



Regione Lombardia
IL CONSIGLIO

DD N. 131

del 23/04/2024

UFFICIO CONTRATTI E ICT

DECRETO DIRIGENZIALE

Oggetto: SERVIZIO DI REGISTRAZIONE AUDIO E VIDEO DELLE TRASMISSIONI DELLE EMITTENTI TELEVISIVE LOCALI LOMBARDE INDIVIDUATE ANNUALMENTE DAL COMITATO REGIONALE PER LE COMUNICAZIONI DELLA LOMBARDIA (CORECOM) E DI SCOMPOSIZIONE DEI RELATIVI DATI, FINALIZZATI ALL'ESERCIZIO DELLE FUNZIONI DI MONITORAGGIO E VIGILANZA DEL PLURALISMO POLITICO-ISTITUZIONALE NEL PERIODO ELETTORALE SVOLTE DAL CORECOM, PER GLI ANNI 2024, 2025, 2026 E 2027 - AFFIDAMENTO DIRETTO, AI SENSI DELL'ART. 50, COMMA 1, LETT. B) DEL DECRETO LEGISLATIVO N. 36/2023, A INFOJUICE S.R.L. DI CORNEDO ALL'ISARCO (BZ).

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;

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 dell'Ufficio di presidenza 3 giugno 2019, n. 229, di attuazione della digitalizzazione dei decreti del segretario generale, dei decreti dirigenziali e dei decreti del datore di lavoro, e di autorizzazione all'assegnazione ai dirigenti competenti per materia degli stanziamenti del bilancio finanziario gestionale, al fine dell'esercizio, da parte degli stessi, di autonomi poteri di spesa, con effetto dal 1° luglio 2019;
- la deliberazione dell'Ufficio di presidenza 14 dicembre 2021, n. 318, *"III provvedimento organizzativo anno 2021"* che ha, tra l'altro, conferito alla sottoscritta l'incarico di dirigente dell'Ufficio Contratti e ICT con decorrenza dal 1° gennaio 2022;
- la deliberazione dell'Ufficio di presidenza 2 novembre 2021, n. 286, *"Determinazioni per l'organizzazione della struttura amministrativa del Consiglio regionale (II Provvedimento organizzativo anno 2021)."* che ha, tra l'altro, conferito al dottore Roberto Saini l'incarico di dirigente del Servizio per il CORECOM e altre Authority regionali, con decorrenza dal 1° dicembre 2021;
- la deliberazione del Consiglio regionale 19 dicembre 2023, n. XII/108, di approvazione del bilancio di previsione finanziario per gli anni 2024-2025-2026 per il funzionamento del Consiglio regionale;
- la deliberazione dell'Ufficio di presidenza 19 dicembre 2023, n. 327, 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 2024-2025-2026;
- la deliberazione dell'Ufficio di presidenza 28 luglio 2021, n. 184 *"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 28 RGPD, nell'ambito dei contratti pubblici per l'acquisizione di beni, servizi e forniture da loro stipulati per dell'Amministrazione;
- la deliberazione dell'Ufficio di presidenza 29 gennaio 2024, n. 24, recante *"Piano Integrato di Attività e Organizzazione (PIAO) del Consiglio regionale della Lombardia, triennio 2024 - 2026 (anno 2024): approvazione"* e in particolare l'allegato 3 della Sottosezione - Rischi corruttivi e trasparenza anni

2024/2026, che disciplina le misure per l'affidamento di servizi e forniture di importo pari o superiore a euro 20.000,00 e inferiore a euro 140.000,00 e individua le fasce economiche per l'applicazione del principio di rotazione degli affidamenti;

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 1° aprile 2023, con efficacia dal 1° luglio 2023 e, in particolare, le seguenti disposizioni:

- 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 per le fasi di programmazione, progettazione, affidamento e per l'esecuzione di ciascuna procedura soggetta al Codice;
- 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;
- 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"*;
- articolo 52, comma 1 - primo periodo -, ai sensi del quale *"nelle procedure di affidamento di cui all'articolo 50, comma 1 lettere a) e b), di importo inferiore a 40.000,00 euro, gli operatori economici attestano con dichiarazione sostitutiva di atto di notorietà il possesso dei requisiti di partecipazione e qualificazione richiesti"*;
- 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"*;
- 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"*;

VISTO il decreto del Segretario generale 21 dicembre 2023, n. 567, di approvazione del bilancio finanziario gestionale per gli anni 2024-2025-2026 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;

VISTA la richiesta di acquisizione (RDA) n. 38 pervenuta all'U.O. Contratti ed economato, completa di pareri, tramite il sistema documentale EDMA, in data 22 settembre 2023, e le sue successive integrazioni, con la quale il dirigente del Servizio per il CORECOM e altre Authority regionali, ha:

- espresso la necessità di acquisire, mediante affidamento diretto, il servizio costituito dalle seguenti attività:
 - monitoraggio della programmazione del campione di emittenti televisive locali private (nel numero di tre l'anno), individuate dal CORECOM, con riferimento all'area del pluralismo politico-istituzionale, nel periodo ricompreso dal trentesimo giorno precedente alla data del voto fino alla data del voto nonché, in caso di ballottaggio, anche nel periodo successivo e fino alla data di svolgimento dello stesso;
 - svolgimento dell'attività di vigilanza a seguito di segnalazioni ricevute dal CORECOM, riguardanti violazioni da parte dell'emittenza televisiva locale delle disposizioni in materia di parità di accesso ai mezzi di comunicazione nel periodo delle campagne elettorali e referendarie;
- descritto le caratteristiche tecniche delle attività richieste;
- dichiarato che non vi sono convenzioni ARIA S.p.A. o Consip attive per l'erogazione del servizio in oggetto;
- stimato la spesa complessiva massima per l'acquisizione del servizio in euro 36.000,00 (oltre IVA al 22%) e individuato la relativa copertura finanziaria;
- indicato la durata del contratto per gli anni 2024-2025-2026-2027;
- individuato i seguenti operatori economici da invitare a presentare il proprio preventivo:
 - CARES SCRL di Pavia (PV);
 - GECA ITALIA S.R.L. di Roma (RM);
 - ISIMM RICERCHE SRL di Roma (RM);
 - INFOJUICE S.R.L. di Cornedo all'Isarco (BZ);
 - CEDAT 85 S.R.L. di San Vito dei Normanni (BR);

RILEVATO che gli operatori economici da invitare sono stati individuati dalla struttura proponente anche in ragione di analoghi affidamenti presso altri CORECOM regionali o l'AGCOM, fruitori di servizi di monitoraggio di emittenti televisive, nell'ambito di un settore di mercato particolare e del numero ristretto di operatori economici che operano in tale specifico settore di servizi;

CONSTATATO che le prestazioni in oggetto non rivestono interesse transfrontaliero certo, secondo quanto previsto dall'articolo 48, comma 2, del Codice, considerato anche il valore dell'affidamento e le caratteristiche tecniche del servizio;

ACQUISITI AGLI ATTI:

- il parere dell'8 settembre 2023, con cui il dirigente dell'Ufficio segreteria dell'Ufficio di presidenza, prevenzione della corruzione, trasparenza e privacy ha evidenziato, in base a quanto riportato nella RDA e nei suoi allegati, che risulta necessaria la designazione del Fornitore come responsabile del trattamento ai sensi dell'art. 28 RGPD, e ha trasmesso l'apposito atto negoziale di designazione;
- il parere del 15 settembre 2023 con cui l'u.o. Prevenzione, protezione e sicurezza nei luoghi di lavoro e servizi ausiliari ha rilevato, in base a quanto riportato al punto 3, della RDA, che il servizio non rientra nelle fattispecie di cui all'articolo 26 del d.lgs. 81/2008;
- il parere del 21 settembre 2023 con cui il responsabile della u.o. Amministrazione digitale del Consiglio regionale, sulla base della RDA non ha

rilevato problematiche di incompatibilità con l'infrastruttura informatica del Consiglio regionale, esprimendo pertanto parere favorevole;

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

DATO ATTO che:

- in data 28 marzo 2024 la sottoscritta, in qualità di RUP, ai sensi dell'articolo 15 del Codice, ha approvato, mediante sottoscrizione digitale il capitolato d'oneri e relativi allegati, predisposto dalla u.o. contratti ed economato e vistato dal dirigente del Servizio per il CORECOM e altre Authority regionali nella medesima data;
- in data 29 marzo 2024, sono stati invitati, tramite la piattaforma Sintel (ID 181327127), a presentare il proprio preventivo per il servizio in oggetto, entro il termine delle ore 10:00 dell'11 aprile 2024, gli operatori economici individuati nella RDA;
- in data 29 marzo 2024, è stata data informazione circa l'avvio dell'interpello di operatori economici sul portale istituzionale dell'Amministrazione, per consentire l'eventuale consultazione di ulteriori soggetti interessati all'esecuzione del servizio;
- entro il termine stabilito dall'avviso di interpello sopraccitato nessun altro operatore economico ha espresso interesse a presentare il proprio preventivo;
- entro il termine fissato, per la presentazione delle offerte, è pervenuto unicamente il preventivo di INFOJUICE S.R.L., codice fiscale e partita IVA 02663760219, avente ID *Sintel* 1712759703714 del 10 aprile 2024;
- in data 11 aprile 2024, si è proceduto all'apertura della busta amministrativa e alla richiesta di chiarimenti alla INFOJUICE S.R.L.;
- acquisiti i chiarimenti dalla società, in data 12 aprile 2024, si è proceduto all'apertura dell'offerta economica;

DATO ATTO che, in data 16 aprile 2024, il RUP verificata la presenza e la regolarità della documentazione prodotta e ritenuta congrua l'offerta economica presentata, sentito il dirigente della struttura proponente, ha proposto di affidare il servizio in argomento alla INFOJUICE S.R.L. di Cornedo all'Isarco (BZ), alle condizioni e modalità del capitolato d'oneri e relativi allegati e al corrispettivo annuo di euro 8.340,00 (oltre IVA del 22%) per il corrispettivo complessivo di euro 33.360,00 (oltre IVA del 22%) per gli anni 2024-2025-2026-2027, come riportato dal rapporto delle attività generato dalla piattaforma Sintel ID 0939980, unito agli atti;

RITENUTO di affidare il servizio in oggetto in ragione altresì del risparmio ottenuto del 7,3% rispetto all'importo stimato del servizio e dell'idoneità delle esperienze pregresse dichiarate, a INFOJUICE S.R.L. di Cornedo all'Isarco (BZ), codice fiscale e partita IVA 02663760219, al corrispettivo offerto dall'operatore economico in sede di procedura;

RITENUTO di impegnare in favore di INFOJUICE S.R.L. la spesa complessiva di euro 30.524,40 (IVA inclusa) sul bilancio finanziario gestionale per gli anni 2024-2025-2026, con imputazione al capitolo 2239 "*CO.RE.COM - Funzioni proprie - Monitoraggio par condicio*", codifica di V livello U.1.03.02.13.999 "*Altri servizi ausiliari n.a.c.*" come segue:

- anno 2024, euro 10.174,80;
- anno 2025, euro 10.174,80;
- anno 2026, euro 10.174,80;

DATO ATTO che la restante somma di euro 10.174,80 (IVA inclusa) farà carico ai competenti fondi che saranno stanziati nei prossimi bilanci, come segue:

- anno 2027, euro 10.174,80;

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 di affidamento (prot. CRL.2024.0006970, prot. CRL.2024.0007018 e prot. CRL.2024.0007023 del 16 aprile 2024);

DATO ATTO che, trattandosi di servizi per un importo inferiore a euro 40.000,00, si procede alla verifica dei requisiti ai sensi dell'articolo 52, comma 1, del Codice, e secondo le indicazioni e tempistiche di cui al decreto del dirigente dell'Ufficio Segreteria dell'ufficio di Presidenza, prevenzione della corruzione trasparenza e privacy dell'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"*, e pertanto il presente provvedimento è immediatamente efficace;

DATO ATTO, altresì che:

