



Regione Lombardia
IL CONSIGLIO

DD N. 424

del 03/12/2025

UFFICIO CONTRATTI E ICT

DECRETO DIRIGENZIALE

Oggetto: SERVIZIO DI MIGRAZIONE DATI, CONFIGURAZIONE, MANUTENZIONE E AGGIORNAMENTO DEI SOFTWARE CLAVIS E DISCOVERY PER LE ESIGENZE DELLA BIBLIOTECA DEL CONSIGLIO REGIONALE E NELL'AMBITO DELLA PARTECIPAZIONE AL POLO SBN L02, PER IL PERIODO DI SESSANTA MESI, CON FACOLTÀ DI PROROGA CONTRATTUALE PER IL PERIODO MASSIMO DI VENTIQUATTRO MESI. AFFIDAMENTO DIRETTO, AI SENSI DELL'ART. 50, COMMA 1, LETT. B), DEL DECRETO LEGISLATIVO N. 36/2023, A COMPERIO S.R.L. DI STANGHELLA (PD), TRAMITE LA PIATTAFORMA CERTIFICATA SINTEL - DECISIONE DI CONTRARRE

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 11 novembre 2024, n. 386 "III Provvedimento organizzativo Anno 2024: conferimento incarichi dirigenziali", che ha, tra l'altro, attribuito alla sottoscritta l'incarico triennale di dirigente dell'Ufficio Contratti e ICT, con decorrenza dal 1° gennaio 2025;
- la deliberazione del Consiglio regionale 17 dicembre 2024, n. XII/662, di approvazione del bilancio di previsione finanziario per gli anni 2025-2026-2027 per il funzionamento del Consiglio regionale;
- la deliberazione dell'Ufficio di presidenza 18 dicembre 2024, n. 423, di approvazione del documento tecnico di accompagnamento e di assegnazione delle quote di bilancio al segretario generale e al datore di lavoro, per gli anni 2025-2026-2027;
- la deliberazione dell'Ufficio di presidenza 3 febbraio 2025, n. 29, recante "Piano integrato di attività e organizzazione (PIAO) del Consiglio regionale della Lombardia triennio 2025 - 2027 (anno 2025): approvazione" e in particolare nella Sottosezione - Rischi corruttivi e trasparenza anni 2025/2027, che disciplina al paragrafo 6.19 - Ulteriori misure di prevenzione della corruzione, con riferimento al settore dei Contratti pubblici, in cui si prevede, tra l'altro, che Per i servizi e le forniture di importo inferiore a euro 40.000,00 il RUP procede all'affidamento all'operatore economico motivatamente individuato, nella richiesta di acquisto (RDA) trasmessa via EDMA, dal dirigente cui afferisce il progetto e al quale fanno capo i relativi poteri di spesa anche senza previo interpello di altri operatori economici;

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 ordine 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 di 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 23 dicembre 2024, n. 543, di approvazione del bilancio finanziario gestionale per gli anni 2025-2026-2027 per il funzionamento del Consiglio regionale e di assegnazione delle quote ai dirigenti, che, per le procedure di affidamento ai sensi dell'articolo 50 del Codice e per le procedure di scelta del contraente ai sensi degli articoli 70 e ss. del Codice, nonché per le concessioni, ha individuato, di norma e fatte salve le diverse disposizioni di singoli atti, come Responsabile unico del progetto (di seguito RUP) ai sensi dell'articolo 15 del Codice, il dirigente dell'Ufficio Contratti e ICT;

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

VISTA la richiesta di acquisizione (di seguito RDA) n. 38 pervenuta all'u.o. Contratti ed economato, completa di pareri e integrazioni, tramite il sistema documentale EDMA, in data 17 novembre 2025, con la quale il dirigente del Servizio Studi, Valutazione delle Politiche e Qualità della Normazione ha:

- espresso la necessità di acquisire il servizio di migrazione dati, configurazione, outsourcing, manutenzione e aggiornamento dei software CLAVIS e DISCOVERY per le esigenze della Biblioteca del Consiglio regionale, anche nell'ambito della partecipazione al Polo SBN L02;
- precisato che il servizio ha:
 - la finalità di fornire un supporto informativo e documentale, per l'esercizio delle funzioni dei Consiglieri regionali, degli organi ed organismi regionali, delle strutture amministrative del Consiglio regionale, della Giunta e degli Enti del sistema regionale e per motivi di studio e ricerca a tutti gli utenti interessati, ai sensi dell'art. 1 del Regolamento della Biblioteca del Consiglio regionale;

- ed inoltre la finalità di assicurare la gestione e l'erogazione dei servizi della Biblioteca, in particolare quelli di seguito indicati:
 - la gestione e la consultazione del catalogo on-line OPAC della Biblioteca consiliare e del Polo SBN L02;
 - la gestione efficiente dei materiali e del servizio di prestito;
 - la partecipazione al Polo SBN L02 anche mediante catalogo condiviso;
- dichiarato che non vi sono convenzioni ARIA S.p.A. o Consip attive per l'erogazione del servizio in oggetto;
- indicato la durata del contratto per un periodo di sessanta mesi, con facoltà di proroga contrattuale per un periodo massimo di ventiquattro mesi, con decorrenza dalla data indicata nella comunicazione di stipulazione del contratto;
- indicato la spesa complessiva per l'acquisizione del servizio in euro 19.500,00 (oltre IVA al 22%), sulla base del preventivo acquisito dall'operatore economico sopra indicato, di cui euro 14.500,00 (oltre IVA al 22%), per il contratto principale ed euro 5.000,00 (oltre IVA al 22%), per l'eventuale periodo di proroga e ha individuato la relativa copertura finanziaria sui competenti fondi di bilancio;
- chiesto di procedere mediante affidamento diretto a Comperio S.r.l., con sede a Stanghella (PD), codice fiscale e Partita IVA 01162350290 , in quanto la società è sviluppatore unico ed esclusivo della suite CLAVIS e DISCOVERY, in uso in numerose biblioteche e sistemi bibliotecari in Italia e in Lombardia. Tali prodotti sono conformi al protocollo SBNMARC dell'Istituto Centrale per il Catalogo Unico delle biblioteche italiane e per le informazioni bibliografiche- ICUU e garantiscono la gestione di poli e sistemi bibliotecari. La soluzione proposta corrisponde poi al fabbisogno attuale dell'Amministrazione, alle esigenze gestionali della Biblioteca consiliare e del Polo SBN L02, in quanto assicura la partecipazione al Polo SBN L02 anche mediante catalogo condiviso, la gestione dei materiali, del prestito, del catalogo della BCRL e del Polo e garantisce, inoltre, l'integrazione in OPAC dei servizi di prestito digitale che la BCRL eroga attualmente tramite la piattaforma Media Library On Line (MLOL) e l'interrogazione simultanea di diverse basi dati e cataloghi, in particolare la gestione del meta-opac condiviso con PoliS-Lombardia, disciplinato dalla convenzione vigente tra Consiglio regionale e PoliS che disciplina all'art.5 la collaborazione tra le rispettive Biblioteche ed infine l'operatore economico garantisce un servizio Saas e un'infrastruttura qualificata ACN (Autorità nazionale per la cybersicurezza) <https://www.acn.gov.it/portale/w/sa-5019> e <https://www.acn.gov.it/portale/w/in-4732>;-
- il suddetto operatore economico è stato, inoltre, individuato in accordo con la biblioteca della Fondazione ENI 'Enrico Mattei' (FEEM) che è capofila e responsabile del Polo SBN Lombardia 2 (Polo SBN L02) al quale la Biblioteca consiliare aderisce (rif. Regolamento BCRL, art.8; Convenzione Consiglio regionale e Fondazione ENI 'Enrico Mattei').
- ritenuto adeguata e conveniente l'offerta dell'operatore economico in considerazione del canone attualmente corrisposto al fornitore attuale;
- indicato di assumere il ruolo e le funzioni di direttore dell'esecuzione del contratto e di incaricare come referente operativo il funzionario responsabile dell'U.O. Studi e Biblioteca;

ACQUISITI AGLI ATTI:

- il parere del 1° settembre 2025 con cui l'u.o. Prevenzione, protezione e sicurezza nei luoghi di lavoro e servizi ausiliari ha rilevato, in base a quanto

riportato nella RDA, che il servizio richiesto non comporta sovrapposizione spazio-temporale con l'attività degli uffici consiliari e pertanto non rientra nelle fattispecie indicate all'articolo 26, del d.lgs. 81/2008;

- il parere del 6 agosto 2025, con cui l'Ufficio Trasparenza, Prevenzione della corruzione e Privacy ha evidenziato, in base a quanto riportato nella RDA, che il servizio in oggetto comporta il trattamento di dati personali di titolarità del Consiglio regionale, e pertanto il Consiglio regionale, in qualità di titolare dei dati, deve procedere, prima dell'inizio delle prestazioni contrattuali che comportino il trattamento di dati personali, rientranti nella titolarità del Consiglio regionale, con separato atto giuridico bilaterale, alla designazione della società affidataria come responsabile del trattamento definendo gli elementi di cui al par. 3 dell'art. 28 del RGPD con efficacia temporale pari a quella del rapporto contrattuale, anche in caso di revoca anticipata, risoluzione o recesso;
- il parere del 1° agosto 2025, con cui il Professional Sistemi, rete e sicurezza ICT, sulla base della RDA, non ha rilevato problematiche di incompatibilità con l'infrastruttura sistemistica del Consiglio regionale, esprimendo pertanto parere favorevole;

DATO ATTO che:

- il servizio è di natura intellettuale;
- le prestazioni in oggetto non rivestono interesse transfrontaliero certo, secondo quanto previsto dall'articolo 48, comma 2, del Codice;
- il principio di rotazione di cui all'articolo 49 del Codice risulta rispettato, considerato che l'operatore economico non è un fornitore uscente;

RITENUTO di:

- acquisire il servizio in argomento mediante affidamento diretto, ai sensi dell'articolo 50, comma 1, lett. b), da svolgere mediante la piattaforma digitale di approvvigionamento certificata Sintel con richiesta di offerta all'operatore economico Comperio S.r.l. con sede legale di Stanghella (PD), come individuato nella RDA n. 38/2025;
- di stimare per l'intera durata contrattuale di sessanta mesi, l'importo complessivo di euro 14.500,00 (oltre IVA al 22%);

DATO ATTO che:

- in data 18 novembre 2025 la sottoscritta, in qualità di RUP, ai sensi dell'articolo 15 del Codice, ha approvato, mediante sottoscrizione digitale il Foglio Patti e condizioni e relativi allegati, predisposto dalla u.o. Contratti ed economato sulla base della RDA n. 38/2025;
- in data 19 novembre 2025 si sono svolte le operazioni relative al lancio della procedura sulla piattaforma telematica di negoziazione Sintel - avente ID 210318772, con invito rivolto a Comperio S.r.l., con sede legale a Stanghella (PD);
- entro il termine ultimo delle ore 18:00 del 28 novembre 2025, è regolarmente pervenuta l'offerta avente ID Sintel 1763974865192 del 24 novembre 2025, presentata dal suddetto operatore economico;
- in data 26 novembre 2025, prima della scadenza del termine di cui al punto precedente, è stata verificata la presenza e la regolarità della documentazione presentata ed è stata ritenuta congrua l'offerta economica presentata;
- nella stessa data, la sottoscritta, in qualità di RUP, ha proposto di affidare il servizio in argomento a Comperio S.r.l., alle condizioni e modalità del Foglio Patti e condizioni e al corrispettivo offerto di euro 14.500,00 (oltre IVA al 22%),

come riportato dal rapporto delle attività generato dalla piattaforma Sintel ID 3335747 unito agli atti;

DATO atto, altresì, che ai fini del requisito di idoneità professionale richiesto (iscrizione alla CCIAA, per attività pertinente con l'oggetto dell'affidamento), Comperio S.r.l. ha dichiarato di essere iscritto al registro delle imprese tenuto dalla Camera di Commercio, Industria, Artigianato e Agricoltura di Padova;

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.2025.0017403, CRL.2025.0017408 e CRL.2025.0017409 del 1° dicembre 2025);

RITENUTO:

- di affidare il servizio in argomento a Comperio S.r.l., con sede legale a Stanghella (PD), codice fiscale e Partita IVA 01162350290, alle condizioni e modalità del Foglio Patti e condizioni e al corrispettivo offerto di euro 14.500,00 (oltre IVA al 22%), con decorrenza dal 1° gennaio 2026 o se successiva dalla data indicata nella comunicazione di stipulazione del contratto, per il periodo di sessanta mesi, con facoltà di proroga contrattuale per un periodo massimo di ventiquattro mesi;
- di impegnare in favore di Comperio S.r.l. la spesa complessiva di euro 8.540,00 (IVA inclusa al 22%) sul bilancio finanziario gestionale per gli anni 2025-2026-2027, con imputazione sul capitolo 2502 "Banche dati on-line", codifica di V livello U.1.03.02.05.003 "Accesso a banche dati e a pubblicazioni on line", come segue:
 - anno 2026: euro 5.490,00 (di cui euro 2.440,00 per le attività propedeutiche all'attivazione del servizio e euro 3.050,00 per un canone annuale);
 - anno 2027: euro 3.050,00 (un canone annuale);la restante somma di euro 9.150,00 farà carico ai competenti fondi che saranno stanziati nei futuri bilanci, come segue:
 - anno 2028: euro 3.050,00 (un canone annuale);
 - anno 2029: euro 3.050,00 (un canone annuale);
 - anno 2030: euro 3.050,00 (un canone annuale);

DATO ATTO che, trattandosi di un servizio di importo inferiore a euro 40.000,00, si procede alla verifica dei requisiti ai sensi dell'art. 52, comma 1, del Codice, e secondo le indicazioni e tempistiche di cui al decreto n. 39/2024, sopra richiamato, e pertanto il presente provvedimento è immediatamente efficace;

DATO ATTO, altresì che:

- la spesa relativa all'eventuale periodo di proroga contrattuale sarà impegnata con successivo decreto dirigenziale;
- ai fini della stipulazione del contratto, ai sensi dell'articolo 53, comma 4, del Codice, l'operatore economico è tenuto a prestare una garanzia definitiva, di cui all'articolo 13 del Foglio Patti e condizioni, pari al 5% dell'importo contrattuale netto con le modalità di cui all'articolo 117 del Codice, a cui non si applicano le riduzioni di cui all'articolo 106, comma 8, del Codice e gli aumenti previsti dall'articolo 117, comma 2;
- 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 e riporterà il CIG che sarà comunicato dall'Amministrazione;

- 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;

DATO ATTO che il Fornitore fattura il corrispettivo contrattuale, ai sensi dell'articolo 6, comma 6 del Foglio patti e condizioni, come segue:

- le attività propedeutiche alla messa in esercizio del servizio, previo benestare del DEC, che certifichi la regolare attivazione del servizio come descritto nel Foglio patti e condizioni e il primo canone annuale all'avvio del servizio, mentre i successivi canoni annuali in via annuale anticipata;
- per l'eventuale periodo di proroga contrattuale di massimo ventiquattro (24) mesi, in via annuale anticipata, fatta salva la diversa modalità indicata nell'atto di proroga in base alle effettive mensilità prorogate;

RITENUTO di individuare:

- quale direttore dell'esecuzione del contratto il dirigente del Servizio Studi, Valutazione delle Politiche e Qualità della Normazione, competente, ferme le previsioni di legge e le previsioni del Foglio Patti e condizioni in allegato, anche per l'eventuale modifica degli impegni di spesa, la liquidazione delle fatture e il rilascio del certificato di regolare esecuzione;
- quale referente operativo del contratto per il Consiglio regionale il funzionario responsabile dell'U.O. Studi e Biblioteca;

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 e risorse strumentali sulla disponibilità dei fondi e la prenotazione della spesa ai sensi dell'articolo 15 del regolamento contabile,

DECRETA

1. di affidare a Comperio S.r.l., con sede legale a Stanghella (PD), codice fiscale e partita IVA 01162350290, ai sensi dell'articolo 50, comma 1, lettera b) del Codice, il servizio in oggetto, per il periodo di sessanta mesi, con decorrenza dal 1° gennaio 2026, o se successiva dalla data indicata nella comunicazione di stipulazione del contratto, alle condizioni e modalità di cui al Foglio Patti e condizioni e relativi allegati, al corrispettivo complessivo di euro 14.500,00 (oltre IVA del 22%), come riportato nell'offerta economica del 24 novembre

2025, avente ID Sintel 1763974865192, presentata dalla suddetta società, con facoltà di proroga contrattuale per un periodo massimo di ventiquattro mesi;

2. di impegnare in favore di Comperio S.r.l. la spesa complessiva di euro 8.540,00 (IVA al 22% inclusa) sul bilancio finanziario gestionale per gli anni 2025-2026-2027, sul capitolo 2502 "Banche dati on-line", codifica di V livello U.1.03.02.05.003 "Accesso a banche dati e a pubblicazioni on line", come segue:
 - anno 2026: euro 5.490,00 (di cui euro 2.440,00 per le attività propedeutiche all'attivazione del servizio e euro 3.050,00 per un canone annuale);
 - anno 2027: euro 3.050,00 (un canone annuale);la restante somma di euro 9.150,00 farà carico ai competenti fondi che saranno stanziati nei futuri bilanci, come segue:
 - anno 2028: euro 3.050,00 (un canone annuale);
 - anno 2029: euro 3.050,00 (un canone annuale);
 - anno 2030: euro 3.050,00 (un canone annuale);;
3. di annettere al presente decreto, quale parte integrante, il Foglio Patti e condizioni 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 dal Fornitore tramite sottoscrizione digitale in sede di procedura di affidamento;
4. di nominare Comperio 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 Foglio patti e condizioni);
5. di individuare quale direttore dell'esecuzione del contratto, competente anche per le attività di cui in premessa, il dirigente del Servizio Studi, Valutazione delle Politiche e Qualità della Normazione e quale referente operativo del contratto per il Consiglio regionale il responsabile dell'U.O. Studi e Biblioteca;
6. di stipulare il contratto, ai sensi dell'articolo 18, comma 1, del Codice, mediante corrispondenza secondo l'uso commerciale, previa acquisizione di copia delle polizze assicurative, della dichiarazione sulla tracciabilità dei flussi finanziari e della garanzia definitiva, di cui rispettivamente agli articoli 5, 12 e 13 del Foglio Patti e condizioni;
7. 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;
8. di disporre l'eventuale proroga contrattuale con successivo decreto dirigenziale, con il quale sarà contestualmente impegnata anche la corrispondente spesa.

