comportare la richiesta di presentare informazioni, dati, documenti e compilazione di questionari di self-assessment (verifiche documentali) nonché l'effettuazione di test, per esempio di vulnerabilità, e l'accesso a locali o macchine e programmi del **Responsabile del trattamento**.

Per la risposta alle richieste di verifiche documentali, al **Responsabile del trattamento** deve essere concesso un termine di almeno 15 (quindici) giorni, salvo che la richiesta sia dovuta alla necessità di rispondere all'Autorità di controllo o all'Autorità giudiziaria. In tali ultime ipotesi il **Responsabile del trattamento** deve garantire una risposta compatibile con gli obblighi del **Titolare** nei confronti di tali Autorità.

Nell'ambito di tali verifiche il **Responsabile del trattamento** fornisce l'assistenza e il supporto necessario, rispondendo alle richieste del **Titolare del trattamento** in relazione ai dati ed ai trattamenti di cui al presente Atto e non ha diritto a compensi aggiuntivi.

Nel caso in cui, all'esito delle verifiche, ispezioni e audit, le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del RGPD o risulti che il **Responsabile del trattamento** agisca in modo difforme o contrario alle istruzioni fornite dal **Titolare**, quest'ultimo applicherà al **Responsabile del trattamento** le penali e le ulteriori conseguenze sul contratto previste nella Convenzione e diffiderà lo stesso ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato.

Il **Responsabile del trattamento** è tenuto a svolgere e fornire la DPIA o l'analisi dei rischi svolta sul progetto di ricerca oggetto del servizio erogato.

Il **Responsabile del trattamento** è tenuto ad informare il **Titolare**, mediante relazione scritta, di tutte le attività svolte in conformità a quanto previsto dal Contratto, ogni qualvolta sia ritenuto necessario dal **Titolare**.

INDIVIDUAZIONE DI MAGGIORI LIVELLI DI SICUREZZA E ADEGUAMENTI ALLA NORMATIVA PRIVACY SOPRAVVENUTA O A ESIGENZE CONTRATTUALI SOPRAVVENUTE

Il **Titolare del trattamento** può proporre al **Responsabile del trattamento** ogni variazione del presente Atto che sia necessaria per adempiere agli obblighi derivanti dalla Normativa Privacy o per tenere conto delle clausole tipo e dei codici di condotta eventualmente adottati ai sensi, rispettivamente, dell'articolo 28, paragrafi 7 e 8, e dell'articolo 40 del RGPD o ai fini delle

certificazioni di cui all'articolo 42.

Il **Responsabile del trattamento** e il **Titolare del trattamento** concordano che provvederanno, se necessario, a integrare o modificare i contenuti del presente Atto in conformità alla Normativa privacy sopravvenuta. Eventuali ulteriori modifiche e integrazioni potranno altresì essere messe a punto in conseguenza degli esiti di nuove valutazioni sui rischi correlati al trattamento e in ragione di evoluzioni tecnologiche rilevanti o comunque per il miglior assolvimento delle prestazioni contrattuali. Il Responsabile del trattamento si impegna a collaborare nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse.

COMUNICAZIONI

Le comunicazioni previste dal presente Atto nei confronti del **Titolare del trattamento** devono essere trasmesse all'indirizzo di posta elettronica certificata del Consiglio regionale (protocollo.generale@pec.consiglio.regione.lombardia.it), all'attenzione del dirigente del Servizio Studi, Valutazione delle Politiche e Qualità della Normazione.

Il **Responsabile del trattamento** ha l'obbligo di comunicare al **Titolare del trattamento** un indirizzo di posta elettronica certificata e gli altri recapiti ai quali inviare le comunicazioni previste dal presente Atto.

DISPOSIZIONI FINALI

In conformità all'art. 82 e ss., il **Responsabile del trattamento** risponde di ogni perdita, costo, spesa, multa e/o sanzione, danno derivante da o in connessione con una qualsiasi violazione delle disposizioni della Convenzione, del decreto di incarico o altro atto, della normativa privacy e dei compiti e istruzioni di cui al presente Atto da parte sua, dei suoi dipendenti o collaboratori o degli eventuali altri responsabili del trattamento di sua designazione.

Il presente Atto e lo svolgimento degli obblighi e attività in esso previsti non comporta alcun diritto del **Responsabile del trattamento** a uno specifico compenso e/o indennità e/o rimborso.

Per le controversie relative al presente atto, si applicano le disposizioni previste nell'Affidamento.

Per tutto quanto non previsto espressamente nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

DATI DI CONTATTO DEI RESPONSABILI DELLA PROTEZIONE DEI DATI PERSONALI (RPD)

Il RPD del Consiglio regionale della Lombardia è contattabile ai seguenti recapiti: rpdp@consiglio.regione.lombardia.it e protocollo.generale@pec.consiglio.regione.lombardia.it.

Il **Responsabile del trattamento** ha l'obbligo di comunicare il nominativo e i dati di contatto del proprio Responsabile per la protezione dei dati personali (art. 37 e ss. del RGPD). Qualora il Fornitore non sia obbligato a nominare il Responsabile della protezione dei dati, sarà tenuto a mettere a disposizione uno specifico indirizzo di posta elettronica per le comunicazioni in materia di protezione dei dati personali.

Il **Responsabile del trattamento** e il **Titolare del trattamento** si danno reciproca informazione di eventuali modifiche relative ai propri Responsabili della protezione dei dati personali o referenti privacy.

ALLEGATI

A.1 *“Elenco dei trattamenti dei dati personali di titolarità del Consiglio regionale della Lombardia affidati al Responsabile del trattamento”*

A.2 *“Elenco delle misure di sicurezza applicate dal Fornitore”*

per il **Consiglio regionale della Lombardia**
Il Dirigente pro tempore dell’Ufficio
Contratti e ICT
(firmato digitalmente)

per la società
il Legale Rappresentante
.....
(firmato digitalmente per accettazione)

ALLEGATO A.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI DI TITOLARITÀ DEL CONSIGLIO REGIONALE AFFIDATI AL FORNITORE IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO

Ai sensi dell'art. 28 RGPD, il Responsabile del trattamento, nella persona del rappresentante legale *pro tempore*, è designato, per quanto sia necessario alla corretta esecuzione delle prestazioni contrattuali, quale responsabile del trattamento dei dati personali, per conto del Consiglio regionale della Lombardia, per i trattamenti e i dati personali indicati nella seguente tabella. Eventuali altri trattamenti di dati personali potranno essere eseguiti dal medesimo Responsabile del trattamento solo a seguito di comunicazione/richiesta scritta da parte del Titolare del trattamento.

Servizio affidato	Finalità e ambito dei trattamenti affidati al Responsabile	Modalità di trattamento e principali trattamenti svolti	Tipologia di dati trattati e categorie di interessati	Responsabile CRL di gestione del servizio e referente operativo CRL
Realizzazione di uno studio sulla partecipazione politica finalizzato ad analizzare le dinamiche della partecipazione al voto dei cittadini della Lombardia e le ragioni dell'astensione	Finalità Attività di ricerca. Produzione di report e rapporti di ricerca. Rilevazione demoscopica mediante somministrazione di questionari con tecnica CAWI (Computer Assisted Web Interviewing) Realizzazione di focus group Realizzazione interviste con esperti Ambito del trattamento Ricerca	Il trattamento è effettuato con l'ausilio di strumenti elettronici e manuali (cartacei). Le operazioni di trattamento autorizzate sono: [X] raccolta [X] registrazione [X] organizzazione [X] strutturazione [X] conservazione [] adattamento [] modifica [] visualizzazione [X] estrazione [X] uso [] comunicazione agli interessati e al Consiglio regionale [] diffusione [] raffronto [] interconnessione [] limitazione [X] cancellazione secondo le istruzioni del Titolare [X] distruzione secondo le istruzioni del Titolare La trasmissione dei dati personali è consentita solo su espressa autorizzazione del Titolare con modalità sicure (es. file criptati con password comunicata con altro canale).	<u>Per tutte le attività</u> Dati personali comuni identificativi e di contatto (es. nome, cognome, indirizzo di posta elettronica/telefono) <u>Rilevazione demoscopica e Focus group</u> Dati sociodemografici comuni: es. età, genere, titolo di studio, professione, condizione lavorativa, composizione del nucleo familiare, comune di residenza, fascia di reddito Dati personali di particolari categorie: opinioni politiche, convinzioni religiose o filosofiche (es. percezione delle istituzioni,	Direttore dell'esecuzione: dirigente Servizio Studi, Valutazione delle Politiche e Qualità della Normazione

		Le prestazioni comportano: - la predisposizione di misure di sicurezza applicativa per garantire integrità, stabilità e riservatezza dei dati personali; - attività tecniche e funzioni di amministratore di sistema; - connessione sicura HTTPS; - la visione in chiaro di dati personali da parte del Fornitore; - l'anonimizzazione dei dati personali. - le registrazioni audio-video dei focus group e audio delle interviste agli esperti, previo consenso informato. Sono escluse attività di profilazione degli interessati. I dati non possono essere utilizzati per altri scopi (salvo se anonimizzati). Conservazione Il Responsabile provvede alla cancellazione dei dati personali decorsi tre mesi dalla presentazione dei risultati della ricerca, salvo diversa istruzione del Titolare e salvo che il diritto dell'Unione o degli Stati membri, cui è soggetto il Responsabile, prescriva la conservazione dei dati personali o salvo anonimizzazione. Il Responsabile garantisce l'integrale trasferimento dei dati al Titolare o	interesse per la politica, motivazioni dell'astensione o della partecipazione, preferenze politiche, autocollocazione politica, fiducia nei partiti e nei leader politici) Interessati: cittadini lombardi di età superiore o uguale a 19 anni (massimo 3.000) <u>Interviste con esperti</u> Dati personali comuni: opinioni, valutazioni e conoscenze specifiche relative al tema della partecipazione politica e dell'astensione Interessati: 3 esperti	
--	--	---	--	--

		a terzi da questi indicati previa anonimizzazione.		
--	--	---	--	--

ALLEGATO A.2 - ELENCO DELLE MISURE DI SICUREZZA

Fermo quanto stabilito con riguardo a specifiche misure di sicurezza nell'Atto di designazione o definito nel progetto di ricerca o in altro atto contrattuale con il Titolare, il **Responsabile del trattamento** nell'ambito delle attività previste contrattualmente garantisce di applicare le seguenti misure di sicurezza:

Sicurezza applicativa	
Barrare le misure adottate	Misure di sicurezza
X	gestione di più profili con privilegi diversi
X	utilizzo credenziali uninominali
X	autenticazione delle utenze username/password
X	utilizzo di password sicure (almeno quattordici caratteri alfanumerici)
X	cambio periodico delle password (almeno ogni sei mesi)
_	autenticazione utenze multifattore
_	utilizzo di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.)
X	supporto di protocolli sicuri e cifrati (HTTPS, SSH v2, ecc.)
X	ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL)
X	Messaggi di posta elettronica inviati devono essere crittografati tramite protocolli crittografici (TLS / SSL)
_	utilizzo di meccanismi di autenticazione basati su crittografia asimmetrica, a chiave pubblica, fornita dal Fornitore, con lunghezza basata sulla criticità della comunicazione (es. 256 bit per le meno critiche, 512 bit per le più critiche)
X	profili di autorizzazione differenziati tra gli utenti
X	funzionalità di "richiesta creazione o cambio della password al primo accesso"
X	blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso
X	accessi utenti registrati su un archivio (log) non cancellabile con il reset
X	gestione dei log di sistema (accessi, allarmi, ecc.)
_	mascheratura della base dati
X	Encryption/cifratura
_	cifratura delle comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell'ente
X	tracciatura delle accessi
X	tracciatura delle modifiche
X	protezione dei dati estratti

Barrare le misure adottate	Misure di sicurezza
X	validazione dei dati in input
X	protezione delle comunicazioni client/server
_	archivi separati tra dati generici e dati particolari (sensibili e/o giudiziari)
X	aggiornamento periodico software utilizzati
X	utilizzo di programmi contro il rischio di intrusione e accesso abusivo
X	utilizzo di programmi antivirus
_	cancellazione dati di navigazione
_	anonimizzazione dati di navigazione
_	filtraggio di indirizzi IP
X	vulnerability assessment
_	utilizzo per l'accesso a internet di un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dall'ente
_	rispetto della politica di sicurezza dell'ente
_	definizione delle specifiche di sicurezza applicate
_	implementazione delle specifiche di sicurezza nel codice e nella struttura della basedati
X	condivisione della documentazione per gestire il servizio
_	Altro

Sicurezza infrastrutturale	
Barrare le misure adottate	Misura di sicurezza
X	gestione di più profili con privilegi diversi
X	utilizzo credenziali uninominali per quanto attiene le componenti infrastrutturali di competenza del responsabile del trattamento
X	gli utenti non devono essere in grado di disattivare o bypassare le impostazioni di sicurezza
X	autenticazione delle utenze username/password
X	utilizzo di password sicure (almeno quattordici caratteri alfanumerici)
_	autenticazione utenze multifattore
X	utilizzo di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.)
X	uso di protocolli sicuri e cifrati (HTTPS, SSH v2, ecc.)
_	utilizzo di meccanismi di autenticazione basati su crittografia asimmetrica, a chiave pubblica, fornita dal Fornitore, con lunghezza basata sulla criticità della comunicazione (es. 256 bit per le meno critiche, 512 bit per le più critiche)

Barrare le misure adottate	Misura di sicurezza
X	profili di autorizzazione differenziati tra gli utenti
X	funzionalità di “richiesta creazione o cambio della password al primo accesso”
X	blocco dell’utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso
X	accessi utenti registrati su un archivio (log) non cancellabile con il reset
X	gestione dei log di sistema (accessi, allarmi, ecc.)
X	programma di backup dei dati
X	programma di backup delle configurazioni
X	protezione/cifratura dei backup
_	archiviazione separata dati comuni e dati particolari (sensibili e/o giudiziari)
X	programma di test dei restore
X	protezione da malware
X	le applicazioni antivirus e le firme di rilevamento devono essere aggiornate almeno su base settimanale
X	protezione/cifratura delle linee di comunicazione
_	cifratura delle comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell’ente
_	isolamento della rete da altri sistemi
X	protezione del traffico tramite Intrusion Detection System
X	protezione del traffico tramite Intrusion Prevention System
X	protezione del traffico tramite Web Application Firewall
X	protezione/cifratura del file system
X	attivazione delle restrizioni di accesso sul file system
X	tracciatura degli accessi amministrativi
_	tracciatura delle attività amministrative
X	tracciatura degli accessi al database
_	tracciatura degli accessi a file system
X	raccolta centralizzata log
_	utilizzo per l’accesso a internet di un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dal CRL
X	programma di protezione dischi rimovibili
_	programma di controllo piattaforma software
X	soluzione di disaster recovery
_	soluzione dlp applicata al contesto
X	dismissione supporti di archiviazione già utilizzati
X	gestione supporti di archiviazione dismessi

Barrare le misure adottate	Misura di sicurezza
☒	verifica annuale dell'operato degli amministratori
☒	aggiornamento delle soluzioni e dei servizi di sicurezza e adeguamento alle normative UE o nazionali senza costi aggiuntivi
☐	presenza di un SOC del fornitore
☒	dispositivi di sicurezza perimetrale su reti del Fornitore (es. Firewall, sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.)
☒	gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente
☐	Altro

Sicurezza fisica per i trattamenti su supporti non elettronici se occasionalmente svolti

Barrare le misure adottate	Misura di sicurezza
☒	limitazione di accesso ai locali deputati al trattamento
☐	profilazione degli accessi in base a ruolo
☐	utilizzo tessere di accesso uninominali limitazione di accesso agli archivi cartacei
☒	limitazione di accesso agli archivi cartacei
☒	archiviazione cartacea distinta per livello di severità
☐	tracciatura degli accessi ai repository di dati cartacei
☐	tracciatura degli accessi ai locali
☒	presenza di sistemi antieffrazione
☒	videosorveglianza locali
☒	movimentazione materiali in modalità sicura
☒	sigillatura contenitori movimentati
☒	Triturazione della documentazione cartacea contenente dati personali
☒	Definizione di regole per la cancellazione sicura dei dati (es. Modello basato sulla norma DIN 66398)
☐	Altro

Sicurezza Organizzativa

Barrare le misure adottate	Misure di sicurezza
☒	formazione privacy del personale

Barrare le misure adottate	Misure di sicurezza
☒	definizione di procedure per assicurare la segretezza
☒	definizione di un elenco dei dipendenti che saranno impiegati sul singolo progetto e sottoscrizione per ogni dipendente di dichiarazioni di riservatezza/confidenzialità
☒	nomina referente privacy
☒	nomina incaricati del trattamento
☐	presenza dpo
☒	definizione di una procedura di data breach
☒	struttura per la prevenzione e gestione degli incidenti informatici
☒	procedura di ripristino dei dati in caso di incidente fisico o tecnico
☒	consegna, entro il giorno successivo, di un report sugli incidenti di sicurezza avvenuti contenente: tipologia di attacco subito, vulnerabilità sfruttate, sequenza temporale degli eventi e contromisure adottate
☐	adozione delle procedure e politiche di sicurezza definite dall'ente
☐	possesso della certificazione ISO/IEC 27001 o, in assenza, di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di un piano di qualità secondo lo standard ISO 10005
☐	piano di auditing annuale sul sistema di sicurezza da parte di società specializzata, approvata dall'ente
☒	possibilità di auditing a richiesta dell'ente
☐	possibilità di verifiche di conformità dei servizi da parte dell'ente
☐	possesso di certificazioni di sicurezza da parte del personale
☐	consegna, entro il giorno successivo alla richiesta, dei log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT
☒	condivisione della documentazione tecnica (schede tecniche, manuali, guide operative) per la corretta configurazione e gestione degli aspetti di sicurezza
☒	dichiarazione di conformità alla normativa vigente in materia di sicurezza cibernetica e al GDPR
☒	spese per il ripristino della situazione preattacco informatico a carico del Fornitore
☒	utilizzo, previa autorizzazione, di repliche dei dati dell'ente solo nel territorio dell'UE
☐	dichiarazione di disponibilità a far parte di un Comitato di Direzione Tecnica
☒	disponibilità alla sottoscrizione di clausola di non divulgazione
☒	gestione di vulnerabilità scoperte sui prodotti oggetto della fornitura senza costi aggiuntivi
☒	monitoraggio e valutazione continua sulla pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite

Barrare le misure adottate	Misure di sicurezza
_	descrizione dettagliata della soluzione tecniche applicate (dispositivi hardware e software impiegato, modalità operative, politiche di sicurezza)
_	Altro

Nei casi in cui si evidenziasse una non piena corrispondenza tra la tipologia di trattamento prevista per l'esecuzione del servizio e le misure di sicurezza richieste, il **Responsabile del trattamento** s'impegna a comunicarlo per scritto al Titolare, fornendo al medesimo l'effettuata analisi del rischio e indicando le misure di sicurezza ritenute adeguate.