- ai fini della stipulazione del contratto, ai sensi dell'articolo 53, comma 4, del Codice, l'operatore è tenuto a prestare una garanzia definitiva pari al 5% dell'importo contrattuale con le modalità di cui all'articolo 117 del Codice;
- il pagamento del corrispettivo contrattuale, soggetto alla tracciabilità dei flussi finanziari, sarà conforme a quanto previsto dall'articolo 3 della Legge 136/2010 e dagli articoli 6 e 7 della Legge 217/2010;
- ai sensi dell'articolo 18, comma 1, secondo periodo, del Codice, trattandosi di affidamento ai sensi dell'articolo 50 del Codice stesso, il contratto sarà stipulato mediante corrispondenza secondo l'uso commerciale;
- il contratto è sottoposto a clausola risolutiva in caso di successivo accertamento di insussistenza dei requisiti dichiarati, come previsto all'articolo 52, comma 2, del Codice, con l'adozione in tal caso dei provvedimenti e delle comunicazioni ivi previsti;
- ai sensi dell'articolo 18, comma 10, come integrato dall'allegato I.4 del Codice, trattandosi di servizi di importo inferiore a euro 40.000,00, il relativo contratto è esente da imposta di bollo;

RITENUTO di nominare INFOJUICE S.R.L. quale Responsabile del trattamento dei dati ai sensi dell'articolo 28 RGPD, in conformità al parere espresso in data 8 settembre 2023, dal dirigente dell'Ufficio Segreteria dell'Ufficio di presidenza, prevenzione della corruzione, trasparenza e privacy, e come da atto di designazione allegato al capitolato d'onori, sottoscritto dall'operatore economico per accettazione in sede di presentazione del preventivo;

RITENUTO di individuare il direttore dell'esecuzione del contratto (di seguito DEC), ai sensi dell'articolo 32, comma 2, dell'allegato II.14 del Codice, nel dirigente del Servizio per il CORECOM e altre authority regionali, competente anche per l'eventuale modifica dell'impegno di spesa nonché per la liquidazione delle fatture e lo svincolo della garanzia definitiva;

DATO ATTO che il Fornitore fattura i corrispettivi contrattuali secondo le modalità riportate all'articolo 8, comma 4, del capitolato d'onori;

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 negli esercizi finanziari nei quali si prevede che l'obbligazione giuridica venga a scadenza;

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

DECRETA

1. di affidare a INFOJUICE S.R.L., di Cornedo all'Isarco (BZ), ai sensi dell'articolo 50, comma 1, lettera b) del Codice, il servizio in oggetto per gli anni 2024-2025-2026-2027, alle condizioni e modalità di cui al capitolato d'oneri e relativi allegati, al corrispettivo annuale di euro 8.340,00 (oltre IVA del 22%) presentata dalla suddetta società e per un importo complessivo di euro 33.360,00 (oltre IVA del 22%) come riportato nell'offerta economica del 10 aprile 2024, avente ID *Sintel* 1712759703714;
2. di impegnare in favore di INFOJUICE S.R.L. la spesa complessiva di euro 30.524,40 (IVA inclusa) sul bilancio finanziario gestionale per gli anni 2024-2025-2026, con imputazione al capitolo 2239 "*CO.RE.COM – Funzioni proprie – Monitoraggio par condicio*", codifica di V livello U.1.03.02.13.999 "*Altri servizi ausiliari n.a.c.*" come segue:
 - anno 2024, euro 10.174,80;
 - anno 2025, euro 10.174,80;
 - anno 2026, euro 10.174,80;
3. che la restante somma di euro 10.174,80 (IVA inclusa) farà carico ai competenti fondi che saranno stanziati nei prossimi bilanci, come segue:
 - anno 2027, euro 10.174,80;
4. di annettere al presente decreto, quale parte integrante, il capitolato d'oneri disciplinante il servizio in oggetto, unitamente all'Allegato D recante la designazione del Fornitore come responsabile del trattamento ai sensi dell'art. 28 RGPD, approvati dalla sottoscritta, in qualità di responsabile unico del progetto mediante sottoscrizione digitale e accettati tramite sottoscrizione dal Fornitore in sede di presentazione del preventivo;
5. di nominare quale direttore dell'esecuzione del contratto il dirigente del Servizio per il CORECOM e altre Authority regionali;
6. di nominare INFOJUICE S.R.L. quale responsabile del trattamento dei dati personali ai sensi dell'articolo 28 RGPD, come da atto di disciplina dei trattamenti (allegato D al capitolato d'oneri);
7. di stipulare il contratto, ai sensi dell'articolo 18, comma 1, del Codice, mediante corrispondenza secondo l'uso commerciale, previa acquisizione della garanzia definitiva e della copertura assicurativa di cui, rispettivamente, agli articoli 15 e 16 del capitolato d'oneri;
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)



Regione Lombardia

IL CONSIGLIO

Servizio di registrazione audio e video delle trasmissioni delle emittenti televisive locali lombarde individuate annualmente dal Comitato regionale per le Comunicazioni della Lombardia (CORECOM) e di scomposizione (catalogazione, elaborazione, organizzazione, anche in formato grafico e tabellare, e conservazione) dei relativi dati finalizzati all'esercizio delle funzioni di monitoraggio e vigilanza del pluralismo politico-istituzionale nel periodo elettorale svolte dal CORECOM Lombardia, per gli anni 2024, 2025, 2026 e 2027.

Sommario

Art. 1 - Definizione delle parti	3
Art. 2 - Direttore dell'esecuzione del contratto	3
Art. 3 - Oggetto, finalità, ambito e durata del contratto	3
Art. 4 - Attività di registrazione	4
Art. 5 - Attività di scomposizione dati	5
Art. 6 - Tempi e modalità di svolgimento del monitoraggio	5
Art. 7 - Referente del Fornitore	6
Art. 8 - Importo stimato del servizio. Modalità e termini di pagamento del corrispettivo	6
Art. 9 - Revisione prezzi	7
Art. 10 - Penali	8
Art. 11 - Clausola risolutiva ai sensi dell'art. 1456 del Codice civile	9
Art. 12 - Risoluzione ai sensi dell'articolo 122 del Codice	9
Art. 13 - Recesso ai sensi dell'articolo 123 del Codice	10
Art. 14 - Tracciabilità dei flussi finanziari	10
Art. 15 - Garanzia definitiva	10
Art. 16 - Responsabilità del Fornitore	11
Art. 17 - Divieto di cessione del contratto e subappalto	12
Art. 18 - Trattamento dei dati personali	12
Art. 19 - Patto di riservatezza	15
Art. 20 - Rispetto del Patto di integrità e relative sanzioni	15
Art. 21 - Rispetto del codice di comportamento dei dipendenti pubblici e del personale del CRL	16
Art. 22 - Divieto di "pantouflage" e relative sanzioni	16
Art. 23 - Segnalazione di violazioni nell'Amministrazione (c.d. whistleblowing) da parte dei lavoratori dei collaboratori delle imprese fornitrici	16
Art. 24 - Stipulazione del contratto e spese	17
Art. 25 - Risoluzioni delle controversie e Foro competente	17
Art. 26 - Indirizzo di posta elettronica certificata del CRL	17

Art. 27 - Disposizioni finali	17
CLAUSOLE CONTRATTUALI DI CUI ALL'ART. 1341 DEL CODICE CIVILE	18
ALLEGATO TECNICO 1 AL CAPITOLATO D'ONERI	19
Allegato D	1

Art. 1 - Definizione delle parti

1. Stazione appaltante, nel prosieguo denominata “Amministrazione” o “CRL”, è il Consiglio regionale della Lombardia, codice fiscale n. 80053570158 e P. IVA 09201010965, con sede in via Fabio Filzi n. 22, C.A.P. 20124, a Milano.
2. Fornitore, nel prosieguo denominato anche “Appaltatore”, è l’operatore economico affidatario del servizio.

Art. 2 - Direttore dell’esecuzione del contratto

1. Ai sensi dell’articolo 114, comma 8, del Codice e dell’articolo 32 dell’allegato II.14 del Codice, il CRL individua quale direttore dell’esecuzione del contratto (di seguito DEC) il dirigente del Servizio per il CORECOM e altre Authority regionali.
2. 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 dell’efficiente e della sollecita esecuzione del contratto.
3. L’eventuale variazione del DEC sarà tempestivamente comunicata dal CRL al Fornitore.
4. Il CRL procederà, per il tramite del DEC, all’accertamento della conformità del servizio rispetto alle prescrizioni contrattuali.
5. Il DEC è competente altresì per l’eventuale modifica dell’impegno di spesa, per la liquidazione della fattura, per l’emissione del certificato di regolare esecuzione nonché per lo svincolo della garanzia definitiva.

Art. 3 - Oggetto, finalità, ambito e durata del contratto

1. Il presente capitolato ha per oggetto la disciplina delle seguenti attività:
 - a) registrazione audio e video delle trasmissioni del campione di emittenti televisive locali private, individuate dal CORECOM;
 - b) scomposizione (catalogazione, elaborazione, organizzazione, anche in formato grafico e tabellare, e conservazione) dei dati delle trasmissioni delle emittenti televisive, individuate dal CORECOM.
2. Il servizio è finalizzato all’esercizio della funzione propria attribuita al CORECOM dalla legge 22 febbraio 2000, n. 28 recante “Disposizioni per la parità di accesso ai mezzi di informazione durante le campagne elettorali e referendarie e per la comunicazione politica”, relativa alla vigilanza del rispetto del pluralismo “politico-istituzionale” da parte dell’emittenza televisiva locale, e in particolare:
 - al monitoraggio della programmazione del campione di emittenti televisive locali private, nel numero di tre l’anno, con riferimento all’area del pluralismo politico-istituzionale, nel periodo ricompreso dal trentesimo giorno precedente alla data del voto fino alla data del voto nonché, in caso di ballottaggio, anche nel periodo successivo e fino alla data di svolgimento dello stesso;

- allo svolgimento dell'attività di vigilanza a seguito di segnalazioni ricevute dal CORECOM, riguardanti violazioni da parte dell'emittenza televisiva locale delle disposizioni in materia di parità di accesso ai mezzi di comunicazione nel periodo delle campagne elettorali e referendarie.
- 3. L'individuazione delle tre emittenti da monitorare e della consultazione elettorale o referendaria annuale oggetto del monitoraggio è effettuata dal CORECOM con una deliberazione da assumersi, di norma, entro il 31 gennaio di ogni anno.
- 4. Per ogni anno del contratto, l'attività di monitoraggio, di cui al comma 1, lettera a), viene effettuata con riferimento ad un solo periodo elettorale. Nel caso nella stessa data siano previste più consultazioni elettorali, il monitoraggio del pluralismo politico-istituzionale è svolto considerando tutte le consultazioni previste.
- 5. Per sessione di monitoraggio si intende il periodo necessario all'espletamento da parte del fornitore di entrambe le attività di cui al comma 1, per ciascun anno e per ciascuna emittente televisiva.
- 6. Le specifiche tecniche per l'esecuzione del servizio sono descritte nell'Allegato tecnico n. 1 al presente capitolato d'oneri.
- 7. Il servizio ha decorrenza dalla data di stipulazione del contratto e termina il 31 dicembre 2027.

Art. 4 - Attività di registrazione

1. Per ogni sessione annuale di monitoraggio il Fornitore procede alla registrazione del segnale audio e video dei programmi trasmessi a partire dal trentesimo giorno precedente alla data del voto, con rilevazione 24 ore su 24, delle emittenti televisive locali individuate dal CORECOM. Nel caso delle elezioni comunali, il periodo di monitoraggio comprende anche il periodo relativo all'eventuale turno di ballottaggio.
2. Per l'attività di vigilanza svolta a seguito di segnalazione, l'attività di registrazione viene effettuata per il periodo richiesto dal CORECOM necessario alla individuazione della presunta violazione, da parte dell'emittenza televisiva locale delle disposizioni in materia di parità di accesso ai mezzi di comunicazione nel periodo delle campagne elettorali e referendarie.
3. Le registrazioni devono presentare per tutta la loro durata il marchio dell'emittente, la data e l'ora di messa in onda delle trasmissioni.
4. Le registrazioni devono essere effettuate in formato .wmv, mp4 o in altro formato compatibile, da concordare preventivamente con il CORECOM, e incise su un disco rigido esterno, chiavetta USB o altra memoria di massa portatile che diviene di proprietà del CORECOM al momento della consegna del bene.
5. Il Fornitore deve conservare i supporti audiovisivi delle registrazioni dei programmi trasmessi dai fornitori di servizi di media audiovisivi monitorati per un periodo di almeno 24 mesi successivi alla data di trasmissione degli stessi. Su richiesta del CORECOM, il Fornitore si impegna, altresì, a recapitare, entro 24 ore, presso i locali della sede di Milano del CORECOM (Palazzo Pirelli, via Fabio Filzi, 22), copia del supporto audiovisivo o a trasmettere via mail copia del filmato nei formati indicati dal CORECOM con sovrimpressione di data ed ora.