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

Foglio Patti e Condizioni

Servizio di migrazione dati, configurazione, manutenzione e aggiornamento dei software CLAVIS e DISCOVERY per le esigenze della Biblioteca del Consiglio regionale, anche nell'ambito della partecipazione al Polo SBN L02, per il periodo di sessanta mesi, con facoltà di proroga contrattuale per il periodo massimo di ventiquattro mesi.

INDICE

Art. 1 - Definizione delle parti	3
Art. 2 - Oggetto, finalità, durata del contratto e opzioni contrattuali	3
Art. 3 - Responsabile unico del progetto e Direttore dell'esecuzione del contratto	4
Art. 4 - Descrizione delle attività e delle tempistiche di esecuzione del servizio	4
Art. 5 - Responsabilità del Fornitore	6
Art. 6 - Corrispettivi, periodicità di fatturazione, contenuti della fatturazione elettronica e modalità di pagamento	7
Art. 7 - Revisione prezzi	9
Art. 8 - Penali	10
Art. 9 - Clausola risolutiva ai sensi dell'articolo 1456 del Codice civile	11
Art. 10 - Risoluzione ai sensi dell'articolo 122 d.lgs. 36/2023	12
Art. 11 - Recesso ai sensi dell'articolo 123 del d.lgs. 36/2023	12
Art. 12 - Tracciabilità dei flussi finanziari	13
Art. 13 - Garanzia definitiva	13
Art. 14 - Divieto di cessione del contratto e subappalto	15
Art. 15 - Trattamento dei dati personali e designazione del Fornitore quale responsabile del trattamento	15
Art. 16 - Patto di riservatezza	18
Art. 17 - Rispetto del codice di comportamento dei dipendenti pubblici e del personale del Consiglio regionale della Lombardia	18
Art. 18 - Rispetto del Patto di integrità e relative sanzioni	19
Art. 19 - Divieto di "pantouflage" e relative sanzioni	19
Art. 20 - Segnalazione di violazioni nell'Amministrazione (c.d. whistleblowing) da parte dei lavoratori e collaboratori delle imprese fornitrici	19

Art. 21 - Stipulazione del contratto	20
Art. 22 - Risoluzione delle controversie e Foro competente	20
Art. 23 - Indirizzo di posta elettronica certificata del Consiglio regionale	20
Art. 24 - Norma finale	20
Clausole del Foglio Patti e condizioni di cui all'art. 1341 c.c.	21
Allegato D	1

Art. 1 - Definizione delle parti

1. Amministrazione, nel prosieguo denominata anche 'Consiglio regionale' è il Consiglio regionale della Lombardia, codice fiscale 80053570158 e P. IVA 09201010965, con sede in via Fabio Filzi n. 22, CAP 20124, a Milano.
2. Fornitore, nel prosieguo denominato anche 'Affidatario', è l'operatore economico Comperio S.r.l., con sede a Stanghella (PD), codice fiscale e Partita IVA 01162350290.

Art. 2 - Oggetto, finalità, durata del contratto e opzioni contrattuali

1. Il contratto ha per oggetto il servizio di migrazione dati, di configurazione, di manutenzione e di aggiornamento dei software denominati "CLAVIS" e "DISCOVERY" per le esigenze della Biblioteca del Consiglio regionale, anche nell'ambito della partecipazione al Polo SBN L02.
2. I software sopra indicati sono applicativi web-based che gestiscono la catalogazione, la localizzazione nel Sistema Bibliotecario Nazionale (SBN) e più in generale il materiale bibliografico e documentale, nonché il servizio di prestito/consultazione della Biblioteca del Consiglio regionale e dell'altra Biblioteca che partecipa al Polo SBN L02.
3. Con i suddetti applicativi è gestito altresì il catalogo visibile agli utenti (Online Public Access Catalogue in breve OPAC) della Biblioteca consiliare, del Polo SBN L02, oltre che il META-OPAC, strumento che consente di interrogare più cataloghi contemporaneamente, condiviso con la Biblioteca di PoliS-Lombardia.
4. La finalità del contratto è quella di assicurare la gestione e l'erogazione dei servizi della Biblioteca, in particolare quelli di seguito indicati:
 - la gestione e la consultazione del catalogo on-line OPAC della Biblioteca consiliare e del Polo SBN L02;
 - la gestione efficiente dei materiali e del servizio di prestito;
 - la partecipazione al Polo SBN L02 anche mediante catalogo condiviso.
5. Il servizio ha altresì lo scopo di fornire un supporto informativo e documentale per l'esercizio delle funzioni dei Consiglieri regionali, degli organi ed organismi regionali, delle strutture amministrative del Consiglio regionale, della Giunta e degli Enti del sistema regionale e per motivi di studio e ricerca a tutti gli utenti interessati, ai sensi dell'art. 1 del Regolamento della Biblioteca del Consiglio regionale.
6. Il contratto ha la durata di sessanta (60) mesi con decorrenza dal 1° gennaio 2026 o se successiva dalla data indicata nella comunicazione di stipulazione, con facoltà di proroga contrattuale ai sensi dell'articolo 120, comma 10, del d.lgs. 36/2023 (di seguito Codice), per un periodo massimo di ventiquattro (24) mesi.
7. Dell'esercizio della facoltà di proroga è data comunicazione al Fornitore tramite posta elettronica certificata con un preavviso di almeno quindici (15) giorni prima della scadenza del contratto. Tale facoltà non costituisce impegno vincolante per l'Amministrazione, che la esercita a proprio insindacabile giudizio, senza che il Fornitore possa avanzare alcuna pretesa al riguardo.

8. In caso di proroga contrattuale disposta dall'Amministrazione, il Fornitore è tenuto a eseguire le prestazioni contrattuali ai prezzi, patti e condizioni stabiliti nel contratto iniziale o alle condizioni di mercato ove più favorevoli per l'Amministrazione.
9. In caso di esercizio dell'opzione di cui al comma 7, il Fornitore non può fare valere il diritto alla risoluzione del contratto.

Art. 3 - Responsabile unico del progetto e Direttore dell'esecuzione del contratto

1. Il Responsabile unico del progetto (di seguito RUP) è il dirigente dell'Ufficio Contratti e ICT.
2. Svolge le funzioni di Direttore dell'esecuzione del contratto (di seguito DEC) il dirigente del Servizio Studi, Valutazione delle Politiche e Qualità della Normazione.
3. Il referente operativo del contratto per il Consiglio regionale è la posizione organizzativa dell'U.O. Studi e Biblioteca (di seguito Referente del CRL).
4. Fermo restando il rispetto delle disposizioni di servizio eventualmente impartite dal RUP, il DEC opera in autonomia in ordine al coordinamento, alla direzione e al controllo tecnico-contabile nell'esclusivo interesse all'efficiente e sollecita esecuzione del contratto.
5. Il DEC è competente altresì per l'eventuale modifica dell'impegno di spesa, per la liquidazione delle fatture e per il rilascio del certificato di regolare esecuzione.
6. L'eventuale variazione del DEC è tempestivamente comunicata dal Consiglio regionale al Fornitore.
7. Le comunicazioni tra il DEC e il Fornitore avvengono per iscritto tramite posta elettronica istituzionale o posta elettronica certificata in modo da garantire la verifica dell'avvenuto recapito delle stesse, al seguente indirizzo:

protocollo.generale@pec.consiglio.regione.lombardia.it
8. Il Consiglio regionale procederà, per il tramite del DEC, all'accertamento della conformità del servizio rispetto alle prescrizioni contrattuali.
9. L'eventuale variazione dei ruoli organizzativi è tempestivamente comunicata dal Consiglio regionale al Fornitore tramite PEC.

Art. 4 - Descrizione delle attività e delle tempistiche di esecuzione del servizio

1. Il Fornitore deve, in particolare:
 - a. provvedere alla migrazione dei dati bibliografici dal formato UNIMARC e dei dati gestionali (es. utenti e prestiti, anche storici) che verranno messi a disposizione dal fornitore uscente;
 - b. rendere disponibili tutti i software sviluppati nella suite CLAVIS e DISCOVERY;
 - c. gestire il Polo SBN L02;
 - d. provvedere alla manutenzione e all'aggiornamento dei software gestionali delle attività bibliotecarie;
 - e. erogare il servizio di help-desk e di assistenza tecnica;
 - f. fornire supporto informativo e di aggiornamento relativo agli applicativi;

- g. provvedere all'integrazione nell'OPAC della Biblioteca del Consiglio regionale (BCRL) dei servizi di prestito digitale che la Biblioteca eroga tramite la piattaforma Media Library On Line (MLOL);
 - h. erogare il meta-catalogo con altre basi dati.
2. Il Fornitore deve assicurare la migrazione dei dati e la messa in esercizio degli applicativi entro dieci (10) settimane dalla decorrenza del contratto.
 3. Il Fornitore deve garantire un servizio di assistenza attraverso il centro di supporto (Comperio Help Center), accessibile all'indirizzo <https://helpcenter.comperio.it/>, con cui è possibile:
 - inoltrare richieste di supporto;
 - verificare lo stato delle richieste aperte;
 - interrogare e navigare i manuali e la knowledge base contenenti informazioni relative ai problemi noti;
 - monitorare lo stato dei servizi cloud in tempo reale.
- In caso di eventi bloccanti, ovvero di interruzioni impreviste del servizio, che rendano impossibile l'accesso al gestionale, il Fornitore garantisce un servizio di pronto intervento.
4. La segnalazione di malfunzionamenti dei sistemi viene gestita dal Fornitore, con la manutenzione correttiva, che avviene, principalmente attraverso i seguenti due canali:
 - i. segnalazioni automatiche che lo stesso software invia in tempo reale al Fornitore in caso di errori inattesi;
 - ii. segnalazioni dirette fornite dagli utenti attraverso il servizio di help-desk.
 5. Nel caso di segnalazioni di cui al comma 4, lettera ii), il Fornitore garantisce i seguenti livelli di servizio:
 - a) per le anomalie bloccanti (gravità 1):
 - i. presa in carico immediata, ossia presa in carico in tempo reale al momento stesso della segnalazione;
 - ii. risoluzione entro un'ora dalla presa in carico;
 - b) per le anomalie di maggiore gravità (gravità 2), errori che riguardano singole funzionalità e precludono l'esecuzione dell'attività richiesta:
 - i. presa in carico entro un'ora dalla segnalazione;
 - ii. risoluzione entro quattro (4) ore dalla presa in carico;
 - c) per le anomalie di minore gravità (gravità 3), errori che riguardano singole funzionalità e non precludono l'esecuzione dell'attività richiesta:
 - i. presa in carico entro sei (6) ore dalla segnalazione;
 - ii. risoluzione entro quarantotto (48) ore dalla presa in carico.
 6. Il Fornitore deve assicurare, inoltre:
 - a) la disponibilità dell'infrastruttura hardware e software di base del sistema centrale, per il 98,5% dei 365 giorni all'anno, pari a 359 giorni all'anno, si esclude il caso di indisponibilità causate da calamità naturali, atti di terrorismo e altri eventi esterni non imputabili al Fornitore;

- b) la risoluzione dei problemi critici evidenziati tramite help-desk, di cui al comma 4, lettera ii), deve essere garantita nel 90% dei casi entro le ventiquattro (24) ore successive alla segnalazione.
7. Il Fornitore deve, inoltre, garantire l'estrazione, su richiesta del DEC o del referente operativo, di dati specifici o aggregati e l'impostazione di query e interrogazioni personalizzate.
 8. Il Fornitore deve assicurare supporto formativo e aggiornamento sugli applicativi, mediante incontri, da svolgersi in modalità on-line o in presenza, per un totale di sei (6) ore per ogni anno di durata del contratto.
 9. Il Fornitore, su richiesta del DEC, inviata tramite posta elettronica certificata, deve garantire l'esportazione dei dati di catalogo, con opzioni di estrazione definite dal committente in base alle proprie esigenze, in un archivio open data in formato adeguato alle specifiche su cui è impostato l'open data istituzionale, su tale formato l'Amministrazione fornirà adeguata documentazione al Fornitore.
 10. Almeno due mesi prima della conclusione del servizio, il Fornitore propone all'Amministrazione un Piano di gestione delle fasi conclusive del contratto. Il Fornitore comunque deve garantire l'estrazione e il trasferimento delle basi dati entro cinque (5) giorni lavorativi dalla ricezione tramite PEC della richiesta del DEC.
 11. Per quanto non espressamente previsto nel presente Foglio patti e condizioni, si rinvia alla descrizione sintetica dei servizi, del Fornitore, allegata al presente Foglio patti e condizioni (ALL.A_Descrizione dei servizi).
 12. Si precisa che, in caso di difformità tra la descrizione sintetica di cui al comma 11 e il presente Foglio patti e condizioni, prevalgono le prescrizioni di quest'ultimo.

Art. 5 - Responsabilità del Fornitore

1. L'Affidatario assume in proprio ogni responsabilità per qualsiasi danno causato 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 dall'Affidatario stesso.
2. L'Affidatario è responsabile per ogni eventuale danno che lo stesso o propri collaboratori, personale dipendente e non dipendente, arrecheranno a persone e/o cose nello svolgimento delle attività connesse al presente contratto.
3. In ragione di quanto precede, senza limitare o ridurre le obbligazioni assunte in base al presente appalto, per le quali l'Affidatario dovrà rispondere integralmente, l'Affidatario si impegna a stipulare le seguenti coperture assicurative:
 - a. una polizza a garanzia della Responsabilità Civile verso Terzi ("RCT") per danni (morte, lesioni personali e danni a cose) a Terzi, con un massimale non inferiore ad euro 1.000.000,00 per sinistro e periodo assicurativo in conseguenza a fatti verificatisi in relazione alle attività oggetto del presente contratto.

La polizza dovrà prevedere la propria operatività anche per:

- committenza;
 - responsabilità personale dipendenti e collaboratori.
- b. una polizza a garanzia della Responsabilità civile prestatori d'Opera ("RCO") per infortuni e le malattie professionali subiti dai prestatori di lavoro di cui l’Affidatario si avvarrà nell'esercizio della attività svolte oggetto del presente appalto con massimale non inferiore ad euro 2.500.000,00 per sinistro con il limite di non inferiore ad euro 1.000.000 per prestatore infortunato.
4. Sulle polizze di cui sopra dovrà essere esclusa ogni facoltà di rivalsa da parte dell’assicurazione nei confronti del Consiglio regionale, salvo il caso di dolo.
 5. Le coperture assicurative avranno efficacia a partire dall’inizio dell’esecuzione del contratto e per tutta la durata contrattualmente prevista.
 6. Qualora il contratto di assicurazione preveda importi o percentuali di scoperto o di franchigia, tali franchigie o scoperti non sono opponibili al Consiglio regionale e resteranno quindi a totale carico dell’Affidatario.
 7. Resta inoltre inteso che, qualora, l’entità dei danni risultasse superiore al massimale sopra indicati, l’Affidatario provvederà al risarcimento del danno, ferma restando la sua intera responsabilità anche per danni causati, nell’esecuzione delle prestazioni contrattuali, eventualmente non coperti dalla predetta polizza assicurativa ovvero eccedenti i massimali assicurati.
 8. L’Affidatario dovrà trasmettere al Consiglio regionale copia - o relativa dichiarazione della Compagnia o Broker di assicurazione - delle polizze di cui sopra, prima della data di loro decorrenza e si impegna a presentare copia della quietanza o appendice di proroga all’Amministrazione prima della scadenza di ogni periodo assicurativo, unitamente alle quietanze di intervenuti pagamenti dei premi. Queste ultime dovranno essere presentate con la periodicità prevista dalle polizze stesse, onde verificare il permanere della validità, nel corso della durata del servizio.
 9. Resta inoltre inteso che l’Affidatario dovrà essere in possesso delle assicurazioni obbligatorie previste dalla legge, tra le quali le assicurazioni contro gli infortuni per i propri dipendenti ai sensi di legge (INAIL – prevenzione contro gli infortuni e altre assicurazioni sociali) e le assicurazioni della Responsabilità Civile Auto (R.C.A.) con massimale unico per evento non inferiore a quello previsto dalla legge per l’utilizzo e la circolazione di veicoli dell’ Affidatario nelle aree pubbliche o ad esse equiparate.

Art. 6 - Corrispettivi, periodicità di fatturazione, contenuti della fatturazione elettronica e modalità di pagamento

1. Il valore complessivo del servizio oggetto dell’affidamento è pari ad euro 19.500,00 (oltre IVA al 22%), di cui euro 14.500,00 (oltre IVA al 22%) per il contratto principale della durata di sessanta (60) mesi ed euro 5.000,00 (oltre IVA al 22%) per il periodo di eventuale proroga del contratto di massimo ventiquattro (24) mesi.