Ulteriori misure di sicurezza potranno essere richieste dal Titolare al **Responsabile del trattamento** qualora alla luce del progetto di ricerca le misure ivi proposte o indicate nell'atto di designazione e nell'allegato A.2 non siano ritenute adeguate al rischio.



Regione Lombardia

IL CONSIGLIO

Foglio Patti e condizioni relativo al servizio di realizzazione dello studio "La partecipazione politica in Lombardia".

Sommario

Art. 1 - Definizione delle parti	3
Art. 2 - Finalità e oggetto del contratto	3
Art. 3 - Durata del contratto	3
Art. 4 - Responsabile Unico del Progetto (RUP), Direttore dell'esecuzione del contratto (DEC) e referenti operativi	3
Art. 5 – Caratteristiche minime dello studio, descrizione delle attività e modalità di esecuzione del servizio	4
Art. 6 – Validazione dei prodotti della ricerca	5
Art. 7 - Cause di forza maggiore o fattori indipendenti dal Fornitore	6
Art. 8 – Diritto d'autore e diffusione dei risultati della ricerca	6
Art. 9 – Corrispettivi e contenuti della fattura elettronica, modalità di fatturazione e pagamento ...	7
Art. 10 – Revisione prezzi	8
Art. 11 – Penali	8
Art. 12 - Risoluzione ai sensi dell'articolo 122 del d.lgs. 36/2023	10
Art. 13 - Recesso ai sensi dell'articolo 123 del d.lgs. 36/2023	10
Art. 14 - Clausola risolutiva dell'art. 1456 del Codice civile	10
Art. 15 – Recesso ai sensi dell'art. 1, comma 13, del d.l. 6 luglio 2012, n. 95	11
Art. 16 - Tracciabilità dei flussi finanziari	11
Art. 17 - Trattamento di dati personali e designazione del Fornitore quale responsabile del trattamento	12
Art. 18 - Patto di riservatezza	15
Art. 19 - Garanzia definitiva	16
Art. 20 - Divieto di "pantouflage" e relative sanzioni	17
Art. 21 – Rispetto del codice di comportamento dei dipendenti pubblici e del personale del Consiglio regionale della Lombardia	17
Art. 22 – Rispetto del Patto di integrità e relative sanzioni	17
Art. 23 - Divieto di cessione del contratto e subappalto	18
Art. 24 - Segnalazione di illeciti nell'Amministrazione da parte dei lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi (c.d. whistleblowing)	19

Art. 25 - Spese di contratto, di registro e accessorie a carico del Fornitore	19
Art. 26 - Indirizzo di posta elettronica certificata del Consiglio regionale.....	19
Art. 27 - Risoluzione delle controversie e Foro competente	19
Art. 28 - Norma finale	19
CLAUSOLE DEL FOGLIO PATTI E CONDIZIONI DI CUI ALL'ART. 1341 DEL CODICE CIVILE	20
Allegato D	21
PREMESSA	21
BASE GIURIDICA E PRINCIPI	22
DURATA.....	23
OBBLIGHI DEL TITOLARE DEL TRATTAMENTO	23
OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO	23
ATTIVITÀ DI VIGILANZA E VERIFICA DEL TRATTAMENTO	36
INDIVIDUAZIONE DI MAGGIORI LIVELLI DI SICUREZZA E ADEGUAMENTI ALLA NORMATIVA PRIVACY SOPRAVVENUTA O A ESIGENZE CONTRATTUALI SOPRAVVENUTE	36
COMUNICAZIONI.....	37
DISPOSIZIONI FINALI	37
DATI DI CONTATTO DEI RESPONSABILI DELLA PROTEZIONE DEI DATI PERSONALI (RPD)	37
ALLEGATI	38
ALLEGATO A.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI DI TITOLARITÀ DEL CONSIGLIO REGIONALE AFFIDATI AL FORNITORE IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO	39
ALLEGATO A.2 - ELENCO DELLE MISURE DI SICUREZZA	41
Allegato 1 – Deliberazione dell'Ufficio di presidenza 24 marzo 2025, n. 100	47

Art. 1 - Definizione delle parti

1. **Amministrazione Appaltante**, nel prosieguo denominata anche 'Amministrazione' o 'Consiglio regionale' è il Consiglio regionale della Lombardia, codice fiscale n. 80053570158 e P. IVA 09201010965, con sede in via Fabio Filzi n. 22, CAP 20124, a Milano.
2. **Fornitore**, nel prosieguo denominato anche 'Affidatario', è l'operatore economico individuato all'esito della procedura di affidamento.

Art. 2 - Finalità e oggetto del contratto

1. Il presente Foglio Patti e condizioni ha per oggetto il servizio di realizzazione dello studio "La partecipazione politica in Lombardia".
2. Il servizio consiste nella realizzazione di uno studio sulla partecipazione politica finalizzato all'analisi delle dinamiche della partecipazione al voto dei cittadini della Lombardia e delle ragioni dell'astensione, con le caratteristiche minime di cui all'articolo 5 del presente Foglio Patti e condizioni, secondo quanto previsto nella deliberazione dell'Ufficio di presidenza 24 marzo 2025, n. 100 (Allegato 1), e secondo quanto dettagliato nel Progetto esecutivo elaborato dal Fornitore, in coerenza con le indicazioni presenti nella richiesta di preventivo.

Art. 3 - Durata del contratto

1. Il contratto ha una durata di 12 mesi, con decorrenza dal 16 giugno 2025, o, se successiva, dalla data di stipulazione del contratto.

Art. 4 - Responsabile Unico del Progetto (RUP), Direttore dell'esecuzione del contratto (DEC) e referenti operativi

1. Ai sensi dell'articolo 15 e dell'articolo 2 dell'Allegato I.2 del d.lgs. 31 marzo 2023, n. 36 (di seguito, anche, Codice), il Consiglio regionale individua quale Responsabile Unico del progetto (RUP) il dirigente dell'Ufficio contratti e ICT.
2. Il Consiglio regionale individua quale Direttore dell'esecuzione del contratto (di seguito DEC) il dirigente del Servizio Studi, Valutazione delle politiche e Qualità della Normazione.
3. Fermo restando il rispetto delle disposizioni di servizio eventualmente impartite dal Responsabile unico del progetto (di seguito RUP), il DEC opera in autonomia in ordine al coordinamento, alla direzione e al controllo tecnico-contabile nell'esclusivo interesse all'efficiente e sollecita esecuzione del contratto.
4. Il DEC è competente altresì per l'eventuale modifica dell'impegno di spesa, per la liquidazione delle fatture, per la redazione del certificato di regolare esecuzione nonché per lo svincolo della garanzia definitiva.
5. L'eventuale variazione del DEC è tempestivamente comunicata dal Consiglio regionale al Fornitore.
6. È referente operativo del contratto il Responsabile dell'Unità Operativa Studi e Biblioteca.

7. Le comunicazioni tra il DEC e il Fornitore avvengono per iscritto tramite posta elettronica istituzionale o posta elettronica certificata, all'indirizzo di cui all'articolo 26, in modo da garantire la verifica dell'avvenuto recapito delle stesse.
8. Il Consiglio regionale procederà, per il tramite del DEC, all'accertamento della conformità del servizio rispetto alle prescrizioni contrattuali.

Art. 5 – Caratteristiche minime dello studio, descrizione delle attività e modalità di esecuzione del servizio

1. Lo studio, a partire da un'analisi della letteratura a tema, dovrà approfondire dinamiche e motivazioni della partecipazione al voto e dell'astensionismo nel territorio lombardo. Andranno dunque analizzati, in serie storica, i dati sulla partecipazione al voto per le tornate elettorali regionali, politiche ed europee, relativi ai livelli regionale, provinciale e comunale mettendoli possibilmente anche in relazione a variabili sociodemografiche selezionate (ad esempio genere, età, istruzione, reddito). Ricorrendo a una pluralità di metodologie e strumenti di indagine di tipo qualitativo e quantitativo, compresa una rilevazione demoscopica che fornisca informazioni statisticamente significative almeno a livello provinciale, lo studio dovrà indagare le caratteristiche sociodemografiche dell'elettorato lombardo partecipante e non partecipante al voto, le ragioni dell'astensione dalla partecipazione, il rapporto con le istituzioni, la politica e le relative priorità.
2. Ad esito delle diverse fasi dell'attività di ricerca il Fornitore deve realizzare i prodotti e le attività seguenti:
 - a) il Rapporto intermedio, da consegnare entro 3 mesi dalla data di decorrenza del servizio (16 giugno o data successiva indicata nella stipulazione del contratto), consistente in una breve relazione (3-5 pagine) sullo stato di avanzamento delle attività di ricerca; il Rapporto dà, se del caso, conto di eventuali aspetti imprevisti che l'attività di ricerca ha incontrato e, ove necessario, propone integrazioni al Progetto esecutivo allo scopo di risolvere eventuali criticità, che l'Amministrazione può decidere se accettare o meno;
 - b) il Rapporto finale di ricerca, da consegnare entro 6 mesi dalla data di decorrenza del servizio, consistente in un documento che espone i risultati della ricerca e ha dimensioni comprese indicativamente fra le 50 e le 100 pagine, con eventuali allegati. È strutturato in capitoli e paragrafi, con titoli esplicativi dei contenuti, redatto con un linguaggio chiaro e accessibile anche ad un pubblico non esperto della materia, organizzato sui seguenti contenuti:
 - i. scopo e metodologia di ricerca;
 - ii. definizione del tema trattato e informazioni di contesto;
 - iii. risultati delle indagini realizzate;
 - iv. conclusioni e indicazioni, spunti di policy;
 - v. indicazione delle fonti e di ulteriori riferimenti documentali;
 - vi. glossario;
 - c) l'Executive Summary, da consegnare entro 6 mesi dalla data di decorrenza del servizio, contestualmente al Rapporto Finale, consistente in un rapporto di sintesi che evidenzia i

principali risultati della ricerca, le sue conclusioni e indicazioni di policy; non deve superare le n. 8 pagine ed è redatto con un linguaggio e soluzioni grafiche di particolare efficacia comunicativa per un pubblico non esperto della materia oggetto di ricerca; la prima sezione del rapporto reca un abstract in italiano e in inglese che, complessivamente, non supera 1 pagina;

d) la Presentazione dei risultati, che offre una illustrazione sintetica dei contenuti e dei risultati della ricerca, corredata da materiali predisposti con un linguaggio e soluzioni grafiche di particolare efficacia comunicativa, da svolgersi entro il termine di durata del contratto nelle giornate definite dagli organi consiliari; il DEC dà al Fornitore un preavviso di almeno 15 giorni;

e) i dati della ricerca, da consegnare unitamente al Rapporto Finale e all'Executive Summary, consistono nei microdati elementari raccolti ed elaborati nel corso della ricerca. Devono essere consegnati in forma strutturata e in formato elaborabile dagli applicativi informatici in uso presso il Consiglio regionale (per dati tabellari strutturati i formati CSV, ODS, XLSX; per documenti testuali i formati ODT, PDF e DOCX), nonché opportunamente anonimizzati.

3. Il Fornitore svolge il servizio in raccordo con le competenti strutture del Consiglio regionale al fine di garantire la più efficace realizzazione dei prodotti attesi. In particolare, il DEC può convocare incontri sullo stato di avanzamento dei lavori, sulle eventuali criticità emerse e sulle azioni da intraprendere per il proseguimento delle attività previste.
4. Il Fornitore deve individuare un responsabile delle attività di ricerca. Il nominativo del responsabile deve essere comunicato al DEC entro 10 giorni dalla stipulazione del contratto.
5. L'Amministrazione si riserva di fornire indicazioni redazionali sul Rapporto finale e sull'Executive Summary, anche con riferimento all'eventuale apposizione del logo del Fornitore.
6. Il gruppo di ricerca deve essere costituito da soggetti che posseggano il profilo professionale indicato nel Progetto esecutivo.

Art. 6 – Validazione dei prodotti della ricerca

1. Il Fornitore trasmette i prodotti di cui all'art. 5, comma 2, lettere a), b) e c), in formato editabile e in formato pdf a mezzo di posta elettronica certificata all'indirizzo PEC del protocollo generale del Consiglio regionale.
2. Il DEC valida i prodotti di cui al comma 1, sulla base dell'aderenza alle prescrizioni del presente Foglio Patti e condizioni, al Progetto esecutivo e, eventualmente, qualora l'Amministrazione accetti le modifiche proposte ai sensi dell'articolo 5, comma 2, lettera a), al Rapporto intermedio.
3. Il DEC comunica al Fornitore gli esiti del processo di validazione ed eventuali indicazioni per la prosecuzione dello studio a mezzo PEC entro 30 giorni dall'avvenuta consegna dei prodotti attesi.
4. Qualora il Rapporto finale e l'Executive Summary non siano conformi a quanto previsto, a seguito del processo di validazione di cui al comma 2, il DEC può stabilire un congruo termine - non superiore a 30 giorni - entro il quale il Fornitore deve adeguare il proprio operato alle condizioni stabilite. Al termine del periodo assegnato, entro i successivi 30 giorni, in caso permangano inadempienze o difformità rispetto a quanto previsto per l'esecuzione del contratto, il DEC si

riserva di inviare formale contestazione al Fornitore tramite PEC, per l'applicazione delle penali previste all'articolo 11.

Art. 7 - Cause di forza maggiore o fattori indipendenti dal Fornitore

1. Nel caso in cui la realizzazione delle attività, e di conseguenza dei prodotti previsti all'articolo 5, comma 2, lettere b), c) ed e), necessitasse di tempi maggiori per cause di forza maggiore o comunque fattori indipendenti dal Fornitore e non prevedibili al momento della presentazione del Progetto esecutivo, il Fornitore può chiedere e concordare con il Consiglio regionale eventuali proroghe ai termini sopra indicati.
2. La richiesta di proroga motivata deve essere presentata tramite posta elettronica certificata al DEC almeno 15 giorni prima della scadenza prevista per la consegna del Rapporto finale di cui all'articolo 5, comma 2, lettera b).
3. Il DEC può accordare proroghe contrattuali che in ogni caso non potranno superare il limite complessivo di 60 giorni, con conseguente differimento del termine finale del contratto a parità di corrispettivi contrattuali.

Art. 8 – Diritto d'autore e diffusione dei risultati della ricerca

1. I prodotti, i risultati e i dati della ricerca di cui al presente servizio sono di proprietà del Consiglio regionale della Lombardia, che è titolare dei diritti d'autore di pubblicazione e utilizzazione economica, fatti salvi i diritti morali.
2. Il Consiglio regionale può rendere pubblici i risultati dello studio e i nomi dei componenti del gruppo di ricerca, anche attraverso il proprio sito web istituzionale e la riproduzione a stampa e in formato digitale del Rapporto finale, dell'Executive Summary e dei materiali utilizzati per la Presentazione dei risultati.
3. Per aggiornare banche dati, registri ed elenchi delle proprie attività, il Fornitore può liberamente utilizzare il titolo dello studio di cui al presente servizio, che non può essere pubblicato senza riferimento all'Amministrazione committente. Il Fornitore può altresì utilizzare i risultati e i dati della ricerca per proprie ulteriori attività, con l'obbligo di fare riferimento all'Amministrazione committente in caso di presentazioni pubbliche. È escluso ogni uso per fini commerciali salvo che l'Amministrazione proceda alla diffusione con una licenza che consenta il riutilizzo per fini commerciali.
4. L'Amministrazione committente potrà diffondere i prodotti di cui al presente servizio con una licenza che ne consenta il riutilizzo a titolo gratuito, a condizione di indicare la fonte e di non stravolgere il significato o messaggio originali.
5. Le parti riconoscono fin da ora che per la natura dell'oggetto, l'attività di ricerca non può comportare invenzioni tali da essere titolo per acquisire eventuali diritti brevettuali e di proprietà industriale.