Art. 5 - Attività di scomposizione dati

1. Il Fornitore dovrà provvedere alla scomposizione delle registrazioni di cui all'articolo 4 secondo le prescrizioni dell'Allegato tecnico n. 1, al presente capitolato d'oneri, trasformandoli in dati di tipo quantitativo e qualitativo.
2. Le risultanze dell'attività di rilevazione e di analisi dei dati svolta devono essere contenute in appositi report da trasmettere con le modalità e nei tempi stabiliti dall'articolo 6.
3. Per report si intendono tutti i documenti (tabelle, grafici, prospetti, etc.) elaborati attraverso specifiche aggregazioni dei dati rilevati in modo da favorire l'interpretazione immediata dei risultati del monitoraggio e l'evidenziazione delle presunte violazioni riscontrate, secondo quanto specificato, con riferimento all'area di monitoraggio politico-istituzionale, nell'allegato tecnico.
4. Il Fornitore dovrà altresì provvedere alla realizzazione di una banca dati che consenta, su richiesta del CORECOM, di effettuare l'elaborazione e l'estrazione dei dati riguardanti la programmazione dell'emittente oggetto dell'atto dell'attività di vigilanza, come indicato nell'Allegato tecnico 1 alla voce "La banca Dati e la Reportistica".

Art. 6 - Tempi e modalità di svolgimento del monitoraggio – Essenzialità delle prestazioni

1. Il monitoraggio della programmazione è effettuato su base bi-settimanale a partire dal trentesimo giorno precedente alla data del voto. Per ogni periodo di monitoraggio è prevista la consegna di un report. Le settimane di monitoraggio partono dalla domenica fino al sabato successivo; il primo monitoraggio bi-settimanale ricomprende anche i giorni decorrenti dal trentesimo giorno precedente la data delle elezioni fino al sabato antecedente la domenica del primo periodo bisettimanale. Per il turno di ballottaggio è previsto un unico monitoraggio.
2. Il Fornitore deve consegnare il disco rigido esterno, la chiavetta USB o altra memoria di massa portatile contenenti le registrazioni eseguite, al protocollo del CRL entro le ore 24:00 del venerdì della settimana successiva al periodo oggetto del monitoraggio.
3. Nello stesso termine indicato al comma precedente, il Fornitore deve inviare, a mezzo PEC, al protocollo del CORECOM, la reportistica indicata nell'Allegato tecnico n.1.
4. Per l'attività di vigilanza svolta a seguito di segnalazione, la consegna delle registrazioni e della reportistica relativa al monitoraggio effettuato deve essere fatta entro sette giorni dall'invio della richiesta.
5. Il CORECOM è proprietario dei report periodici di cui ai commi precedenti e può disporne liberamente.
6. Il CORECOM può richiedere al Fornitore, tramite PEC, chiarimenti, precisazioni e integrazioni alla reportistica di cui ai commi precedenti, che devono essere forniti entro i tre giorni successivi alla data prevista per la consegna degli stessi.
7. Le prestazioni richieste ai commi precedenti è essenziale che siano fornite secondo le indicazioni e nei termini prescritti, al fine di consentire lo svolgimento, in tempo utile, da parte del Corecom, delle funzioni di vigilanza allo stesso attribuite dalla legge 22 febbraio 2000, n. 28.

8. L'amministrazione si riserva la facoltà, fatta salva l'applicazione delle penali di cui all'articolo 10, decorsi tre giorni dai termini stabiliti ai commi 2, 3 e 4 senza che il Fornitore abbia consegnato le registrazioni e i report annuali ivi previsti e decorso il termine di cui al comma 6, senza che il Fornitore abbia ottemperato a quanto ivi richiesto, di non accettare la prestazione e, conseguentemente, di non riconoscere il corrispettivo contrattuale previsto per la stessa. Nel caso in cui gli inadempimenti riguardino un report bi-settimanale non sarà corrisposta la metà del corrispettivo contrattuale annuale previsto.

Art. 7 - Referente del Fornitore

1. Il Fornitore entro il termine di cinque giorni dalla data di stipulazione del contratto, ovvero in caso di esecuzione anticipata delle prestazioni contrattuali, entro cinque giorni dalla data di avvio delle stesse, deve comunicare al DEC il nominativo di un referente per il servizio a cui è attribuito il compito di:
 - a. essere il punto di riferimento del CORECOM presso il Fornitore per tutta la durata del contratto;
 - b. partecipare alle riunioni indette dal DEC per riferire sulle attività svolte e su quelle in corso di svolgimento.
2. La sostituzione del referente, in corso di esecuzione, deve essere comunicata al DEC entro il termine di cinque giorni dall'avvenuta sostituzione.

Art. 8 - Importo stimato del servizio. Modalità e termini di pagamento del corrispettivo

1. L'importo annuale stimato del servizio è pari a euro 9.000,00 (oltre IVA), per un importo complessivo di euro 36.000,00 (oltre IVA).
2. L'Amministrazione riconosce al Fornitore gli importi offerti in sede di presentazione del preventivo ritenuto congruo dal CRL.
3. Il corrispettivo si riferisce a tutte le attività oggetto del presente capitolato eseguite a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali e includono tutti gli oneri e spese derivanti al Fornitore dall'esecuzione del contratto e dall'osservanza di leggi e regolamenti, inclusi imposte, tasse e oneri previdenziali e assistenziali.
4. Il Fornitore fattura il corrispettivo annuale previa consegna al CRL delle registrazioni e dei report relativi al monitoraggio effettuato per il periodo elettorale dell'anno di riferimento e previo rilascio dell'attestazione di regolare esecuzione contrattuale da parte del DEC.
5. Il DEC dispone la liquidazione della fattura per il corrispettivo annuale, dopo aver accertato la sua regolare emissione.
6. L'Amministrazione provvede al pagamento del corrispettivo entro 30 giorni dal ricevimento di regolare fattura in favore del conto corrente indicato dal Fornitore nel modulo di cui all'articolo 14.
7. 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”, e deve riportare obbligatoriamente i seguenti dati:

- Intestazione: Consiglio regionale della Lombardia
 - Sede: via Fabio Filzi, 22 – Milano (MI)
 - 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.1.3.3.2
 - CIG contratto (campo 2.1.2.7), comunicato dopo l’aggiudicazione;
 - Esigibilità IVA (campo 2.2.2.7): S “Scissione dei pagamenti”.
8. Nel caso in cui la fattura sia priva dei dati richiesti al comma precedente, 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.
 9. Eventuali contestazioni o irregolarità di fatturazione, anche diverse da quelle richiamate al comma precedente, sospendono comunque il termine di pagamento, con facoltà per l’Amministrazione di procedere ai sensi del medesimo comma.
 10. Ai sensi dell’articolo 31 del decreto-legge 21 giugno 2013, n. 69, convertito con modificazioni dalla legge 9 agosto 2013, n. 98, al fine di procedere al pagamento delle prestazioni contrattuali, il CRL acquisisce d’ufficio il Documento Unico di Regolarità Contributiva (di seguito DURC).
 11. 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.
 12. In ogni caso, 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 del contratto, previo rilascio del DURC. L’IVA esposta nella fattura deve comunque essere calcolata sul corrispettivo pieno.
 13. Per i pagamenti di importo superiore a euro 5.000,00, il CRL, prima di effettuare il pagamento, procede inoltre alla verifica prevista dall’articolo 48-bis del D.P.R. 29 settembre 1973, n. 602, così come modificata dall’articolo 1, commi 986 e 987, lettere a) e b), della legge 27 dicembre 2017, n. 205, secondo le modalità stabilite dal D.M. 18/01/2008, n. 40.

Art. 9 - Revisione prezzi

1. Ai sensi dell’articolo 60, del Codice, al termine della prima annualità contrattuale, è facoltà del Fornitore e dell’Amministrazione chiedere la revisione dei prezzi, dandone adeguata motivazione, avendo riguardo alle variazioni rilevate dall’ISTAT in riferimento all’indice dei prezzi al consumo delle famiglie di operai e impiegati (indice F.O.I. calcolato al netto dei consumi di tabacchi) avendo riguardo all’indice rilevato nel mese di sottoscrizione del contratto e quello rilevato nel medesimo mese dell’anno successivo.
2. L’Amministrazione si riserva la facoltà di procedere d’ufficio in caso di variazione in diminuzione.
3. La revisione è riconosciuta se le variazioni accertate risultano superiori al 5 per cento dell’importo complessivo del contratto e operano nella misura dell’80 per cento della variazione

stessa, in relazione alle prestazioni da eseguire.

4. I nuovi prezzi determinati a seguito della revisione di cui a questo articolo saranno applicati alle prestazioni contrattuali svolte dopo la revisione a partire dalla prima fatturazione utile.

Art. 10 - Penali

1. Fatte salve le difformità e il ritardo nell'adempimento delle prestazioni descritte nel presente capitolato che siano dovute a cause di forza maggiore o comunque non imputabili al Fornitore, è facoltà del DEC applicare le penali previste dai commi successivi, previa contestazione inviata al Fornitore per il tramite di PEC. Il Fornitore ha facoltà di formulare controdeduzioni, per il tramite di PEC, entro il terzo giorno lavorativo successivo a quello della formale contestazione.
2. Il DEC, valutate le ragioni addotte dal Fornitore, potrà procedere all'applicazione delle seguenti penali:
 - a) in caso di consegna delle registrazioni o dei report oltre i termini stabiliti all'articolo 6, commi 2, 3 e 4, il Fornitore è tenuto a corrispondere, una penale pari all'1 per mille dell'importo netto contrattuale, per ogni giorno di ritardo, fatto salvo quanto previsto all'articolo 6, comma 8;
 - b) in caso di mancato riscontro dei chiarimenti, precisazioni e integrazioni nei termini di cui all'articolo 6, comma 6, è applicata una penale pari all'1 per mille dell'importo netto contrattuale, per ogni giorno di ritardo, fatto salvo quanto previsto all'articolo 6, comma 8;
 - c) in caso di violazione del Patto di integrità di cui all'articolo 20, può essere applicata una penale di importo compreso tra l'1% e il 5% dell'importo netto contrattuale.
3. L'elenco di fattispecie di cui al comma 2 non ha carattere di tassatività. In caso di disservizio o inadempimento diverso da quelli contemplati, il DEC potrà irrogare al Fornitore, in relazione alla gravità del fatto, una penale tra l'1 % e il 5 %, dell'importo netto contrattuale.
4. Tutti i menzionati importi sono da considerarsi IVA esclusa e detraibili dal totale imponibile della fattura successiva all'accertamento della violazione.
5. Le penali sono arrotondate per eccesso alla seconda cifra decimale.
6. In caso di applicazione di penali, è fatto comunque salvo il risarcimento dell'eventuale maggior danno subito dal CRL ai sensi dell'articolo 1382 del Codice civile;
7. Per la riscossione delle penali e la rifusione degli eventuali ulteriori danni e spese il CRL può rivalersi anche tramite trattenuta, per compensazione, sui crediti vantati dal Fornitore nei confronti del CRL, nonché sulla garanzia definitiva prestata che, in tal caso, dovrà essere reintegrata secondo quanto previsto all'articolo 15, comma 7.
8. 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.
9. La richiesta e/o il pagamento delle penali non esonera il Fornitore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere l'obbligo di pagamento della medesima penale, fatto salvo quanto previsto all'articolo 6, comma 8.