2. L'importo per il contratto principale di euro 14.500,00 è così suddiviso: euro 2.000,00 (oltre IVA al 22%), per le attività propedeutiche all'avvio del servizio di cui all'articolo 4, comma 1, lettere a) e b) e n. 5 canoni annuali di euro 2.500,00 ciascuno (oltre IVA al 22%). L'importo per il periodo di eventuale proroga del contratto per massimo 24 mesi è di euro 5.000,00, oltre IVA, corrispondente a n. 2 canoni annuali di euro 2.500,00 ciascuno (oltre IVA al 22%).
3. Gli oneri per la sicurezza per rischi da interferenza sono pari a zero euro.
4. Il Consiglio regionale riconosce all'Affidatario gli importi offerti in sede di presentazione dell'offerta.
5. I corrispettivi si riferiscono al servizio oggetto dell'affidamento eseguito a perfetta regola d'arte e nel pieno adempimento delle modalità e delle prescrizioni contrattuali e includono tutti gli oneri derivanti al Fornitore dall'esecuzione del contratto e dall'osservanza di leggi e regolamenti. È escluso il rimborso di eventuali spese sostenute dal Fornitore a qualsiasi titolo.
6. Il Fornitore fattura i corrispettivi contrattuali di cui al comma 1 nel modo seguente:
 - per le attività propedeutiche alla messa in esercizio del servizio di cui all'articolo 4, comma 1, lettere a) e b), solo dopo il rilascio del benestare del DEC, che certifichi la regolare attivazione dello stesso, come descritto dal presente Foglio patti e condizioni;
 - i canoni annuali in via anticipata; il primo canone è corrisposto a seguito della regolare attivazione del servizio;
 - per l'eventuale periodo di proroga contrattuale di massimo ventiquattro (24) mesi, in via annuale anticipata, fatta salva la diversa modalità indicata nell'atto di proroga, in base alle effettive mensilità prorogate.
7. L'Amministrazione provvede al pagamento del corrispettivo, previa verifica da parte del DEC della regolarità della fatturazione, entro trenta (30) giorni dal ricevimento di regolare fattura in favore del conto corrente indicato dal Fornitore nel modulo di cui all'articolo 12.
8. 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.6.4.2.5;
 - CIG contratto (campo 2.1.2.7), comunicato al Fornitore dopo l'affidamento;
 - Esigibilità IVA (campo 2.2.2.7): S "Scissione dei pagamenti".
9. 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.

10. 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.
11. 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 Consiglio regionale acquisisce d'ufficio il Documento Unico di Regolarità Contributiva (di seguito DURC).
12. 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.
13. 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.
14. Qualora ne ricorrano i presupposti, Il Consiglio regionale, 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. 7 - Revisione prezzi

1. Ai sensi degli articoli 9 e 60 del Codice, qualora nel corso di esecuzione del contratto si verifichino particolari condizioni di natura oggettiva, che determinano una variazione, in aumento o in diminuzione, del costo del servizio superiore al cinque per cento dell'importo complessivo, i prezzi sono aggiornati, nella misura dell'ottanta per cento della variazione stessa, in relazione alle prestazioni da eseguire.
2. Ai fini della determinazione della variazione dei prezzi l'Amministrazione, ai sensi dall'Allegato II.2 bis al Codice, utilizza l'indice dei prezzi alla produzione dei servizi, nel caso specifico l'indice ISTAT 62 - "Produzione di software, consulenza informatica e attività connesse", con base 2021, corrispondente al CPV 72200000-7 – "Programmazione di software e servizi di consulenza" pubblicato trimestralmente, unitamente alla relativa metodologia di calcolo, sul portale istituzionale dell'ISTAT in conformità alle pertinenti disposizioni normative europee e nazionali in materia di comunicazione e diffusione dell'informazione statistica ufficiale.
3. I nuovi prezzi determinati a seguito della revisione sono applicati alle prestazioni contrattuali svolte dopo la revisione a partire dalla prima fatturazione utile. In nessun caso la revisione dei prezzi potrà avere effetto sulle prestazioni già eseguite.
4. Nel caso di contratti di subappalto e di subcontratti si applica quanto disciplinato dall'allegato II.2-bis del Codice. A tal proposito il Fornitore è tenuto a inserire nei contratti

con i propri subappaltatori e subfornitori una clausola di revisione prezzi, come previsto all'articolo 14.

Art. 8 - Penali

1. Il DEC ha facoltà di contestare le prestazioni contrattuali, entro il termine di quindici (15) giorni, qualora a seguito di controlli ravvisi inadempienze, difformità e ritardo negli adempimenti rispetto alle attività e alle modalità di esecuzione indicate all'articolo 4. La contestazione viene formulata al Fornitore dal DEC per il tramite di PEC. Il Fornitore ha facoltà di formulare controdeduzioni, per il tramite di PEC, entro il termine perentorio di cinque (5) giorni dal ricevimento della formale contestazione.
2. Il DEC, valutate le ragioni addotte dal Fornitore, può procedere all'applicazione delle seguenti penali:
 - a) ritardo nella messa in esercizio degli applicativi decorse dieci (10) settimane dalla decorrenza del contratto (articolo 4, comma 2): 1,5 per mille dell'importo netto contrattuale, per ogni giorno di ritardo;
 - b) indisponibilità dell'infrastruttura hardware e/o software per oltre sei (6) giorni in un anno (articolo 4, comma 6, lettera a): l'1 per mille dell'importo netto contrattuale, per ogni giorno in più rispetto ai sei (6) giorni;
 - c) in caso di mancato rispetto dei livelli di servizi previsti all'articolo 4, comma 5, lettera a), punti i e ii: lo 0,5 per mille dell'importo netto contrattuale, per ogni ora di ritardo, rispetto alle tempistiche ivi previste, fino a un massimo dello 1,5 per mille dell'importo netto contrattuale giornaliero;
 - d) in caso di mancato rispetto dei livelli di servizi previsti all'articolo 4, comma 5, lettera b), punti i e ii: lo 0,5 per mille dell'importo netto contrattuale, ogni due ore di ritardo, rispetto alle tempistiche ivi previste, fino a un massimo dello 1,5 per mille dell'importo netto contrattuale giornaliero;
 - e) In caso di mancato rispetto dei livelli di servizi previsti all'articolo 4, comma 5, lettera c), punti i e ii: lo 0,5 per mille dell'importo netto contrattuale, ogni quattro ore di ritardo, rispetto alle tempistiche ivi previste, fino a un massimo dello 1,5 per mille dell'importo netto contrattuale giornaliero;
 - f) mancata consegna delle basi dati entro cinque (5) giorni lavorativi dalla richiesta inviata dal DEC (articolo 4, comma 10): l'1,5 per mille dell'importo netto contrattuale, per ogni giorno di ritardo rispetto ai cinque (5) giorni previsti;
 - g) in caso di violazione del Patto di integrità di cui all'articolo 18: una penale tra l'1% e il 5% dell'importo netto contrattuale;
 - h) mancata esecuzione delle attività o violazioni non gravi degli obblighi di cui agli articoli 15 e 16: euro 100,00 per ogni violazione.
3. Le fattispecie riportate al comma 2 non hanno carattere di tassatività. In caso di disservizio o inadempimento diverso da quelli contemplati al comma 2, il DEC può irrogare al Fornitore,

in relazione alla gravità del fatto, una penale compresa tra lo 0,5 per mille e l'1,5 per mille dell'importo contrattuale netto.

4. Le penali espresse in percentuale sono arrotondate alla seconda cifra decimale per eccesso.
5. Le penali per il ritardo non possono comunque superare, complessivamente, il 10 per cento dell'importo netto contrattuale. Durante il periodo di proroga, l'importo netto contrattuale, ai fini dell'applicazione delle penali, è costituito dalla somma del corrispettivo previsto per il contratto principale e per il periodo di proroga.
6. In caso di applicazione di penali, è fatto salvo il risarcimento dell'eventuale maggior danno subito dal Consiglio regionale ai sensi dell'articolo 1382 del Codice civile.
7. Per la riscossione delle penali e la rifusione degli eventuali ulteriori danni il Consiglio regionale potrà rivalersi anche tramite trattenuta, per compensazione, sui crediti vantati dal Fornitore nei confronti del Consiglio regionale, nonché sulla garanzia definitiva prestata che, in tal caso, dovrà essere reintegrata secondo quanto previsto all'articolo 13.
8. La richiesta o il pagamento delle penali di cui al presente articolo non esonera in nessun caso il Fornitore dall'adempimento dell'obbligazione per la quale si è reso inadempiente e che ha fatto sorgere la penale. In caso di mancata esecuzione delle attività o di esecuzione gravemente imperfetta non è dovuto alcun corrispettivo.
9. Fatta salva l'applicazione delle penali, nei casi in cui il Fornitore ometta di eseguire, anche parzialmente, la prestazione oggetto del contratto con le modalità ed entro i termini previsti, il Consiglio regionale si riserva la facoltà di ordinare ad altro soggetto l'esecuzione parziale o totale di quanto omesso dal Fornitore, cui saranno addebitati i relativi costi e i danni eventualmente derivati al Consiglio regionale, dandone comunicazione al Fornitore via PEC, con un preavviso di sette (7) giorni di calendario.
10. Qualora l'inesatto adempimento o il ritardo siano determinati da cause di forza maggiore, Il Fornitore deve notificare immediatamente tale circostanza alla competente struttura tramite PEC.
11. In caso di applicazione delle penali, l'Amministrazione provvede a darne comunicazione all'ANAC, in osservanza della normativa vigente in materia.

Art. 9 - Clausola risolutiva ai sensi dell'articolo 1456 del Codice civile

1. Fatta salva l'applicazione delle penali di cui all'articolo 8, il Consiglio regionale ha facoltà, previa comunicazione scritta da inviare al Fornitore a mezzo PEC con cui dichiara che intende avvalersi della presente clausola, di risolvere il contratto ai sensi dell'articolo 1456 del Codice civile, con incameramento della garanzia al verificarsi delle seguenti ipotesi:
 - a) in caso di applicazione di penali per un ammontare totale almeno pari al dieci per cento del corrispettivo contrattuale netto, comprensivo dell'eventuale corrispettivo del periodo di proroga qualora esercitata tale facoltà;
 - b) in caso di violazione degli obblighi di tracciabilità finanziaria richiamati all'articolo 12;

- c) in caso di mancata completa reintegrazione della garanzia definitiva di cui all'articolo 13, eventualmente escussa, entro il termine di dieci giorni naturali e consecutivi dal ricevimento della relativa richiesta tramite PEC da parte del Consiglio regionale;
 - d) in caso di violazione del divieto di cessione del contratto di cui all'articolo 14;
 - e) in caso di gravi violazioni delle norme in materia di protezione dei dati personali e delle norme relative al patto di riservatezza di cui agli articoli 15 e 16;
 - f) in caso di violazione dei codici di condotta di cui all'articolo 17;
 - g) in caso di violazione del Patto di integrità di cui all'articolo 18;
 - h) in caso di mancato rispetto della normativa vigente in materia di lavoro, d'infortuni sul lavoro, d'igiene, di previdenza sociale e di tutti gli obblighi previsti dal d.lgs. 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;
 - i) in caso di verifiche con esito negativo in merito al possesso dei requisiti di ordine generale e di ordine speciale di partecipazione dichiarati in sede di procedura, fatte salve le ulteriori conseguenze previste ai sensi dell'articolo 52, comma 2, del Codice.
2. L'Amministrazione può dichiarare risolto il contratto a proprio insindacabile giudizio e potrà provvedere a stipulare un nuovo contratto, addebitando le maggiori spese che dovessero derivare da prezzi meno favorevoli per l'Amministrazione stessa e fatto salvo il risarcimento del maggior danno.
3. In caso di risoluzione del contratto ai sensi del presente articolo, l'Amministrazione provvede a darne comunicazione all'ANAC, in osservanza della normativa vigente in materia.

Art. 10 - Risoluzione ai sensi dell'articolo 122 d.lgs. 36/2023

- 1. L'Amministrazione può risolvere il contratto di appalto 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 al servizio regolarmente eseguito, decurtato degli oneri aggiuntivi derivanti dallo scioglimento del contratto, fatto salvo quanto previsto al comma 6 del medesimo articolo.
- 3. In caso di risoluzione del contratto ai sensi del presente articolo, l'Amministrazione provvede a darne comunicazione all'ANAC, in osservanza della normativa vigente in materia.

Art. 11 - Recesso ai sensi dell'articolo 123 del d.lgs. 36/2023

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

a venti (20) giorni, decorsi i quali il Consiglio regionale prende in consegna i servizi ed effettua la verifica della regolare esecuzione degli stessi.

Art. 12 - Tracciabilità dei flussi finanziari

1. Il Fornitore assume tutti gli obblighi di tracciabilità finanziaria di cui all'articolo 3 della legge 13 agosto 2010, n. 136, così come interpretato e modificato dagli articoli 6 e 7 del decreto-legge 12 novembre 2010, n. 187, convertito dalla legge 17 dicembre 2010 n. 217. A tal fine, il Fornitore sottoscrive, su richiesta del Consiglio regionale, la dichiarazione di tracciabilità dei flussi finanziari, contenente tra l'altro gli estremi del conto corrente dedicato ai pagamenti relativi al presente contratto e la aggiorna tempestivamente in caso di modifica dei dati ivi dichiarati.
2. Il Fornitore si impegna a notificare tempestivamente eventuali variazioni che si verificassero nelle modalità di pagamento e, in difetto di tale notificazione, esonera il Consiglio regionale da ogni responsabilità per i pagamenti eseguiti.
3. I subappaltatori e i subcontraenti, a qualunque titolo coinvolti nella esecuzione del contratto, sono tenuti, unitamente al Fornitore, al rispetto della normativa sulla tracciabilità dei flussi finanziari (articolo 3, comma 1, legge 136/2010).
4. Ai sensi dell'articolo 119, comma 2, ultimo periodo, del d.lgs. 36/2023, *“L'affidatario comunica alla stazione appaltante, prima dell'inizio della prestazione, per tutti i sub-contratti che non sono subappalti, stipulati per l'esecuzione dell'appalto, il nome del sub-contraente, l'importo del subcontratto, l'oggetto del lavoro, servizio o fornitura affidati. Sono, altresì, comunicate alla stazione appaltante eventuali modifiche a tali informazioni avvenute nel corso del sub-contratto. È altresì fatto obbligo di acquisire autorizzazione integrativa qualora l'oggetto del subappalto subisca variazioni e l'importo dello stesso sia incrementato”*.
5. Come previsto all'articolo 3, comma 1, della legge n. 136/2010 *“La stazione appaltante verifica che nei contratti sottoscritti con i subappaltatori e i subcontraenti della filiera delle imprese a qualsiasi titolo interessate ai lavori, ai servizi e alle forniture di cui al comma 1 sia inserita, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari di cui alla presente legge”*.
6. L'appaltatore, il subappaltatore o il subcontraente che ha notizia dell'inadempimento della propria controparte agli obblighi di tracciabilità finanziaria è tenuto a darne immediata comunicazione alla stazione appaltante e alla prefettura - ufficio territoriale del Governo della provincia di Milano.

Art. 13 - 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 106, comma 8, del Codice e gli aumenti previsti dall'articolo 117, comma 2.

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. La garanzia fideiussoria deve essere emessa e firmata digitalmente; essa deve essere altresì verificabile telematicamente presso L'emittente ovvero gestita in tutte le fasi mediante ricorso a piattaforme operanti con tecnologie basate su registri distribuiti ai sensi dell'articolo 8-ter, comma 1, del decreto-legge 14 dicembre 2018, n. 135, convertito, con modificazioni, dalla legge 11 febbraio 2019, n. 12, o su registri elettronici qualificati ai sensi del Regolamento (UE) n. 910/2014. Le piattaforme, operanti con tecnologie basate su registri distribuiti o su registri elettronici, sono conformi alle caratteristiche stabilite dall'AGID con il provvedimento di cui all'articolo 26, comma 1.
4. Il beneficiario della polizza fideiussoria è il Consiglio regionale della Lombardia.
5. La cauzione (o fideiussione) è prestata a garanzia dell'adempimento di tutte le obbligazioni del contratto e del risarcimento dei danni derivanti dall'eventuale inadempimento delle obbligazioni stesse, salva comunque la risarcibilità del maggior danno.
6. Il Consiglio regionale ha il diritto di valersi della garanzia, nei limiti dell'importo massimo garantito, per l'eventuale maggiore spesa sostenuta per il completamento del servizio 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 prestata il servizio.
7. La garanzia cessa di avere effetto solo alla data di emissione del certificato di regolare esecuzione. Il Consiglio regionale può richiedere al soggetto affidatario la reintegrazione della garanzia ove questa sia venuta meno in tutto o in parte. Diversamente, il Consiglio regionale si riserva la facoltà di avvalersi della clausola di cui all'articolo 9 comma 1, lettera c).
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 dell'articolo 106 del Codice, ove richiamate dall'articolo 117 del medesimo Codice, salvo quanto previsto al comma 1.

Art. 14 - Divieto di cessione del contratto e subappalto

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

Art. 15 - Trattamento dei dati personali e designazione del Fornitore quale responsabile del trattamento

1. Ai fini del presente foglio patti e condizioni e dei suoi allegati, s'intende per "Normativa privacy", il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito, "RGPD"), il d.lgs. 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (di seguito "Codice privacy"), nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile in Italia, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali.
2. Le prestazioni contrattuali comportano l'affidamento al Fornitore di attività di trattamento, anche con l'ausilio di strumenti elettronici, di dati personali di cui è titolare il Consiglio regionale. Ai sensi dell'art. 28 RGPD, il Fornitore, nella persona del legale rappresentante pro

tempore, in qualità di aggiudicatario, assume la qualifica di Responsabile del trattamento dei dati personali trattati, per conto del Consiglio regionale (Titolare del trattamento), nell'ambito dell'esecuzione delle prestazioni di cui al presente foglio patti e condizioni ed è tenuto alla piena e diligente esecuzione dei compiti indicati nell'allegato D, che costituisce parte integrante e sostanziale del presente foglio patti e condizioni.