Art. 9 – Corrispettivi e contenuti della fattura elettronica, modalità di fatturazione e pagamento

1. Al Fornitore è riconosciuto il corrispettivo offerto in sede di procedura, formulato sulla base dell'importo stimato dall'Amministrazione e indicato nella richiesta di preventivo.
2. Il Fornitore fattura il corrispettivo contrattuale, previo ricevimento della validazione dei prodotti di cui all'articolo 6 del presente Foglio Patti e condizioni e previo benestare del DEC sulla regolare esecuzione per quanto riguarda la Presentazione dei risultati di cui all'articolo 5, comma 2, lettera d), con le seguenti scadenze:
 - il 40% a seguito della validazione del Rapporto intermedio;
 - il 50% a seguito della validazione del Rapporto finale e dell'Executive Summary;
 - il 10% a seguito dello svolgimento della Presentazione dei risultati.
3. I corrispettivi si riferiscono al servizio oggetto dell'affidamento eseguito a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali e includono tutti gli oneri derivanti al Fornitore dall'esecuzione del contratto e dall'osservanza di leggi e regolamenti. È escluso il rimborso di eventuali spese sostenute dal Fornitore a qualsiasi titolo.
4. L'Amministrazione liquida la fattura, previa verifica della sua correttezza da parte del DEC. Il pagamento è disposto entro trenta giorni dal ricevimento di regolare fattura, in favore del conto corrente indicato dall'affidatario ai sensi dell'articolo 16.
5. La fattura deve essere emessa secondo le prescrizioni del decreto del ministro dell'economia e delle finanze del 23 gennaio 2015 *“Modalità e termini per il versamento dell'imposta sul valore aggiunto da parte delle pubbliche amministrazioni”*, pubblicato nella Gazzetta Ufficiale della Repubblica italiana - Serie Generale n. 27 del 3 febbraio 2015, come modificato da ultimo dal decreto del Ministro dell'economia e delle finanze del 9 gennaio 2018, pubblicato nella Gazzetta Ufficiale della Repubblica italiana n. 14 del 18 gennaio 2018, e riportare obbligatoriamente i seguenti dati:
 - Intestazione: **Consiglio regionale della Lombardia**
 - Sede: Via Fabio Filzi, 22 – 20124 Milano
 - Codice Univoco Ufficio di IPA (campo 1.1.4): **UFIRHM**
 - Codice fiscale del Consiglio regionale (campo 1.4.1.2): **80053570158**
 - Repertorio contratto (campo 2.1.3.2): **2023/XII.3.2.4.23**
 - CIG contratto (campo 2.1.3.7): **comunicato in sede di stipulazione al Fornitore**
 - Esigibilità IVA (campo 2.2.2.7): S *“Scissione dei pagamenti”*.
6. Nel caso in cui la fattura sia priva dei dati richiesti al comma 5, l'Amministrazione non procede con la liquidazione e chiede al Fornitore l'emissione di una nota di credito a completo storno della fattura irregolare e la contestuale emissione di una fattura contenente i dati richiesti.
7. Eventuali contestazioni o irregolarità di fatturazione, anche diverse da quelle richiamate al comma 6, sospendono comunque il termine di pagamento, con facoltà per l'Amministrazione di procedere ai sensi del medesimo comma.
8. Ai sensi dell'articolo 31 del decreto-legge 21 giugno 2013, n. 69, convertito con modificazioni dalla legge 9 agosto 2013, n. 98, il Consiglio regionale acquisisce d'ufficio il documento unico di regolarità contributiva (DURC), che ha validità di centoventi giorni dalla data del rilascio, tra

l'altro, per il pagamento del corrispettivo contrattuale e per l'attestazione di regolare esecuzione.

9. In caso di inadempienza contributiva risultante dal DURC e di ritardato pagamento delle retribuzioni dovute al personale impiegato nell'esecuzione dell'appalto, si procederà ai sensi dell'articolo 11, comma 6, del Codice.
10. Ai sensi dell'articolo 11, comma 6, del Codice, sull'importo netto progressivo delle prestazioni contrattuali è operata una ritenuta dello 0,50 per cento. Le ritenute possono essere svincolate soltanto in sede di liquidazione del saldo finale, dopo la verifica della regolare esecuzione della fornitura, previo rilascio del documento unico di regolarità contributiva. L'IVA esposta nella fattura deve comunque essere calcolata sul corrispettivo pieno.
11. Il Consiglio regionale, prima di effettuare il pagamento, qualora ne ricorrano i presupposti, procede alla verifica prevista dall'art. 48-bis del D.P.R. 29 settembre 1973, n. 602, così come modificata dall'art. 1, commi 986 e 987, lettere a) e b), della legge 27 dicembre 2017, n. 205, secondo le modalità stabilite dal D.M. 18 gennaio 2008, n. 40.

Art. 10 – Revisione prezzi

1. Ai sensi degli articoli 9 e 60 del Codice, qualora nel corso di esecuzione del contratto si verificino particolari condizioni di natura oggettiva, che determinano una variazione, in aumento o in diminuzione, del costo del servizio superiore al cinque per cento dell'importo complessivo, i prezzi sono aggiornati, nella misura dell'ottanta per cento della variazione stessa, in relazione alle prestazioni da eseguire.
2. Ai fini della determinazione della variazione dei prezzi l'Amministrazione, ai sensi dell'art. 11 comma 4 e della tabella D) dall'Allegato II.2 bis al Codice, utilizzerà l'indice dei prezzi al consumo, nel caso specifico l'indice IR 732 "Ricerche di mercato e sondaggi di opinione" collegato al CPV 79310000-0 "Servizi di ricerca di mercato", pubblicato, unitamente alla relativa metodologia di calcolo, sul portale istituzionale dell'ISTAT in conformità alle pertinenti disposizioni normative europee e nazionali in materia di comunicazione e diffusione dell'informazione statistica ufficiale.
3. I nuovi prezzi determinati a seguito della revisione sono applicati alle prestazioni contrattuali svolte dopo la revisione a partire dalla prima fatturazione utile. In nessun caso la revisione dei prezzi potrà avere effetto sulle prestazioni già eseguite.

Art. 11 – Penali

1. Il DEC ha facoltà di contestare eventuali inadempienze, qualora, a seguito di controlli, ravvisi difformità o ritardo negli adempimenti contrattuali. La contestazione viene formulata al Fornitore dal DEC per il tramite di PEC.
2. Il Fornitore ha facoltà di formulare controdeduzioni, per il tramite di PEC, entro il termine perentorio di cinque (5) giorni dal ricevimento della formale contestazione.
3. Il direttore dell'esecuzione del contratto, valutate le ragioni addotte dal Fornitore, sentito il RUP, può procedere all'applicazione delle seguenti penali nelle seguenti ipotesi:

- a) mancato rispetto dei tempi di consegna dei prodotti di cui all'articolo 5 o 7: l'1,5 per mille dell'importo netto contrattuale, per ogni giorno di ritardo;
 - b) mancato adeguamento, su richiesta del DEC, nei termini previsti all'articolo 6, comma 4, del Rapporto finale e dell'Executive Summary ai requisiti previsti dal presente Foglio Patti e condizioni e dal Progetto esecutivo e, eventualmente, dal Rapporto intermedio, qualora l'Amministrazione accetti le modifiche proposte ai sensi dell'articolo 5, comma 2, lettera a): l'1,5 per mille per ogni giorno di ritardo;
 - c) nel caso in cui l'adeguamento, richiesto dal DEC, del Rapporto finale e dell'Executive Summary ai requisiti previsti dal presente Foglio Patti e condizioni, dal Progetto esecutivo e, eventualmente, dal Rapporto intermedio (qualora l'Amministrazione accetti le modifiche proposte ai sensi dell'articolo 5, comma 2, lettera a), non soddisfi detti requisiti: un valore compreso tra lo 0,5 e l'1,5 per mille dell'importo contrattuale netto a seconda del grado di inadempimento;
 - d) mancato rispetto dei termini per la comunicazione del responsabile designato di cui all'articolo 5, comma 4: 1,5 per mille per ogni giorno di ritardo;
 - e) violazione del Patto di integrità di cui all'articolo 22 del Foglio Patti e condizioni: una penale tra l'1% e il 5% dell'importo netto contrattuale;
 - f) violazione degli obblighi di riservatezza di cui all'articolo 18: euro 100,00 per ogni violazione.
4. Le fattispecie riportate al comma 3 non hanno carattere di tassatività. In caso di disservizio, ritardo o inadempimento diverso da quelli contemplati al comma 2, il DEC può irrogare al Fornitore, in relazione alla gravità del fatto, una penale compresa tra lo 0,5 per mille e l'1,5 per mille dell'importo contrattuale netto.
 5. Le penali espresse in percentuale sono arrotondate alla seconda cifra decimale per eccesso.
 6. Le penali per il ritardo non possono comunque superare, complessivamente, il 10 per cento dell'importo netto contrattuale.
 7. In caso di applicazione di penali, è fatto salvo il risarcimento dell'eventuale maggior danno subito dal Consiglio regionale ai sensi dell'articolo 1382 del Codice civile.
 8. Inoltre, nei casi in cui il Fornitore ometta di eseguire, anche parzialmente, la prestazione oggetto del contratto con le modalità ed entro i termini previsti, il Consiglio regionale si riserva la facoltà di ordinare ad altro soggetto l'esecuzione parziale o totale di quanto omissso dal Fornitore, al quale saranno addebitati i relativi costi e i danni eventualmente derivati al Consiglio regionale.
 9. Per la riscossione delle penali e la rifusione degli eventuali ulteriori danni il Consiglio regionale può rivalersi tramite trattenuta per compensazione sui crediti vantati dall'affidatario nei confronti del Consiglio, ovvero sulla garanzia definitiva prestata che, in tal caso, dovrà essere reintegrata.
 10. Qualora l'inesatto adempimento o il ritardo siano determinati da cause di forza maggiore, il Fornitore dovrà notificare immediatamente tale circostanza alla competente struttura tramite PEC, fornendo le necessarie motivazioni a comprova.

11. In caso di applicazione delle penali, l'Amministrazione provvederà a darne comunicazione all'ANAC, in osservanza della normativa vigente in materia.

Art. 12 - Risoluzione ai sensi dell'articolo 122 del d.lgs. 36/2023

1. L'Amministrazione può risolvere il contratto di appalto ai sensi dell'art. 122 del Codice.
2. In tutti i casi di risoluzione del contratto, il Fornitore ha diritto soltanto al pagamento delle prestazioni regolarmente eseguite, decurtato degli oneri aggiuntivi derivanti dallo scioglimento del contratto, fatto salvo quanto previsto al comma 6 del medesimo articolo.

Art. 13 - Recesso ai sensi dell'articolo 123 del d.lgs. 36/2023

1. L'Amministrazione può recedere dal contratto in qualunque momento ai sensi dell'articolo 123 del Codice. All'Affidatario è riconosciuta un'indennità, pari al decimo dei servizi non eseguiti, calcolata sulla differenza tra l'importo dei quattro quinti del prezzo posto a base dell'affidamento, depurato del ribasso d'asta, e l'ammontare netto dei servizi eseguiti, secondo quanto previsto all'articolo 11 dell'allegato II.14, del Codice.
2. L'esercizio del diritto di recesso è manifestato dall'Amministrazione appaltante mediante una formale comunicazione all'Affidatario da darsi per iscritto con un preavviso non inferiore a venti giorni, decorsi i quali il Consiglio regionale prende in consegna i servizi ed effettua la verifica della regolare esecuzione degli stessi.

Art. 14 - Clausola risolutiva dell'art. 1456 del Codice civile

1. Fatta salva l'applicazione delle penali di cui all'articolo 11, il Consiglio regionale ha facoltà, previa comunicazione scritta da inviare al Fornitore a mezzo PEC con cui dichiara che intende avvalersi della presente clausola, di risolvere il contratto ai sensi dell'articolo 1456 del Codice civile, con incameramento della garanzia al verificarsi delle seguenti ipotesi:
 - a) in caso di applicazione di penali per un ammontare pari ad almeno il dieci per cento dei corrispettivi contrattuali;
 - b) in caso di violazione degli obblighi di tracciabilità finanziaria richiamati dall'articolo 16;
 - c) in caso di gravi violazioni delle norme in materia di protezione dei dati personali e degli obblighi assunti in qualità di responsabile del trattamento di cui agli articoli 17 e 18;
 - d) in caso di mancata completa reintegrazione della garanzia definitiva di cui all'articolo 19, eventualmente escussa, entro il termine di dieci giorni naturali e consecutivi dal ricevimento della relativa richiesta tramite PEC da parte del Consiglio regionale;
 - e) in caso di violazione dei codici di comportamento di cui all'articolo 21;
 - f) in caso di violazione del patto di integrità di cui all'articolo 22;
 - g) in caso di violazione del divieto di cessione del contratto o delle norme sul subappalto di cui all'articolo 23;
 - h) in caso di mancato rispetto della normativa vigente in materia di lavoro, d'infortuni sul lavoro, d'igiene, di previdenza sociale e di tutti gli obblighi previsti dal d.lgs. n. 81 del 2008

oppure inosservanza degli obblighi previsti dai contratti collettivi di categoria, nazionali e regionali, anche dopo la loro scadenza e fino alla loro sostituzione;

- i) in caso di verifiche con esito negativo in merito al possesso dei requisiti generali e speciali di partecipazione dichiarati in sede di procedura, fatte salve le ulteriori conseguenze previste ai sensi dell'articolo 52, comma 2, del Codice.
2. L'Amministrazione potrà dichiarare risolto il contratto a proprio insindacabile giudizio e potrà provvedere, inoltre, a stipulare un nuovo contratto, addebitando le maggiori spese che dovessero derivare da prezzi meno favorevoli per l'Amministrazione stessa e fatto salvo il risarcimento del maggior danno.

Art. 15 – Recesso ai sensi dell'art. 1, comma 13, del d.l. 6 luglio 2012, n. 95

1. Ai sensi dell'art. 1 comma 13 del d.l. 6 luglio 2012, n. 95, convertito in legge 7 agosto 2012, n. 135, il Consiglio regionale ha diritto di recedere in qualsiasi tempo dal presente contratto, previa formale comunicazione all'appaltatore con preavviso non inferiore a quindici giorni e previo pagamento delle prestazioni già eseguite oltre al decimo delle prestazioni non ancora eseguite, nel caso in cui, tenuto conto anche dell'importo dovuto per le prestazioni non ancora eseguite, i parametri delle convenzioni stipulate da Consip S.p.A. ai sensi dell'articolo 26, comma 1, della legge 23 dicembre 1999, n. 488, successivamente alla stipulazione del contratto siano migliorativi rispetto a quelli del contratto stipulato e l'appaltatore non acconsenta ad una modifica delle condizioni economiche tale da rispettare il limite di cui all'articolo 26, comma 3, della legge 488/1999.

Art. 16 - Tracciabilità dei flussi finanziari

1. Il Fornitore assume tutti gli obblighi di tracciabilità finanziaria di cui all'articolo 3 della legge 13 agosto 2010, n. 136, così come interpretato e modificato dagli articoli 6 e 7 del decreto-legge 12 novembre 2010, n. 187, convertito dalla legge 17 dicembre 2010 n. 217. A tal fine, il Fornitore sottoscrive, su richiesta del Consiglio regionale, la dichiarazione di tracciabilità dei flussi finanziari, contenente tra l'altro gli estremi del conto corrente dedicato ai pagamenti relativi al presente contratto e la aggiorna tempestivamente in caso di modifica dei dati ivi dichiarati.
2. Il Fornitore si impegna a notificare tempestivamente eventuali variazioni che si verificassero nelle modalità di pagamento e, in difetto di tale notificazione, esonera il Consiglio regionale da ogni responsabilità per i pagamenti eseguiti.
3. I subappaltatori e i subcontraenti, a qualunque titolo coinvolti nella esecuzione del contratto, sono tenuti, unitamente al Fornitore, al rispetto della normativa sulla tracciabilità dei flussi finanziari (articolo 3, comma 1, legge 136/2010).
4. Ai sensi dell'articolo 119, comma 2, ultimo periodo, del Codice, "L'affidatario comunica alla stazione appaltante, prima dell'inizio della prestazione, per tutti i sub-contratti che non sono subappalti, stipulati per l'esecuzione dell'appalto, il nome del sub-contraente, l'importo del subcontratto, l'oggetto del lavoro, servizio o fornitura affidati. Sono, altresì, comunicate alla stazione appaltante eventuali modifiche a tali informazioni avvenute nel corso del sub-

contratto. È altresì fatto obbligo di acquisire autorizzazione integrativa qualora l'oggetto del subappalto subisca variazioni e l'importo dello stesso sia incrementato".

5. Come previsto all'articolo 3, comma 1, della legge n. 136/2010 "La stazione appaltante verifica che nei contratti sottoscritti con i subappaltatori e i subcontraenti della filiera delle imprese a qualsiasi titolo interessate ai lavori, ai servizi e alle forniture di cui al comma 1 sia inserita, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla presente legge".
6. L'appaltatore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria è tenuto a darne immediata comunicazione alla stazione appaltante e alla prefettura - ufficio territoriale del Governo della provincia di Milano.

Art. 17 - Trattamento di dati personali e designazione del Fornitore quale responsabile del trattamento

1. Ai fini del presente Foglio Patti e condizioni e dei suoi allegati, s'intende per "Normativa privacy", 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 d.lgs. 30 giugno 2003, n. 196, recante "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" (di seguito "Codice privacy"), alle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018, nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile in Italia, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali.
2. Le prestazioni contrattuali comportano l'affidamento al Fornitore di attività di trattamento, anche con l'ausilio di strumenti elettronici, di dati personali di cui è titolare il Consiglio regionale. Ai sensi dell'art. 28 RGPD, il Fornitore, nella persona del legale rappresentante pro tempore, in qualità di aggiudicatario, assume la qualifica di Responsabile del trattamento dei dati personali trattati, per conto del Consiglio regionale (Titolare del trattamento), nell'ambito dell'esecuzione delle prestazioni di cui al presente Foglio Patti e condizioni.
3. Il Fornitore si impegna, nel definire i contenuti del progetto di ricerca e nella sua attuazione, a dare conto del rispetto delle citate previsioni. Il Fornitore si impegna a procedere al trattamento dei dati personali di terzi esclusivamente nei limiti necessari per lo svolgimento delle attività previste dal progetto di ricerca oggetto del servizio affidato, secondo quanto previsto dal presente contratto e in successivi atti e documenti di attuazione del progetto, e a non svolgere trattamenti ulteriori e in nessun caso a divulgarli. Il Fornitore è tenuto a consegnare le informazioni sul trattamento previste dagli artt. 13 e 14 RGPD, a evadere tempestivamente le

richieste degli interessati e a fornire la collaborazione necessaria in modo da agevolare l'esercizio dei diritti da parte degli interessati di cui agli articoli 15 e ss. RGPD.