Art. 11 - Clausola risolutiva ai sensi dell'art. 1456 del Codice civile

1. Fatta salva l'applicazione delle penali di cui all'articolo 10, il CRL ha altresì facoltà, previa comunicazione scritta, da inviare al Fornitore a mezzo PEC, con cui dichiara che intende avvalersi della presente clausola di risoluzione del contratto ai sensi dell'art. 1456 del Codice civile, con incameramento della garanzia definitiva, al verificarsi di una o più delle seguenti ipotesi:
 - a) in caso di applicazione di penali per un ammontare totale pari al dieci per cento del corrispettivo contrattuale netto;
 - b) in caso di inosservanza dei termini previsti ai commi 2, 3, 4 e 6, dell'articolo 6, per due volte nel corso del contratto;
 - c) in caso di violazione degli obblighi di tracciabilità finanziaria richiamati dall'articolo 14;
 - d) in caso di violazione dei codici di condotta di cui all'articolo 21;
 - e) in caso di violazione del divieto di cessione del contratto o delle norme sul subappalto di cui all'articolo 17;
 - f) 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. 9 aprile 2008, n. 81, oppure inosservanza degli obblighi previsti dai contratti collettivi di categoria, nazionali e regionali, anche dopo la loro scadenza fino alla loro sostituzione, come previsto all'articolo 11 del Codice;
 - g) in caso di mancata completa reintegrazione della garanzia definitiva di cui all'articolo 15, eventualmente escussa, entro il termine di dieci giorni naturali e consecutivi dal ricevimento della relativa richiesta tramite PEC da parte del CRL;
 - h) in caso nello svolgimento delle prestazioni stabilite nel contratto si dovessero verificare ritardi o situazioni di inadempimento tali da non consentire il raggiungimento, nei tempi previsti, degli obiettivi ed interessi pubblici connessi al contratto stesso;
 - i) in caso di sopravvenuti gravi motivi di pubblico interesse.
2. L'Amministrazione potrà dichiarare risolto il contratto a proprio insindacabile giudizio e potrà provvedere a stipulare un nuovo contratto, addebitando al Fornitore le maggiori spese che dovessero derivare da prezzi meno favorevoli per l'Amministrazione stessa e fatto salvo il risarcimento del maggior danno.
3. In tal caso, al Fornitore sarà accreditato il semplice importo del servizio regolarmente effettuato, con deduzione, però, dell'ammontare delle penali per i ritardi eventualmente già maturati al momento della risoluzione; tutto ciò con opportuna salvezza di ogni ragione ed azione per rivalsa di danni in conseguenza dell'inadempimento da parte dello stesso Fornitore dei suoi impegni contrattuali.

Art. 12 - Risoluzione ai sensi dell'articolo 122 del Codice

1. L'Amministrazione può risolvere il contratto ai sensi dell'articolo 122 del Codice.
2. In tutti i casi di risoluzione del contratto il Fornitore ha diritto soltanto al pagamento delle prestazioni relative ai servizi regolarmente eseguiti, 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 Codice

1. L'Amministrazione può recedere dal contratto in qualunque momento ai sensi dell'articolo 123 del Codice.
2. L'esercizio del diritto di recesso è manifestato mediante una formale comunicazione al Fornitore da darsi per iscritto con un preavviso non inferiore a venti giorni.
3. L'Amministrazione può recedere dal contratto in qualunque momento purché tenga indenne l'appaltatore del pagamento delle prestazioni relative ai servizi eseguiti, oltre al decimo dell'importo dei servizi non eseguiti, calcolato secondo quanto previsto dell'allegato II.14 del Codice.

Art. 14 - 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 CRL, 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 CRL da ogni responsabilità per i pagamenti eseguiti.

Art. 15 – Garanzia definitiva

1. Ai sensi dell'articolo 53, comma 4, del Codice, il Fornitore per la sottoscrizione del contratto deve costituire una garanzia definitiva a sua scelta sotto forma di cauzione o fideiussione, pari al 5% dell'importo contrattuale netto. Non si applicano le riduzioni di cui all'articolo 117, co. 2, e all'art. 106, co. 8, D.lgs. 36/2023.
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 può essere rilasciata da imprese bancarie o assicurative che rispondano ai requisiti di solvibilità previsti dalle leggi che ne disciplinano le rispettive attività ovvero dagli intermediari finanziari iscritti nell'albo di cui all'articolo 106 del d.lgs. 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.
4. Il beneficiario della polizza fideiussoria è il CRL.
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 CRL 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 CRL può richiedere al Fornitore la reintegrazione della garanzia ove questa sia venuta meno in tutto o in parte. Diversamente, il CRL si riserva la facoltà di avvalersi della clausola di cui all'articolo 11, comma 1, lettera g).
8. Ai sensi di legge la garanzia è svincolata dopo l'accertamento, da parte del DEC, della completa ottemperanza alle clausole contrattuali.
9. Alla garanzia di cui al presente articolo si applicano le disposizioni in materia di garanzia provvisoria dall'articolo 106 del Codice, ove richiamate dall'articolo 117 del medesimo Codice., salvo quanto previsto al comma 1.

Art. 16 - Responsabilità del Fornitore

1. L'Appaltatore assume in proprio ogni responsabilità per qualsiasi danno causato dallo stesso a persone e/o cose, in virtù dell'esecuzione delle prestazioni contrattuali, ovvero in dipendenza di omissioni, negligenze o altre inadempienze occorse in occasione dell'esecuzione delle prestazioni contrattuali ad esso riferibili, anche se eseguite da parte di terzi nominati dal Fornitore.
2. L'Appaltatore è responsabile altresì per ogni eventuale danno che propri collaboratori, dipendenti, contraenti arrecheranno a persone e/o cose nello svolgimento delle attività connesse al presente capitolato d'oneri.
3. L'Appaltatore si obbliga a manlevare e tenere indenne la Stazione appaltante dalle pretese che terzi dovessero avanzare in relazione ai danni derivanti dall'esecuzione delle prestazioni contrattuali.
4. In ragione di quanto precede, senza limitare o ridurre le obbligazioni assunte in base al presente capitolato d'oneri, per le quali dovrà rispondere integralmente, l'Appaltatore si impegna a stipulare una polizza RCT/O che presti le seguenti garanzie:
 - **Responsabilità civile verso terzi ("RCT")**, per danni (morte, lesioni personali e danni a cose) a Terzi con un massimale non inferiore ad euro 1.000.000 per sinistro e periodo assicurativo in conseguenza a fatti verificatisi in relazione alle attività oggetto del presente appalto, compresa la responsabilità derivante da:
 - danni da interruzione di attività di Terzi;
 - danni da incendio;
 - proprietà, conduzione, locazione e uso di fabbricati e/o macchinari.

Le garanzie di cui sopra dovranno essere presentate con un limite di massimale non inferiore a euro 500.000.

- **Responsabilità civile prestatori d'Opera ("RCO")** per infortuni e le malattie professionali subiti dai prestatori di lavoro di cui l'Appaltatore si avvarrà nell'esercizio della attività svolte oggetto del presente Capitolato con un massimale non inferiore ad euro 1.000.000 per sinistro, con un limite per prestatore infortunato non inferiore ad euro 1.000.000.

Le coperture assicurative avranno efficacia a partire dall'inizio dell'esecuzione del contratto e per tutta la durata contrattualmente prevista.

5. L'Appaltatore dovrà trasmettere al CRL copia delle polizze di cui sopra prima dell'inizio dell'esecuzione del contratto, nonché impegnarsi a presentare copia della quietanza o appendice di proroga alla Società prima della scadenza di ogni periodo assicurativo.
6. L'Appaltatore dovrà dare immediata comunicazione oltre che alla Compagnia di Assicurazione anche al CRL di ogni evento suscettibile di arrecare danno e di ogni sinistro comunque segnalato o avvenuto in danno di persone e/o cose e dovrà tenere aggiornato il CRL di ogni sviluppo in merito.

Art. 17 - Divieto di cessione del contratto e subappalto

1. Il Fornitore esegue in proprio i servizi compresi nel contratto. La cessione del contratto è nulla, fatte salve le ipotesi previste dall'articolo 120, comma 1, lett. d), del Codice.
2. È altresì nullo l'accordo con cui sia affidata a terzi l'integrale esecuzione delle prestazioni contrattuali.
3. Il subappalto è ammesso secondo le disposizioni dell'articolo 119 del Codice, e il Fornitore è tenuto agli obblighi di deposito e comunicazione di cui all'articolo stesso, compresi quelli riferiti ai subcontraenti e alle attività non riconducibili alla definizione di subappalto (contratti continuativi di cooperazione, servizio e/o fornitura sottoscritti in epoca anteriore alla indizione della procedura).
4. In caso di contravvenzione al divieto di cui al comma 1 o di violazione delle procedure di cui al comma 3, il CRL potrà avvalersi della clausola risolutiva di cui all'articolo 11, comma 1, lettera e).
5. Non si configurano come attività affidate in subappalto le prestazioni secondarie, accessorie o sussidiarie rese in favore del Fornitore in forza di contratti continuativi di cooperazione, servizio o fornitura sottoscritti in epoca anteriore all'affidamento del contratto. I relativi contratti sono trasmessi al CRL prima o contestualmente alla sottoscrizione del contratto.

Art. 18 - Trattamento dei dati personali

1. Ai fini del presente capitolato e dei suoi allegati, si 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, non-ché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (di seguito "Codice privacy"), nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile al servizio affidato, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali e le prescrizioni previste dalle "Misure minime di sicurezza ICT per le pubbliche amministrazioni" pubblicate dall'Agid, quando applicabili.

2. Le prestazioni contrattuali comportano l'Affidamento al Fornitore di attività di trattamento, anche con l'ausilio di strumenti elettronici e informatici, 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 o di suo procuratore, assume la qualifica di Responsabile del trattamento dei dati personali trattati, per conto del CRL (Titolare del trattamento), nell'ambito dell'esecuzione delle prestazioni di cui al presente capitolato ed è tenuto alla piena e diligente esecuzione dei compiti indicati nel presente capitolato e nel suo allegato A1, che costituisce parte integrante e sostanziale del capitolato stesso e del relativo contratto.
3. Il Fornitore tratta esclusivamente i dati personali, anche di particolari categorie, rientranti nella titolarità del Consiglio regionale necessari per le attività di monitoraggio e vigilanza sulle trasmissioni radiotelevisive, come definite nel capitolato e nell'allegato tecnico n. 1, sulla base delle disposizioni normative e regolamentari ivi previste, garantendo la funzionalità e sicurezza dei dispositivi a tutela della riservatezza, integrità e disponibilità dei dati. In ogni caso, tutti i dati personali possono essere trattati esclusivamente nell'ambito e solo nei limiti in cui sia indispensabile per effettuare le prestazioni contrattuali.
4. Il Fornitore è obbligato a conservare i dati personali esclusivamente per i tempi stabiliti dal presente contratto e dalle norme di legge applicabili in materia.
5. Il Fornitore deve garantire di avere un'organizzazione adeguata all'esecuzione dell'incarico di trattamento dei dati personali connesso alle prestazioni contrattuali, in termini di conoscenza specialistica, affidabilità, risorse e 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, assicurando il pieno rispetto, per sé e per i propri dipendenti e collaboratori, delle istruzioni sul trattamento dei dati personali dell'allegato A2, oltre che di tutte le norme di legge in materia applicabili. A tale fine il Fornitore è tenuto a trasmettere, su richiesta, 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 con riferimento all'applicativo.
6. Il Fornitore garantisce, per l'ambito di trattamento affidato, la messa in atto delle misure tecniche e organizzative adeguate affinché il trattamento di dati personali avvenga in conformità con le prescrizioni della Normativa Privacy vigente, impegnandosi a consentire al Consiglio regionale le attività di verifica ai sensi dell'art. 28, par. 3, RGPD.