3. Il Fornitore tratta esclusivamente i dati personali necessari per lo svolgimento delle operazioni funzionali a garantire l'utilizzo degli applicativi necessari per l'erogazione del servizio, inclusi migrazione, attivazione, mantenimento, aggiornamento e gestione, assistenza e supporto tecnico, garantendo la funzionalità e la sicurezza degli applicativi e dei dati utilizzati, inclusi quelli generati dalla piattaforma, nonché la conformità alla normativa sui cookies, sulla sicurezza informatica e alla Normativa privacy. In ogni caso, tutti i dati personali possono essere trattati dal Fornitore nell'ambito e solo nei limiti in cui sia indispensabile per effettuare le prestazioni contrattuali, garantendo la tutela della riservatezza, l'integrità e la disponibilità dei dati.
4. Il Fornitore garantisce, per l'ambito di trattamento affidato, la messa in atto delle misure tecniche ed organizzative necessarie 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.
5. Il Fornitore è obbligato a conservare i dati personali esclusivamente per i tempi stabiliti dal presente foglio patti e condizioni e dalle norme di legge applicabili in materia, comunque non oltre un mese dal termine del contratto, salva diversa indicazione del Titolare.
6. Il Fornitore è tenuto a presentare all'Amministrazione garanzie in termini di conoscenza specialistica, affidabilità, risorse, anche in ordine all'adozione di misure tecniche, logiche ed organizzative idonee per assicurare che i trattamenti dei dati personali affidatigli avvengano in conformità alla normativa Privacy; a tale fine il Fornitore è tenuto a trasmettere, 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 organizzative, tecniche e di sicurezza implementate anche con riferimento agli applicativi. Il Fornitore deve mantenere, per tutta la durata dell'affidamento, un'organizzazione adeguata all'esecuzione dell'incarico di trattamento dei dati personali connesso alle prestazioni contrattuali, garantendo il pieno rispetto, per sé e per i propri dipendenti e collaboratori, delle istruzioni sul trattamento dei dati personali dell'allegato D, oltre che di tutte le norme di legge in materia applicabili.
7. 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 RGPD.

8. Il Fornitore è obbligato a collaborare con il Titolare del trattamento per il rispetto delle norme sulla protezione dei dati personali e deve fornire al Consiglio regionale la documentazione e le informazioni necessarie in relazione ai servizi svolti e alle misure di sicurezza applicate e garantire l'assistenza necessaria per garantire il rispetto della Normativa privacy, compresa, se richiesta, l'assistenza alla redazione dell'analisi del rischio per la protezione dei dati personali (art. 32 e 35 RGPD) secondo le procedure di cui alla deliberazione 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. allegata alla documentazione di gara e ss.mm.ii.
9. Il Fornitore ha l'obbligo di comunicare un recapito per comunicazioni relative 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.
10. 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.
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 rinnovo, ripetizione, differimento, aumento del quinto o proroga. La designazione cessa 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. Il Fornitore è responsabile per tutta la durata dell'affidamento per l'esatta osservanza dello stesso e della designazione, per sé e per i 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 oppure al termine del contratto, anche anticipato per recesso o risoluzione, il Fornitore s'impegna a seguire le istruzioni impartite dal Titolare, provvedendo alle operazioni richieste dal Titolare stesso, inclusa la restituzione e la cancellazione dei dati, salva la conservazione di eventuali dati che il Fornitore deve conservare per obbligo di legge.
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 deve essere effettuata in conformità dell'art. 28, par. 2 e 4, RGPD. Il Fornitore è autorizzato a ricorrere ad ulteriori Responsabili per l'esecuzione delle prestazioni.
15. In conformità agli articoli 82 e 83, 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 del presente foglio patti e condizioni, della Normativa privacy e dei compiti e istruzioni di cui all'allegato D 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. 16 - Patto di riservatezza

1. Ferme le disposizioni di cui al precedente articolo, i dati economici, finanziari, patrimoniali o di qualunque altro genere, che vengano a conoscenza del Fornitore, in ragione dei servizi resi per il Consiglio regionale, sono riservati. I dati e le informazioni, non oggetto di pubblicazione in base alla legge, fermo il divieto di cui al comma 13 dell'articolo precedente, venute a conoscenza del Fornitore in relazione all'esecuzione del 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 contratto.
2. Il Fornitore è tenuto a mantenere riservati tali dati, a non divulgarli in alcun modo e a non utilizzarli per scopi diversi da quelli relativi all'esecuzione del contratto. Il Fornitore è responsabile per l'esatta osservanza da parte dei propri dipendenti o collaboratori impegnati nell'esecuzione delle prestazioni contrattuali dei suddetti obblighi di riservatezza.
3. Tale clausola deve intendersi vincolante anche dopo la cessazione del contratto.
4. Il Consiglio regionale s'impegna a trattare, in conformità al d.lgs. 196/2003 e al RGPD, i dati personali conferiti dal Fornitore per le sole finalità di definizione e gestione del contratto e dei relativi pagamenti, provvedendo alle comunicazioni e alle pubblicazioni dei dati relativi all'affidamento secondo quanto previsto dal d.lgs. 36/2023, dal d.lgs. 33/2013 e dalle altre norme in materia come descritto nell'informativa sul trattamento dei dati personali di cui all'art. 13 e 14 RGPD allegata alla documentazione della procedura di affidamento.

Art. 17 - Rispetto del codice di comportamento dei dipendenti pubblici e del personale del Consiglio regionale della Lombardia

1. Il Fornitore, con la sottoscrizione del presente Foglio Patti e condizioni, si impegna a osservare e a far osservare ai propri dipendenti e collaboratori a qualsiasi titolo gli obblighi di condotta previsti dal d.p.r. 16 aprile 2013, n. 62 "Codice di comportamento dei dipendenti

pubblici” pubblicato nella Gazzetta Ufficiale n. 129 del 4.06.2013 e dal Codice di Comportamento del personale del Consiglio regionale della Lombardia adottato con Deliberazione dell’Ufficio di Presidenza 24.10.2022 n. 356 entrambi disponibili al seguente link: <https://www.consiglio.regione.lombardia.it/wps/portal/crl/home/amministrazione-trasparente/personale/codice-disciplinare-e-di-condotta>.

Art. 18 - 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 impiegati nel presente servizio gli obblighi di condotta previsti dal “Patto di integrità per le procedure di affidamento di lavori, servizi e forniture” (di seguito Patto) per le procedure di affidamento di lavori, servizi e forniture, approvato con decreto dirigenziale 31 ottobre 2025, n. 359, allegato alla documentazione di procedura e comunque disponibile sul sito istituzionale del Consiglio regionale.
2. Il Fornitore ha l’onere di pretendere il rispetto del Patto anche dai propri subfornitori. La clausola che prevede il rispetto degli obblighi derivanti dal Patto deve essere inserita nei contratti stipulati dall’Affidatario con i propri subfornitori.
3. La violazione degli obblighi del Patto da parte del Fornitore comporta, alternativamente o cumulativamente, l’applicazione di una delle sanzioni di cui all’art. 4 del Patto.
4. Il Consiglio regionale può non avvalersi della risoluzione del contratto qualora lo ritenga pregiudizievole agli interessi pubblici, quali indicati dall’articolo 121, comma 2, del Codice del processo amministrativo, approvato con d.lgs. 2 luglio 2010, n. 104, salvo in ogni caso il diritto al risarcimento del danno.

Art. 19 - 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 ad essi riferiti.

Art. 20 - Segnalazione di violazioni nell’Amministrazione (c.d. whistleblowing) da parte dei lavoratori e 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 dell’Amministrazione consiliare che, nell’interesse pubblico

e dell'integrità del Consiglio regionale, segnalano al Responsabile della prevenzione della corruzione e della trasparenza (RPCT) del Consiglio regionale le violazioni di norme nazionali ed europee che consistono in illeciti penali, civili, contabili e amministrativi, di cui siano venuti a conoscenza in ragione del rapporto di lavoro/collaborazione, non possono essere sanzionati, demansionati, licenziati, trasferiti, o sottoposti ad altra misura, determinata dalla segnalazione, avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro. L'adozione di misure ritenute ritorsive nei confronti del segnalante può essere segnalata all'ANAC per i provvedimenti di competenza. Sono previste forme di garanzia della riservatezza dell'identità del segnalante il cui nominativo non può essere comunicato se non con il consenso del segnalante o in caso di legittima richiesta dell'Autorità giudiziaria e contabile.

2. Il Fornitore è tenuto a informare i propri dipendenti o collaboratori a qualsiasi titolo impegnati in prestazioni o servizi per l'Amministrazione consiliare della tutela di cui al comma 1 e a renderli edotti che sul portale del Consiglio regionale è messa a disposizione, nella sezione "Segnalazione di violazioni nell'amministrazione (whistleblowing)", la "Procedura per la segnalazione di violazioni nell'Amministrazione (c.d. whistleblowing) ai sensi del decreto legislativo 24/2023", con i dati di contatto del RPCT, le istruzioni e il link alla piattaforma web "Segnalazione illeciti", nonché l'informativa sul trattamento dei dati personali.

Art. 21 - Stipulazione del contratto

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

Art. 22 - Risoluzione delle controversie e Foro competente

1. 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. 23 - Indirizzo di posta elettronica certificata del Consiglio regionale

1. Le comunicazioni a mezzo di posta elettronica certificata destinate al Consiglio regionale devono essere spedite al seguente indirizzo:
protocollo.generale@pec.consiglio.regione.lombardia.it.

Art. 24 - Norma finale

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

Firma digitale per accettazione

Clausole del Foglio Patti e condizioni di cui all'art. 1341 c.c.

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

Ai sensi e per gli effetti dell'articolo 1341 del Codice civile, sono individuate le clausole di cui agli articoli 5 (Responsabilità del Fornitore), 7 (Revisione dei prezzi), 8 (Penali), 9 (Clausola risolutiva ai sensi dell'art. 1456 del Codice civile), 11 (Recesso ai sensi dell'art. 123 del d.lgs. 36/2023), 15 (Trattamento dei dati personali e designazione del Fornitore quale responsabile del trattamento), 16 (Patto di riservatezza), 17 (Rispetto del codice di comportamento dei dipendenti pubblici e del personale del Consiglio regionale della Lombardia), 18 (Rispetto del Patto di integrità e relative sanzioni) e 22 (Risoluzione delle controversie e Foro competente), del presente Foglio Patti e condizioni.

Allegato D

Atto di designazione come responsabile del trattamento dei dati personali e individuazione dei trattamenti consentiti, delle finalità, della tipologia dei dati personali e dei compiti del responsabile del trattamento, ai sensi dell'art. 28 del Regolamento UE 2016/679 del 27 aprile 2016, per il servizio di migrazione dati, configurazione, manutenzione e aggiornamento dei software CLAVIS e DISCOVERY per le esigenze della Biblioteca del Consiglio regionale, anche nell'ambito della partecipazione al Polo SBN L02

Sommario

PREMESSA	3
DURATA	4
OBBLIGHI DEL TITOLARE DEL TRATTAMENTO	4
OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO	5
PERSONALE E ALTRI COLLABORATORI	6
SISTEMA DI AUTENTICAZIONE PER GLI INCARICATI DEL RESPONSABILE E PER I DIPENDENTI DEL TITOLARE	7
AMMINISTRATORI DI SISTEMA	9
RISPETTO DELLA NORMATIVA SUI COOKIES	10
MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE	10
ASSISTENZA PER L'UTILIZZO DEGLI APPLICATIVI DEL RESPONSABILE	13
OPERAZIONI DA ESEGUIRE SUI DATI PERSONALI AL TERMINE DELL'AFFIDAMENTO, ANCHE ANTICIPATO	14
OBBLIGHI DI INFORMAZIONE E COLLABORAZIONE	15
DESIGNAZIONE DI SUB-RESPONSABILI (ART. 28, PAR. 2 E 4, RGPD)	16
GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA E VIOLAZIONI DI DATI PERSONALI (<i>DATA BREACH</i>)	17
LUOGO DI TRATTAMENTO E TRASFERIMENTO DI DATI PERSONALI	18
OBBLIGHI DEL RESPONSABILE RELATIVI ALL'INFRASTRUTTURA CLOUD UTILIZZATA PER L'EROGAZIONE DEL SERVIZIO	19
ATTIVITÀ DI VIGILANZA E VERIFICA DEL TRATTAMENTO	19
INDIVIDUAZIONE DI MAGGIORI LIVELLI DI SICUREZZA E ADEGUAMENTI ALLA NORMATIVA PRIVACY SOPRAVVENUTA O A ESIGENZE CONTRATTUALI SOPRAVVENUTE	20
COMUNICAZIONI	20
DISPOSIZIONI FINALI	20
DATI DI CONTATTO DEI RESPONSABILI DELLA PROTEZIONE DEI DATI PERSONALI (RPD)	20
ALLEGATI	21
Allegato A.1 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI DI TITOLARITÀ DEL CONSIGLIO REGIONALE AFFIDATI AL FORNITORE IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO	22
Allegato A.2 - ELENCO DELLE MISURE DI SICUREZZA	1

Allegato A.3 - (MODELLO PER LA COMUNICAZIONE DEGLI ESTREMI IDENTIFICATIVI DEGLI AMMINISTRATORI DI SISTEMA ESTERNI OPERANTI SU SISTEMI DEL TITOLARE DEL TRATTAMENTO)7

PREMESSA

Ai fini del presente Atto, s'intende per:

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

Il presente atto è stato predisposto al fine di specificare, ai sensi dell'art. 28 del Regolamento (UE) 2016/679, i trattamenti di dati personali affidati dal Consiglio regionale al Fornitore definendo la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi gravanti sul Titolare e sul Responsabile del trattamento.

Il **Titolare del trattamento** e il **Responsabile del trattamento** dichiarano reciprocamente di essere informati e di acconsentire che i dati personali forniti o raccolti in conseguenza dell'affidamento

sono trattati esclusivamente per le finalità ivi indicate ed in conformità a quanto previsto dalla vigente normativa in materia di protezione dei dati personali.

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

Le premesse e gli allegati **A.1** (Elenco dei trattamenti dei dati personali di titolarità del Consiglio regionale della Lombardia effettuati dal Fornitore in qualità di Responsabile del trattamento) e **A.2** (Elenco delle misure di sicurezza applicate dal Fornitore) e **A.3** (Facsimile per comunicazione degli estremi identificativi degli amministratori di sistema esterni), costituiscono parte integrante e sostanziale del presente Atto.

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

DURATA

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

La designazione e il presente Atto cesseranno automaticamente di avere efficacia in ipotesi di risoluzione, recesso o perdita di efficacia dell'Affidamento, salvo il tempo eventualmente necessario a consentire al Consiglio regionale di recuperare i dati personali, come contrattualmente definito, comunque fino alla cessazione delle attività svolte a favore del Titolare del trattamento.

Parimenti, in caso di ripetizione, rinnovo, proroga, aumento del quinto e differimento a ogni titolo della durata dell'Affidamento, la designazione e il presente Atto continueranno a produrre i propri effetti senza necessità di ulteriori atti delle parti.

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

OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

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

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

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

OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

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

Il **Responsabile del trattamento** esegue esclusivamente i trattamenti di cui all’Allegato A.1, richiesti dal Titolare del trattamento e indispensabili per l’esecuzione delle prestazioni contrattuali in modo lecito e secondo correttezza, per scopi legittimi e determinati assicurando l’esattezza e la completezza dei dati e garantendo il rispetto dei principi di necessità, proporzionalità, pertinenza e non eccedenza, e svolge i compiti sotto indicati, come descritto nell’Affidamento o concordate con il Titolare con altro valido atto scritto, attenendosi alla Normativa Privacy e rispettando gli obblighi di cui al presente Atto e alle istruzioni impartite dal Titolare del trattamento.

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 decorso un mese dalla conclusione dell’affidamento, salvo diversa richiesta del Titolare.

Il **Responsabile del trattamento** è autorizzato a effettuare copie di dati in ambienti di test o pre-produzione per le attività di migrazione o manutenzione. tali dati devono essere cancellati non appena terminate le predette attività.

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, incluso per la

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

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

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

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

PERSONALE E ALTRI COLLABORATORI

Il **Responsabile del trattamento** adotta le misure appropriate per garantire la conformità al presente Atto delle attività e dei comportamenti dei suoi dipendenti 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 mediante la sottoscrizione di apposite dichiarazioni, le cui copie saranno messe a disposizione del Titolare del trattamento su richiesta per l'esercizio delle attività di controllo e vigilanza di propria competenza.