4. Il Fornitore tratta esclusivamente i dati personali necessari per la realizzazione di uno studio sulla partecipazione politica finalizzato ad analizzare le dinamiche della partecipazione al voto dei cittadini della Lombardia e le ragioni dell'astensione secondo quanto specificato nel presente Foglio Patti e condizioni e nel Progetto esecutivo, in conformità alla normativa applicabile in materia, alla Normativa privacy e alle Regole deontologiche applicabili in materia. In ogni caso, tutti i dati personali possono essere trattati dal Fornitore nell'ambito e solo nei limiti in cui sia indispensabile per effettuare le prestazioni contrattuali, garantendo la tutela della riservatezza, l'integrità e la disponibilità dei dati.
5. Il Fornitore è tenuto a presentare all'Amministrazione garanzie in termini di conoscenza specialistica, affidabilità, risorse, anche in ordine all'adozione di misure tecniche, logiche ed organizzative idonee per assicurare che i trattamenti dei dati personali affidatigli avvengano in conformità alla normativa Privacy; a tale fine il Fornitore è tenuto a trasmettere una relazione in cui descrive il proprio sistema di gestione dei dati personali in conformità al RGPD anche in termini di adeguatezza al rispetto delle previsioni dell'allegato di designazione come responsabile del trattamento, nonché le misure tecniche e di sicurezza implementate.
6. Ai sensi e per gli effetti di cui all'art. 28 RGPD, il Fornitore è tenuto a sottoscrivere, prima dell'inizio delle prestazioni contrattuali che comportino il trattamento di dati personali rientranti nella titolarità del Consiglio regionale, un separato atto giuridico bilaterale che definisca gli elementi di cui al paragrafo 3 dell'art. 28 citato e in particolare, i dati trattati, i trattamenti svolti e le misure tecniche e organizzative che il Fornitore deve mettere in atto per garantire la protezione dei dati personali trattati, secondo quanto definito nell'allegato D) che potrà essere integrato sulla base della relazione di cui al comma 5, del progetto di ricerca presentato in sede di presentazione del preventivo o successivamente, e dovrà essere comunque sottoscritto prima dell'inizio delle attività di trattamento da parte del Responsabile. Il Fornitore s'impegna a dare al Titolare tutte le informazioni necessarie per la definizione dell'atto, precisando le misure di sicurezza, la tipologia di dati trattati e il luogo di trattamento. Tale atto avrà un'efficacia temporale pari a quella del rapporto contrattuale, anche in caso di revoca anticipata, risoluzione o recesso.
7. L'atto prevederà, in ogni caso, in capo al Fornitore:
 - l'impegno al pieno rispetto degli obblighi derivanti direttamente dalle disposizioni in materia di protezione dei dati personali sul responsabile del trattamento dei dati personali e all'esecuzione dei compiti e al rispetto delle istruzioni impartite dal Consiglio regionale della Lombardia, fermo restando quanto previsto nelle altre disposizioni del Foglio Patti e condizioni/contratto;
 - la dichiarazione di avere una struttura e una organizzazione adeguata all'esecuzione dell'incarico di trattamento dei dati personali connesso alle prestazioni contrattuali impegnandosi a mantenerla adeguata alla rilevanza dell'incarico stesso, garantendo il pieno

rispetto, per sé e per i propri dipendenti e collaboratori, delle disposizioni sul trattamento dei dati personali;

- l'impegno a trattare i dati personali nel rispetto dei principi di necessità, pertinenza e non eccedenza, in modo lecito e secondo correttezza, per scopi legittimi e determinati, assicurando l'esattezza, la completezza e l'integrità dei dati registrati e conservati nell'applicativo;
- l'impegno a non svolgere trattamenti di dati personali ulteriori rispetto a quelli affidati e comunque non finalizzati all'adempimento delle prestazioni contrattuali o di obblighi di legge connessi alle prestazioni contrattuali stesse;
- l'impegno a garantire, per l'ambito di trattamento affidato, che i dati del Titolare del trattamento sono trattati nel territorio dell'Unione Europea o dello Spazio Economico Europeo ovvero nel territorio di Paesi non appartenenti allo Spazio Economico Europeo ritenuti adeguati tramite decisione della Commissione europea ai sensi degli art. 45 e 46 del Regolamento UE 2016/679;
- l'impegno a sub delegare il trattamento ad altri responsabili in conformità a quanto previsto nell'atto di designazione di cui al comma 6;
- il divieto di comunicazione a soggetti terzi, non coinvolti nell'esecuzione della prestazione, e la diffusione dei dati personali;
- l'impegno a fornire ogni informazione necessaria per la compilazione del registro delle attività di trattamento e per garantire l'esercizio dei diritti degli interessati di cui agli art. 12 e ss. RGPD, fornendo in particolare agli stessi le informazioni sul trattamento dei loro dati;
- l'impegno a collaborare con il Titolare del trattamento per il rispetto delle norme sulla protezione dei dati personali e fornire al Consiglio regionale la documentazione e le informazioni necessarie in relazione ai servizi svolti e alle misure di sicurezza applicate e garantire l'assistenza necessaria per garantire il rispetto della Normativa privacy, compresa, se richiesta, l'assistenza alla redazione dell'analisi del rischio per la protezione dei dati personali (articoli 32 e 35 RGPD) secondo le procedure di cui alla deliberazione Ufficio di presidenza 4 novembre 2019, n. 423 recante "Metodologia per l'analisi del rischio e la valutazione di impatto per la protezione dei dati personali da applicare ai trattamenti di dati personali del Consiglio regionale della Lombardia" e ss.mm.ii. allegata alla richiesta di preventivo;
- l'obbligo di consentire attività di verifica e controllo da parte del Consiglio regionale della Lombardia per accertare la conformità del trattamento alle istruzioni impartite;
- l'obbligo di comunicare, senza ritardo, e comunque entro 24 (ventiquattro) ore dal momento in cui ne ha avuto conoscenza, ogni violazione dei dati o altro accadimento che possa aver comportato un impatto sui dati personali, violandone la riservatezza o comunque esponendoli a rischio;
- l'obbligo di designare i soggetti incaricati del trattamento e a vincolarli legalmente alla riservatezza e al rispetto delle istruzioni di cui all'atto stesso, garantendo loro una formazione adeguata in materia di protezione dei dati personali e impartendo loro, per

iscritto, specifiche istruzioni e indicazioni relative al trattamento dei dati affidato, fornendo le necessarie informazioni sulle operazioni che possono essere compiute e prevedendo in particolare l'obbligo di mantenere l'assoluto riserbo sui dati personali o le informazioni acquisite e il divieto di compiere ogni altra operazione che possa compromettere la sicurezza dei dati o comportare la diffusione illecita degli stessi

- l'obbligo di comunicare il nominativo e i dati di contatto del proprio Responsabile per la protezione dei dati personali (art. 37 e ss. RGPD) o, qualora non tenuto alla nomina, di un referente per la privacy.
8. L'eventuale designazione come responsabile del trattamento è efficace per tutta la durata del rapporto contrattuale, fino alla scadenza dello stesso. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti o collaboratori impegnati nell'esecuzione delle prestazioni contrattuali, che devono essere vincolati legalmente ai medesimi obblighi di riservatezza.
 9. In caso di revoca della designazione come responsabile del trattamento ovvero al termine del contratto, anche anticipato per recesso o risoluzione, il Fornitore s'impegna a seguire le istruzioni impartite dal Titolare, provvedendo alla restituzione completa dei dati al Consiglio regionale ovvero alle altre operazioni richieste dal Titolare stesso, salva la conservazione dei dati e della documentazione cui il Fornitore è tenuto per obbligo di legge.
 10. È in ogni caso fatto divieto al Fornitore di eseguire trattamenti non finalizzati all'esecuzione delle attività affidate e in particolare è fatto divieto di pubblicare, cedere, donare o altrimenti disporre dei dati, senza la preventiva ed espressa richiesta o autorizzazione dell'Amministrazione consiliare.
 11. Il Fornitore, in qualità di responsabile del trattamento, mantiene indenne e manlevato il Titolare del trattamento da ogni perdita, costo, spesa, multa e/o sanzione, danno e da ogni responsabilità di qualsiasi natura derivante da o in connessione con una qualsiasi violazione delle disposizioni del presente Foglio Patti e condizioni e dei compiti e istruzioni dal Titolare da parte sua o di ogni sub appaltatore di cui si avvale in conformità all'art. 82 del regolamento (UE) 2016/679.

Art. 18 - Patto di riservatezza

1. Ferme le disposizioni di cui al precedente articolo, i dati economici, finanziari, patrimoniali o di qualunque altro genere, che vengano a conoscenza del Fornitore, in ragione dei servizi resi per il Consiglio regionale, sono riservati. I dati e le informazioni, non oggetto di pubblicazione in base alla legge, fermo il divieto di cui al comma 10 dell'articolo precedente, venute a conoscenza del Fornitore in relazione all'esecuzione del presente contratto e le informazioni che transitano attraverso le apparecchiature di rilevazione, elaborazione, trasferimento, archiviazione dei dati del Fornitore non debbono in alcun modo e in nessuna forma essere comunicate e divulgate a terzi, né debbono essere utilizzate da parte del Fornitore o da parte di chiunque collabori alle sue attività per fini diversi da quelli contemplati nel presente Foglio Patti e condizioni/contratto.

2. Il Fornitore è tenuto a mantenere riservati tali dati, a non divulgarli in alcun modo e a non utilizzarli per scopi diversi da quelli relativi all'esecuzione del contratto. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti o collaboratori impegnati nell'esecuzione delle prestazioni contrattuali dei suddetti obblighi di riservatezza.
3. Tale clausola deve intendersi vincolante anche dopo la cessazione del presente contratto.
4. Il Consiglio regionale s'impegna a trattare, in conformità al d.lgs. 196/2003 e al RGPD, i dati personali conferiti dal Fornitore per le sole finalità di definizione e gestione del contratto e dei relativi pagamenti, provvedendo alle comunicazioni e alle pubblicazioni dei dati relativi all'affidamento secondo quanto previsto dal d.lgs. 36/2023, dal d.lgs. 33/2013 e dalle altre norme in materia come descritto nell'informativa sul trattamento dei dati personali di cui agli articoli 13 e 14 RGPD allegata alla richiesta di preventivo.

Art. 19 - Garanzia definitiva

1. Ai sensi dell'articolo 53, comma 4, del Codice, il Fornitore per la sottoscrizione del contratto deve costituire una garanzia definitiva sotto forma di cauzione o fideiussione, pari al 5% dell'importo contrattuale netto. Non si applicano le riduzioni previste dall'articolo 106, comma 8, e gli aumenti previsti dall'articolo 117, comma 2, del Codice.
2. La cauzione è costituita con versamento della somma garantita presso l'istituto incaricato del servizio di tesoreria, a titolo di pegno a favore dell'Amministrazione, esclusivamente tramite il sistema Pago PA.
3. La garanzia fideiussoria, a scelta dell'appaltatore, può essere rilasciata da imprese bancarie o assicurative che rispondano ai requisiti di solvibilità previsti dalle leggi che ne disciplinano le rispettive attività, oppure dagli intermediari finanziari iscritti nell'albo di cui all'articolo 106 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, che svolgono in via esclusiva o prevalente attività di rilascio di garanzie e che sono sottoposti a revisione contabile da parte di una società di revisione iscritta nell'apposito albo e che abbiano i requisiti minimi di solvibilità richiesti dalla vigente normativa bancaria assicurativa. La garanzia fideiussoria deve essere emessa e firmata digitalmente; essa deve essere altresì verificabile telematicamente presso l'emittente ovvero gestita mediante ricorso a piattaforme operanti con tecnologie basate su registri distribuiti ai sensi dell'art. 8-ter, comma 1, del decreto-legge 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla legge 11 febbraio 2019, n. 12.
4. Il beneficiario della polizza fideiussoria è il Consiglio regionale della Lombardia.
5. La cauzione (o fideiussione) è prestata a garanzia dell'adempimento di tutte le obbligazioni del contratto e del risarcimento dei danni derivanti dall'eventuale inadempimento delle obbligazioni stesse, salva comunque la risarcibilità del maggior danno.
6. Il Consiglio regionale ha il diritto di valersi della garanzia, nei limiti dell'importo massimo garantito, per l'eventuale maggiore spesa sostenuta per il completamento dei servizi nel caso di risoluzione del contratto disposta in danno dell'esecutore e ha il diritto di valersi della cauzione per provvedere al pagamento di quanto dovuto dall'esecutore per le inadempienze derivanti

dalla inosservanza di norme e prescrizioni dei contratti collettivi, delle leggi e dei regolamenti sulla tutela, protezione, assicurazione, assistenza e sicurezza fisica dei lavoratori comunque presenti nei luoghi dove viene prestato il servizio.

7. La garanzia cessa di avere effetto solo alla data di emissione del certificato di regolare esecuzione. Il Consiglio regionale può richiedere all’Affidatario la reintegrazione della garanzia ove questa sia venuta meno in tutto o in parte. Diversamente, il Consiglio regionale si riserva la facoltà di avvalersi della clausola di cui all’articolo 14, comma 1, lettera d).
8. Ai sensi di legge la garanzia è svincolata dopo l’accertamento, da parte del DEC, della completa ottemperanza alle clausole contrattuali.

Art. 20 - Divieto di “pantouflage” e relative sanzioni

1. Ai sensi dell’articolo 53, comma 16-ter, del d.lgs. 30 marzo 2001, n. 165, i dipendenti che, negli ultimi tre anni di servizio, hanno esercitato poteri autoritativi o negoziali per conto delle pubbliche amministrazioni di cui all'articolo 1, comma 2, del medesimo decreto legislativo, non possono svolgere, nei tre anni successivi alla cessazione del rapporto di pubblico impiego, attività lavorativa o professionale presso i soggetti privati destinatari dell'attività della pubblica amministrazione svolta attraverso i medesimi poteri.
2. I contratti conclusi e gli incarichi conferiti in violazione di tale divieto sono nulli ed è fatto divieto ai soggetti privati che li hanno conclusi o conferiti di contrattare con le pubbliche amministrazioni per i successivi tre anni, con obbligo di restituzione dei compensi eventualmente percepiti e accertati a essi riferiti.

Art. 21 – Rispetto del codice di comportamento dei dipendenti pubblici e del personale del Consiglio regionale della Lombardia

1. Il Fornitore, con la sottoscrizione del presente Foglio Patti e condizioni, si impegna a osservare e a far osservare ai propri dipendenti e collaboratori a qualsiasi titolo gli obblighi di condotta previsti dal d.p.r. 16 aprile 2013, n. 62 “Codice di comportamento dei dipendenti pubblici” pubblicato nella Gazzetta Ufficiale n. 129 del 4 giugno 2013 e dal Codice di Comportamento del personale del Consiglio regionale della Lombardia adottato con Deliberazione dell’Ufficio di Presidenza 24 ottobre 2022 n. 356, allegato alla richiesta di preventivo e comunque disponibile sul sito istituzionale del Consiglio regionale.

Art. 22 – Rispetto del Patto di integrità e relative sanzioni

1. Il Fornitore si impegna a osservare e a far osservare ai propri dipendenti e collaboratori a qualsiasi titolo gli obblighi di condotta previsti dal Patto di integrità (di seguito Patto) per le procedure di affidamento di lavori, servizi e forniture, approvato con deliberazione dell’Ufficio di presidenza 28 ottobre 2015, n. 400, allegato alla documentazione di procedura e comunque disponibile sul sito istituzionale del Consiglio regionale.
2. In esso i riferimenti al d.lgs. 163/2006 e al d.lgs. 50/2016, devono intendersi riferiti alle corrispondenti disposizioni del Codice, ai sensi dell’articolo 226, comma 5, del Codice stesso.

3. Il Fornitore ha l'onere di pretendere il rispetto del Patto anche dai propri subfornitori. La clausola che prevede il rispetto degli obblighi derivanti dal Patto deve essere inserita nei contratti stipulati dall'Affidatario con i propri subfornitori.
4. La violazione degli obblighi del Patto da parte del Fornitore comporta, alternativamente o cumulativamente, l'applicazione di una penale di cui all'articolo 11, comma 3, lettera e), la revoca dell'affidamento, la risoluzione del contratto ai sensi dell'articolo 1456 del Codice civile.
5. Il Consiglio regionale può non avvalersi della risoluzione del contratto qualora lo ritenga pregiudizievole agli interessi pubblici, quali indicati dall'articolo 121, comma 2, del Codice del processo amministrativo, approvato con d.lgs. 2 luglio 2010, n. 104.

Art. 23 - Divieto di cessione del contratto e subappalto

1. La cessione del contratto è nulla, fatte salve le ipotesi previste dall'articolo 120, comma 1, lett. d) del Codice.
2. Il ricorso al subappalto è ammesso nei limiti e con le modalità di cui all'articolo 119 del Codice, fermo restando che non può essere affidata a terzi l'integrale esecuzione delle prestazioni o lavorazioni oggetto del contratto di appalto. Il subappalto è autorizzato dall'Amministrazione qualora ricorrano le condizioni di cui al comma 4 del suindicato articolo. Il Fornitore e il subappaltatore sono responsabili in solido nei confronti della Stazione Appaltante dell'esecuzione delle prestazioni oggetto del contratto di subappalto.
3. I contratti di subappalto sono stipulati, in misura non inferiore al 20 per cento delle prestazioni subappaltabili, con piccole e medie imprese, come definite dall'articolo 1, comma 1, lettera o) dell'allegato I.1 del D. Lgs. 36/2023. Gli operatori economici possono indicare nella propria offerta una diversa soglia di affidamento delle prestazioni che si intende subappaltare alle piccole e medie imprese per ragioni legate all'oggetto o alle caratteristiche delle prestazioni o al mercato di riferimento.
4. Ai sensi dell'articolo 119, comma 3 del Codice, qualora il Fornitore affidi a terze parti prestazioni secondarie, accessorie o sussidiarie in forza di contratti continuativi di cooperazione, servizio o fornitura sottoscritti in epoca anteriore alla indizione della procedura finalizzata all'affidamento del presente servizio è tenuto a trasmettere i relativi contratti al Consiglio regionale prima o contestualmente alla sottoscrizione del contratto di appalto.
5. Fermo quanto previsto all'articolo 16 del presente Foglio Patti e condizioni, nei contratti di subappalto o nei subcontratti comunicati alla stazione appaltante è obbligatorio l'inserimento di clausole di revisione prezzi riferite alle prestazioni o lavorazioni oggetto del subappalto o del subcontratto e determinate incoerenza con quanto previsto degli articoli 8 e 14 dell'allegato II.2-bis, del Codice, che si attivano al verificarsi delle particolari condizioni di natura oggettiva di cui all'articolo 60, comma 2, dello stesso Codice.
6. Nel caso in cui l'esecuzione delle prestazioni affidate in subappalto sia oggetto di ulteriore subappalto si applicano a quest'ultimo le disposizioni previste dall'art.119 del d.lgs. 36/2023 e da altri articoli del codice in tema di subappalto.