7. Il Fornitore 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) o, qualora non sia tenuto alla nomina, di un referente per le questioni connesse al trattamento dei dati personali, e, salva la deroga di cui all'art. 20, par. 5, RGPD, di tenere il registro delle attività di trattamento dei dati personali effettuate per conto del Titolare e, su richiesta, di mettere tale registro a disposizione del Titolare e/o del Garante per la protezione dei dati personali.
8. In ragione delle attività affidate, il Fornitore s'impegna a redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche, appositamente designate, che svolgeranno le attività con privilegi di amministratore di sistema, definendone le funzioni e gli ambiti operativi di intervento, e garantisce ogni misura per l'assolvimento delle prescrizioni e degli obblighi di cui al provvedimento del Garante per la protezione dei dati personali del 27.11.2008 sugli amministratori di sistema, dandone conferma annuale al Consiglio regionale.
9. Il Fornitore garantisce, 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.
10. Il Fornitore è obbligato a collaborare con il Titolare del trattamento per il rispetto delle norme sulla protezione dei dati personali e a fornire, per quanto di competenza in relazione ai servizi svolti e alle misure di sicurezza applicate, la documentazione e le informazioni necessarie per l'analisi del rischio e la valutazione di impatto sulla protezione dei dati ai sensi degli artt. 32 e 35 RGPD, o che siano comunque necessarie al Titolare per dare attuazione alle norme sulla protezione dei dati personali e per garantire i diritti e le libertà degli interessati, secondo le procedure di cui alla deliberazione dell'Ufficio di presidenza del 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. allegata alla documentazione di gara.
11. La designazione come Responsabile del trattamento è efficace per tutta la durata del rapporto contrattuale, fino alla scadenza dello stesso e conserva la sua efficacia in caso di differimento, rinnovo o proroga. 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.
12. 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. Il Fornitore non potrà trattenere copia dei dati personali rientranti nella titolarità del Consiglio regionale se non per il tempo e le necessità connesse agli adempimenti contrattuali nei rapporti con il Consiglio regionale o ad altri obblighi di legge, se previsti.
13. 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.

14. L'individuazione di ulteriori Responsabili del trattamento dovrà essere effettuata in conformità all'art. 28, par. 2 e 4, RGPD.
15. In conformità all'art. 82 e seguenti, il Responsabile del trattamento risponde di ogni perdita, costo, spesa, danno derivante da o connesso con una qualsiasi violazione delle disposizioni del presente capitolato, della Normativa privacy e dei compiti e istruzioni di cui all'allegato A1 da parte sua, dei suoi dipendenti o collaboratori o degli eventuali altri responsabili del trattamento di sua designazione.
16. Ogni altra attività di trattamento ulteriore rispetto quella di cui al comma 3 rientra nella titolarità autonoma del Fornitore, che in tale veste risponde della liceità del trattamento e del rispetto delle disposizioni in materia di protezione dei dati personali.

Art. 19 – 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 CRL, sono riservati. I dati e le informazioni, non oggetto di pubblicazione in base alla legge, fermo il divieto di cui al comma 13 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 capitolato.
2. Il Fornitore si obbliga 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. Il presente patto di riservatezza deve intendersi vincolante anche dopo la cessazione del contratto.
4. Il CRL s'impegna a trattare, in conformità al d.lgs. 196/2003 e del 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. 36/2016, dal d.lgs. 33/2013 e dalle altre norme in materia, come descritto nell'informativa sul trattamento dei dati personali di cui agli artt. 13 e 14 del RGPD.

Art. 20 - 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 per le procedure di affidamento di lavori, servizi e forniture approvato con deliberazione dell'Ufficio di Presidenza n. 400 del 28 ottobre 2015.

2. Il Fornitore ha l'onere di pretendere il rispetto del Patto anche dai propri subcontraenti. La clausola che prevede il rispetto degli obblighi derivanti dal Patto deve essere inserita nei contratti stipulati dall'appaltatore con i propri subcontraenti.
3. La violazione degli obblighi del Patto da parte del Fornitore comporta, alternativamente o cumulativamente, l'applicazione di una penale di importo compreso tra l'1% e il 5% del valore del contratto, la revoca dell'aggiudicazione, la risoluzione del contratto ai sensi dell'articolo 1456 del Codice civile e l'incameramento della cauzione definitiva. Il CRL può non avvalersi della risoluzione del contratto qualora la 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. 21 - Rispetto del codice di comportamento dei dipendenti pubblici e del personale del CRL

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 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 CRL adottato con Deliberazione dell'Ufficio di Presidenza 24 ottobre 2022 n. 356.

Art. 22 - 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. 23 - Segnalazione di violazioni nell'Amministrazione (c.d. whistleblowing) da parte dei lavoratori dei collaboratori delle imprese fornitrici

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 del CRL che, nell'interesse pubblico e dell'integrità del CRL, segnalano al Responsabile della prevenzione della corruzione e della trasparenza (di seguito RPCT) del CRL 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. Il Fornitore è tenuto a informare i propri dipendenti o collaboratori a qualsiasi titolo impegnati in prestazioni o servizi per il CRL della tutela di cui al comma 1 e a renderli edotti che sul portale del CRL 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. 24 – Stipulazione del contratto e spese

1. Il contratto è stipulato ai sensi dell'articolo 18, comma 1, del Codice, mediante corrispondenza secondo l'uso commerciale.
2. L'imposta di bollo ai sensi del D.P.R. 642/1972, è a carico del Fornitore ed è determinata in base alla tabella di cui all'Allegato I.4. del Codice.

Art. 25 – Risoluzioni delle controversie e Foro competente

1. Per ogni controversia concernente il contratto o comunque connessa all'esecuzione dello stesso si applicano le disposizioni del Libro V, Parte II, Titolo II, del Codice, in materia di rimedi alternativi alla tutela giurisdizionale.
2. Esperiti non utilmente tali rimedi, in caso di controversie di qualsiasi natura inerenti al contratto e alla sua esecuzione, le parti concordano nel riconoscere la competenza esclusiva del Foro di Milano.

Art. 26 - Indirizzo di posta elettronica certificata del CRL

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

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

Art. 27 - Disposizioni finali

1. Ogni modifica o integrazione del presente capitolato o del contratto deve risultare da atto scritto, non essendo ammesse modifiche o integrazioni orali.
2. Per quanto non espressamente previsto dal presente capitolato si applicano le disposizioni di legge vigenti in materia.
3. I rinvii alle disposizioni di legge e ai provvedimenti amministrativi si intendono effettuati ai relativi testi vigenti al momento della sottoscrizione del contratto.

CLAUSOLE CONTRATTUALI 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 6 (Tempi e modalità di svolgimento del monitoraggio – Essenzialità delle prestazioni), 9 (Revisione prezzi), 10 (Penali), 11 (Risoluzione ai sensi dell'articolo 1456 del Codice civile), 12 (Risoluzione ai sensi dell'articolo 122 del Codice), 13 (Recesso ai sensi dell'articolo 123 del Codice), 16 (Responsabilità del Fornitore), 17 (Divieto di cessione del contratto e subappalto), 18 (Trattamento dei dati personali), 19 (Patto di riservatezza), 20 (Rispetto del Patto di integrità e relative sanzioni), 21 (Rispetto del codice di comportamento dei dipendenti pubblici e del personale del CRL) e 25 (Risoluzioni delle controversie e Foro competente) del presente capitolato d'oneri.

ALLEGATO TECNICO n.1 AL CAPITOLATO D'ONERI

Premessa

Il presente Allegato tecnico al capitolato speciale d'oneri (di seguito, "Allegato tecnico") contiene le specifiche tecniche per l'esecuzione del servizio.

Il decreto legislativo 8 novembre 2021, n. 208 (Testo unico dei servizi di media audiovisivi - "TUSMA") indica il principio del pluralismo tra i principi fondamentali del sistema radiotelevisivo (art. 4). In particolare, per garantire il rispetto del principio del cd. "pluralismo interno" il legislatore prevede *"l'accesso di tutti i soggetti politici alle trasmissioni di informazione in condizioni di parità di trattamento e di imparzialità, nelle forme e secondo le modalità indicate dalla legge"* (art. 6, comma 2, lett. c).

La legge 22 febbraio 2000, n. 28, recante "Disposizioni per la parità di accesso ai mezzi di informazione durante le campagne elettorali e referendarie e per la comunicazione politica", come modificata dalla legge n. 313/2003, (d'ora innanzi anche "la Legge") disciplina l'accesso ai mezzi di informazione per la comunicazione politica al fine di *"garantire la parità di trattamento e l'imparzialità rispetto a tutti i soggetti politici"*. La Legge disciplina, in particolare, *"l'accesso ai mezzi di informazione durante le campagne per l'elezione al Parlamento europeo, per le elezioni politiche, regionali e amministrative e per ogni referendum"* (art. 1).

Al fine di garantire la parità di trattamento e l'imparzialità a tutti i soggetti politici, le organizzazioni rappresentative delle emittenti radiofoniche e televisive locali, come previsto dall'art. 11-quater della Legge, hanno adottato il Codice di autoregolamentazione in materia di attuazione del principio del pluralismo, recepito con Decreto del Ministero delle Comunicazioni 8 aprile 2004.

Il programma di informazione è definito dalla Legge come *"il telegiornale, il giornale radio e comunque il notiziario o altro programma di contenuto informativo, a rilevante presenza giornalistica, caratterizzato dalla correlazione ai temi dell'attualità e della cronaca"* (art. 11-ter, comma 1, lett. b), mentre per **programma di comunicazione politica** s'intende *"ogni programma in cui assuma carattere rilevante l'esposizione di opinioni e valutazioni politiche manifestate attraverso tipologie di programmazione che comunque consentano un confronto dialettico tra più opinioni, anche se conseguito nel corso di più trasmissioni"* art. 11-ter, comma 1, lett. c).

Dalla data di convocazione dei comizi per le elezioni e fino alla chiusura delle operazioni di voto, nelle trasmissioni informative riconducibili alla responsabilità di una specifica testata giornalistica registrata, la presenza di candidati, esponenti di partiti e movimenti politici, membri del Governo, delle giunte e consigli regionali e degli enti locali deve essere limitata esclusivamente alla esigenza di assicurare la completezza e l'imparzialità dell'informazione. Tale presenza è vietata in tutte le altre trasmissioni (art. 1, comma 5 della legge 10 dicembre 1993, n. 515).

La vigilanza sul rispetto della Legge è rimessa ai Co.re.com. come funzione propria. L'art. 10 dispone infatti che l'Autorità si avvalga dei Co.re.com. per lo svolgimento dell'attività istruttoria, delineando una forma di cooperazione, *rectius* di collaborazione istruttoria, con i Co.re.com.

Il monitoraggio delle trasmissioni televisive

Il monitoraggio è funzionale ai compiti di vigilanza e controllo sulla programmazione delle emittenti locali affidati ai Co.re.com. In questa sede viene illustrata la metodologia di effettuazione del monitoraggio in materia di pluralismo politico-istituzionale, che i Co.re.com. sono chiamati ad effettuare per adempiere a una funzione propria, attribuita loro dalla Legge e dalle delibere di attuazione dell'Agcom in materia di par condicio nell'esercizio dell'attività di vigilanza in materia di rispetto dei principi generali del sistema radiotelevisivo.

Il monitoraggio consiste in una serie di attività finalizzate alla raccolta sistematica, oggettiva e standardizzata, per ciascun programma registrato, di informazioni o dati elementari. La raccolta sistematica si traduce nell'effettuare rilevazioni con cadenza periodica fissa; nel caso del monitoraggio del pluralismo, la rilevazione dei dati è svolta quotidianamente, 24 ore su 24, su tutta la programmazione televisiva. Con l'espressione raccolta oggettiva e standardizzata si intende che le rilevazioni vengono condotte sulla base di criteri certi, convenzionali e ripetibili.

In particolare, il monitoraggio del pluralismo politico-istituzionale è finalizzato a rilevare nei programmi televisivi:

- tutti i soggetti individuali (la persona fisica, ad esempio, il singolo esponente di un partito politico) e collettivi (ad esempio, un partito politico inteso come l'insieme degli esponenti), che hanno spazio nella programmazione quotidiana trasmessa dai fornitori di servizi di media audiovisivi - cioè i soggetti che parlano o di cui si parla - nella programmazione e i tempi da essi fruiti;
- i temi che i soggetti propongono all'opinione pubblica.

Le principali attività del monitoraggio sono:

- la registrazione dei programmi emessi da ciascun fornitore di servizi media audiovisivi monitorato e la verifica della registrazione effettuata;
- la schedatura dei programmi e la raccolta dei dati secondo criteri predefiniti;
- il controllo di qualità dei dati rilevati (individuazione di eventuali errori di rilevazione);
- la registrazione informatica dei dati rilevati, se non contestuale alla schedatura;
- la verifica dei dati registrati;
- la possibilità di elaborazione statistica dei dati e organizzazione dei dati aggregati in tabelle, secondo format previamente predisposti.