- a) 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/cancellazione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti/cancellati 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 PER GLI INCARICATI DEL RESPONSABILE E PER I DIPENDENTI DEL TITOLARE

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

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

- a) prevedere profili di autorizzazione di accesso per ogni singolo soggetto incaricato/autorizzato al trattamento o gruppo omogeneo e configurarli prima dell'inizio dei trattamenti in modo adeguato alle mansioni svolte e agli ambiti di trattamento affidati;
- b) assicurarsi che a ogni soggetto incaricato/autorizzato sia assegnata una credenziale di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione del soggetto autorizzato al trattamento associato a una parola chiave (password) riservata e conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e a uso esclusivo dell'incaricato/autorizzato, eventualmente associato a un codice identificativo o a una parola chiave. Non è ammessa la creazione di credenziali non nominative, salvo specifica richiesta del Titolare;
- c) prescrivere necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso a uso esclusivo del soggetto incaricato/autorizzato al trattamento;
- d) assicurare che per la componente riservata della credenziale di autenticazione siano previste adeguate misure di sicurezza;
- e) richiedere al soggetto interessato di utilizzare sempre le proprie credenziali personali mantenendole riservate, evitando di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire l'individuazione dell'autore del trattamento;

- f) assicurare che la parola chiave, quando prevista sia composta da almeno quattordici (14) caratteri misti alfanumerici; essa non deve contenere riferimenti agevolmente riconducibili all'Incaricato e deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi, ovvero predisporre un sistema di autenticazione multifattoriale con un ulteriore fattore di autenticazione oltre al codice di identificazione e alla password;
- g) assicurare che l'utenza venga bloccata dopo un numero di tentativi falliti di accesso pari a tre;
- h) assicurare un sistema di reset della password previa identificazione del richiedente;
- i) assicurare che il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri incaricati, neppure in tempi diversi e assicurare che sia operata la disattivazione delle credenziali di autenticazione o delle abilitazioni di accesso del personale in caso venga a cessare la necessità di accesso da parte del soggetto incaricato autorizzato al trattamento o intervenga un'inattività per più di tre mesi;
- j) predisporre le necessarie procedure affinché, in caso di prolungata assenza o impedimento dell'incaricato/autorizzato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, si possa comunque assicurare la disponibilità di dati o strumenti elettronici;
- k) verificare a intervalli almeno annuali le autorizzazioni in essere;
- l) implementare un sistema di autenticazione a due fattori su richiesta del Titolare in base al livello di rischio dei trattamenti di dati personali e alle prescrizioni delle norme di riferimento;
- m) adottare misure per prevenire e contrastare attacchi informatici di tipo credential stuffing (testing username/password pairs obtained from the breach of another site), brute force (testing multiple passwords from dictionary or other source against a single account) e password spraying (testing a single weak password against).

Il **Responsabile del trattamento** è tenuto ad applicare le prescrizioni minime di sicurezza sopra riportate anche alle credenziali di autenticazione fornite agli incaricati/autorizzati del Titolare del trattamento per gli applicativi utilizzati per l'erogazione del servizio. Diverse misure di sicurezza applicate al sistema di autenticazione possono essere autorizzate per iscritto dal Titolare del trattamento, previa verifica della loro adeguatezza rispetto ai rischi per i dati personali.

Su richiesta del direttore dell'esecuzione o di suo delegato, il **Responsabile del trattamento** è tenuto ad operare l'attivazione e la disattivazione delle credenziali di autenticazione per i soggetti indicati dal Titolare in caso venga a cessare la necessità di accesso.

È consentita l'implementazione di ulteriori o diverse misure di sicurezza rispetto a quanto sopra solo qualora le misure garantiscano un maggior livello di sicurezza.

Il Responsabile del trattamento mette a disposizione un inventario delle utenze presenti nel sistema con i relativi profili di autorizzazione assegnati, disponibile al Titolare per sua rendicontazione e analisi degli accessi.

Il **Responsabile del trattamento** è tenuto ad adottare un sistema di salvataggio dei log di accesso al sistema in modo che il Titolare possa esportarli.

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

AMMINISTRATORI DI SISTEMA

Per quanto riguarda le attività degli amministratori di sistema svolti su infrastrutture e reti proprie o nella propria disponibilità, 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, e garantire ogni altra misura per l'assolvimento delle prescrizioni e degli obblighi di cui al provvedimento del Garante per la protezione dei dati personali del 27.11.2008 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.

Qualora nel corso delle attività si rendesse necessario lo svolgimento di attività da parte di AdS del Responsabile del trattamento su infrastrutture e reti del Consiglio, gli estremi identificativi degli AdS designati dovranno essere comunicati al Titolare mediante sottoscrizione e trasmissione di apposito modello contenuto nell'allegato A.3. Il Titolare, nel rispetto delle policies di sicurezza da esso stabilite, s'impegna a garantire, se necessario, l'accesso al proprio sistema informatico mediante rilascio di idonee credenziali da parte dell'Ufficio preposto, al momento dell'assegnazione del servizio e previa designazione degli amministratori di sistema.

I nomi degli AdS sono inseriti in apposito Elenco aggiornato dal Titolare e consultabile dagli interessati nella sezione privacy della Intranet consiliare.

L'attività degli AdS è soggetta a monitoraggio, ai sensi del provvedimento del Garante per la protezione dei dati personali del 27.11.2008 sugli amministratori di sistema e successive modifiche e integrazioni, da parte di Aria S.p.a. o suo subfornitore o da altro soggetto in qualità di responsabile del trattamento del Consiglio regionale. Il sistema di access log garantisce le verifiche necessarie e è dotato di sistemi di allerta nel caso di anomalie sull'utilizzo delle credenziali degli AdS (es. accesso in orario notturno, ripetuti tentativi di accesso falliti) comunicando al Consiglio regionale l'occorrenza di tali anomalie.

Il Provvedimento del Garante prevede che sia tenuta traccia degli accessi logici effettuati dagli AdS ai sistemi amministrati. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono svolte. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo di tempo, non inferiore a sei mesi.

Per access log si intende la registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o del tentativo di accesso da parte di un AdS o all'atto della sua

disconnessione nell'ambito di collegamenti interattivi a server, postazioni di lavoro, data base e sistemi di sicurezza informatica.

Il **Responsabile del trattamento** è tenuto a informare i soggetti designati come ADS di quanto stabilito nel presente atto con riferimento alla loro attività.

RISPETTO DELLA NORMATIVA SUI COOKIES

Il **Responsabile del trattamento** si impegna a garantire che gli applicativi web utilizzati per il servizio siano configurati al fine di garantire il trattamento dei soli dati degli utenti indispensabili all'erogazione del servizio, nel rispetto di quanto definito dal provvedimento del Garante per la protezione dei dati personali n. 231 del 10 giugno 2021 recante "Linee guida cookie e altri strumenti di tracciamento" pubblicato sulla Gazzetta Ufficiale n. 163 del 9 luglio 2021 e di quanto definito nell'allegato A.1. del presente atto.

Il **Responsabile del trattamento** fornisce al Titolare del trattamento le informazioni e il supporto necessari per assicurare la corretta informazione degli interessati circa il rispetto e la conformità del portale alla normativa sui cookies e ai provvedimenti anche futuri del Garante, mettendo a disposizione sulla piattaforma apposita cookie policy e informativa per gli utilizzatori, anche assistendolo il Titolare nella redazione dell'informativa che lo stesso mette a disposizione degli interessati, e mettendo in atto le misure tecniche e organizzative che si rendano all'uopo necessarie, nonché garantendo l'effettuazione di un monitoraggio circa la rispondenza del servizio web alla normativa e la trasmissione di apposito report al Titolare.

Le eventuali difformità rilevate devono essere immediatamente comunicate al Titolare affinché assuma le necessarie determinazioni.

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

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

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

personali effettuato dalle imprese di sviluppo e produzione di software gestionale, adottato dal Garante per la protezione dei dati personali in data 7 ottobre 2024.

Il **Responsabile del trattamento** è tenuto ad assicurare l'anonimizzazione di tutti o parte dei dati da migrare sugli applicativi forniti, a richiesta e secondo le istruzioni del Titolare.

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

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

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

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

- l'accesso ai dati tramite sistema di autenticazione;
- la protezione del computer tramite programmi contro il rischio di intrusione e l'accesso abusivo in accordo ai requisiti di legge aggiornati almeno semestralmente e comunque in occasione di ogni versione disponibile dalla casa costruttrice, anche per i sistemi non connessi in rete o che non accedono a Internet;
- la modifica e l'aggiornamento, ogni qualvolta vi sia la disponibilità e comunque entro un congruo periodo di tempo non superiore a sei mesi, dei programmi utilizzati, o almeno alla valutazione degli impatti sull'aggiornamento.

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

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

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

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

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

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

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

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

Il **Responsabile del trattamento** garantisce di applicare le misure minime di sicurezza individuate nell’allegato A.2. e le altre misure di sicurezza definite nell’Affidamento.

Tra queste rientrano anche le misure di sicurezza definite nel Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale qualora l’applicativo utilizzato sia su Data Center del Responsabile, oppure su Data Center esterni resi disponibili da sub-fornitori del Responsabile.

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

Il **Responsabile del trattamento** è tenuto a predisporre e mettere a disposizione la documentazione degli strumenti utilizzati per trattare i dati (indicazione del DB utilizzato, strumento di scrittura del codice, sistema di conservazione dei documenti prodotti), definendo le misure di sicurezza poste a

tutela dei dati (profili di accesso al DB, crittografia del DB, dialogo tra applicazione e DB e protezione delle password, ecc.).

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

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

ASSISTENZA PER L'UTILIZZO DEGLI APPLICATIVI DEL RESPONSABILE

L'erogazione del servizio di assistenza e di accesso da remoto alle piattaforme devono avvenire mediante connessione VPN, anche con MFA su richiesta del Titolare.

Le attività svolte dagli operatori con utenze privilegiate devono essere tracciate e monitorate.

Gli operatori incaricati dell'assistenza devono accertarsi che le richieste di assistenza provengano da un soggetto identificato e preventivamente autorizzato dal Titolare (ad esempio tramite autenticazione sulla piattaforma di ticketing).

Gli operatori incaricati dell'assistenza devono richiedere al Titolare in modo tracciabile le autorizzazioni necessarie ai fini dell'erogazione del servizio di assistenza (ad esempio, la condivisione dello schermo, il controllo condiviso dell'applicativo, il trasferimento dei file e la registrazione delle attività).

L'eventuale copia o trasferimento di archivi o base dati del Titolare per finalità di assistenza o manutenzione deve essere preventivamente ed espressamente autorizzata dal Titolare stesso.

I DB/archivi del Titolare devono essere conservati per il tempo strettamente necessario all'esecuzione dell'attività di assistenza e immediatamente cancellati qualora non più necessari per l'esecuzione delle operazioni di assistenza.

Le copie dei DB/archivi del Titolare prelevati per finalità di assistenza devono essere trasferite tramite canali sicuri e protetti, salvate in ambienti dotati delle opportune misure di sicurezza e non devono essere sottoposti a backup allo scopo di minimizzare il trattamento, salvo anonimizzazione. Qualora durante le attività di assistenza fosse necessario stampare documenti o informazioni, tali documenti devono rimanere nell'esclusiva disponibilità dell'operatore e da questi devono essere protetti contro accessi non autorizzati. Al termine dell'attività, i documenti dovranno essere distrutti.

Sono adottati processi e strumenti di assistenza che assicurino la tracciabilità degli interventi richiesti ed eseguiti (piattaforma di ticketing).

Al termine dell'affidamento i DB/archivi del Titolare contenenti le richieste di assistenza devono essere anonimizzati su richiesta del Titolare prima della restituzione allo stesso o del trasferimento ad altro soggetto.

OPERAZIONI DA ESEGUIRE SUI DATI PERSONALI AL TERMINE DELL'AFFIDAMENTO, ANCHE ANTICIPATO

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

- alla restituzione completa dei dati personali di titolarità del Consiglio regionale, di cui abbia disponibilità;
- alla distruzione di eventuale documentazione contenente i dati personali di cui all'allegato A.1, salvo sia obbligatorio conservare alcuni documenti in ragione degli adempimenti amministrativi e contabili stabiliti dalla legge o di specifica richiesta da parte del Titolare del trattamento;
- alle altre operazioni richieste dal Titolare del trattamento stesso o previste dall'Affidamento, compresa la cancellazione dei dati personali di cui all'allegato A.1. dai supporti elettronici e informatici utilizzati con modalità che non ne consentano il recupero, in conformità al provvedimento del Garante per la protezione dei dati personali 13 ottobre 2008 in materia di rifiuti di apparecchiature elettriche ed elettroniche (RAEE) e misure di sicurezza dei dati personali.

In questo ambito risulta necessario procedere a:

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

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

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

Rimangono ferme le eventuali specificazioni definite nell'Affidamento.

OBBLIGHI DI INFORMAZIONE E COLLABORAZIONE

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

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

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

Il **Responsabile del trattamento** è comunque tenuto a fornire al Titolare le informazioni necessarie alla compilazione del "Registro delle attività di trattamento" e delle informative sul trattamento dei dati personali per gli interessati, come previsto dalla Normativa privacy, anche curando ogni necessario rapporto con gli eventuali sub responsabili e a mettere a disposizione del **Titolare del trattamento** le informazioni necessarie all'espletamento delle attività di revisione, comprese le ispezioni richieste dallo stesso Titolare del trattamento o da altro soggetto da esso autorizzato, al fine di rilevare il rispetto degli obblighi previsti dalla Normativa privacy e dal contenuto specifico dell'Affidamento del servizio richiamato nel presente Atto.

Il **Responsabile del trattamento** deve evadere tempestivamente le richieste del Titolare e impegnarsi alla collaborazione necessaria in modo da consentire l'esercizio dei diritti da parte degli interessati, richiamati dalla Normativa privacy.

Nel caso in cui il **Responsabile del trattamento** riceva, da parte dell'interessato, un'istanza per l'esercizio dei suoi diritti ai sensi degli artt. da 15 a 22 RGPD è tenuto a inoltrarla prontamente al **Titolare del trattamento**.

Il Titolare provvederà a informare gli interessati ai sensi della Normativa privacy (articoli 13 e 14 RGPD); al fine di consentire tale attività, il **Responsabile del trattamento** deve fornire tutte le informazioni richieste dal Titolare.

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.

Il **Responsabile del trattamento** è tenuto a redigere e rendere consultabile agli interessati per gli applicativi web utilizzati per erogare il servizio le informazioni di cui agli articoli 13 e 14 RGPD in accordo con il Titolare del trattamento, fornendone copia previamente all'inizio dell'erogazione del servizio. Il testo definitivo comunque deve essere disponibile al momento dell'accesso agli applicativi utilizzati dal **Responsabile del trattamento** per erogare il servizio. Parimenti, su richiesta del Titolare, con riferimento alle attività di trattamento svolte in occasione della formazione erogata in presenza.

DESIGNAZIONE DI SUB-RESPONSABILI (ART. 28, PAR. 2 E 4, RGPD)

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

Il **Responsabile del trattamento**, in sede di designazione di sub-responsabili, deve informare il **Titolare del trattamento**, al fine di consentire, come previsto dall'art. 28 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 quest'ultima potrà procedere all'effettuazione delle designazioni nei confronti dei sub-responsabili del trattamento individuati.

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

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

Il **Responsabile del trattamento** rimane comunque interamente responsabile nei confronti del Titolare 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 ed è tenuto alla gestione di ogni rapporto con tale soggetto a garanzia della protezione dei dati personali di titolarità del Consiglio regionale e al rispetto della Normativa Privacy.

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

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

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

Il **Responsabile del trattamento** è tenuto a fornire la DPIA o l'analisi dei rischi svolta sul servizio erogato, a richiesta del Titolare.

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

GESTIONE DEGLI INCIDENTI DI SICUREZZA INFORMATICA E VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

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

Fermo quanto previsto nell'affidamento, il **Responsabile del trattamento** è tenuto a comunicare al Titolare, senza ingiustificato ritardo, entro al massimo 24 ore dalla conoscenza dell'evento, ogni violazione dei dati o di incidenti informatici o altro accadimento che possa aver comportato un impatto sui dati personali del Consiglio regionale della Lombardia, **Titolare del trattamento**, violandone la riservatezza, integrità, disponibilità o comunque esponendoli a rischio, secondo quanto richiesto dalla Normativa privacy vigente.

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

La comunicazione deve contenere almeno le seguenti informazioni:

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

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

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

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

Il Responsabile del trattamento è tenuto a comunicare i numeri di reperibilità relativi alle figure di Security Manager, a garanzia di una corretta e tempestiva erogazione di tutti i servizi a suo carico, di cui viene riportato di seguito un elenco esemplificativo ma non esaustivo:

- comunicazione e gestione di incidenti di sicurezza;
- comunicazione e gestione di eventi di data breach;
- test tecnici e/o organizzativi di Disaster Recovery;
- attivazione dei servizi in Disaster Recovery;
- piano di rientro dal Disaster Recovery.

LUOGO DI TRATTAMENTO E TRASFERIMENTO DI DATI PERSONALI

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

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

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

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

- 1) trasferire i dati personali a un titolare del trattamento o a un responsabile del trattamento in un paese terzo o in un'organizzazione internazionale situati fuori dall'Unione europea;

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

OBBLIGHI DEL RESPONSABILE RELATIVI ALL'INFRASTRUTTURA CLOUD UTILIZZATA PER L'EROGAZIONE DEL SERVIZIO

In caso di utilizzo di cloud per l'erogazione del servizio, il **Responsabile del trattamento** garantisce di utilizzare un'infrastruttura cloud conforme alle «best-practice» del settore e si impegna a adeguarla ovvero a mantenerla adeguata alle necessità dell'incarico stesso, garantendo il pieno rispetto degli obblighi e adempimenti previsti dalla normativa europea e italiana in materia.

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

ATTIVITÀ DI VIGILANZA E VERIFICA DEL TRATTAMENTO

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

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

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

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

Il **Responsabile del trattamento** è tenuto ad informare su richiesta, e comunque 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. Il Responsabile del trattamento si impegna a collaborare nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse.