Art. 24 - Segnalazione di illeciti nell'Amministrazione da parte dei lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi (c.d. whistleblowing)

1. Ai sensi del d.lgs. 24/2023, i lavoratori e i collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'Amministrazione consiliare che, nell'interesse pubblico e dell'integrità del Consiglio regionale della Lombardia, segnalano al Responsabile della prevenzione della corruzione e della trasparenza (RPCT) del Consiglio regionale le violazioni di norme nazionali ed europee che consistono in illeciti penali, civili, contabili e amministrativi, di cui siano venuti a conoscenza in ragione del rapporto di lavoro/collaborazione, non possono essere sanzionati, demansionati, licenziati, trasferiti, o sottoposti ad altra misura, determinata dalla segnalazione, avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro. L'adozione di misure ritenute ritorsive nei confronti del segnalante può essere segnalata all'ANAC per i provvedimenti di competenza. Sono previste forme di garanzia della riservatezza dell'identità del segnalante il cui nominativo non può essere comunicato se non con il consenso del segnalante o in caso di legittima richiesta dell'Autorità giudiziaria e contabile.
2. L'affidatario è tenuto a informare i propri dipendenti o collaboratori a qualsiasi titolo impegnati in prestazioni o servizi per l'Amministrazione consiliare della tutela di cui al comma 1 e a renderli edotti che sul portale del Consiglio regionale è messa a disposizione, nella sezione "Segnalazione di violazioni nell'amministrazione (whistleblowing)", la "Procedura per la segnalazione di violazioni nell'Amministrazione (c.d. whistleblowing) ai sensi del decreto legislativo 24/2023", con i dati di contatto del RPCT, le istruzioni e il link alla piattaforma web "Segnalazione illeciti", nonché l'informativa sul trattamento dei dati personali.

Art. 25 - Spese di contratto, di registro e accessorie a carico del Fornitore

1. Il contratto Il contratto è stipulato, per corrispondenza secondo l'uso del commercio, ai sensi dell'articolo 18, comma 1, del Codice.
2. Come disciplinato dall'Allegato I.4 del Codice, il contratto è esente dall'imposta di bollo.

Art. 26 - Indirizzo di posta elettronica certificata del Consiglio regionale

1. Le comunicazioni a mezzo di posta elettronica certificata destinate al Consiglio regionale devono essere spedite al seguente indirizzo:

protocollo.generale@pec.consiglio.regione.lombardia.it

Art. 27 - Risoluzione delle controversie e Foro competente

1. In caso di controversie di qualsiasi natura inerenti al contratto e alla sua esecuzione è competente il Foro di Milano.

Art. 28 - Norma finale

1. Per tutto quanto non espressamente previsto nel presente Foglio Patti e condizioni si applica la normativa vigente in materia. Tutti i riferimenti a disposizioni legislative e regolamentari sono da intendersi riferite alla formulazione della norma in vigore al momento dell'aggiudicazione.

CLAUSOLE DEL FOGLIO PATTI E CONDIZIONI DI CUI ALL'ART. 1341 DEL CODICE CIVILE

Ai sensi e per gli effetti dell'articolo 1341 del Codice Civile, sono individuate le clausole di cui agli articoli 10 (Revisione prezzi), 11 (Penali), 12 (Risoluzione ai sensi dell'art. 122 del D. Lgs. 36/2023), 13 (Recesso ai sensi dell'art. 123 del D. Lgs. 36/2023), 14 (Clausola risolutiva ai sensi dell'articolo 1456 del Codice civile), 17 (Trattamento dei dati personali), 21 (Rispetto del codice di comportamento dei dipendenti pubblici e del personale del Consiglio regionale della Lombardia), 22 (Rispetto del Patto di integrità e relative sanzioni) e 27 (Risoluzione delle controversie e Foro competente), del presente Foglio Patti e condizioni.

Allegato D

Atto di designazione come responsabile del trattamento dei dati personali e individuazione dei trattamenti consentiti, delle finalità, della tipologia dei dati personali e dei compiti del responsabile del trattamento, ai sensi dell'art. 28 del Regolamento UE 2016/679 del 27 aprile 2016, per la realizzazione dello studio 'La partecipazione politica in Lombardia'.

PREMESSA

Ai fini del presente Atto, s'intende per:

- **Titolare del trattamento**, ai sensi dell'articolo 4, n. 7, RGPD, il Consiglio regionale della Lombardia [di seguito denominato anche "Consiglio regionale" o "Titolare del trattamento"], C.F. 80053570158, nella persona del dirigente pro tempore dell'Ufficio Contratti e ICT, domiciliato per la carica presso la sede del Consiglio regionale della Lombardia in Milano, via Fabio Filzi n. 22, in conformità alla deliberazione dell'Ufficio di presidenza 1 aprile 2019, n. 111 (Definizione dell'assetto organizzativo privacy – Articolazione delle competenze in materia di protezione in materia di protezione di dati personali (Regolamento (UE) 2016/679 e d.lgs. 2003 come modificato dal d.lgs. 101/2018) e alla deliberazione dell'Ufficio di Presidenza 28 luglio 2021, n. 184 (Aggiornamento 2021 dell'assetto organizzativo privacy) e ss.mm.ii;
- **Responsabile del trattamento**, ai sensi dell'articolo 4, n. 8, RGPD, è il Fornitore, aggiudicatario del servizio, in persona del proprio Legale Rappresentante pro tempore, domiciliato presso la società che rappresenta;
- **Normativa privacy**, 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 e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), di seguito denominato RGPD, il d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, [di seguito denominato: Codice Privacy] e ogni altra disposizione di contenuto normativo sulla protezione dei dati personali applicabile sul territorio nazionale, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali;
- "sub-responsabile del trattamento", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, soggetto terzo, al quale il Responsabile del trattamento abbia affidato l'esecuzione di specifiche attività di trattamento ai sensi dell'art. 28, paragrafi 2 e 4, RGPD;
- "affidamento", il Foglio Patti e condizioni/contratto definito nel decreto di aggiudicazione e/o in ogni altro atto contrattuale tra il Consiglio regionale e il Fornitore;
- per le altre definizioni si rinvia all'art. 4 RGPD.

Il presente atto è stato predisposto al fine di specificare, ai sensi dell'art. 28 del Regolamento (UE) 2016/679, i trattamenti di dati personali affidati dal Consiglio regionale al Fornitore definendo la

durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi gravanti sul Titolare e sul Responsabile del trattamento.

Il **Titolare del trattamento** e il **Responsabile del trattamento** dichiarano reciprocamente di essere informati e di acconsentire che i dati personali forniti o raccolti in conseguenza dell'affidamento sono trattati esclusivamente per le finalità ivi indicate ed in conformità a quanto previsto dalla vigente normativa in materia di protezione dei dati personali.

A tal fine il **Responsabile del trattamento** è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto dell'affidamento e si impegna ad effettuare, per conto del Titolare del trattamento, le sole operazioni di trattamento necessarie a tal fine, nei limiti delle finalità ivi specificate, nel rispetto della Normativa privacy e delle istruzioni fornite, come definitivi nell'Allegato A.1.

Le premesse e gli allegati **A.1** (Elenco dei trattamenti dei dati personali di titolarità del Consiglio regionale della Lombardia effettuati dal Fornitore in qualità di Responsabile del trattamento) e **A.2** (Elenco delle misure di sicurezza applicate dal Fornitore) costituiscono parte integrante e sostanziale del presente Atto.

Rimangono valide le prescrizioni e gli obblighi, anche relativi alle misure di sicurezza applicate, definiti nell'affidamento richiamato in premessa e negli eventuali altri atti allegati allo stesso, nonché in eventuali altri atti successivi stipulati tra le parti.

I dati economici, finanziari, patrimoniali o di qualunque altro genere, che vengano a conoscenza del Fornitore, in ragione dei servizi resi per il Consiglio regionale, sono riservati. Il Consiglio regionale s'impegna a trattare, in conformità al Codice privacy e al RGPD, i dati personali conferiti dal Fornitore per le sole finalità di definizione e gestione del servizio e dei relativi pagamenti, provvedendo alle comunicazioni e alle pubblicazioni dei dati relativi all'affidamento secondo quanto previsto dal d.lgs. 36/2023, dal d.lgs. 33/2013 e dalle altre norme in materia.

BASE GIURIDICA E PRINCIPI

Il trattamento di dati personali è effettuato in quanto indispensabile per il perseguimento delle finalità di ricerca connesse al progetto di cui all'Affidamento. La base giuridica del trattamento è il consenso dei partecipanti alla ricerca e l'esecuzione di un compito di interesse pubblico (art. 6, lett. a) ed e) RGPD).

Il trattamento dei dati personali nell'ambito dell'Affidamento deve essere effettuato in stretta aderenza ai principi di liceità, pertinenza, minimizzazione dei dati e limitazione della conservazione di cui all'art. 5 RGPD, in maniera da garantire un'adeguata sicurezza e da impedire eventuali trattamenti non autorizzati, la perdita o la modificazione accidentale dei dati stessi.

Il trattamento si conforma altresì alle disposizioni specifiche relative al trattamento per finalità di ricerca scientifica e in particolare all'art. 89 del RGPD, agli articoli 104 e seguenti del Codice Privacy e alle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018" (G.U. n. 11 del 14 gennaio 2019), denominate di seguito Regole deontologiche.

DURATA

La designazione a **Responsabile del trattamento** e le clausole del presente Atto hanno durata pari a quella dell’Affidamento.

La designazione e il presente Atto cesseranno automaticamente di avere efficacia in ipotesi di risoluzione, recesso o perdita di efficacia dell’Affidamento, salvo il tempo eventualmente necessario a consentire al Consiglio regionale di recuperare i dati personali, come contrattualmente definito. Parimenti, in caso di rinnovo, proroga e differimento a ogni titolo della durata dell’Affidamento, la designazione e il presente Atto continueranno a produrre i propri effetti senza necessità di ulteriori atti delle parti.

Il **Responsabile del trattamento** s’impegna a mantenere riservati i dati e le informazioni personali conosciute in ragione dei servizi resi e della presente designazione, anche dopo la cessazione di efficacia del presente Atto.

OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

Con riguardo alle tipologie di dati personali e categorie di interessati indicati nell’allegato A.1 del presente Atto, il Consiglio regionale verifica e garantisce, per quanto di competenza in qualità di Titolare del trattamento, la liceità del trattamento e il rispetto dei principi applicabili al trattamento di dati personali, ai sensi della Normativa Privacy, delle norme dello Statuto della Regione Lombardia, del Regolamento generale del Consiglio regionale e delle disposizioni della legge regionale e della legge statale applicabili alle diverse fattispecie e della deliberazione del Consiglio regionale 6 maggio 2014, n. X/378 (Regolamento per il trattamento dei dati personali sensibili e giudiziari di cui è Titolare il Consiglio Regionale della Lombardia (pubblicato sul BURL n. 20 serie ordinaria del 15 maggio 2014).

Il **Titolare del trattamento** s’impegna a fare un uso appropriato dei servizi forniti dal **Responsabile del trattamento** per garantire un livello di sicurezza adeguato e fare un uso responsabile delle credenziali, dei sistemi e dei dispositivi utilizzati per accedere ai servizi forniti dal **Responsabile del trattamento**.

Il **Titolare del trattamento** s’impegna a rispettare i termini per le comunicazioni, le autorizzazioni e le richieste di informazioni e di attivazione dei poteri di verifica di cui al presente Atto.

OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

Il **Responsabile del trattamento** dichiara di avere una struttura e un’organizzazione adeguata all’esecuzione dell’incarico di trattamento dei dati personali del Titolare del trattamento e s’impegna a mantenerla adeguata alla rilevanza dell’incarico stesso, garantendo il pieno rispetto per sé e per i propri dipendenti e collaboratori a qualunque titolo della Normativa Privacy e di quanto prescritto nel presente Atto.

Il **Responsabile del trattamento** esegue esclusivamente i trattamenti di cui all’Allegato A.1, richiesti dal Titolare del trattamento e indispensabili per l’esecuzione delle prestazioni contrattuali in modo lecito e secondo correttezza, per scopi legittimi e determinati assicurando l’esattezza e la

completezza dei dati e garantendo il rispetto dei principi di necessità, proporzionalità, pertinenza e non eccedenza, e garantisce lo svolgimento dei compiti sotto indicati.

In particolare, il **Responsabile del trattamento** tratterà dati personali per la realizzazione di uno studio sulla partecipazione politica finalizzato ad analizzare le dinamiche della partecipazione al voto dei cittadini della Lombardia e le ragioni dell'astensione, anche mediante una rilevazione demoscopica che fornisca informazioni statisticamente significative, indagando le caratteristiche sociodemografiche dell'elettorato lombardo partecipante e non partecipante al voto, le ragioni dell'astensione dalla partecipazione, il rapporto con le istituzioni, la politica e le relative priorità.

Il **Responsabile del trattamento** si impegna a specificare in apposito progetto di ricerca la tipologia di dati personali trattati, le categorie di interessati, le fonti di acquisizione, garantendo la liceità dell'acquisizione dei dati stessi, nonché le misure di sicurezza applicate al trattamento.

Con riguardo ai dati personali e alle categorie di interessati indicati nell'allegato A.1. e raccolti direttamente dal **Responsabile del trattamento**, lo stesso verifica e garantisce, per quanto di competenza in qualità di **Responsabile del trattamento**, la liceità del trattamento e il rispetto dei principi applicabili al trattamento di dati personali, nonché delle **Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 del 19 dicembre 2018 pubblicate sulla G.U n. 11 del 14 gennaio 2019.**

Il **Responsabile del trattamento** provvede direttamente agli adempimenti privacy, compresa la redazione e consegna, previo accordo con il Titolare del trattamento, agli interessati delle informazioni di cui agli artt. 13 e 14 RGPD e delle dichiarazioni liberatorie anche per il rispetto delle previsioni in materia di diritto di cui alla l. 22 aprile 1941, n. 633, qualora necessarie, e all'acquisizione del consenso al trattamento dei dati personali.

Il **Responsabile del trattamento** può acquisire ed utilizzare, ai fini della ricerca, ulteriori dati rispetto ai dati di cui sopra, anche mediante la somministrazione di interviste (telefoniche o meno), questionari, survey e media diaries, previa acquisizione del consenso, e autorizzazione scritta del Titolare del trattamento, che costituirà un'integrazione del presente Atto.

I dati personali non devono essere oggetto di comunicazione e diffusione né di trasferimento su sistemi di soggetti terzi. Il rapporto finale della ricerca deve contenere esclusivamente dati in forma anonima e aggregata, in stretta applicazione dei criteri di minimizzazione del rischio di re-identificazione degli interessati, secondo quanto definito nelle Regole deontologiche e in considerazione di quanto espresso dal EDPB e dal gruppo di lavoro europeo Art. 29 sulle tecniche di anonimizzazione e pseudonimizzazione.

Il **Responsabile del trattamento** si attiene alle istruzioni del Titolare, tra cui rientrano anche le prescrizioni di cui al provvedimento recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni" di cui alla circolare del 18 aprile 2017, n. 2/2017, recante "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»" e, in quanto compatibili, le Linee guida sulla sicurezza nel procurement ICT (Determinazione n. 220/2020 del 17 maggio 2020 Agid), ai provvedimenti di ACN (ad es. in materia di infrastrutture e servizi cloud per le PPAA, Linee guida per la conservazione delle password, atti regolamentari della disciplina cyber).

Il **Responsabile del trattamento** deve adottare tutte le misure di sicurezza appropriate per garantire il rispetto delle citate regole deontologiche, nonché della normativa in materia di protezione dei dati personali. A tal fine è tenuto a presentare un progetto di ricerca, redatto conformemente agli standard metodologici del pertinente settore disciplinare, anche al fine di documentare che il trattamento sia effettuato per idonei ed effettivi scopi statistici o scientifici, in cui siano indicate le misure di sicurezza.

Il **Responsabile del trattamento** è autorizzato a svolgere le attività di trattamento indispensabili per lo svolgimento del servizio affidato, come descritto nell’Affidamento o concordate con il **Titolare** con altro valido atto scritto, attenendosi alla Normativa Privacy e rispettando gli obblighi di cui al presente Atto e alle istruzioni impartite dal Titolare del trattamento, in modo lecito e secondo correttezza, per scopi legittimi e determinati assicurando l’esattezza e la completezza dei dati e garantendo il rispetto dei principi di necessità, proporzionalità, pertinenza e non eccedenza.

Senza specifica autorizzazione del Titolare, il **Responsabile del trattamento** non può effettuare trattamenti di dati personali ulteriori e comunque non finalizzati all’adempimento delle prestazioni contrattuali o di obblighi di legge connessi alle prestazioni contrattuali stesse.

Il **Responsabile del trattamento** non è autorizzato a effettuare copie permanenti dei dati personali, se non su espressa autorizzazione scritta del **Titolare del trattamento** e deve in ogni caso conservare i dati personali temporaneamente acquisiti, solo per il tempo strettamente necessario alle esigenze e agli adempimenti contrattuali con il Consiglio regionale e agli altri obblighi di legge, se previsti; tali dati devono essere cancellati con modalità che ne garantiscano la certa non recuperabilità, documentando per iscritto le operazioni a tal fine eseguite entro tre mesi dalla conclusione dell’affidamento, salvo diversa richiesta del Titolare. I dati personali trattati per l’attività di ricerca verranno consegnati al Consiglio regionale previamente anonimizzati.

Le operazioni di cancellazione sicura e a norma dei dati dai supporti, sistemi e reti del **Responsabile del trattamento** devono essere documentate e in merito dell’avvenuta effettuazione e conclusione positiva delle stesse il Responsabile del trattamento deve rilasciare apposita dichiarazione ai sensi del D.P.R. 445/2000.

Il **Titolare del trattamento** può autorizzare il **Responsabile del trattamento** a copiare, duplicare, riprodurre o registrare i dati indispensabili per l’esecuzione dell’attività affidata, solo per il tempo strettamente necessario allo svolgimento della stessa e mettendo in atto le necessarie precauzioni da concordare con il Titolare del trattamento per la trasmissione/trasferimento e ogni misura di sicurezza necessaria a garantire la riservatezza dei dati tenendo conto dei rischi correlati e della natura anche sensibile dei dati stessi. In ogni caso, il **Responsabile del trattamento** garantisce che la trasmissione/trasferimento dei dati avvenga su canali sicuri o in forma criptata (per esempio, HTTPS e SSH v2; file criptati con password comunicata con altro canale), salvo che sia diversamente richiesto e autorizzato dal Titolare del trattamento.