Ai fini della verifica del pluralismo sono oggetto di monitoraggio i seguenti programmi:

- programmi di comunicazione politica (art. 11- ter, l. n. 28/00);

- messaggi autogestiti (artt. 4 e 11- quater, l. n. 28/00);
- programmi di informazione:
 - a) notiziari, con l'eccezione dei servizi teletext;
 - b) programmi di informazione/approfondimento;
 - c) talk show;
 - d) documentari;
 - e) attualità (la rilevazione va condotta su rotocalchi, trasmissioni di servizio, inaugurazioni, premiazioni, manifestazioni di piazza);
 - f) eventi religiosi, con l'esclusione della S. Messa.

Si illustrano di seguito i criteri da seguire per le rilevazioni.

La schedatura dei programmi e la raccolta dei dati

La schedatura e l'analisi dei programmi e la raccolta dei dati rappresentano il passaggio più delicato e impegnativo dell'intero processo lavorativo del monitoraggio. Sebbene la qualità dei dati rilevati dipenda dalla qualità dell'intero processo, in genere le maggiori criticità si riscontrano nel lavoro di analisi dei programmi (computo dei tempi e attribuzione delle categorie dei soggetti e degli argomenti). Inoltre, assumono rilevanza strategica anche altri fattori, riguardanti la struttura organizzativa e, soprattutto, la formazione dei rilevatori, quest'ultima essenziale per la corretta schedatura/analisi della programmazione.

Per ciascuna trasmissione oggetto di monitoraggio, la raccolta dei dati viene effettuata sulla base di una scheda di rilevazione predisposta ad hoc. Nella scheda vengono registrate informazioni/dati elementari relativi a:

- gli elementi identificativi del programma;
- i soggetti individuali e collettivi che fruiscono direttamente lo spazio nel programma per rappresentare personalmente le proprie tesi (c.d. "soggetti che parlano"), ovvero i soggetti che fruiscono indirettamente dello spazio nel programma (soggetti di cui si parla nel corso del programma); per soggetto individuale si intende la persona fisica, ad esempio il singolo esponente di un partito politico, etc.; per soggetto collettivo si intende, ad esempio, un partito politico inteso come l'insieme degli esponenti;
- gli argomenti, vale a dire i temi trattati nel corso del programma anche in relazione ai soggetti che hanno spazio in video (ad esempio, le diverse posizioni sulla riforma del sistema pensionistico);
- la descrizione della struttura della trasmissione (format) e degli eventi informativi che si susseguono in sequenza in ciascun programma e in ciascun telegiornale (c.d. scaletta);
- i tempi fruiti nel programma direttamente dai soggetti per rappresentare personalmente le proprie tesi, in relazione agli argomenti esposti, i tempi fruiti indirettamente dai soggetti di cui si parla nel corso del programma, e i tempi di trattazione dei diversi argomenti.

Il monitoraggio ha carattere eminentemente “quantitativo” perché il rispetto del pluralismo viene verificato principalmente attraverso il computo dei tempi che i media dedicano ai soggetti e ai temi da essi trattati nei diversi programmi.

Oltre ai tempi, comunque, il monitoraggio permette di rilevare altri elementi funzionali alla verifica delle disposizioni di legge in materia di pluralismo; ad esempio, nel caso dei programmi di comunicazione politica, la rilevazione dell’orario di messa in onda, permette di verificare in periodo elettorale la collocazione dei contenitori nelle diverse fasce orarie previste dai regolamenti mentre, in programmi diversi da quelli di comunicazione politica e messaggi autogestiti, la rilevazione degli argomenti può far emergere l’eventuale presenza di indicazioni di voto, vietata dalla normativa vigente.

Gli elementi identificativi

- **Telegiornali**

Costituiscono elementi identificativi di ciascun telegiornale: il fornitore di servizi media audiovisivi; la rete/testata giornalistica; la data di messa in onda; l’edizione; l’orario di messa in onda e di conclusione; la durata complessiva (al netto della pubblicità); il nome del conduttore/dei conduttori.

- **Programmi diversi dai telegiornali:**

Costituiscono elementi identificativi di ciascun programma: il fornitore di servizi media audiovisivi; la rete/testata giornalistica; il titolo del programma; la data di messa in onda; l’orario di messa in onda e di conclusione; la durata complessiva (al netto della pubblicità); la periodicità del programma (giornaliero, settimanale, bi/trisettimanale); il nome del conduttore/dei conduttori.

I soggetti

Per ogni soggetto devono essere rilevate le seguenti informazioni:

- nome e cognome; - sesso; - tempi televisivi dedicati (tempi di parola, di notizia, di antenna, di argomento in relazione ad un soggetto);
- categoria di appartenenza (partito/istituzione).

La classificazione dei soggetti nelle categorie di appartenenza deve essere condotta sulla base di specifici elenchi predefiniti dall’Autorità. In particolare:

- la classificazione dei soggetti del pluralismo politico-istituzionale nei programmi di informazione, compresi i telegiornali, e negli altri programmi, esclusi quelli di comunicazione politica, deve essere effettuata sulla base di elenchi definiti ad hoc per ciascun contesto regionale secondo i criteri definiti dall’Autorità, come riportati nel manuale delle procedure operative del 2009;

- la classificazione dei soggetti della comunicazione politica e dei messaggi autogestiti deve essere condotta sulla base dell'elenco dei soggetti politici aventi diritto secondo le previsioni della legge n. 28/00, come modificata dalla legge n. 313/03 e dalle delibere emanate dall'Autorità

Gli argomenti

Per ciascun argomento trattato nel corso di un programma monitorato, anche in relazione ad un soggetto, devono essere rilevati: descrizione sintetica del/i tema/temi esposto/i; classificazione di ciascun tema/argomento in una specifica macrocategoria e microcategoria, secondo un elenco predefinito; calcolo dei tempi televisivi dedicati: tempo dedicato all'argomento da un singolo soggetto o tempo dedicato all'argomento dall'intera trasmissione, o da parte di essa.

La classificazione degli argomenti deve essere effettuata secondo un elenco di categorie che riproponga, con aggiustamenti funzionali alle peculiarità del monitoraggio locale, quello utilizzato dall'Autorità per le rilevazioni sulle emittenti nazionali. L'elenco dell'Agcom, riportato di seguito, contenuto nell'allegato tecnico al Capitolato speciale d'onori del monitoraggio del pluralismo politico e sociale sui servizi di media audiovisivi e radiofonici in ambito nazionale, pubblicato sul sito dell'Autorità, può essere sottoposto a verifiche periodiche ed essere eventualmente aggiornato. Le modifiche, da apportare all'elenco dell'Autorità ai fini delle rilevazioni di ambito locale, devono essere previamente concordate con l'Agcom.

La tabella seguente elenca le categorie degli argomenti utilizzato per il monitoraggio delle emittenti di ambito nazionale dall'Autorità.

POLITICA E ATTIVITÀ ISTITUZIONALI

Attività di partiti

Elezioni

Amministrazioni locali

Attività del Governo

Attività del Parlamento

Attività del Quirinale

Referendum

Unione europea

Altro

ESTERI

Politica

Cronaca

Medio Oriente

Guerra/pace

Relazioni e organismi internazionali

Terrorismo e criminalità internazionali

Altro

CRONACA

Cronaca giudiziaria

Cronaca nera

Altro

COSTUME E SOCIETÀ

Cronaca rosa

Curiosità

Costume/tendenze

Turismo/viaggi/enogastronomia

Moda

Tempo libero

Altro

MASS MEDIA E SPETTACOLO

Informazione

Mass media e nuove tecnologie

TV

Radio

Cinema

Musica

Teatro

Editoria/libri

CULTURA E ISTRUZIONE

Beni culturali

Scuola

Università

Ricerca

Altro

GIUSTIZIA

Dibattito sulla giustizia

Questioni inerenti ai processi

Questioni inerenti alle carceri

Altro

ECONOMIA, FINANZA E LAVORO

Finanza, Borsa e mercati

Fisco e consumatori

Economia europea

Lavoro e produzione

Occupazione/disoccupazione/condizioni di lavoro

Infortuni sul lavoro

Sindacati e organizzazioni di categoria

Scioperi

Altro

SOCIETÀ

Questioni riguardanti soggetti “deboli”

Droga

Infanzia

I tempi

Per i programmi televisivi, si possono computare cinque diversi tempi:

- tempo di parola;
- tempo di notizia;
- tempo di antenna;
- tempo di argomento in relazione ad un soggetto;
- tempo di argomento.

Nel caso del telegiornale, la verifica del pluralismo viene effettuata su ciascuna edizione, calcolando tutti i tempi sopra indicati. Per quanto attiene agli altri programmi, la verifica del pluralismo è circoscritta al computo dei tempi di parola, di argomento e di argomento in relazione ad un soggetto.

Il **tempo di notizia** è quello dedicato dal giornalista/conduuttore dei programmi di informazione quotidiana (telegiornali) all'illustrazione di un argomento/evento in relazione ad un soggetto individuale (un singolo ministro) o collettivo (ad es. tutto il Governo). A titolo indicativo, se il giornalista parla dei programmi del Ministro dell'Interno, tale tempo di notizia va rilevato come tempo di notizia del singolo ministro e classificato come tempo di notizia della categoria di riferimento “Governo”, che comprende tutti i ministri e sottosegretari; se il giornalista parla del programma di tutto il Consiglio dei Ministri, anche tale tempo di notizia va attribuito alla categoria di riferimento “Governo”.

Il **tempo di parola** è quello in cui ciascun soggetto parla direttamente in voce. Il monitoraggio consiste nel rilevare i singoli interventi in voce di ciascun soggetto e nel classificarli come tempi dei soggetti previsti dagli elenchi allegati. A titolo indicativo, i singoli interventi in voce di un esponente di un partito vengono rilevati come tempi del soggetto individuale e contestualmente attribuiti al partito corrispondente (classificazione). Qualora si voglia conoscere il tempo di parola di un partito politico in un certo periodo, occorre sommare i singoli tempi di parola degli esponenti di quel partito rilevati nel tempo t.

Il **tempo di antenna** è quello complessivamente dedicato a ciascun soggetto individuale e collettivo (sommatoria di tempo di notizia e di parola).

Il **tempo di argomento** in relazione ad un soggetto indica il tempo di parola dedicato da ciascun soggetto individuale alla trattazione di uno specifico argomento (tema). A titolo indicativo, prendendo a riferimento il soggetto “Presidente del Consiglio dei Ministri”, si computano gli interventi in voce (tempi di parola) del Presidente del Consiglio in tema di giustizia, in tema di ambiente, etc..

Il tempo di argomento indica il tempo complessivamente dedicato alla trattazione di un argomento nell’ambito di programmi di informazione quotidiana o di altri programmi. In questo caso, si computano i tempi di tutti i diversi soggetti, giornalisti compresi, che hanno trattato un certo argomento.

La banca dati e la reportistica

Il monitoraggio si conclude con l’implementazione della banca dati, che può essere anche contestuale alla fase di schedatura e analisi. I dati ivi contenuti possono essere utilizzati nell’ambito delle attività procedimentali e anche diffusi all’esterno, come rendicontazione degli esiti del monitoraggio effettuato.

La banca dati deve essere organizzata in sezioni interoperabili fra loro che consentano la gestione e la consultazione di tutti i dati elementari rilevati, attraverso un applicativo che debba consentire anche l’esportazione dei dati in ambiente M.S. Office e Adobe Acrobat; l’interfaccia dovrà essere organizzata in modo da permettere, in maniera facile e guidata, di effettuare interrogazioni su tutti i campi del database e di poter utilizzare i dati rilevati sia a livello disaggregato, sia a livello aggregato. La banca dati, per esempio, deve quindi poter essere interrogata per conoscere sia il tempo di parola di un singolo esponente in una data trasmissione di un x giorno (dato disaggregato) o il computo del tempo di parola di tutti i soggetti politici presenti in un programma di informazione “X” in un arco temporale di 15 giorni (dato aggregato). I risultati delle rilevazioni condotte su ciascun fornitore di servizi media audiovisivi devono essere organizzati in report periodici nelle scansioni temporali previste dalla normativa.