COMUNICAZIONI

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

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

DISPOSIZIONI FINALI

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

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

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

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

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

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

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

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

ALLEGATI

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

A.2 "Elenco delle misure di sicurezza applicate dal Fornitore"

A.3 "Modello Facsimile per la comunicazione degli estremi identificativi degli amministratori di sistema esterni operanti su sistemi del Titolare del trattamento"

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

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

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

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

Servizio affidato	Finalità e ambito dei trattamenti affidati al Responsabile	Tipologia di dati trattati e categorie di interessati	Responsabile CRL di gestione del servizio e referente operativo CRL	Subresponsabile del trattamento
--------------------------	---	--	--	--

Servizio di migrazione dati, configurazione, manutenzione e aggiornamento dei software CLAVIS e DISCOVERY per le esigenze della Biblioteca del Consiglio regionale, anche nell'ambito della partecipazione al Polo SBN L02.	- Assicurare la gestione e l'erogazione dei servizi della biblioteca - Gestione e consultazione del catalogo online (OPAC) della Biblioteca consiliare e del Polo SBN 02 - Gestione efficiente dei materiali e del servizio di prestito Partecipazione al Polo SBN L02 anche mediante catalogo condiviso - Contribuire alla diffusione della conoscenza e fornire supporto informativo e documentale Formazione e aggiornamento in modalità online (sincrona e asincrona) e in presenza Manutenzione - Garanzia della funzionalità e sicurezza e della conformità alle norme di legge Garanzia della inalterabilità dei dati - Sicurezza e stabilità del portale di accesso agli applicativi online - Conformità alle previsioni in materia di cookies Migrazione del gestionale attuale verso nuovo applicativo - Gestione delle richieste di assistenza degli operatori e archivio delle richieste - Backup - Supporto e assistenza tecnica	Dipendenti e tirocinanti del Consiglio regionale, Giunta regionale ed enti del Sireg, Consiglieri regionali, componenti della Giunta regionale: Dati personali (nome e cognome, codice fiscale, indirizzo di posta elettronica istituzionale, numero di telefono, ente e ufficio di appartenenza, dati relativi ai prodotti presi in prestito) Dipendenti del Consiglio regionale abilitati ad accedere all'applicativo: - Dati personali (credenziali di autenticazione qualora nominative, orario di accesso, dati di navigazione e log, eventuali cookie generati dalla piattaforma); - Dati di telemetria (Codice utente collegato, Username, Gruppo applicativo di appartenenza, IP utilizzato, Versione del browser in uso, Azione effettuata, Errori applicativi (se presenti)) - Motivazioni dei ticket e relativa classificazione. Dati personali di qualsivoglia tipo ivi contenuti; - dati relativi alla formazione (presenza/assenza, esito).	Direttore dell'esecuzione: dirigente Servizio Studi, Valutazione delle Politiche e Qualità della Normazione	Hetzner Online GmbH
--	---	--	--	----------------------------

	- Gestione amministrativa - Consentire l'estrazione di dati statistici specifici o aggregati - interoperabilità con altri applicativi			
--	---	--	--	--

Modalità di trattamento e principali trattamenti svolti

Il trattamento è effettuato con l'ausilio di strumenti elettronici.

Le operazioni di trattamento autorizzate sono:

|X| raccolta |X| registrazione |X| organizzazione |_| strutturazione |X| conservazione |_| adattamento |_| modifica |X| visualizzazione |X| estrazione |X| uso |X| comunicazione agli interessati e al Consiglio regionale |_| diffusione |_| raffronto |_| interconnessione |_| limitazione |X| cancellazione secondo le istruzioni del Titolare del trattamento |X| distruzione secondo le istruzioni del Titolare del trattamento |_| copia, duplicazione, riproduzione e registrazione solo su autorizzazione del Titolare del trattamento.

La trasmissione dei dati personali è consentita solo con modalità sicure (es. file criptati con password comunicata con altro canale).

Le prestazioni comportano, tra gli altri:

- la predisposizione di misure di sicurezza applicativa per garantire integrità, stabilità e riservatezza dei dati personali;
- attività tecniche e funzioni di amministratore di sistema;
- connessione sicura HTTPS con crittografia/autenticazione tramite SSL/TLS;
- accesso ai servizi mediante dispositivi fissi;
- download di materiale;
- comunicazioni ed istruzioni tecniche ed operative per risoluzione di problemi o lo svolgimento dei corsi di formazione;
- tracciamento accesso degli utenti con indicazione data ed orario di accesso (logged in) e di uscita (logged out), ip di accesso, cookie statistici, tentativi di accesso errati;
- estrazione di documenti di monitoraggio sull'utilizzo della piattaforma;
- autenticazione tramite accesso con proprie credenziali con possibilità di prevedere sistemi di autenticazione a più fattori (MFA);
- profilazione degli accessi con gestione dei ruoli e dei permessi;
- applicazione alle credenziali di autenticazione di metodi sicuri di cifratura che non ne consentano la visione in chiaro da parte di terzi;
- messa a disposizione di infrastrutture in cloud, conformi ai requisiti di sicurezza e accessibilità previsti dalla normativa per le infrastrutture e i servizi cloud delle pubbliche amministrazioni;
- conservazione dei dati anche in apposita piattaforma web;
- registrazione degli eventi formativi in presenza;
- assistenza tecnica;
- interoperabilità con piattaforma MLOL;

- migrazione dei dati dal precedente applicativo all'applicativo oggetto del servizio;
- anonimizzazione dei dati contenuti nell'applicativo e relativi alle richieste di assistenza su richiesta del Titolare;
- attività di backup e soluzione disaster recovery;
- risoluzione di malfunzionamenti, aggiornamenti e modifiche;
- gestione del servizio di ticketing;
- interventi di manutenzione adeguativa e sviluppo di nuove funzionalità necessarie per migliorare o evolvere il software.

Sono escluse attività di profilazione degli utenti.

Le prestazioni possono essere effettuate presso la sede del Consiglio ovvero da remoto utilizzando un collegamento crittografato VPN con autenticazione a due fattori su richiesta del Consiglio regionale.

I dati non possono essere utilizzati per altri scopi (salvo se anonimizzati).

Il sistema di gestione del processo di controllo utenti/accessi deve avvenire nel rispetto dei principi di sicurezza informatica, per confermare che gli utenti siano chi dicono di essere e che abbiano il diritto di accedere in base a criteri di accesso e identità concordati con il Titolare.

Il sistema finale di auditing e monitoraggio del servizio può comportare il trattamento esclusivamente di dati non riconducibili agli interessati.

Conservazione

Per i log, cookies, dati di navigazione e di telemetria: massimo sei mesi.

Per gli altri dati: il Responsabile provvede alla cancellazione dei dati personali entro un mese dalla conclusione dell'affidamento, salvo diversa istruzione del Titolare e salvo che il diritto dell'Unione o degli Stati membri, cui è soggetto il Responsabile, prescriva la conservazione dei dati personali. Il Responsabile garantisce l'integrale trasferimento dei dati contenuti nei sistemi e supporti utilizzati per il trattamento al Titolare o a terzi da questi indicati con modalità e organizzazione tali da consentirne il trattamento secondo le modalità previste per l'erogazione del servizio oggetto dell'incarico e protetti da crittografia. Su richiesta i dati devono essere anonimizzati prima alla conclusione del contratto (es. dati relativi alle richieste di assistenza, dati contenuti nel gestionale relativi alle utenze e agli utenti non più attivi).

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

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

Sicurezza infrastrutturale

Barrare le misure adottate	Misura di sicurezza
X	gestione di più profili con privilegi diversi
X	utilizzo credenziali uninominali per quanto attiene le componenti infrastrutturali di competenza del responsabile del trattamento
X	gli utenti non devono essere in grado di disattivare o bypassare le impostazioni di sicurezza
X	autenticazione delle utenze username/password
X	utilizzo di password sicure (almeno quattordici caratteri alfanumerici)

Barrare le misure adottate	Misura di sicurezza
☐	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
☒	protezione/cifratura dei backup
☐	archiviazione separata dati comuni e dati particolari (sensibili e/o giudiziari)
☒	programma di test dei restore
☒	protezione da malware
☒	le applicazioni antivirus e le firme di rilevamento devono essere aggiornate almeno su base settimanale
☒	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
☒	protezione del traffico tramite Intrusion Detection System
☒	protezione del traffico tramite Intrusion Prevention System
☒	protezione del traffico tramite Web Application Firewall
☒	protezione/cifratura del file system
☒	attivazione delle restrizioni di accesso sul file system
☒	tracciatura degli accessi amministrativi
☐	tracciatura delle attività amministrative

Barrare le misure adottate	Misura di sicurezza
 X 	tracciatura degli accessi al database
 _ 	tracciatura degli accessi a file system
 X 	raccolta centralizzata log
 _ 	utilizzo per l'accesso a internet di un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dal CRL
 X 	programma di protezione dischi rimuovibili
 _ 	programma di controllo piattaforma software
 X 	soluzione di disaster recovery
 _ 	soluzione dlp applicata al contesto
 X 	dismissione supporti di archiviazione già utilizzati
 X 	gestione supporti di archiviazione dismessi
 X 	verifica annuale dell'operato degli amministratori
 X 	aggiornamento delle soluzioni e dei servizi di sicurezza e adeguamento alle normative UE o nazionali senza costi aggiuntivi
 _ 	presenza di un SOC del fornitore
 X 	dispositivi di sicurezza perimetrale su reti del Fornitore (es. Firewall, sistemi di Network Detection ed Event & Log Monitoring, SIEM, ecc.)
 X 	gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente
 _ 	Altro

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

Barrare le misure adottate	Misura di sicurezza
 X 	limitazione di accesso ai locali deputati al trattamento
 _ 	profilazione degli accessi in base a ruolo
 _ 	utilizzo tessere di accesso uninominali limitazione di accesso agli archivi cartacei
 X 	limitazione di accesso agli archivi cartacei
 X 	archiviazione cartacea distinta per livello di severità

Barrare le misure adottate	Misura di sicurezza
_	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)
_	Altro

Sicurezza Organizzativa

Barrare le misure adottate	Misure di sicurezza
X	formazione privacy del personale
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
_	possesso della certificazione ISO/IEC 27001 o, in assenza, di un Sistema di Gestione della

Barrare le misure adottate	Misure di sicurezza
	Sicurezza delle Informazioni (SGSI) di un piano di qualità secondo lo standard ISO 10005
☐	piano di auditing annuale sul sistema di sicurezza da parte di società specializzata, approvata dall'ente
☒	possibilità di auditing a richiesta dell'ente
☐	possibilità di verifiche di conformità dei servizi da parte dell'ente
☐	possesso di certificazioni di sicurezza da parte del personale
☐	consegna, entro il giorno successivo alla richiesta, dei log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT
☒	condivisione della documentazione tecnica (schede tecniche, manuali, guide operative) per la corretta configurazione e gestione degli aspetti di sicurezza
☒	dichiarazione di conformità alla normativa vigente in materia di sicurezza cibernetica e al GDPR
☒	spese per il ripristino della situazione preattacco informatico a carico del Fornitore
☒	utilizzo, previa autorizzazione, di repliche dei dati dell'ente solo nel territorio dell'UE
☐	dichiarazione di disponibilità a far parte di un Comitato di Direzione Tecnica
☒	disponibilità alla sottoscrizione di clausola di non divulgazione
☒	gestione di vulnerabilità scoperte sui prodotti oggetto della fornitura senza costi aggiuntivi
☒	monitoraggio e valutazione continua sulla pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite
☐	descrizione dettagliata della soluzione tecniche applicate (dispositivi hardware e software impiegato, modalità operative, politiche di sicurezza)
☐	Altro

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

Allegato A.3 - (MODELLO PER LA COMUNICAZIONE DEGLI ESTREMI IDENTIFICATIVI DEGLI AMMINISTRATORI DI SISTEMA ESTERNI OPERANTI SU SISTEMI DEL TITOLARE DEL TRATTAMENTO)

Al
Dirigente dell'Ufficio Contratti e ICT del
Consiglio regionale della Lombardia

e p.c.

Ufficio Trasparenza, Prevenzione della
corruzione e Privacy del Consiglio regionale
della Lombardia

Via Fabio Filzi, 22
20124 – Milano

protocollo.generale@pec.consiglio.regione.lomb
ardia.it

Oggetto: Comunicazione degli estremi identificativi degli amministratori di sistema esterni in insourcing - DSG 6 aprile 2016, n. 135 "Revisione e aggiornamento delle regole tecniche e organizzative per la designazione e l'attività degli amministratori di sistema del Consiglio regionale della Lombardia" - Provvedimento del Garante per la protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" - 27 novembre 2008 e successive modificazioni e integrazioni.

Riferimenti contrattuali: _____ (indicare gli estremi del provvedimento di aggiudicazione o del contratto)

La/Il sottoscritta/o _____, in qualità di legale rappresentante di _____ e di responsabile del trattamento, con riferimento al servizio affidato relativo a _____ (indicare l'oggetto del contratto), in conformità al provvedimento del Garante dei dati personali citato in oggetto,

dichiaro, ai sensi e per gli effetti dell'art. 47 del DPR 445/2000,

consapevole che l'art. 75 del DPR 445 del 2000 punisce la non veridicità delle dichiarazioni rese con la decadenza dai benefici goduti e che in base all'articolo 76 del medesimo decreto le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti ai sensi del Codice penale e delle leggi speciali in materia,

di aver provveduto alla designazione degli Amministratori di sistema (di seguito ADS) che, per conto di questa società, opereranno presso il Consiglio regionale della Lombardia durante l'esecuzione del contratto, di cui di seguito s'indicano gli estremi identificativi e gli ambiti operativi assegnati.

(Da compilare per ogni ADS designato, replicando se del caso la tabella):

Nome e Cognome			
Qualifica, funzione o area organizzativa di appartenenza			
Luogo e data di nascita			
Numero di documento identità in corso di validità		<i>(Indicare estremi-numero, data e organo emittente)</i>	
Tipologia di ADS:		☐ Amministratore di dominio ☐ Amministratore di <i>server</i> ☐ Amministratore di apparati di rete ☐ Amministratore di apparati di sicurezza ☐ Amministratore di base di dati ☐ Amministratore di sistemi <i>software</i> complessi ☐ Amministratore delle postazioni di lavoro ☐ Amministratore sito <i>web</i> – <i>web master</i> ☐ Altro (_____) <i>(Indicare la tipologia di ADS)</i>	
Funzioni essenziali:			
Ambiti operativi:			
Denominazione SERVER	Impiego	Applicativi	Sistemi che trattano dati personali dei lavoratori (SI/NO)

Con riferimento alle suddette designazioni, il sottoscritto _____ dichiara altresì:

- di aver provveduto alla previa valutazione dell'idoneità delle persone sopraindicate allo svolgimento delle mansioni affidate in termini di affidabilità, competenze tecniche, esperienza e piena conoscenza della normativa in materia di protezione dei dati personali;
- di aver provveduto alle designazioni con atto individuale, sottoscritto per accettazione da parte degli ADS designati e di averli informati circa le prescrizioni contenute nel DSG 135/2016 "Revisione e aggiornamento delle regole tecniche e organizzative per la designazione e l'attività degli amministratori di sistema del Consiglio regionale della Lombardia" in particolare con riguardo alla pubblicità interna dei nomi degli ADS e delle

- attività di verifica, anche mediante sistema centralizzato di controllo sugli accessi, svolti periodicamente dal Consiglio regionale della Lombardia, nonché in merito alle responsabilità anche penali derivanti da un illecito trattamento dei dati di titolarità del Consiglio regionale;
- di aver fornito agli ADS designati le istruzioni necessarie al corretto svolgimento delle mansioni affidate, con particolare riferimento alla garanzia di gestione lecita, corretta e sicura dei dati ai sensi del d.lgs. 196/2003 e delle migliori prassi in materia di sicurezza digitale e delle *policy* definite nell'Amministrazione consiliare, verificando la piena conoscenza e comprensione delle istruzioni stesse;
 - di aver obbligato gli ADS designati alla massima riservatezza sui dati e sulle informazioni conosciuti in ragione dell'attività presso il Consiglio regionale;
 - di impegnarsi a trasmettere in ogni momento al Consiglio regionale copia delle designazioni effettuate per consentire verifiche interne o in caso di richiesta del Garante per il trattamento dei dati personali.

Milano _____

Firmato digitalmente

Il legale rappresentante

CLOUD PER SISTEMI BIBLIOTECARI DESCRIZIONE SINTETICA DEI SERVIZI

ver. 20251111

Contenuto

Servizi cloud per Sistemi bibliotecari.....	2
Servizio di manutenzione e assistenza dei software.....	2
Manutenzione correttiva.....	2
Manutenzione ordinaria di tipo sistemistico.....	4
Manutenzione migliorativa e co-progettazione.....	4
Supporto alla configurazione e gestione.....	4
Monitoraggio infrastruttura.....	5
Istanze temporanee degli applicativi.....	6
Rilascio degli aggiornamenti.....	6
Accesso ai servizi di assistenza.....	7
Formazione.....	9
Automazioni, configurazioni particolari e integrazioni.....	9
Automazioni.....	10
Configurazioni particolari.....	10
Integrazioni.....	11
Outsourcing del sistema.....	12
Infrastruttura per l'hosting.....	12
Data Server Protection.....	13
Backup delle informazioni vitali.....	13
Accesso ai dati.....	13
Misure antispam per l'invio mail.....	14
Certificati di sicurezza e privacy.....	14
Descrizione delle attività e cronoprogramma per l'avvio dei servizi.....	15
Fase 1: Analisi delle specificità del cliente per una idonea migrazione ed integrazione delle procedure.....	15
Fase 2: Analisi dei dati da migrare e verifica della loro disponibilità.....	15
Fase 3: Migrazione di prova, verifiche ed eventuali procedure di correzione.....	16
Fase 4: Formazione degli operatori del sistema.....	16
Fase 5: Attività di verifica della configurazione dei dispositivi presso le biblioteche.....	17
Fase 6: Migrazione definitiva ed avvio del sistema in produzione.....	17
Schema riassuntivo del cronoprogramma.....	18
Piano di gestione delle fasi conclusive del contratto.....	18



Servizi cloud per Sistemi bibliotecari

Comperio sviluppa, mantiene e gestisce numerosi servizi cloud per Sistemi bibliotecari. Nel tempo si è consolidato un *ecosistema* di strumenti, metodologie e risorse umane per gestire in modo efficace la segnalazione dei problemi, la loro pronta ed efficace soluzione, l'ottimizzazione e il monitoraggio delle installazioni. L'evoluzione e il miglioramento di Clavis sono gestiti attraverso un rapporto continuo e diretto con la *community* delle biblioteche che utilizzano l'applicativo, la quale fornisce suggerimenti e idee che aiutano a migliorare costantemente le funzionalità e i servizi erogati; per specifiche attività di analisi di nuovi progetti e relativi sviluppi, Comperio mette a disposizione le proprie risorse umane, con le loro competenze sia tecniche che biblioteconomiche.