Salvo con riguardo ai dati e ai documenti resi pubblici dal Titolare del trattamento o che siano tali per natura (per esempio provvedimenti normativi), è fatto assoluto divieto al **Responsabile del trattamento** di diffondere i dati e di comunicarli a terzi, senza previa, espressa e scritta autorizzazione del Titolare del trattamento.

Il **Responsabile del trattamento** non è autorizzato a comunicare a terzi, pubblicare, cedere, donare o altrimenti disporre dei dati personali di titolarità del Consiglio regionale, senza la preventiva ed espressa richiesta o autorizzazione dell'Amministrazione consiliare, salvo non sia richiesto da disposizioni di legge e con riguardo ai dati e ai documenti resi pubblici dal Titolare o che siano tali per natura (per esempio provvedimenti normativi).

Il **Responsabile del trattamento** informa immediatamente il **Titolare del trattamento** qualora a suo parere un'istruzione del Titolare violi la Normativa Privacy.

Personale e altri collaboratori

Il **Responsabile del trattamento** adotta le misure appropriate per garantire la conformità al presente Atto delle attività e dei comportamenti dei suoi dipendenti, altri soggetti –ricercatori, responsabili e persone autorizzate al trattamento– che fossero coinvolti nella ricerca ed eventuali appaltatori e sub-responsabili relativamente al loro ambito di prestazione. Tali soggetti devono adottare una dichiarazione di impegno a conformarsi alle regole deontologiche, al progetto di ricerca e al presente atto.

Il **Responsabile del trattamento** provvede in particolare a che gli operatori assegnati al trattamento sotto la sua autorità, compresi gli amministratori di sistema, siano autorizzati per iscritto o con modalità tracciabile agli specifici trattamenti necessari per lo svolgimento delle loro mansioni e siano adeguatamente istruiti e formati in materia di protezione dei dati personali, predisponendo e attuando un piano di formazione, nonché vincolati legalmente al rispetto degli obblighi di riservatezza di cui al presente Atto (art. 29 RGPD e art. 2-*quaterdecies* d.lgs. 196/2003) mediante la sottoscrizione di apposite dichiarazioni, le cui copie saranno messe a disposizione del Titolare del trattamento su richiesta per l'esercizio delle attività di controllo e vigilanza di propria competenza.

Il **Responsabile del trattamento** provvede altresì affinché ai dati personali accedano solo gli operatori incaricati obbligandoli a conformare il proprio comportamento alle seguenti prescrizioni: a) i dati personali possono essere utilizzati soltanto per gli scopi previsti nell'Affidamento; b) i dati personali devono essere conservati in modo da evitarne la dispersione, la sottrazione e ogni altro uso non conforme alla legge e alle istruzioni ricevute; c) i dati personali di cui si venga a conoscenza in occasione dello svolgimento della prestazione principale o di attività a essa strumentali non possono essere diffusi, né altrimenti utilizzati per interessi privati, propri o altrui; d) i comportamenti non conformi alle norme sulla protezione dei dati personali o l'eventuale smarrimento o perdita dei dati o delle credenziali di autenticazione sono immediatamente comunicati ai referenti del Titolare del trattamento. e) i dati personali sono custoditi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate; f) nel caso di comunicazioni telefoniche o vocali scambiate durante lo svolgimento delle proprie attività in merito a dati personali del Titolare i comportamenti tenuti si conformano alla necessità di garantire la riservatezza delle informazioni trattate.

Il **Responsabile del trattamento** risponde per l'esatta osservanza degli obblighi di riservatezza e per l'esatta e diligente applicazione dei compiti e delle istruzioni di cui al presente atto, da parte

dei propri dipendenti o collaboratori o altre persone fisiche impegnati, su suo incarico, nell'esecuzione delle prestazioni contrattuali.

In relazione ai soggetti incaricati al trattamento che agiscono sotto la sua autorità, il **Responsabile del trattamento** è tenuto a istruirli sulla normativa privacy e sugli obblighi di cui presente Atto, predisponendo ed attuando un piano di formazione destinato ai soggetti incaricati autorizzati al trattamento.

Sistema di autenticazione per gli incaricati del Responsabile

Il **Responsabile del trattamento** è tenuto a predisporre un sistema di autenticazione per gli applicativi/postazioni di lavoro/piattaforme telematiche e analoghi strumenti che consentono l'accesso ai dati personali del **Titolare del trattamento**, che garantisca la riservatezza.

Il **Responsabile del trattamento**, con riguardo al sistema di autenticazione, è tenuto alle seguenti misure minime:

- a) prevedere profili di autorizzazione di accesso per ogni singolo soggetto incaricato/autorizzato al trattamento o gruppo omogeneo e configurarli prima dell'inizio dei trattamenti in modo adeguato alle mansioni svolte e agli ambiti di trattamento affidati;
- b) assicurarsi che a ogni soggetto incaricato/autorizzato sia assegnata una credenziale di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione del soggetto autorizzato al trattamento associato a una parola chiave (*password*) riservata e conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e a uso esclusivo dell'incaricato/autorizzato, eventualmente associato a un codice identificativo o a una parola chiave. Non è ammessa la creazione di credenziali non nominative, salvo specifica richiesta del Titolare;
- c) prescrivere necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso a uso esclusivo del soggetto incaricato/autorizzato al trattamento;
- d) assicurare che per la componente riservata della credenziale di autenticazione siano previste adeguate misure di sicurezza;
- e) richiedere al soggetto interessato di utilizzare sempre le proprie credenziali personali mantenendole riservate, evitando di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire l'individuazione dell'autore del trattamento;
- f) assicurare che la parola chiave, quando prevista sia composta da almeno quattordici (14) caratteri misti alfanumerici; essa non deve contenere riferimenti agevolmente riconducibili all'Incaricato e deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi, ove non presente un ulteriore fattore di autenticazione oltre al codice di identificazione e alla password;
- g) assicurare che l'utenza venga bloccata dopo un numero di tentativi falliti di accesso pari a tre;

- h) assicurare un sistema di reset della password che consenta l'identificazione del richiedente;
- i) assicurare che il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri incaricati, neppure in tempi diversi e assicurare che sia operata la disattivazione delle credenziali di autenticazione o delle abilitazioni di accesso del personale in caso venga a cessare la necessità di accesso da parte del soggetto incaricato autorizzato al trattamento o intervenga un'inattività per più di tre mesi;
- j) predisporre le necessarie procedure affinché, in caso di prolungata assenza o impedimento dell'incaricato/autorizzato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, si possa comunque assicurare la disponibilità di dati o strumenti elettronici;
- k) verificare a intervalli almeno annuali le autorizzazioni in essere;
- l) implementare un sistema di autenticazione a due fattori su richiesta del Titolare in base al livello di rischio dei trattamenti di dati personali e alle prescrizioni delle norme di riferimento;
- m) adottare misure per prevenire e contrastare attacchi informatici di tipo credential stuffing (testing username/password pairs obtained from the breach of another site), brute force (testing multiple passwords from dictionary or other source against a single account) e password spraying (testing a single weak password against)

È consentita l'implementazione di ulteriori o diverse misure di sicurezza rispetto a quanto sopra solo qualora le misure garantiscano un maggior livello di sicurezza, incluso un sistema di autenticazione MFA su richiesta del Titolare.

Il **Responsabile del trattamento** adotta, per la conservazione delle password degli utenti, di adeguate tecniche crittografiche quali le funzioni di derivazione di chiavi crittografiche (Key Derivation Function) che offrono garanzie in caso di loro esfiltrazione dai sistemi informatici del Produttore (cfr. OWASP Password Storage Cheat Sheet, NIST 800-63B Digital Identity Guidelines).

Amministratori di sistema

Per quanto riguarda le attività degli amministratori di sistema svolti su infrastrutture e reti proprie il **Responsabile del trattamento** deve redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche, appositamente designate, dal Responsabile stesso, che espletano nell'ambito delle attività previste dal contratto, funzioni di Amministratori di Sistema (AdS), con la definizione delle funzioni e dell'ambito operativo a ciascuno assegnato, e garantire ogni altra misura per l'assolvimento delle prescrizioni e degli obblighi di cui al provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 sugli amministratori di sistema e successive modifiche e integrazioni.

Il **Responsabile del trattamento** garantisce l'applicazione delle misure previste dal citato Provvedimento del Garante dandone conferma scritta al Titolare su richiesta.

Misure di sicurezza tecniche e organizzative

Il **Responsabile del trattamento** deve assicurare, per le componenti di sua competenza e per tutta la durata dell’Affidamento, in ogni momento, che la sicurezza fisica e logica dei dati oggetto di trattamento sia conforme alle norme vigenti. Le misure di sicurezza adottate, ai sensi dell’art. 32 del RGPD, devono in ogni situazione uniformarsi allo “standard” di maggiore sicurezza fra le disposizioni di legge e gli elementi contrattuali e/o progettuali.

Le misure di sicurezza adottate devono in ogni situazione uniformarsi allo “standard” di maggiore sicurezza fra le disposizioni di legge e gli elementi contrattuali/progettuali indicati nell’Atto di affidamento, tra cui le misure di cui al provvedimento recante “Misure minime di sicurezza ICT per le pubbliche amministrazioni” di cui alla circolare del 18 aprile 2017, n. 2/2017, recante “Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»”, alle Linee guida sulla sicurezza nel procurement ICT (Determinazione n. 220/2020 del 17 maggio 2020 Agid) e ai provvedimenti di ACN (ad es. in materia di infrastrutture e servizi cloud per le PPAA, Linee guida per la conservazione delle password, atti regolamentari della disciplina cyber) e il Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale.

Il **Responsabile del trattamento** è tenuto a implementare e mantenere efficaci le misure tecniche e organizzative, per proteggere i dati del Titolare del trattamento da distruzione, perdita, alterazione, divulgazione o accesso non autorizzati o accidentali

Il **Responsabile del trattamento** si impegna a individuare e adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenendo conto, fra l’altro, della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche nonché della tecnologia applicabile e dei costi di attuazione. Tali misure comprendono, ove opportuno:

- i) la cifratura dei dati personali;
- ii) i mezzi che permettono di garantire la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
- iii) i mezzi che permettono di ripristinare tempestivamente la disponibilità e l’accesso ai dati personali in caso d’incidente fisico o tecnico;
- iv) una procedura (messa a disposizione del titolare su richiesta) mirata a testare, verificare e valutare regolarmente l’efficacia delle misure di sicurezza tecniche e organizzative al fine di garantire la sicurezza del trattamento.

I sistemi del **Responsabile del trattamento** devono in particolare essere dotati di misure di protezione perimetrali logico-fisiche e i sistemi software, i programmi utilizzati e la protezione antivirus devono essere costantemente aggiornati sia sui server sia sulle postazioni di lavoro. L’adeguamento alle misure minime di sicurezza implica, tra l’altro, la presenza di un adeguato sistema informatico che renda possibile:

- l’accesso ai dati tramite sistema di autenticazione;
- la protezione del computer tramite programmi contro il rischio di intrusione e l’accesso abusivo in accordo ai requisiti di legge aggiornati almeno semestralmente e comunque in occasione di ogni

versione disponibile dalla casa costruttrice, anche per i sistemi non connessi in rete o che non accedono a Internet;

- la modifica e l'aggiornamento, ogni qualvolta vi sia la disponibilità e comunque entro un congruo periodo di tempo non superiore a sei mesi, dei programmi utilizzati, o almeno alla valutazione degli impatti sull'aggiornamento.

Il **Responsabile del trattamento** adotta sistemi di back up, di continuità operative e disaster recovery e s'impegna a garantire che l'accesso in rete ai dati personali avvenga su canali sicuri o in forma criptata.

Il **Responsabile del trattamento** s'impegna a garantire l'accesso in rete ai dati personali e la comunicazione degli stessi avvenga su canali sicuri o in forma criptata (per esempio. HTTPS, SSH v2), salvo che sia diversamente richiesto e autorizzato dal **Titolare del trattamento**.

Il **Responsabile del trattamento** effettua test di penetrazione con cadenza periodica (quantomeno al rilascio di ogni major release), adotta un piano di miglioramento che analizzi le vulnerabilità emerse dai VA e PT e dai bollettini di sicurezza pubblici e di fornitori terzi e ne preveda una adeguata gestione/risoluzione, svolgendo periodicamente test di vulnerabilità sugli applicativi messi a disposizione del Titolare.

Il **Responsabile del trattamento** assicura la separazione degli ambienti di test e sviluppo rispetto ad ambienti di produzione e la previsione di misure di accesso mediante credenziali e privilegi diversi in modo da ridurre al minimo i rischi.

Il **Responsabile del trattamento** può aggiornare o modificare le misure di sicurezza garantite al momento dell'Affidamento e/o stabilite nel decreto di incarico o atto successivo a condizione che tali aggiornamenti e modifiche non comportino il degrado della sicurezza complessiva dei servizi e dei sistemi, dandone comunicazione al **Titolare del trattamento**.

Il **Responsabile del trattamento** è tenuto, in caso di modifiche e di implementazioni di nuovi servizi o di regole afferenti ai dispositivi utilizzati nell'ambito dell'incarico richiamato nelle premesse, a condividere con il **Titolare del trattamento** le informazioni che abbiano rilievo sul trattamento dei dati personali ed è tenuto, prima di procedere alla messa in uso di tali implementazioni sui dati stessi a ottenerne l'autorizzazione scritta.

Salvo l'impegno del **Responsabile del trattamento** a fornire tutte le informazioni necessarie al **Titolare del trattamento** per rispettare la Normativa Privacy, gli interventi di modifica e le innovazioni necessarie per la sicurezza dei servizi telematici che non investono la fruizione del servizio e non modificano le modalità di trattamento dei dati né la tipologia dei dati trattati, come interventi sul codice e sulla gestione tecnica della infrastruttura, non sono soggetti a preventiva autorizzazione da parte del **Titolare del trattamento**.

Nello stesso modo, non necessitano di preventiva autorizzazione gli interventi urgenti per la sicurezza e la garanzia di continuità del servizio, per i quali il **Responsabile del trattamento** si impegna a fornire successivamente le informazioni sulle modifiche effettuate al Titolare.

Il **Responsabile del trattamento** garantisce di applicare le misure minime di sicurezza individuate nell'allegato A.2. e le altre misure di sicurezza definite nell'Affidamento. Tra queste rientrano anche le misure di sicurezza definite nel progetto di ricerca.

Il **Responsabile del trattamento** deve descrivere nella relazione in cui descrive il proprio sistema di gestione dei dati personali in conformità al RGPD come le misure tecniche e di sicurezza implementate siano adeguate a garantire che il progetto di ricerca rispetti la normativa privacy, anche documentando esperienze pregresse simili.

Il Titolare, qualora ritenga che le misure ivi indicate non siano sufficienti rispetto al livello di rischio, potrà richiedere l'implementazione di ulteriori misure di sicurezza.

Il **Responsabile del trattamento** è tenuto a fornire, su richiesta del **Titolare del trattamento**, informazioni di dettaglio sulle misure di sicurezza adottate in relazione al trattamento dei dati personali, secondo quanto previsto dal presente atto e dall'art. 32 del RGDP, nonché a documentare l'adozione delle stesse e la valutazione della loro idoneità ai sensi del già menzionato articolo e, in genere, della normativa Privacy.

Il **Responsabile del trattamento** è tenuto a predisporre e mettere a disposizione la documentazione degli strumenti utilizzati per trattare i dati (indicazione del DB utilizzato, strumento di scrittura del codice, sistema di conservazione dei documenti prodotti), definendo le misure di sicurezza poste a tutela dei dati (profili di accesso al DB, crittografia del DB, dialogo tra applicazione e DB e protezione delle password, ecc.).

Il **Responsabile del trattamento** è tenuto altresì a informare immediatamente il **Titolare del trattamento**, nel caso in cui riscontri carenze in relazione alla sicurezza del trattamento, nell'ambito delle verifiche sulle misure di sicurezza adottate nel trattamento dei dati personali, che il **Responsabile del trattamento** è tenuto a effettuare regolarmente.

Con riguardo ai trattamenti di dati personali svolti occasionalmente senza ausilio di strumenti elettronici e informatici, il **Responsabile del trattamento** se nel caso deve provvedere a che gli archivi fisici siano adeguatamente custoditi e l'accesso sia riservato solo ai soggetti autorizzati. Devono essere definite le procedure di deposito, custodia, consegna, restituzione e compartimentazione dei documenti contenenti dati personali e, in ragione della particolare natura dei dati personali, predisposti contenitori separati e serrati con appositi strumenti e definita una procedura di gestione delle chiavi.

Operazioni da eseguire sui dati personali al termine dell'affidamento, anche anticipato

In caso di revoca della designazione come **Responsabile del trattamento** oppure al termine dell'affidamento, anche anticipato per recesso o risoluzione, il **Responsabile del trattamento**, in accordo con il Titolare, è tenuto:

- alla restituzione completa dei dati personali di titolarità del Consiglio regionale, di cui abbia disponibilità, previa anonimizzazione;
- alla distruzione di eventuale documentazione contenente i dati personali di cui all'allegato A.1, salvo sia obbligatorio conservare alcuni documenti in ragione degli adempimenti amministrativi e contabili stabiliti dalla legge o di specifica richiesta da parte del Titolare del trattamento o anonimizzazione;
- alle altre operazioni richieste dal Titolare del trattamento stesso o previste dall'Affidamento, compresa la cancellazione dei dati personali di cui all'allegato A.1. dai supporti elettronici e

informatici utilizzati con modalità che non ne consentano il recupero, in conformità al provvedimento del Garante per la protezione dei dati personali 13 ottobre 2008 in materia di rifiuti di apparecchiature elettriche ed elettroniche (RAEE) e misure di sicurezza dei dati personali, salvo anonimizzazione.

In questo ambito risulta necessario procedere a: a) emanare adeguate istruzioni di comportamento a tutti i soggetti incaricati autorizzati al trattamento; b) effettuare una ricognizione completa di tutti i supporti di memoria che possano essere riutilizzabili (sia su parti di tipo asportabile sia di quelli presenti in aree di memoria interne al sistema operativo od in programmi), ove possano trovarsi dati; c) esaminare tutti i nuovi supporti, sistema operativo e programmi, che vengono inseriti nel sistema di trattamento dei dati, analizzando i possibili rischi ed impartendo specifiche istruzioni ai soggetti incaricati autorizzati al trattamento.