Per report si intendono tabelle di dati aggregati relativi ai telegiornali, ai programmi, alla comunicazione politica e ai messaggi autogestiti.

LA COMUNICAZIONE POLITICA

Per “**comunicazione politica radiotelevisiva**” si intende “*ogni programma in cui assuma carattere rilevante l’esposizione di opinioni e valutazioni politiche manifestate attraverso tipologie di programmazione che comunque consentano un confronto dialettico tra più opinioni, anche se conseguito nel corso di più trasmissioni*” (cfr. art. 2, co. 1, lett. c), del Codice di autoregolamentazione di cui al decreto del Ministro delle comunicazioni dell’8 aprile 2004).

La disciplina prevista per la comunicazione politica non si applica alla diffusione di notizie nei programmi di informazione (art. 2, co. 2, della l. n. 28/2000): infatti, alla comunicazione politica si applica il criterio, di matrice anglosassone, del cd. “equal time rule”, il quale postula una distribuzione paritaria degli spazi tra i vari soggetti politici, in particolare durante il periodo elettorale.

L’offerta di programmi di comunicazione politica è obbligatoria per le concessionarie radiofoniche nazionali e le concessionarie televisive nazionali con obbligo di informazione che trasmettono in chiaro (art. 2, co. 4), **è invece facoltativa per le emittenti radiofoniche e televisive locali** anche nel periodo elettorale (art. 3, co. 1, citato Codice). L’art. 2, co. 4, della legge 28/2000, inoltre, nello stabilire che l’offerta di programmi di comunicazione politica è obbligatoria per le concessionarie televisive e radiofoniche nazionali, aggiunge che “La partecipazione ai programmi medesimi è in ogni caso gratuita”.

Tale ultima previsione appare sintomatica della ratio sottesa alla legge in materia di par condicio volta a non consentire alcuna forma di comunicazione politica a pagamento; i messaggi autogestiti a pagamento costituiscono infatti l’unica forma possibile di cessione a titolo oneroso di spazi di comunicazione politica sulle emittenti locali.

Sebbene si faccia espressa menzione delle emittenti nazionali, non vi è dubbio che la previsione appena richiamata abbia portata generale dal momento che la norma in esame delinea i principi generali della comunicazione politica radiotelevisiva.

Giova sottolineare che tali disposizioni, previste per le concessionarie televisive e radiofoniche ex analogiche, trovano ora applicazione nei confronti dei fornitori di servizi di media audiovisivi locali, ormai tutti in tecnica digitale, ai sensi e per gli effetti del nuovo Testo unico dei servizi di media audiovisivi e del nuovo Regolamento relativo alla radiodiffusione televisiva terrestre in tecnica digitale.

Circa l’ammissibilità di forme di comunicazione politica a pagamento sulle emittenti televisive locali, l’Autorità ha rilevato come il pagamento di un corrispettivo risulti confliggere in re ipsa con i principi di obiettività, completezza, lealtà, imparzialità, apertura alle diverse opinioni e tendenze politiche che presidiano l’informazione radiotelevisiva sui quali si fonda la legge, anche dopo la novella del 2003.

I messaggi autogestiti e i sondaggi politico – elettorali

I messaggi recano la motivata esposizione di un programma o di un’opinione politica, possono essere gratuiti o a pagamento. La trasmissione di messaggi autogestiti gratuiti è facoltativa per le emittenti

private e obbligatoria per la concessionaria del servizio pubblico radiotelevisivo. Le emittenti locali possono trasmettere messaggi politici autogestiti a pagamento.

Il messaggio deve essere sempre riconoscibile come tale, recando in sovrimpressione per tutta la sua durata la scritta “messaggio politico autogestito”; in radio il messaggio deve essere preceduto e seguito da un annuncio audio di identico contenuto e deve recare altresì l’indicazione del committente. I messaggi autogestiti gratuiti non sono computati nel calcolo dei limiti di affollamento pubblicitario previsti dalla legge.

Quanto ai sondaggi politico-elettorali si intendono come tali la *“Rilevazione sull’esito delle elezioni e sugli orientamenti politici e di voto degli elettori, volta a cogliere l’orientamento politico ed elettorale dei cittadini e i trend delle intenzioni di voto nei confronti di partiti politici e di candidati”*.

La materia trova compiuta disciplina nel combinato disposto degli articoli 8 e 10 della legge 28/2000 e 6 e ss. del Regolamento (delibera n. 256/10/CSP). Si precisa che i Co.re.com hanno competenza a vigilare e avviare procedimenti solo con riferimento alla violazione del silenzio nei quindici giorni antecedenti al voto e relativamente a questioni in materia di pubblicazione della nota informativa.

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 il servizio di registrazione audio-video delle trasmissioni delle emittenti televisive locali lombarde e di scomposizione dei relativi dati, finalizzati all'esercizio delle funzioni di monitoraggio e vigilanza del pluralismo politico-istituzionale nel periodo elettorale

Sommario

PREMESSA	2
DURATA	3
OBBLIGHI DEL TITOLARE DEL TRATTAMENTO	3
OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO	4
Personale e altri collaboratori	5
Sistema di autenticazione	6
Amministratori di sistema	7
Misure di sicurezza tecniche e organizzative	7
Operazioni da eseguire sui dati personali al termine dell'affidamento, anche anticipato	10
Obblighi di informazione e collaborazione	10
Designazione di sub-responsabili (art. 28, par. 2 e 4, RGPD)	11
Gestione degli incidenti di sicurezza informatica e violazioni di dati personali (<i>data breach</i>)	13
Luogo di trattamento e trasferimento di dati personali	13
Obblighi del responsabile relativi all'infrastruttura cloud eventualmente utilizzata per l'erogazione del servizio	14
ATTIVITÀ DI VIGILANZA E VERIFICA DEL TRATTAMENTO	14
INDIVIDUAZIONE DI MAGGIORI LIVELLI DI SICUREZZA E ADEGUAMENTI ALLA NORMATIVA PRIVACY	
SOPRAVVENUTA O A ESIGENZE CONTRATTUALI SOPRAVVENUTE	15
COMUNICAZIONI	15
DISPOSIZIONI FINALI	15
DATI DI CONTATTO DEI RESPONSABILI DELLA PROTEZIONE DEI DATI PERSONALI (RPD)	16
ALLEGATI	16
ALLEGATO A.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI DI TITOLARITÀ DEL CONSIGLIO REGIONALE AFFIDATI AL FORNITORE IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO	17
ALLEGATO A.2 - ELENCO DELLE MISURE DI SICUREZZA	18

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 oggetto, nella persona del legale rappresentante pro tempore, domiciliato per la carica presso la sede dell'aggiudicatario;
- **"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, par. 2 e 4, RGPD;
- **"affidamento"**, il capitolato/contratto definito nel decreto di aggiudicazione e/o in ogni altro atto contrattuale tra il Consiglio regionale e il Fornitore che disciplini il servizio in oggetto;
- per le altre definizioni si rinvia all'art. 4 RGPD.

Tutto ciò premesso,

il Consiglio regionale della Lombardia, come sopra rappresentato, in qualità di **Titolare del trattamento**, designa il Fornitore, che accetta, quale **Responsabile del trattamento** dei dati personali, ai sensi e per gli effetti dell'art. 28 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 per fornire il servizio oggetto dell'affidamento, nei limiti delle finalità ivi specificate, nel rispetto della Normativa privacy e delle istruzioni fornite.

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 contrattuali successivi stipulati tra le parti.

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.

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. 50/2016, dal d.lgs. 33/2013 e dalle altre norme in materia.

DURATA

La designazione a **Responsabile del trattamento** del Fornitore, come sopra rappresentato, 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 proroga, rinnovo, differimento e ripetizione a ogni titolo della durata dell'affidamento, la designazione e il presente Atto si considereranno automaticamente prorogati per pari durata.

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 di autenticazione 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** 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)»”, le “Linee guida per lo sviluppo del software sicuro” emesse dall’Agenzia per l’Italia digitale del 21 novembre 2017, le Linee guida sulla sicurezza nel procurement ICT (Determinazione n. 220/2020 del 17 maggio 2020 Agid) e, se applicabili, le circolari AgID n. 2 “Criteri per la qualificazione dei Cloud Service Provider per la PA” e n. 3 “Criteri per la qualificazione di servizi SaaS per il Cloud della PA” del 2018.

Il **Responsabile del trattamento** è autorizzato a svolgere le attività di trattamento, sia con modalità elettroniche sia con modalità cartacee, indispensabili per lo svolgimento del servizio affidato, come descritto nel presente Atto, nell’Affidamento principale o concordate con il Titolare con 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 rispetto a quelli indicati nel presente Atto e nei suoi allegati 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, concluso decorsi 24 mesi successivi alla data di trasmissione oggetto di registrazione, salvo diversa richiesta del Titolare (es. trasferimento dei sistemi e supporti stessi al Titolare o a terzi da questi indicati).

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.

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

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

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 ed eventuali appaltatori e sub-responsabili relativamente al loro ambito di prestazione.

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, messe a disposizione del Titolare del trattamento su richiesta.

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.

Sistema di autenticazione

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;
- 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 tra cui, almeno, un sistema di login con criptazione sicura;
- 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 otto 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 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 sei mesi;
- i) 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;
- j) verificare, a intervalli almeno annuali, le autorizzazioni in essere.

Medesime prescrizioni si applicano anche ai sistemi di autenticazione del personale o altro incaricato del Titolare qualora venga messa a disposizione dal **Responsabile del trattamento** un servizio web o piattaforma per accedere ai servizi di cui al contratto.

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 espleteranno, 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, a relazionare annualmente il **Titolare del trattamento** sulla loro attività, nonché 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 27.11.2008 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 periodica conferma 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.

I sistemi e la rete del **Responsabile del trattamento** devono essere adeguati alle 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, se applicabili, le circolari AgID n. 2 “Criteri per la qualificazione dei Cloud Service Provider per la PA” e n. 3 “Criteri per la qualificazione di servizi SaaS per il Cloud della PA” del 2018 e la Determinazione AgID n. 628/2021 del 15 dicembre 2021 - Adozione del “Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione”.

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 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 password;
- 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. In caso di segnalazione di vulnerabilità, il **Responsabile del trattamento** deve provvedere tempestivamente all'aggiornamento dei programmi utilizzati con le versioni disponibili o alla valutazione degli altri interventi necessari per garantire la sicurezza dei dati;
- 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 deve prevedere l'adozione di copie di back-up e il ripristino dei dati in tempi certi e comunque non

superiori a sette giorni e s’impegna a garantire che l’accesso in rete ai dati personali su canali sicuri o in forma criptata, salvo che sia diversamente richiesto e autorizzato dal Titolare del trattamento.

Il **Responsabile del trattamento** può aggiornare o modificare le misure di sicurezza garantite al momento dell’affidamento e/o stabilite nel capitolato/contratto 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, di implementazioni di nuovi servizi o di regole afferenti a piattaforme tecnologiche utilizzate 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, 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 anche le misure di sicurezza individuate nell’allegato A.2 nonché quelle indicate nel capitolato e nell’allegato tecnico.

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 GDPR, 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. A tal fine, mette a disposizione del Titolare gli atti, documenti e manuali in cui vengono illustrate le misure di sicurezza e organizzative adottate per garantire il rispetto della normativa e la riservatezza dei dati personali oggetto del trattamento.

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 senza ausilio di strumenti elettronici e informatici, il **Responsabile del trattamento** 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

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

- alla restituzione completa dei dati personali (in formato digitale e/o cartaceo) di titolarità del Consiglio regionale, di cui abbia disponibilità;
- alla distruzione di eventuale propria documentazione cartacea contenente i dati personali e alla cancellazione dei dati personali dai propri sistemi elettronici al termine del rapporto contrattuale, dopo aver effettuato le operazioni di cui sopra, con modalità che non consentano il recupero dei dati personali, salvo sia obbligatorio conservarla in ragione degli adempimenti amministrativi e contabili stabiliti dalla legge o di specifica richiesta da parte del Titolare del trattamento;
- alle altre operazioni richieste dal Titolare del trattamento stesso, 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.

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.