La suite di applicativi integrati che compongono l'offerta di servizi cloud per Sistemi Bibliotecari consiste nelle seguenti applicazioni web:

- **Clavis**, un software open source che permette di gestire in modo efficiente e completo tutte le operazioni delle biblioteche. Nato per ottimizzare la circolazione del materiale all'interno di grandi reti bibliotecarie, consente di ridurre i costi di movimentazione agevolando le attività di prestito da parte di operatori e utenti.
- **Discovery**, il catalogo pubblico per gli utenti (OPAC) integrato in un content management system (CMS) che permette anche l'attivazione delle funzioni di gestione della community e degli eventi. La soluzione più flessibile per la creazione di una piattaforma unica che permetta agli utenti delle biblioteche di navigare il catalogo, effettuare prenotazioni, salvare contenuti e interagire con altri lettori; ai bibliotecari di pubblicare online contenuti, eventi e bibliografie in modo semplice e veloce.
- **Clavis Metacatalogo**, l'applicazione per la gestione di dati catalografici, sia bibliografici che, più generalmente, documentali, in grado di far dialogare sistemi diversi per l'arricchimento e il mantenimento della base dati. Questo innovativo sistema consente un controllo granulare di tutti i dati di catalogazione e la possibilità di implementare automatismi per l'importazione da sorgenti diverse. Supporta nativamente i principali standard per la descrizione delle informazioni e permette di aggiungere e far convivere tra molte famiglie di metadati.

Comperio utilizza strumenti web on line per gestire:

1. richieste di assistenza (issue tracking);
2. monitoraggio in realtime dei server e delle performance percepite dagli utenti;
3. sistemi di controllo di versione per il codice;
4. automazione degli aggiornamenti in orari notturni;
5. manualistica e documentazione online;
6. condivisione delle proposte di miglioria tra le reti bibliotecarie per la selezione delle priorità sviluppo.

Servizio di manutenzione e assistenza dei software

Manutenzione correttiva

La manutenzione correttiva consiste nelle attività di risoluzione dei problemi sugli applicativi che compongono i servizi cloud. Questi possono essere individuati principalmente attraverso due



canali:

1. **segnalazioni automatiche di incidenti** che gli applicativi notificano a Comperio;
2. **segnalazioni dirette** fornite dagli utenti attraverso il servizio di assistenza.

Ogni segnalazione viene analizzata da Comperio per effettuare il corretto *triage*, che consiste nell'assegnazione del corretto valore di gravità e nell'identificare l'area di intervento (es.: errore nel codice sorgente, incongruenza dati presente nel database, problema sistemistico, ecc.).

Segnalazioni automatiche di incidenti

Gli applicativi notificano in tempo reale e automaticamente il verificarsi di incidenti o errori inattesi. Le notifiche vengono ricevute da Comperio e contengono informazioni contestuali all'errore che ne permettono l'analisi per comprendere la natura e l'impatto dell'anomalia.

Segnalazioni dirette

Comperio fornisce un servizio di assistenza ai propri clienti tramite un'apposito centro di supporto (Comperio Help Center), accessibile all'indirizzo <https://helpcenter.comperio.it>, con cui è possibile:

- inoltrare richieste di supporto e verificare lo stato delle richieste aperte;
- interrogare e navigare i manuali e la knowledge base contenenti informazioni relative ai problemi noti;
- monitorare lo stato dei servizi cloud in tempo reale.

L'apertura di segnalazioni da parte dei clienti avviene tramite autenticazione per gli utenti abilitati da Comperio. È possibile aprire richieste di supporto compilando un modulo in cui inserire le informazioni rilevanti rispetto alla situazione. Il team di assistenza verificherà la richiesta e risponderà con l'indicazione delle successive fasi per la risoluzione, che potrebbero comprendere rimandi alle guide online o indicazioni di *workaround*.

Livelli di servizio

All'apertura della richiesta il team di assistenza svolge un'attività di triage per identificare la correttezza della tipologia di richiesta e la presenza di informazioni sufficienti alla risoluzione. Non tutte le richieste effettuate attraverso il Comperio Help Center si riferiscono ad anomalie che hanno un impatto sull'operatività del cliente, ma in questi casi il team di assistenza assegna un livello di gravità che determina il tempo di presa in carico e risoluzione:

Tipo di segnalazione	Descrizione	Presa in carico	Risoluzione
Anomalia bloccante (gravità 1)	Un prodotto mantenuto da Comperio è completamente inaccessibile. <i>Esempi: il portale Discovery non è raggiungibile; non è possibile fare login alla propria istanza Clavis</i>	immediata	entro 1 ora dalla presa in carico Questa tempistica esclude tutte le situazioni in cui l'anomalia non dipenda da Comperio, come ad esempio: chiusura della server farm, rete Internet non funzionante, attacchi informatici, aggiornamenti/manutenzioni programmate.
Anomalia maggiore (gravità 2)	Il cliente non può portare a termine un'operazione fondamentale e non esiste	entro 1 ora	entro 4 ore dalla presa in carico



	un'alternativa. <i>Esempi: non è possibile eseguire una ricerca nel catalogo perchè Solr non risponde</i>		
Anomalia minore (gravità 3)	L'anomalia non blocca l'operatività del cliente. <i>Esempi: un plugin di esportazione dati da scaffale non è funzionante</i>	entro 6 ore	entro 48 ore dalla presa in carico

Manutenzione ordinaria di tipo sistemistico

La manutenzione ordinaria sistemistica dei Servizi Cloud Comperio prevede l'aggiornamento dei software necessari all'esercizio (come ad esempio: sistemi operativi, web server, PHP, MySQL, Apache Solr, storage condivisi, cron jobs, servizi SIP2, ecc.), applicando regolarmente aggiornamenti di sicurezza o intervenendo direttamente sul sistema per migliorarne le *performance* e la semplicità di gestione.

Manutenzione migliorativa e co-progettazione

Attraverso il *Comperio Help Center* è possibile aprire anche richieste di nuove funzionalità o miglioria degli applicativi. Comperio analizza periodicamente questo elenco di segnalazioni, ordinandole per quelle maggiormente condivise ed inserendole nella lista delle richieste evolutive approvate e destinate a realizzazione. Ogni volta che una funzionalità richiesta dagli utenti è pianificata all'interno di una release, vengono informati gli utenti che ne avevano fatto richiesta o altri che potrebbero esserne interessati, fornendo anche una stima della data di rilascio della funzionalità desiderata.

Gli sviluppi del Sistema Bibliotecari, come l'attivazione di nuovi servizi o collaborazioni, potrebbe rendere necessaria la collaborazione di competenze diverse per la fase di analisi delle nuove necessità, di progettazione degli strumenti tecnici opportuni e per la loro realizzazione. Per queste attività Comperio mette a disposizione del Cliente le proprie risorse umane, specificatamente in ambito biblioteconomico e in ambito informatico. La collaborazione si realizza attraverso incontri di analisi presso la sede del cliente o di Comperio, oppure attraverso meeting on-line.

Supporto alla configurazione e gestione

Molte richieste dei clienti e, conseguentemente, molte attività di Comperio riguardano la richiesta di supporto per configurare gli applicativi (Clavis, Discovery, Autonotificatore, ChatBot, ecc.) in modo rispondano il più possibile alle esigenze operative dei fruitori. Tali attività sono particolarmente impegnative e necessarie in fase di avvio di nuove installazioni, ma spesso si realizzano in corso d'opera, man mano che il Cliente scopre le molteplici possibilità di configurazione e parametrizzazione degli applicativi. Per particolari esigenze, Comperio realizza componenti software personalizzate, in grado di implementare o modificare automaticamente i dati a fronte di particolari situazioni od eventi.



A questo proposito Comperio si impegna nella formazione di utenti esperti (*key users*) dei Sistemi bibliotecari, in modo da renderli il più possibile autonomi nelle attività di amministrazione e parametrizzazione degli applicativi.

Monitoraggio infrastruttura

Nell'ambito della gestione proattiva e reattiva, Comperio nel corso degli anni ha integrato nei suoi applicativi diversi sistemi di telemetria che permettono il continuo monitoraggio in tempo reale delle *performance* delle applicazioni web sia dal lato server che dal lato client. Questi sistemi forniscono numerosi indicatori, tra cui i tempi di risposta delle applicazioni, per cui sono stati impostati dei valori di soglia (*threshold*) utili a identificare tempestivamente eventuali riduzioni delle performance (ad es. query lente sul database, ecc.).

Attraverso i servizi di monitoraggio della sua infrastruttura e degli applicativi, Comperio può:

- ottenere rapporti dettagliati sullo stato e le performance delle tecnologie impiegate (dal browser web utilizzato fino alle query SQL nel server MySQL);
- analizzare e controllare in modo continuativo e automatizzato il traffico e le risorse della sua infrastruttura;
- rispondere in modo rapido e adeguato ai possibili problemi percepiti dall'utenza relativi alla lentezza delle connessioni o ad altre difficoltà di rete.

Ogni singola transazione degli applicativi compresi nei Servizi Cloud Comperio, permette di ottenere dati come:

- tempi di risposta del client;
- numero di chiamate;
- stima dell'impatto sul database relazionale;
- stima dell'impatto sul motore di ricerca.

Soglie di allerta

Sono state definite delle soglie di allerta nel caso di performance troppo basse o anomalie nel funzionamento dell'infrastruttura. Questo consente di decidere su quali transazioni o risorse intervenire per prime e di individuare più velocemente le componenti di sistema che necessitano di ottimizzazione.

Status page

Per quanto riguarda la reportistica, al fine di permettere al cliente di verificare il rispetto delle SLA previste, viene messo a disposizione un sistema consultabile da parte del cliente stesso in tempo reale; si tratta di un sito web di tipo "Status page" che registra la situazione delle manutenzioni in corso e lo stato dei sistemi.

Il sito è strutturato secondo i diversi componenti dei Servizi Cloud Comperio e riporta le seguenti sezioni:

- *Component Summary*: mostra lo stato in tempo reale e i dettagli operativi dei servizi.
- *Component Status History*: registra per 90 giorni solari i dati storici sulla disponibilità dei servizi; cliccando su ciascun componente è possibile ottenere dettagli circa le performance del servizio.
- *Incident History*: registra giornalmente gli eventi anomali o irregolari



Istanze temporanee degli applicativi

Se necessario, Comperio può predisporre un ambiente “clone” dell’istanza cloud presso i propri datacenter. Questo tipo di ambienti possono servire, ad esempio, per la riproduzione di problemi riscontrati nell’uso degli applicativi, oppure come ambienti di pre-produzione per la dimostrazione delle novità prima del rilascio di un aggiornamento, oppure per scopi formativi. Questo permette di svolgere varie attività senza dover interferire con gli ambienti di esercizio. È inoltre possibile che i dati presenti nell’istanza temporanea siano anonimizzati.

Rilascio degli aggiornamenti

Il *release management* dei Servizi Cloud Comperio è gestito interamente da Comperio che pianifica e realizza le nuove versioni e ne cura la distribuzione alle reti bibliotecarie.

Tutti i Servizi Cloud Comperio utilizzano un sistema di *continuous integration* e controllo di versione, per cui presentano un numero progressivo che permette di conoscere la versione del prodotto utilizzata. Il rilascio di una nuova versione comporta correzioni di errori o malfunzionamenti, modifica di funzionalità esistenti oppure nuove funzionalità. Queste vengono elencate nella pagina **Note di rilascio**, cioè la lista delle attività di sviluppo realizzate, con l’indicazione dell’eventuale impatto che le nuove funzionalità potrebbero avere rispetto alla versione precedente. Vengono inoltre segnalate eventuali attività che i referenti dovranno eseguire subito dopo l’aggiornamento (es.: impostazione di nuovi parametri, pulizia cache dei browser, ecc.).

Tipologie di rilascio

Gli aggiornamenti agli applicativi vengono categorizzati per facilitarne la comprensione ai clienti. I rilasci potrebbero essere definiti:

- **Hotfix**, ovvero una modifica al codice legata alla risoluzione di un bug urgente o problema di sicurezza informatica;
- **Maintenance Release**, ovvero un aggiornamento legato alla manutenzione ordinaria di tipo sistemistico;
- **Minor Release**, una nuova versione dell’applicativo che può comprendere risoluzione di bug non urgenti e migliorie alle funzionalità esistenti;
- **Major Release**, una versione significativamente aggiornata della base codice dell’applicativo che può comprendere risoluzione di bug, migliorie a funzionalità esistenti e nuove funzionalità.

Fase di test e validazione

Prima del rilascio in produzione di una minor o major release, vengono create una o più istanze temporanee degli applicativi, predisposte per rispecchiare le diverse configurazioni possibili delle reti bibliotecarie: presenza o meno di modulo SBN, gestione della circolazione a bacini, mancanza di gestione dell’inventario, gestione delle authority in modalità avanzata, ecc.

È possibile avvalersi della collaborazione dei responsabili delle reti bibliotecarie, sia per pianificare controlli alle nuove funzionalità ed evitare “regressioni”, sia per permettere l’eventuale creazione di materiale comunicativo e formativo per i bibliotecari in modo da verificare che la release non presenti “regressioni” o altri problemi, soprattutto in relazioni a situazioni specifiche dell’installazione Clavis.

Durante questa fase, Comperio procede all’aggiornamento della documentazione online degli applicativi, presente sul Comperio Help Center, che può comprendere modifiche al manuale o creazione di guide o video tutorial. Questi materiali vengono poi integrati nelle Note di rilascio, per facilitarne la consultazione.



Pianificazione e impatto del rilascio

Una volta terminata la fase di test e validazione, viene pianificato il rilascio (deployment) della nuova release. L'aggiornamento dell'applicativo viene pianificato in modo da minimizzare l'impatto sui servizi e consentire un eventuale "rollback" alla release precedente in caso di imprevisti. Comperio ha una completa flessibilità negli orari degli aggiornamenti durante tutte le 24 ore e tutti i giorni della settimana.

In linea generale, gli aggiornamenti sono applicati durante i fine settimana in orari notturni dopo le 23:00 per rendere pressoché inesistente l'interruzione del servizio.

A titolo esemplificativo, vengono riportate di seguito le tempistiche e le fasi per una major release:

- Pull degli aggiornamenti software dal repository dei sorgenti di Comperio → tempo necessario: < 5 minuti
- Applicazione delle query di aggiornamento e degli eventuali script di post-upgrade → tempo necessario: < 30 minuti
- (opzionale) Rigenerazione cache dei dati bibliografici → tempo necessario: ~ 3 ore
- (opzionale) Re-indicizzazione del catalogo in Solr → tempo necessario: ~ 30 minuti

Frequenza dei rilasci

Lo sviluppo in ottica di *continuous integration* e la minimizzazione dell'impatto nel rilascio, permette a Comperio di effettuare rilasci di tipo *hotfix* e *maintenance release* just in time, ovvero al verificarsi delle condizioni che determinano la necessità di aggiornare gli applicativi. Per quanto riguarda le *minor release*, ovvero aggiornamenti che riguardano risoluzione di bug non urgenti e migliorie alle funzionalità esistenti, Comperio si impegna ad effettuare un rilascio semestralmente. Per quanto riguarda le *major release*, l'impegno di Comperio è di effettuare almeno 1 o 2 rilasci all'anno.

Accesso ai servizi di assistenza

Comperio Help Center

Comperio mette a disposizione tutte le risorse informative necessarie all'utilizzo dei propri applicativi sul proprio portale di supporto. Questo contiene: manuali dei singoli applicativi, knowledge base delle domande più frequenti ricevute dal servizio di assistenza, guide per attività specifiche e video formativi. A partire dal portale è inoltre possibile: consultare la Status Page degli applicativi, aprire una richiesta di assistenza, consultare le SLA e le altre policy.

Richieste di assistenza

Per le richieste di assistenza è necessario utilizzare il portale messo a disposizione all'indirizzo <https://webcomperio.atlassian.net/servicedesk/customer/portals>. L'accesso al portale avviene tramite autenticazione ed è riservato ai referenti di sistema oppure al responsabile di una biblioteca che abbia un contratto di servizio in essere con Comperio (ad es. per un prodotto hardware).

Dopo l'accesso al portale, i clienti sono invitati a indicare la tipologia di richiesta e a compilare un apposito modulo che permette al team di assistenza di prendere in carico tempestivamente la segnalazione.

È possibile selezionare le seguenti tipologie di richieste:

- **Supporto nell'utilizzo del prodotto:** il cliente necessita di aiuto nell'utilizzare alcune delle funzionalità di un prodotto Comperio.



- **Errore o malfunzionamento del prodotto:** il prodotto Comperio non funziona o è impossibile portare a termine una determinata attività.
- **Richieste di configurazione o modifiche ai valori predefiniti:** per richieste di modifica alla configurazione, ai valori predefiniti degli applicativi o per aggiornamenti massivo di dati.
- **Biblioteconomia, catalogazione, SBN:** per richieste di informazioni in ambito biblioteconomico, domande specifiche riguardanti la catalogazione oppure riguardanti SBN.
- **Statistiche, report e stampe:** per richiedere modifiche o supporto nei report di stampa o di tipo statistico.
- **Attività Centro Servizi:** riservato alle richieste da parte dei clienti per cui Comperio svolge il ruolo di Centro Servizi e relative alla gestione degli operatori e delle rispettive autorizzazioni, alle configurazioni di sistema, all'inserimento di informazioni e avvisi in OPAC, ecc.
- **Richieste amministrative e commerciali:** per questioni amministrative o per la richiesta di quotazione su prodotti, materiali di consumo o servizi.
- **Suggerimenti di sviluppo:** per formulare suggerimenti e proposte per lo sviluppo di un prodotto Comperio.