In caso di occasionali trattamenti svolti senza ausilio di strumenti elettronici e informatici, è necessario procedere con la triturazione del supporto al fine di non consentire l'identificazione degli interessati.

Delle operazioni di cancellazione compiute e degli obblighi di conservazione ulteriori, il **Responsabile del trattamento** è tenuto a rilasciare apposita dichiarazione scritta e firmata dal legale rappresentante al **Titolare del trattamento**.

Rimangono ferme le eventuali specificazioni definite nell'Affidamento.

Obblighi di informazione e collaborazione

Il **Responsabile del trattamento** deve fornire la documentazione e le informazioni necessarie in relazione ai servizi svolti e alle misure di sicurezza applicate e dare l'assistenza necessaria per garantire il rispetto della Normativa privacy.

In particolare, il **Responsabile del trattamento** deve dare assistenza e collaborare, fornendo la documentazione e le informazioni necessarie anche con riguardo alle misure di sicurezza, nello svolgimento e nella redazione dei documenti relativi all'analisi del rischio per la protezione dei dati personali e alla valutazione di impatto sulla protezione dei dati personali (art. 32 e 35 RGPD), secondo le procedure di cui alla deliberazione dell'Ufficio di Presidenza 4.11.2019, n. 423 recante "Metodologia per l'analisi del rischio e la valutazione di impatto per la protezione dei dati personali da applicare ai trattamenti di dati personali del Consiglio regionale della Lombardia" e ss.mm.ii.

Il **Responsabile del trattamento**, ai sensi dell'art. 30, paragrafo 2, del RGPD, salva la deroga di cui al medesimo articolo, tiene il registro delle attività relative al trattamento dei dati personali effettuate per conto del Titolare e, su richiesta, mette tale registro a disposizione del Titolare e/o del Garante per la protezione dei dati personali.

Il **Responsabile del trattamento** è comunque tenuto a fornire al Titolare le informazioni necessarie alla compilazione del "Registro delle attività di trattamento" e delle informative sul trattamento dei dati personali per gli interessati, come previsto dalla Normativa privacy, anche curando ogni necessario rapporto con gli eventuali sub responsabili e a mettere a disposizione del **Titolare del trattamento** le informazioni necessarie all'espletamento delle attività di revisione, comprese le ispezioni richieste dallo stesso **Titolare del trattamento** o da altro soggetto da esso autorizzato, al

fine di rilevare il rispetto degli obblighi previsti dalla Normativa privacy e dal contenuto specifico dell’Affidamento del servizio richiamato nel presente Atto.

Il **Responsabile del trattamento** deve evadere tempestivamente le richieste del Titolare e impegnarsi alla collaborazione necessaria in modo da consentire l’esercizio dei diritti da parte degli interessati, richiamati dalla Normativa privacy. Nel caso in cui il **Responsabile del trattamento** riceva, da parte dell’interessato, un’istanza per l’esercizio dei suoi diritti ai sensi degli artt. da 15 a 22 RGPD è tenuto ad evaderla, informando prontamente il **Titolare del trattamento**.

Il **Responsabile del trattamento** deve collaborare attivamente con l’Autorità Garante per la Protezione dei dati personali e le Autorità Pubbliche, per consentire a queste ultime l’esercizio delle proprie attività istituzionali, quali richieste di informazioni, attività di controllo mediante accessi e ispezioni, relativamente ai trattamenti oggetto del presente Atto, informando immediatamente il Titolare di qualsiasi richiesta e/o comunicazione relativa ai dati personali pervenutagli dal Garante e da qualsiasi Autorità.

Qualora il **Titolare** debba svolgere una revisione della valutazione del rischio ai sensi degli articoli 32 e 35 RGPD, il **Responsabile del trattamento** si impegna a fornire le informazioni necessarie anche in merito alle misure di sicurezza applicate.

Designazione di sub–responsabili (art. 28, paragrafi 2 e 4, RGPD)

Il **Responsabile del trattamento** ha la facoltà di ricorrere ad altri responsabili del trattamento di dati personali (sub - responsabili del trattamento) nell’ambito delle attività di trattamento di dati personali per conto del Consiglio regionale della Lombardia. Ai sensi dell’art. 28, paragrafo 2, del RGPD, tale facoltà è da intendersi quale autorizzazione scritta generale da parte del Consiglio regionale della Lombardia, **Titolare del trattamento**, nei confronti del **Responsabile del trattamento** per le attività sopra menzionate, salvo l’obbligo di comunicazione nei termini sotto specificati.

Il **Responsabile del trattamento**, in sede di designazione di sub-Responsabili, deve informare il **Titolare del trattamento**, al fine di consentire, come previsto dall’art. 28 paragrafo 2 RGPD, di poter manifestare eventuale formale opposizione a tale designazione entro e non oltre il termine di quindici giorni dalla ricezione della comunicazione; decorso il termine quest’ultima potrà procedere all’effettuazione delle designazioni nei confronti dei sub-responsabili del trattamento individuati.

In ogni caso, la designazione di un sub-responsabile del trattamento da parte del **Responsabile del trattamento** è possibile a condizione che su tale soggetto siano imposti gli stessi obblighi in materia di protezione dei dati contenuti nel presente Atto, incluse garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti richiesti dalla Normativa privacy e dal rischio correlato al trattamento e che sia la garanzia che il trattamento sia svolto nel territorio dell’Unione Europea o nel territorio di Paesi non appartenenti allo Spazio Economico Europeo ritenuti adeguati tramite decisione della Commissione europea ai sensi degli art. 45 e 46 del Regolamento UE 2016/679.

Il **Responsabile del trattamento** deve inviare al **Titolare del trattamento**, su richiesta di quest'ultimo, la documentazione relativa alla designazione del sub-responsabile del trattamento per l'esercizio delle prerogative stabilite dall'art. 28 RGPD.

Il **Responsabile del trattamento** rimane comunque interamente responsabile nei confronti del Consiglio regionale della Lombardia con riguardo all'adempimento degli obblighi in materia di protezione dei dati da parte del sub-responsabile del trattamento, ai sensi dell'art. 28, paragrafo 4, RGPD ed è tenuto alla gestione di ogni rapporto con tale soggetto a garanzia della protezione dei dati personali di titolarità del Consiglio regionale e al rispetto della Normativa Privacy.

Il **Titolare del trattamento** può in qualsiasi momento verificare le garanzie e le misure tecniche e organizzative del sub-responsabile del trattamento, tramite audit e ispezioni, anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inidonee, il Titolare del trattamento può chiedere la presentazione di garanzie sufficienti entro un termine congruo.

Nel caso in cui all'esito delle verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del RGPD o risulti che il sub-responsabile agisca in modo difforme o contrario alle istruzioni fornite dal Titolare del trattamento, quest'ultimo applicherà al **Responsabile del trattamento** le penali e le ulteriori conseguenze sul contratto previste nell'Affidamento e diffiderà lo stesso a far adottare al sub-responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato.

Il **Responsabile del trattamento** garantisce che i dati personali non siano utilizzati dagli altri sub – responsabili per finalità non connesse allo svolgimento delle prestazioni di cui all'Affidamento, salvo che l'interessato non esprima, in autonomia e in aggiunta a quanto previsto nel presente Atto, valido consenso agli ulteriori trattamenti nel rispetto della Normativa privacy e previa informativa.

Gestione degli incidenti di sicurezza informatica e violazioni di dati personali (*data breach*)

Il **Responsabile del trattamento** è tenuto ad adottare un piano di gestione degli incidenti di sicurezza, conforme alla Normativa Privacy e ai provvedimenti del Garante per la protezione dei dati personali.

Fermo quanto previsto nell'Affidamento, il **Responsabile del trattamento** è tenuto a comunicare al Titolare, senza ingiustificato ritardo, ogni violazione dei dati o di incidenti informatici o altro accadimento che possa aver comportato un impatto sui dati personali del Consiglio regionale della Lombardia, **Titolare del trattamento**, violandone la riservatezza, integrità, disponibilità o comunque esponendoli a rischio, secondo quanto richiesto dalla Normativa privacy vigente.

Il **Responsabile del trattamento** è dotato di un modello di comunicazione al **Titolare del trattamento** per i casi di violazione dei dati personali conforme alla Normativa Privacy e ai provvedimenti del Garante per la protezione dei dati personali.

La comunicazione deve contenere almeno le seguenti informazioni:

- i) la descrizione della natura del *data breach* compresi, ove possibile, le categorie e il numero approssimativo d'interessati colpiti dalla violazione nonché le categorie e il numero approssimativo di registrazioni dei dati personali oggetto della violazione;

- ii) il nome e i dati di contatto del responsabile per la protezione dei dati o di altro punto di contatto del responsabile, presso cui ottenere informazioni ulteriori;
- iii) la descrizione delle probabili conseguenze del *data breach*;
- iv) se del caso, tenendo conto della natura del trattamento, dei servizi e del contratto, la descrizione delle misure adottate dal responsabile o di quelle di cui propone l'adozione per porre rimedio al *data breach* ovvero attenuarne i possibili effetti negativi.

La comunicazione deve avvenire anche qualora la violazione sia solo presunta o esista un sospetto, pur in assenza di certezze.

La comunicazione deve essere rivolta al Dirigente dell'Ufficio Contratti e ICT all'indirizzo: protocollo.generale@pec.consiglio.regione.lombardia.it e sistema.informativo@consiglio.regione.lombardia.it, nonché per conoscenza all'indirizzo rpdp@consiglio.regione.lombardia.it.

Eventuali modifiche o precisazioni sulla procedura possono essere oggetto di separato accordo con il Titolare del trattamento.

Le informazioni e i dati relativi alla violazione sono mantenuti riservati, fermi restando gli obblighi di notifica e comunicazione previsti dagli articoli 33 e 34 RGPD.

Luogo di trattamento e trasferimento di dati personali

I dati personali trattati dal **Responsabile del trattamento** per l'erogazione dei servizi, di cui all'Affidamento, sono ubicati in architetture e storage dedicati o logicamente separati.

Il **Responsabile del trattamento** assicura che la porzione dedicata ai dati del Titolare del trattamento è ubicata nel territorio dell'Unione Europea o nel territorio di Paesi non appartenenti allo Spazio Economico Europeo ritenuti adeguati tramite decisione della Commissione europea ai sensi degli art. 45 e 46 del Regolamento UE 2016/679 presso data center in cui, compatibilmente alla tipologia, vengono eseguite le procedure automatizzate per l'eventuale conservazione, duplicazione, backup e ripristino dei dati.

Il **Responsabile del trattamento** assicura che il trasferimento dei dati personali trattati avvenga su canali sicuri o in forma criptata (per esempio: HTTPS, SSH v2).

Il **Responsabile del trattamento**, in assenza di una decisione della Commissione europea o di garanzie adeguate ai sensi degli artt. 45 e 46 del Regolamento UE 2016/679, non può:

- 1) trasferire i dati personali a un titolare del trattamento o a un responsabile del trattamento in un paese terzo o in un'organizzazione internazionale situati fuori dall'Unione europea;
- 2) trasferire il trattamento di dati personali a un sub - responsabile del trattamento in un paese terzo situato fuori dall'Unione europea;
- 3) far elaborare i dati personali dal responsabile del trattamento in un paese terzo situato fuori dall'Unione europea.

Obblighi del responsabile relativi all'infrastruttura cloud utilizzata per l'erogazione del servizio

In caso di utilizzo di cloud per l'erogazione del servizio, il **Responsabile del trattamento** garantisce di utilizzare un'infrastruttura cloud conforme alle «best-practice» del settore e si impegna a

adeguarla ovvero a mantenerla adeguata alle necessità dell'incarico stesso, garantendo il pieno rispetto degli obblighi e adempimenti previsti dalla normativa europea e italiana in materia.

Il **Responsabile del trattamento** garantisce in particolare di utilizzare un'infrastruttura cloud conforme ai requisiti minimi previsti dai provvedimenti di ACN vigenti, da ultimo dal Regolamento unico per le infrastrutture e i servizi cloud di ACN (Decreto Direttoriale n. 21007/24 del 27 giugno 2024) e ss.mm.ii.

ATTIVITÀ DI VIGILANZA E VERIFICA DEL TRATTAMENTO

Per sorvegliare l'osservanza del presente Atto, il **Titolare del trattamento** può effettuare periodiche azioni di verifica. Tali verifiche possono comportare la richiesta di presentare informazioni, dati, documenti e compilazione di questionari di self-assessment (verifiche documentali) nonché l'effettuazione di test, per esempio di vulnerabilità, e l'accesso a locali o macchine e programmi del **Responsabile del trattamento**.

Per la risposta alle richieste di verifiche documentali, al **Responsabile del trattamento** deve essere concesso un termine di almeno 15 (quindici) giorni, salvo che la richiesta sia dovuta alla necessità di rispondere all'Autorità di controllo o all'Autorità giudiziaria. In tali ultime ipotesi il **Responsabile del trattamento** deve garantire una risposta compatibile con gli obblighi del **Titolare** nei confronti di tali Autorità.

Nell'ambito di tali verifiche il **Responsabile del trattamento** fornisce l'assistenza e il supporto necessario, rispondendo alle richieste del **Titolare del trattamento** in relazione ai dati ed ai trattamenti di cui al presente Atto e non ha diritto a compensi aggiuntivi.

Nel caso in cui, all'esito delle verifiche, ispezioni e audit, le misure di sicurezza dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del RGPD o risulti che il **Responsabile del trattamento** agisca in modo difforme o contrario alle istruzioni fornite dal **Titolare**, quest'ultimo applicherà al **Responsabile del trattamento** le penali e le ulteriori conseguenze sul contratto previste nella Convenzione e diffiderà lo stesso ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato.

Il **Responsabile del trattamento** è tenuto a svolgere e fornire la DPIA o l'analisi dei rischi svolta sul progetto di ricerca oggetto del servizio erogato.

Il **Responsabile del trattamento** è tenuto ad informare il Titolare, mediante relazione scritta, di tutte le attività svolte in conformità a quanto previsto dal Contratto, ogni qualvolta sia ritenuto necessario dal Titolare.

INDIVIDUAZIONE DI MAGGIORI LIVELLI DI SICUREZZA E ADEGUAMENTI ALLA NORMATIVA PRIVACY SOPRAVVENUTA O A ESIGENZE CONTRATTUALI SOPRAVVENUTE

Il **Titolare del trattamento** può proporre al **Responsabile del trattamento** ogni variazione del presente Atto che sia necessaria per adempiere agli obblighi derivanti dalla Normativa Privacy o per tenere conto delle clausole tipo e dei codici di condotta eventualmente adottati ai sensi, rispettivamente, dell'articolo 28, paragrafi 7 e 8, e dell'articolo 40 del RGPD o ai fini delle

certificazioni di cui all'articolo 42.

Il **Responsabile del trattamento** e il **Titolare del trattamento** concordano che provvederanno, se necessario, a integrare o modificare i contenuti del presente Atto in conformità alla Normativa privacy sopravvenuta. Eventuali ulteriori modifiche e integrazioni potranno altresì essere messe a punto in conseguenza degli esiti di nuove valutazioni sui rischi correlati al trattamento e in ragione di evoluzioni tecnologiche rilevanti o comunque per il miglior assolvimento delle prestazioni contrattuali. Il Responsabile del trattamento si impegna a collaborare nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse.

COMUNICAZIONI

Le comunicazioni previste dal presente Atto nei confronti del **Titolare del trattamento** devono essere trasmesse all'indirizzo di posta elettronica certificata del Consiglio regionale (protocollo.generale@pec.consiglio.regione.lombardia.it), all'attenzione del dirigente del Servizio Studi, Valutazione delle Politiche e Qualità della Normazione.

Il **Responsabile del trattamento** ha l'obbligo di comunicare al **Titolare del trattamento** un indirizzo di posta elettronica certificata e gli altri recapiti ai quali inviare le comunicazioni previste dal presente Atto.

DISPOSIZIONI FINALI

In conformità all'art. 82 e ss., il **Responsabile del trattamento** risponde di ogni perdita, costo, spesa, multa e/o sanzione, danno derivante da o in connessione con una qualsiasi violazione delle disposizioni della Convenzione, del decreto di incarico o altro atto, della normativa privacy e dei compiti e istruzioni di cui al presente Atto da parte sua, dei suoi dipendenti o collaboratori o degli eventuali altri responsabili del trattamento di sua designazione.

Il presente Atto e lo svolgimento degli obblighi e attività in esso previsti non comporta alcun diritto del **Responsabile del trattamento** a uno specifico compenso e/o indennità e/o rimborso.

Per le controversie relative al presente atto, si applicano le disposizioni previste nell'Affidamento.

Per tutto quanto non previsto espressamente nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

DATI DI CONTATTO DEI RESPONSABILI DELLA PROTEZIONE DEI DATI PERSONALI (RPD)

Il RPD del Consiglio regionale della Lombardia è contattabile ai seguenti recapiti: rpdp@consiglio.regione.lombardia.it e protocollo.generale@pec.consiglio.regione.lombardia.it.

Il **Responsabile del trattamento** ha l'obbligo di comunicare il nominativo e i dati di contatto del proprio Responsabile per la protezione dei dati personali (art. 37 e ss. del RGPD). Qualora il Fornitore non sia obbligato a nominare il Responsabile della protezione dei dati, sarà tenuto a mettere a disposizione uno specifico indirizzo di posta elettronica per le comunicazioni in materia di protezione dei dati personali.

Il **Responsabile del trattamento** e il **Titolare del trattamento** si danno reciproca informazione di eventuali modifiche relative ai propri Responsabili della protezione dei dati personali o referenti privacy.

ALLEGATI

A.1 *“Elenco dei trattamenti dei dati personali di titolarità del Consiglio regionale della Lombardia affidati al Responsabile del trattamento”*

A.2 *“Elenco delle misure di sicurezza applicate dal Fornitore”*

per il **Consiglio regionale della Lombardia**
Il Dirigente pro tempore dell’Ufficio
Contratti e ICT
(firmato digitalmente)

per la società
il Legale Rappresentante
.....
(firmato digitalmente per accettazione)

ALLEGATO A.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI DI TITOLARITÀ DEL CONSIGLIO REGIONALE AFFIDATI AL FORNITORE IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO

Ai sensi dell'art. 28 RGPD, il Responsabile del trattamento, nella persona del rappresentante legale *pro tempore*, è designato, per quanto sia necessario alla corretta esecuzione delle prestazioni contrattuali, quale responsabile del trattamento dei dati personali, per conto del Consiglio regionale della Lombardia, per i trattamenti e i dati personali indicati nella seguente tabella. Eventuali altri trattamenti di dati personali potranno essere eseguiti dal medesimo Responsabile del trattamento solo a seguito di comunicazione/richiesta scritta da parte del Titolare del trattamento.