Eventuali documenti cartacei contenenti dati personali di cui all'allegato A.1. devono essere smaltiti previa triturazione al fine di non consentire l'identificazione degli interessati.

Possono essere conservati i dati personali limitatamente a quanto previsto da obblighi di legge connessi a adempimenti amministrativi, fiscali e contabili ed esclusivamente per le finalità previste dalla legge.

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'Atto di affidamento del servizio.

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.

Salvo che non si applichi l'esenzione di cui all'art. 30, par. 5, RGPD, il **Responsabile del trattamento**, ai sensi dell'art. 30, par. 2 del RGPD, 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 a inoltrarla prontamente al **Titolare del trattamento**.

Il **Responsabile del trattamento** è tenuto a redigere e rendere consultabile agli interessati le informazioni di cui agli articoli 13 e 14 RGPD, in accordo con 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, par. 2 e 4, RGPD)

Il **Responsabile del trattamento**, nei termini di cui all'affidamento, ha la facoltà di ricorrere ad altri responsabili del trattamento di dati personali (sub-responsabili del trattamento).

Il **Responsabile del trattamento** comunica al Titolare nel termine di 10 (dieci) giorni dalla designazione con il presente Atto il nominativo dei sub-responsabili nominati nell'ambito del servizio oggetto dell'affidamento.

Il **Responsabile del trattamento**, in sede di designazione di ulteriori sub-responsabili, deve informare il **Titolare del trattamento**, al fine di consentire, come previsto dall'art. 28, par. 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 il **Responsabile del trattamento** 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 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.

A tal fine, il **Responsabile del trattamento** invia al Titolare del trattamento, una comunicazione che contenga:

- i) l'identità e i dati di contatto del sub-responsabile;
- ii) le attività di trattamento che il Responsabile del trattamento intende affidare al sub-responsabile;
- iii) il luogo dove verrà effettuato il trattamento e l'ubicazione esatta dei server di cui il sub-responsabile si serve per il trattamento dei dati personali (con l'indicazione dell'eventuale ricorso al cloud);
- iv) la data in cui è stato concluso il contratto tra il responsabile e il sub-responsabile (condizionato alla mancata opposizione).

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, par. 4, RGPD. Su richiesta del **Titolare del trattamento**, il **Responsabile del trattamento** invia al **Titolare** la documentazione relativa alla designazione del sub-responsabile del trattamento per l'esercizio delle prerogative stabilite dall'art. 28 RGPD.

Il **Titolare del trattamento** potrà in qualsiasi momento verificare le garanzie e le misure tecniche e organizzative del sub-responsabile, tramite audit e ispezioni anche avvalendosi di soggetti terzi. Nel caso in cui tali garanzie risultassero insussistenti o inadeguate il **Titolare** potrà 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 inapplicabili o inadeguate rispetto al rischio del trattamento o, comunque, inadeguate ad assicurare l'applicazione del RGPD o risulti che il sub-responsabile 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 nell'affidamento e diffonderà 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.

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 dall'atto di affidamento, il **Responsabile del trattamento** è tenuto a comunicare al Titolare, senza ingiustificato ritardo, e comunque entro 24 (ventiquattro) ore dal momento in cui ne ha avuto conoscenza, ogni violazione dei dati o di incidenti informatici o altro accadimento che possa aver comportato un impatto sui dati personali del **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 staff.privacyanticorruzione@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.

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 eventualmente utilizzata per l'erogazione del servizio

Qualora necessario per l'erogazione del servizio, il **Responsabile del trattamento** garantisce di utilizzare un'infrastruttura *cloud* conforme alle «*best-practice*» del settore e si impegna ad 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 dalle circolari AgID n. 2 e n. 3 del 2018.

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.

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 nell'affidamento 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 ad informare almeno una volta all'anno il Titolare, mediante relazione scritta, di tutte le attività svolte in conformità a quanto previsto dal Contratto e, comunque, 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, par. 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.

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 per il Corecom e altre Authority regionali.

Il Fornitore 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 dell'affidamento, 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 al seguente recapito pec: protocollo.generale@pec.consiglio.regione.lombardia.it.

Il Fornitore 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 Responsabile 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)

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 Fornitore, 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
Servizio registrazione audio-video delle trasmissioni delle emittenti televisive locali lombarde e di scomposizione dei relativi dati, finalizzati all'esercizio delle funzioni di monitoraggio e vigilanza del pluralismo politico-istituzionale nel periodo elettorale	Finalità Attività di monitoraggio sulle trasmissioni delle emittenti televisive locali lombarde nell'area pluralismo politico e sociale, (decreto legislativo 8 novembre 2021, n. 208, legge 22 febbraio 2000, n. 28, Decreto del Ministero delle Comunicazioni 8 aprile 2004, delibere agcom in materia) Ambito del trattamento Manuale e informatico	Il trattamento è effettuato con strumenti cartacei ed elettronici. Le operazioni di trattamento autorizzate sono: ☒ raccolta ☒ registrazione ☒ organizzazione ☐ strutturazione ☒ conservazione ☐ adattamento ☐ modifica ☐ visualizzazione ☐ estrazione ☒ uso ☒ comunicazione agli interessati e al Consiglio regionale ☐ diffusione ☐ raffronto ☐ interconnessione ☐ limitazione ☒ cancellazione secondo le istruzioni del Titolare ☒ distruzione secondo le istruzioni del Titolare ☐ copia, duplicazione, riproduzione e registrazione solo su autorizzazione del Titolare del trattamento ☐ altro Le prestazioni comportano: - la predisposizione di misure di sicurezza per garantire integrità, stabilità e riservatezza dei dati personali; - attività tecniche e funzioni di amministratore di sistema; - connessione sicura HTTPS; - trattamento di dati particolari; - trasmissione della reportistica finale su canali sicuri; messa a disposizione di applicativo per consultazione ed estrazione dei dati. Conservazione: 24 mesi successivi alla data di trasmissione.	Dati personali (Nome e cognome; Sesso; Tempi televisivi dedicati; Categoria di appartenenza (partito/istituzione); opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale origine razziale o etnica; immagine, audio) di soggetti politici. Possono essere trattati altri dati personali di qualsiasi categoria e di altri interessati ripresi nelle trasmissioni televisive.	Direttore dell'esecuzione: dirigente del Servizio per il Corecom e altre Authority regionali

ALLEGATO A.2 - ELENCO DELLE MISURE DI SICUREZZA

Fermo quanto stabilito con riguardo a specifiche misure di sicurezza nell'Atto di designazione o definito 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	Trattamenti per i quali è applicata la misura di sicurezza
☐	gestione di più profili con privilegi diversi*	Trattamenti di cui all'allegato A.1
☒	utilizzo credenziali uninominali	
☒	autenticazione delle utenze username/password	
☒	utilizzo di password sicure (almeno otto caratteri alfanumerici)	
☒	cambio periodico delle password (almeno ogni sei mesi)	
☐	autenticazione utenze multifattore	
☐	utilizzo di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.)	
☒	supporto 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)	
☒	profili di autorizzazione differenziati tra gli utenti	
☒	funzionalità di "richiesta creazione o cambio della password al primo accesso"	
☒	blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso	
☐	accessi utenti registrati su un archivio (log) non cancellabile con il reset*	
☐	gestione dei log di sistema (accessi, allarmi, ecc.)	
☐	mascheratura della base dati	
☒	Encryption/cifatura	
☐	cifatura delle comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell'ente*	
☒	tracciatura delle modifiche	
☒	protezione dei dati estratti	
☒	validazione dei dati in input	
☒	protezione delle comunicazioni client/server	
☐	archivi separati tra dati generici e dati particolari (sensibili e/o giudiziari)	
☒	aggiornamento periodico software utilizzati	
☒	utilizzo di programmi contro il rischio di intrusione e accesso abusivo	
☒	utilizzo di programmi antivirus	
☐	cancellazione dati di navigazione	
☐	anonimizzazione dati di navigazione	
☐	filtraggio di indirizzi IP	

Barrare le misure adottate	Misure di sicurezza	Trattamenti per i quali è applicata la misura di sicurezza
☐	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	
☒	condivisione della documentazione per gestire il servizio	
☒	tracciatura degli accessi limitatamente alla profilatura delle funzionalità applicative direttamente gestite.	
☒	tracciatura delle modifiche dei dati	
☒	protezione delle comunicazioni client/server riguardo servizi direttamente gestiti	
☐	archivi separati tra dati personali generici e dati di particolari categorie o relativi a condanne penali o a reati	
☐	altro (specificare)	

Sicurezza infrastrutturale

Barrare le misure adottate	Misura di sicurezza	Trattamenti per i quali è applicata la misura di sicurezza
☐	gestione di più profili con privilegi diversi	Trattamenti di cui all'allegato A.1
☒	utilizzo credenziali uninominali per quanto attiene le componenti infrastrutturali di competenza del responsabile del trattamento	
☒	autenticazione delle utenze username/password	
☒	utilizzo di password sicure (almeno otto caratteri alfanumerici)	
☐	autenticazione utenze multifattore	
☐	utilizzo di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.)	
☒	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)	
☒	profili di autorizzazione differenziati tra gli utenti	
☒	funzionalità di "richiesta creazione o cambio della password al primo accesso"	
☐	blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso	
☐	accessi utenti registrati su un archivio (log) non cancellabile con il reset	
☐	gestione dei log di sistema (accessi, allarmi, ecc.)	
☒	programma di backup dei dati	
☒	programma di backup delle configurazioni	

Barrare le misure adottate	Misura di sicurezza	Trattamenti per i quali è applicata la misura di sicurezza
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	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	
_	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	
_	programma di protezione dischi rimovibili	
_	programma di controllo piattaforma software	
X	soluzione di disaster recovery	
_	soluzione dlp applicata al contesto	
_	dismissione supporti di archiviazione già utilizzati	
_	gestione supporti di archiviazione dismessi	
X	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.)	
_	altro (specificare)	

Sicurezza fisica per i trattamenti su supporti non elettronici

Barrare le misure adottate	Misura di sicurezza	Trattamenti per i quali è applicata la misura di sicurezza
X	limitazione di accesso ai locali deputati al trattamento	Trattamenti di cui all'allegato A.1
_	profilazione degli accessi in base a ruolo	
_	utilizzo tessere di accesso uninominali limitazione di accesso agli archivi cartacei	

Barrare le misure adottate	Misura di sicurezza	Trattamenti per i quali è applicata la misura di sicurezza
X	limitazione di accesso agli archivi cartacei	
X	archiviazione cartacea distinta per livello di severità	
_	tracciatura degli accessi ai repository di dati cartacei	
_	tracciatura degli accessi ai locali	
X	presenza di sistemi antieffrazione	
X	videosorveglianza locali	
X	movimentazione materiali in modalità sicura	
X	sigillatura contenitori movimentati	
X	Triturazione della documentazione cartacea contenente dati personali	
X	Definizione di regole per la cancellazione sicura dei dati (es. Modello basato sulla norma DIN 66398)	
_	Altre [specificare]	

Sicurezza Organizzativa

Barrare le misure adottate	Misure di sicurezza	Trattamenti per i quali è applicata la misura di sicurezza
X	formazione privacy del personale	Trattamenti di cui all'allegato A.1
X	definizione di procedure per assicurare la segretezza	
X	definizione di un elenco dei dipendenti che saranno impiegati sul singolo progetto e sottoscrizione per ogni dipendente di dichiarazioni di riservatezza/confidenzialità	
X	nomina referente privacy	
X	nomina incaricati del trattamento	
_	presenza dpo	
X	definizione di una procedura di data breach	
X	struttura per la prevenzione e gestione degli incidenti informatici	
X	procedura di ripristino dei dati in caso di incidente fisico o tecnico	
X	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	
_	possesto 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	
X	possibilità di auditing a richiesta dell'ente	
_	possibilità di verifiche di conformità dei servizi da parte dell'ente	
_	possesto 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	

Barrare le misure adottate	Misure di sicurezza	Trattamenti per i quali è applicata la misura di sicurezza
☒	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*	
☐	descrizione dettagliata della soluzione tecniche applicate (dispositivi hardware e software impiegato, modalità operative, politiche di sicurezza) *	
☐	altro (specificare)	

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.