Servizio affidato	Finalità e ambito dei trattamenti affidati al Responsabile	Modalità di trattamento e principali trattamenti svolti	Tipologia di dati trattati e categorie di interessati	Responsabile CRL di gestione del servizio e referente operativo CRL
Realizzazione di uno studio sulla partecipazione politica finalizzato ad analizzare le dinamiche della partecipazione al voto dei cittadini della Lombardia e le ragioni dell'astensione	Finalità Attività di ricerca. Produzione di report e rapporti di ricerca. Rilevazione demoscopica mediante somministrazione di questionari (survey) Ambito del trattamento Ricerca	Il trattamento è effettuato con l'ausilio di strumenti elettronici e manuali (cartacei). Le operazioni di trattamento autorizzate sono: [X] raccolta [X] registrazione [X] organizzazione [X] strutturazione [X] conservazione ☐ adattamento ☐ modifica ☐ visualizzazione [X] estrazione [X] uso ☐ comunicazione agli interessati e al Consiglio regionale ☐ diffusione ☐ raffronto ☐ interconnessione ☐ limitazione [X] cancellazione secondo le istruzioni del Titolare [X] distruzione secondo le istruzioni del Titolare La trasmissione dei dati personali è consentita solo su espressa autorizzazione del Titolare con modalità sicure (es. file criptati con password comunicata con altro canale).	Dati personali comuni (es. nome, cognome, indirizzo di posta elettronica/telefono, sesso, provincia di residenza, età) Dati personali di particolari categorie: opinioni politiche, convinzioni religiose o filosofiche Altri dati: caratteristiche sociodemografiche dell'elettorato lombardo partecipante e non partecipante al voto, le ragioni dell'astensione dalla partecipazione, il rapporto con le istituzioni, la politica e le relative priorità, previa autorizzazione del Titolare. Interessati: cittadini lombardi (massimo 5.000)	Direttore dell'esecuzione: dirigente Servizio Studi, Valutazione delle Politiche e Qualità della Normazione

		Le prestazioni comportano: - la predisposizione di misure di sicurezza applicativa per garantire integrità, stabilità e riservatezza dei dati personali; - attività tecniche e funzioni di amministratore di sistema; - connessione sicura HTTPS; - la visione in chiaro di dati personali da parte del Fornitore; - l'anonimizzazione dei dati personali. Sono escluse attività di profilazione degli interessati. I dati non possono essere utilizzati per altri scopi (salvo se anonimizzati). Conservazione Il Responsabile provvede alla cancellazione dei dati personali decorsi tre mesi dalla presentazione dei risultati della ricerca, salvo diversa istruzione del Titolare e salvo che il diritto dell'Unione o degli Stati membri, cui è soggetto il Responsabile, prescriva la conservazione dei dati personali o salvo anonimizzazione. Il Responsabile garantisce l'integrale trasferimento dei dati al Titolare o a terzi da questi indicati previa anonimizzazione.		
--	--	--	--	--

ALLEGATO A.2 - ELENCO DELLE MISURE DI SICUREZZA

Fermo quanto stabilito con riguardo a specifiche misure di sicurezza nell'Atto di designazione o definito nel progetto di ricerca o in altro atto contrattuale con il Titolare, il **Responsabile del trattamento** nell'ambito delle attività previste contrattualmente garantisce di applicare le seguenti misure di sicurezza:

Sicurezza applicativa	
Barrare le misure adottate	Misure di sicurezza
X	gestione di più profili con privilegi diversi
X	utilizzo credenziali uninominali
X	autenticazione delle utenze username/password
X	utilizzo di password sicure (almeno quattordici caratteri alfanumerici)
X	cambio periodico delle password (almeno ogni sei mesi)
_	autenticazione utenze multifattore
_	utilizzo di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.)
X	supporto di protocolli sicuri e cifrati (HTTPS, SSH v2, ecc.)
X	ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL)
X	Messaggi di posta elettronica inviati devono essere crittografati tramite protocolli crittografici (TLS / SSL)
_	utilizzo di meccanismi di autenticazione basati su crittografia asimmetrica, a chiave pubblica, fornita dal Fornitore, con lunghezza basata sulla criticità della comunicazione (es. 256 bit per le meno critiche, 512 bit per le più critiche)
X	profili di autorizzazione differenziati tra gli utenti
X	funzionalità di "richiesta creazione o cambio della password al primo accesso"
X	blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso
X	accessi utenti registrati su un archivio (log) non cancellabile con il reset
X	gestione dei log di sistema (accessi, allarmi, ecc.)
_	mascheratura della base dati
X	Encryption/cifratura
_	cifratura delle comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell'ente
X	tracciatura delle accessi
X	tracciatura delle modifiche
X	protezione dei dati estratti

Barrare le misure adottate	Misure di sicurezza
X	validazione dei dati in input
X	protezione delle comunicazioni client/server
_	archivi separati tra dati generici e dati particolari (sensibili e/o giudiziari)
X	aggiornamento periodico software utilizzati
X	utilizzo di programmi contro il rischio di intrusione e accesso abusivo
X	utilizzo di programmi antivirus
_	cancellazione dati di navigazione
_	anonimizzazione dati di navigazione
_	filtraggio di indirizzi IP
X	vulnerability assessment
_	utilizzo per l'accesso a internet di un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dall'ente
_	rispetto della politica di sicurezza dell'ente
_	definizione delle specifiche di sicurezza applicate
_	implementazione delle specifiche di sicurezza nel codice e nella struttura della basedati
X	condivisione della documentazione per gestire il servizio
_	Altro

Sicurezza infrastrutturale	
Barrare le misure adottate	Misura di sicurezza
X	gestione di più profili con privilegi diversi
X	utilizzo credenziali uninominali per quanto attiene le componenti infrastrutturali di competenza del responsabile del trattamento
X	gli utenti non devono essere in grado di disattivare o bypassare le impostazioni di sicurezza
X	autenticazione delle utenze username/password
X	utilizzo di password sicure (almeno quattordici caratteri alfanumerici)
_	autenticazione utenze multifattore
X	utilizzo di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.)
X	uso di protocolli sicuri e cifrati (HTTPS, SSH v2, ecc.)
_	utilizzo di meccanismi di autenticazione basati su crittografia asimmetrica, a chiave pubblica, fornita dal Fornitore, con lunghezza basata sulla criticità della comunicazione (es. 256 bit per le meno critiche, 512 bit per le più critiche)

Barrare le misure adottate	Misura di sicurezza
X	profili di autorizzazione differenziati tra gli utenti
X	funzionalità di “richiesta creazione o cambio della password al primo accesso”
X	blocco dell’utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso
X	accessi utenti registrati su un archivio (log) non cancellabile con il reset
X	gestione dei log di sistema (accessi, allarmi, ecc.)
X	programma di backup dei dati
X	programma di backup delle configurazioni
X	protezione/cifratura dei backup
_	archiviazione separata dati comuni e dati particolari (sensibili e/o giudiziari)
X	programma di test dei restore
X	protezione da malware
X	le applicazioni antivirus e le firme di rilevamento devono essere aggiornate almeno su base settimanale
X	protezione/cifratura delle linee di comunicazione
_	cifratura delle comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell’ente
_	isolamento della rete da altri sistemi
X	protezione del traffico tramite Intrusion Detection System
X	protezione del traffico tramite Intrusion Prevention System
X	protezione del traffico tramite Web Application Firewall
X	protezione/cifratura del file system
X	attivazione delle restrizioni di accesso sul file system
X	tracciatura degli accessi amministrativi
_	tracciatura delle attività amministrative
X	tracciatura degli accessi al database
_	tracciatura degli accessi a file system
X	raccolta centralizzata log
_	utilizzo per l’accesso a internet di un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dal CRL
X	programma di protezione dischi rimovibili
_	programma di controllo piattaforma software
X	soluzione di disaster recovery
_	soluzione dlp applicata al contesto
X	dismissione supporti di archiviazione già utilizzati
X	gestione supporti di archiviazione dismessi

Barrare le misure adottate	Misura di sicurezza
☒	verifica annuale dell'operato degli amministratori
☒	aggiornamento delle soluzioni e dei servizi di sicurezza e adeguamento alle normative UE o nazionali senza costi aggiuntivi
☐	presenza di un SOC del fornitore
☒	dispositivi di sicurezza perimetrale su reti del Fornitore (es. Firewall, sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.)
☒	gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente
☐	Altro

Sicurezza fisica per i trattamenti su supporti non elettronici se occasionalmente svolti

Barrare le misure adottate	Misura di sicurezza
☒	limitazione di accesso ai locali deputati al trattamento
☐	profilazione degli accessi in base a ruolo
☐	utilizzo tessere di accesso uninominali limitazione di accesso agli archivi cartacei
☒	limitazione di accesso agli archivi cartacei
☒	archiviazione cartacea distinta per livello di severità
☐	tracciatura degli accessi ai repository di dati cartacei
☐	tracciatura degli accessi ai locali
☒	presenza di sistemi antieffrazione
☒	videosorveglianza locali
☒	movimentazione materiali in modalità sicura
☒	sigillatura contenitori movimentati
☒	Triturazione della documentazione cartacea contenente dati personali
☒	Definizione di regole per la cancellazione sicura dei dati (es. Modello basato sulla norma DIN 66398)
☐	Altro

Sicurezza Organizzativa

Barrare le misure adottate	Misure di sicurezza
☒	formazione privacy del personale

Barrare le misure adottate	Misure di sicurezza
☒	definizione di procedure per assicurare la segretezza
☒	definizione di un elenco dei dipendenti che saranno impiegati sul singolo progetto e sottoscrizione per ogni dipendente di dichiarazioni di riservatezza/confidenzialità
☒	nomina referente privacy
☒	nomina incaricati del trattamento
☐	presenza dpo
☒	definizione di una procedura di data breach
☒	struttura per la prevenzione e gestione degli incidenti informatici
☒	procedura di ripristino dei dati in caso di incidente fisico o tecnico
☒	consegna, entro il giorno successivo, di un report sugli incidenti di sicurezza avvenuti contenente: tipologia di attacco subito, vulnerabilità sfruttate, sequenza temporale degli eventi e contromisure adottate
☐	adozione delle procedure e politiche di sicurezza definite dall'ente
☐	possesso della certificazione ISO/IEC 27001 o, in assenza, di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di un piano di qualità secondo lo standard ISO 10005
☐	piano di auditing annuale sul sistema di sicurezza da parte di società specializzata, approvata dall'ente
☒	possibilità di auditing a richiesta dell'ente
☐	possibilità di verifiche di conformità dei servizi da parte dell'ente
☐	possesso di certificazioni di sicurezza da parte del personale
☐	consegna, entro il giorno successivo alla richiesta, dei log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT
☒	condivisione della documentazione tecnica (schede tecniche, manuali, guide operative) per la corretta configurazione e gestione degli aspetti di sicurezza
☒	dichiarazione di conformità alla normativa vigente in materia di sicurezza cibernetica e al GDPR
☒	spese per il ripristino della situazione preattacco informatico a carico del Fornitore
☒	utilizzo, previa autorizzazione, di repliche dei dati dell'ente solo nel territorio dell'UE
☐	dichiarazione di disponibilità a far parte di un Comitato di Direzione Tecnica
☒	disponibilità alla sottoscrizione di clausola di non divulgazione
☒	gestione di vulnerabilità scoperte sui prodotti oggetto della fornitura senza costi aggiuntivi
☒	monitoraggio e valutazione continua sulla pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite

Barrare le misure adottate	Misure di sicurezza
_	descrizione dettagliata della soluzione tecniche applicate (dispositivi hardware e software impiegato, modalità operative, politiche di sicurezza)
_	Altro

Nei casi in cui si evidenziasse una non piena corrispondenza tra la tipologia di trattamento prevista per l'esecuzione del servizio e le misure di sicurezza richieste, il **Responsabile del trattamento** s'impegna a comunicarlo per scritto al Titolare, fornendo al medesimo l'effettuata analisi del rischio e indicando le misure di sicurezza ritenute adeguate.

Ulteriori misure di sicurezza potranno essere richieste dal Titolare al **Responsabile del trattamento** qualora alla luce del progetto di ricerca le misure ivi proposte o indicate nell'atto di designazione e nell'allegato A.2 non siano ritenute adeguate al rischio.

Allegato 1 – Deliberazione dell'Ufficio di presidenza 24 marzo 2025, n. 100



Regione Lombardia
IL CONSIGLIO

UFFICIO di PRESIDENZA

Fascicolo CRL.2023/XII.3.2.4.7 Seduta n. 11 del 24/03/2025 Deliberazione n. 100

Presenti i componenti dell'Ufficio di presidenza:

Federico ROMANI

Presidente

Giacomo BASAGLIA COSENTINO

Vice Presidente

Emilio DELBONO

Vice Presidente

Alessandra CAPPELLARI

Consigliere Segretario

Jacopo SCANDELLA

Consigliere Segretario

Assiste il Segretario **Mario DI STEFANO**

OGGETTO: INIZIATIVE DI STUDIO E RICERCA ANNO 2025: 'LA PARTECIPAZIONE POLITICA IN LOMBARDIA': DETERMINAZIONI.

Il Segretario Generale: GIUSEPPINA PANIZZOLI

Struttura proponente:

Servizio Studi, Valutazione delle Politiche e Qualità della Normazione - La Dirigente:
SILVIA SNIDER

Il presente atto si compone di n. 4 pagine, comprensive dell'allegato.

L'UFFICIO DI PRESIDENZA DEL CONSIGLIO REGIONALE

VISTO lo Statuto d'autonomia della Lombardia, approvato con legge statutaria 30 agosto 2008, n. 1, e in particolare l'articolo 22, che sancisce l'autonomia di bilancio, amministrativa, contabile, patrimoniale, funzionale e organizzativa del Consiglio regionale;

VISTO il decreto legislativo 23 giugno 2011, n. 118, e in particolare l'articolo 67, come introdotto dal decreto legislativo 10 agosto 2014, n. 126, a norma del quale le Regioni assicurano l'autonomia contabile del Consiglio regionale;

RICHIAMATA la deliberazione del Consiglio regionale 17 dicembre 2024, n. XII/662, di approvazione del bilancio di previsione finanziario per gli anni 2025-2026-2027 per il funzionamento del Consiglio regionale;

RICHIAMATA la deliberazione dell'Ufficio di presidenza del 18 dicembre 2024, n. 423, di approvazione del documento tecnico di accompagnamento e di assegnazione delle quote di bilancio al Segretario generale e al Datore di lavoro, per gli anni 2025-2026-2027;

CONSIDERATO che il Consiglio regionale si avvale di apporti scientifici di soggetti qualificati per la realizzazione di attività di studio e ricerca per l'esercizio delle proprie funzioni;

CONSIDERATO l'interesse ad approfondire il tema della partecipazione politica dei cittadini lombardi al fine, tra l'altro, di comprendere le ragioni dell'astensione dal voto;

RITENUTO pertanto di prevedere, nell'ambito delle attività di studio e ricerca del Consiglio regionale, la realizzazione dello studio sulla partecipazione politica dei cittadini in Lombardia definito nella scheda allegata, per fornire un contributo di conoscenza e approfondimento avvalendosi di apporti tecnici qualificati per assicurare rigore scientifico;

VERIFICATE da parte del dirigente proponente la legittimità e la regolarità tecnico amministrativa della presente proposta di deliberazione;

VERIFICATA da parte del dirigente del Servizio Programmazione finanziaria e Risorse strumentali la copertura finanziaria della spesa;

all'unanimità dei voti espressi a scrutinio palese

DELIBERA

1. di approvare la realizzazione dello studio 'La partecipazione politica in Lombardia', così come definito nella scheda allegata alla presente deliberazione quale parte integrante e sostanziale;
2. di autorizzare la spesa complessiva massima di euro 38.000,00 che trova copertura alla Missione 1, Programma n. 11, Macroaggregato 103 del bilancio di previsione finanziario 2025-2026-2027 del Consiglio regionale;

3. di dare mandato al dirigente del Servizio Studi, Valutazione delle Politiche e Qualità della Normazione per l'attuazione della presente deliberazione.

Il Segretario
Mario Di Stefano

Il Presidente
Federico Romani

*Documento firmato digitalmente, ai sensi dell'articolo 24 del d.lgs. 7 marzo 2005, n. 82
(Codice dell'amministrazione digitale)*

‘LA PARTECIPAZIONE POLITICA IN LOMBARDIA’

L'attività consiste nella **realizzazione di uno studio sulla partecipazione politica finalizzato ad analizzare le dinamiche della partecipazione al voto dei cittadini della Lombardia e le ragioni dell'astensione**, da concludersi entro sei mesi dall'avvio (salvo proroghe motivate che non potranno superare il limite complessivo di 60 giorni) e con un costo massimo pari ad euro 38.000.

L'attività ricomprende la **presentazione dei risultati dello studio** agli organi consiliari che potrà avere anche forma di evento pubblico.

Lo studio a partire da un'analisi della letteratura a tema dovrà approfondire dinamiche e motivazioni della partecipazione al voto e dell'astensionismo nel territorio lombardo.

Andranno dunque analizzati, in serie storica, i dati sulla partecipazione al voto per le tornate elettorali regionali, politiche ed europee, relativi ai livelli regionale, provinciale e comunale mettendoli possibilmente anche in relazione a variabili sociodemografiche selezionate (ad esempio genere, età, istruzione, reddito).

Ricorrendo a una pluralità di metodologie e strumenti di indagine di tipo qualitativo e quantitativo, compresa una rilevazione demoscopica che fornisca informazioni statisticamente significative almeno a livello provinciale, lo studio dovrà indagare le caratteristiche sociodemografiche dell'elettorato lombardo partecipante e non partecipante al voto, le ragioni dell'astensione dalla partecipazione, il rapporto con le istituzioni, la politica e le relative priorità.