Gestione delle richieste

Il processo che porta dall'apertura della richiesta alla sua risoluzione è contraddistinto da alcune fasi visibili sul portale e che corrispondono agli stati in cui può trovarsi in uno qualsiasi momento la richiesta. Attraverso il portale il cliente può risolvere in autonomia una richiesta aperta per errore o non più valida.

Per tutte le richieste, ad eccezione dei suggerimenti di sviluppo, gli stati in cui può trovarsi una richiesta sono i seguenti:

- **Aperta:** è lo stato predefinito in cui si trovano tutte le richieste appena aperte. Il cliente riceve una mail automatica con la conferma dell'avvenuta creazione della richiesta sul portale. Appena possibile il team di assistenza effettua il triage necessario a identificare correttamente tutti gli elementi della richiesta necessari alla sua risoluzione.
- **Attesa informazioni:** la richiesta è stata analizzata e il team di assistenza ha richiesto al cliente l'integrazione delle informazioni riportate con dettagli necessari all'esecuzione delle attività. Il cliente può rispondere via mail oppure attraverso il portale. Nel caso di mancata risposta da parte del cliente entro 7 giorni dalla richiesta di informazioni da parte del team di assistenza, la richiesta viene automaticamente spostata nello stato Risolta e il cliente riceve una notifica via mail.
- **Attesa approvazione:** perché la richiesta possa essere affrontata dal team di assistenza è necessaria un'approvazione interna (ad esempio dall'ufficio amministrativo o dal team di sviluppo). Non è richiesta nessuna azione da parte del cliente e solitamente cerchiamo di elaborare questo stato in tempi rapidi.
- **In lavorazione:** la richiesta è stata presa in carico da Comperio e verrà gestita nel minor tempo possibile dal team di assistenza.
- **Risolta:** la richiesta è stata risolta dal team assistenza. Nel caso ci fossero ulteriori richieste da parte del cliente è possibile rispondere via mail alla notifica di risoluzione, oppure aggiungere un commento alla richiesta risolta sul portale. Una richiesta risolta può essere riaperta entro 5 giorni dalla data di risoluzione, altrimenti passerà automaticamente allo stato Chiusa.
- **Rifiutata:** la richiesta non è valida e non può essere gestita da Comperio. In questo caso il cliente riceve una notifica via mail con le motivazioni del rifiuto (ad esempio una richiesta su un prodotto hardware o software non mantenuto da Comperio).



- **Chiusa:** dopo 5 giorni dalla risoluzione, nel caso non siano più stati aggiunti commenti alla richiesta, questa passa automaticamente a Chiusa e non è più possibile intervenire o modificarla.

Nel caso di richieste del tipo *Errore o malfunzionamento del prodotto* e a seconda del livello di gravità, il team di assistenza potrebbe indicare dei workaround temporanei. Nel caso di modifiche sostanziali all'applicativo potremmo fornire ai clienti un codice di lavorazione interno, che fa riferimento ai processi di sviluppo (ad es. CNG-123 o DNG-123). Lo stesso codice viene poi utilizzato all'interno delle *Note di rilascio* che accompagnano i rilasci periodici di aggiornamenti degli applicativi, per permettere al cliente di essere certo che una certa richiesta è stata caricata in produzione.

Assistenza tramite connessione remota

Qualora lo ritenga utile, il team di assistenza potrà concordare con l'operatore che effettua una segnalazione di accedere in modalità remota alla postazione di lavoro della biblioteca, al fine di verificare configurazioni specifiche o problemi della postazione di lavoro. Questo tipo di intervento è particolarmente utile soprattutto per le segnalazioni legate all'hardware (ad es. postazioni di autoprestito, tavolette RFID, ecc).

Pronto intervento

Per quanto riguarda l'attività straordinaria di assistenza, ovvero segnalazioni di interruzioni impreviste del servizio che rendano impossibile l'accesso ai Servizi Cloud Comperio o al Comperio Help Center, i clienti sono invitati a consultare innanzitutto la Status Page per verificare lo stato degli applicativi e, soprattutto, se l'incidente è già stato preso in carico da Comperio. Nel caso in cui non ci fossero segnalazioni sulla Status Page, è possibile contattare il numero del pronto intervento 0425471482.

Formazione

Le attività formative sono ordinariamente realizzate da personale Comperio. Il piano di formazione viene solitamente concordato all'inizio dell'anno con la Direzione del Sistema bibliotecario o della Biblioteca, e potrebbe riguardare:

- aspetti particolari sull'uso degli applicativi;
- aggiornamenti su nuove procedure;
- sessioni di analisi di particolari esigenze e condivisione di progetti di sviluppo;
- aggiornamenti o approfondimenti di argomento biblioteconomico;
- temi relativi alla gestione dei servizi al pubblico.

I corsi possono essere svolti in presenza oppure online, attraverso lezioni frontali oppure esercitazioni. Comperio mette anche a disposizione risorse video per l'auto-formazione, sempre disponibili per i clienti dei Servizi Cloud.

Automazioni, configurazioni particolari e integrazioni

Ciascun Servizio Cloud Comperio può prevedere l'integrazione con moduli aggiuntivi oppure configurazioni specifiche legate al contesto del Sistema Bibliotecario. Queste configurazioni o moduli possono determinare modifiche all'interfaccia degli applicativi (ad es. attraverso l'abilitazione di nuovi pulsanti) oppure l'attivazione di particolari automatismi.



Automazioni

Gli applicativi che compongono i Servizi Cloud Comperio permettono di definire regole automatiche da applicare al verificarsi di alcune condizioni. Queste possono riguardare la gestione degli utenti, della circolazione, delle notifiche, della catalogazione, ecc.

Di seguito elenchiamo i principali automatismi presenti negli applicativi:

- **Campi nelle schede utente o esemplare**, permette di pre-compilare campi selezionati dalle schede degli utenti o degli esemplari per velocizzare le procedure di registrazione.
- **Revoca automatica**, permette di definire le regole per la revoca temporanea dei diritti di circolazione agli utenti in ritardo sulla restituzione dei prestiti.
- **Tempo di quarantena dei documenti**, si tratta di una procedura automatizzata che modifica la classe di prestabilità dell'esemplare al rientro da un prestito per un certo intervallo di tempo definito.
- **Autonotificatore**, permette di spedire notifiche agli utenti in maniera autonoma e senza l'intervento dell'operatore. Le notifiche possono essere mandate su diversi canali (SMS, Mail, ChatBot, App dove abilitata) stabilendo le regole di invio e l'ordine di passaggio a un altro canale di notifica in caso di indisponibilità del prioritario.
- **Immagini di copertina, abstract e indici**, ovvero l'import automatico o la connessione tramite EAN/ISBN ai record bibliografici di: copertine, abstract e indici della saggiistica, dei quali Comperio mantiene un repository condiviso assicurandone la disponibilità e la corretta licenza d'uso senza oneri per il Sistema Bibliotecario.

Configurazioni particolari

- **Circolazione per bacini**, permette la gestione di un sistema di circolazione a bacini (o sotto-reti) tramite un'unica installazione di Clavis. È stato pensato e sviluppato soprattutto per rispondere alle esigenze di grosse reti di cooperazione, con un numero elevato di biblioteche distribuite su un ampio territorio e rispondere quindi ad esigenze di ottimizzazione della logistica nella movimentazione dei materiali.
- **Spostamento automatico delle prenotazioni**, abbinato alla circolazione a bacini, permette di ricalcolare i tempi di attesa e spostare automaticamente una prenotazione tra bacini diversi al verificarsi di determinate regole sui tempi di attesa previsti.
- **Selfservice check-in**, è il servizio di ritiro dei documenti pronti al prestito effettuato in autonomia da parte degli utenti. La sicurezza della gestione dei dati personali è garantita dall'introduzione di un codice univoco per l'utente e all'anonimizzazione dei cavalieri dove informazioni identificative quali contatti e indirizzi sono oscurate, mentre il nome e cognome dell'utente sono sostituiti dal codice utente.
- **Template di catalogazione** (funzionalità specifica di *Clavis MetaCatalogo*), ovvero dei modelli di catalogazione che possono essere applicati a record preesistenti o quando si crea un nuovo record, a seconda del tipo di entità o del tipo di materiale o genere. Servono per guidare il catalogatore rendendo visibili, nascondendo o riordinando i campi di catalogazione scelti dal sistema.
- **Dizionari di metadati** (funzionalità specifica di *Clavis MetaCatalogo*), ovvero la possibilità di definire e avere a disposizione nella gestione del catalogo, famiglie di metadati diversi, rappresentando qualsiasi tipologia di elemento si voglia descrivere: dal materiale archivistico, a quello museale, ai manoscritti, alle risorse digitali/digitalizzate, ma anche per esempio descrizioni di banche dati, eventi ecc... L'espressività descrittiva è garantita dalla possibilità di avere a disposizione i metadati specifici di ogni dominio di interesse, senza essere vincolati ad esempio allo standard UNIMARC utilizzato nel contesto bibliografico. Il sistema non prevede un limite alla presenza, coesistenza e



creazione di dizionari differenti, ed è pensato per poter accogliere metadati che possono nel tempo evolversi ed essere modificati. Possono convivere standard di metadattazione come il Dublin Core, MARC21, UNIMARC, RDA, ISAD, SBNMARC ecc.

- **Importazione di record bibliografici**, gli applicativi del Servizio Cloud Comperio permettono la cattura di record UNIMARC o MARC21 da qualsiasi server nazionale o internazionale che abbia a disposizione un accesso Z39.50 (es.: OpacSBN, Library Of Congress e altri cataloghi internazionali, basi dati universitarie e di elevata specializzazione, ecc.). È sempre inoltre possibile configurare l'importazione di record da altre basi dati Comperio, previo accordo con gli enti gestori. Comperio in particolare mette a disposizione l'importazione dalla base dati CLIC e che contiene catalogazioni complete di oggetti bibliografici pubblicati e commercializzati in Italia dal 2010. Esiste inoltre la possibilità di configurare l'importazione di record bibliografici da basi dati commerciali, in particolare il catalogo dei libri in commercio e IBS.
- **Importazione di record di autorità**, è possibile l'importazione e l'aggiornamento del Thesaurus multiculturale del Nuovo Soggettario Italiano, prodotto da BNCF e reso disponibile nel formato SKOS (Simple Knowledge Organisation System). Il sistema di importazione, elaborato da Comperio, effettua automaticamente lo schiacciamento delle voci di autorità identiche, lo spostamento automatico dei legami da forme varianti a forme accettate, l'importazione delle relazioni tra termini (BT/NT, RT, UF/USE, UF+/USE+), oltre alla definizione di etichette di nodo e termini apicali. L'importazione viene automaticamente aggiornata quando BNCF rende disponibile un nuovo rilascio.

Integrazioni

I Servizi Cloud Comperio sono progettati e sviluppati per integrarsi nativamente con un vasto ecosistema di applicativi e tecnologie, sia hardware che software, sia di Comperio che di terze parti. Questo è possibile attraverso l'aggiunta di moduli o applicativi appositi che abilitano determinate funzionalità o attraverso specifiche configurazioni dei Servizi Cloud in presenza di determinate condizioni.

- **SBN**

Qualora il Sistema Bibliotecario decida di costituire un Polo SBN, i Servizi Cloud Comperio permettono il dialogo con l'Indice SBN attraverso il protocollo SBNMarc a livello massimo (livello 4) per tutte le tipologie di materiale. Il dialogo con l'indice di SBN è integrato direttamente all'interno di Clavis, in modo da offrire all'operatore una interazione quanto più possibile trasparente e confortevole. Comperio offre assistenza nelle eventuali attività di configurazione e gestione del Polo, soprattutto per quanto riguarda gli aspetti di gestione delle peculiarità del catalogo.

- **Chatbot**

I Chatbot sono bot creati per utenti e operatori: consentono di interagire attraverso il linguaggio naturale fornendo risposte e, grazie all'integrazione con l'applicativo Clavis, possono effettuare determinate azioni di recupero di informazioni o, nel caso del bot per operatori, compiere operazioni di catalogazione e circolazione. Attualmente i chatbot sono disponibili nella piattaforma Telegram, installando l'applicazione sul proprio smartphone o attraverso l'interfaccia web.

- **Tecnologia RFID**

Radio-Frequency IDentification (identificazione a radiofrequenza) è una tecnologia per l'identificazione e/o memorizzazione automatica di informazioni basata sulla capacità di



memorizzare dati in particolari etichette elettroniche chiamate TAG (o anche transponder), e sulla capacità di queste di rispondere all'interrogazione a distanza da parte di appositi apparati fissi o portatili, chiamati reader (o anche lettori).

Per l'integrazione della tecnologia RFID è stato sviluppato un particolare applicativo chiamato *ClavisClient* (compatibile con sistemi operativi Windows o Linux). Avviando il *ClavisClient* sul pc dell'operatore, durante l'utilizzo del gestionale sarà possibile: scrivere il tag sul chip RFID, leggere i tag sul chip RFID. Le operazioni di lettura e scrittura sono nativamente integrate nell'interfaccia di Clavis per facilitare il lavoro degli operatori.

- **Netmanager**

Nel caso in cui la biblioteca utilizzi la nostra tecnologia Netmanager per la gestione della navigazione in biblioteca, sia wifi che tramite postazioni fisse, gli applicativi integrano nativamente gli strumenti di controllo e gestione. Attraverso Clavis è infatti possibile il monitoraggio e il controllo delle sessioni e del consumo di banda, la configurazione di un *walled garden* per l'accesso profilato degli utenti e la creazione di report e statistiche d'utilizzo.

- **Gestione presenze utenti**

In presenza di sistemi di rilevazione del passaggio di utenti quali varchi anti-taccheggio, tornelli o conta persone, è possibile attivare all'interno degli applicativi una apposita pagina per il monitoraggio e la gestione degli accessi alla biblioteca.

- **Wordpress**

Sono state sviluppate numerose integrazioni con Wordpress, il Content Management System (CMS) più popolare e diffuso. Queste possono avvenire sia attraverso l'utilizzo di apposite API per la pubblicazione di contenuti specifici del catalogo, che attraverso l'adozione integrata del CMS come strumento per la pubblicazione dell'OPAC. In questo secondo caso, è possibile personalizzare l'intera istanza di Wordpress e utilizzarla come piattaforma integrata per ricerca di dati nel catalogo, la gestione delle prenotazioni e dei prestiti da parte degli utenti, la pubblicazione di eventi, bibliografie e altri contenuti da parte delle biblioteche.

- **SPID**

È possibile integrare e rendere disponibile agli utenti l'autenticazione tramite SPID o altro Identity Provider richiesto dal Sistema Bibliotecario.

Outsourcing del sistema

Infrastruttura per l'hosting

L'infrastruttura globale è costituita da diversi server fisici o virtuali direttamente gestiti dal personale Comperio. Esistono diversi nodi con tecnologia Proxmox VE nel datacenter Fastweb di Milano che compongono l'infrastruttura principale del nostro Private Cloud dal quale vengono erogati gli applicativi compresi nel Servizio Cloud. Altri server Linux sono presenti in datacenter in Europa presso i datacenter di Hetzner.

I nodi del cluster principale sono protetti da firewall che consente gli accessi amministrativi solo dagli IP autorizzati. Sono aperte solo le porte TCP/UDP strettamente necessarie all'erogazione dei servizi o solo da e verso i server opportuni. Un sistema di WAF (Web Application Firewall) è



attivo sul load balancer che smista il traffico verso le applicazioni SaaS erogate da Comperio che si occupa di ispezionare transazioni sospette e di segnalare ed eventualmente bloccare ogni richiesta.

Data Server Protection

La protezione dei server avviene su diversi livelli. Un livello fisico in quanto tutti i server sono presso datacenter che garantiscono livelli di sicurezza elevati: controllo accessi, videosorveglianza, profilazione, garanzia di continuità di servizio, ridondanza. A livello logico, i log dei server sono memorizzati anche su sistema esterno che effettua segnalazioni su ogni accesso ai server effettuato.

Un sistema di Intrusion Detection dedicato, controlla costantemente tutti i file di configurazione, i processi e le porte attive sui server. Un WAF ispeziona il traffico HTTP/HTTPS delle applicazioni SaaS alla ricerca di tentativi di attacchi e permette di effettuare virtual patch in caso vengano riscontrate vulnerabilità applicative e si decida di bloccarle in attesa che un fix software sia pronto.

Per ogni componente critica utilizziamo un approccio $N + 1$ (dove N è il numero di server necessari all'erogazione di un servizio) che permette di garantire ridondanza. Adottiamo un approccio di "insicurezza generale" per cui le connessioni tra server sono ugualmente protette da chiavi crittografiche e inoltre limitate solo a connessioni provenienti da IP fidati.

Backup delle informazioni vitali

Tutti i dati degli applicativi sono gestiti per garantire il massimo livello di integrità e disponibilità. Per questo sono sottoposti a procedure di backup e archiviazione in siti alternativi a quello principale, ma sempre all'interno della Comunità Europea, come parte delle normali operazioni di Comperio. Le informazioni vitali collegate ai servizi contrattualizzati sono replicate in 3 copie in tempo reale su tre server distinti e una copia su un quarto server è in replica ritardata di 24 ore. Ogni giorno sono effettuati backup completi dei singoli database clienti che vengono distribuiti su tre storage server distinti in due datacenter diversi. Sono mantenuti gli ultimi 7-30-60 giorni di backup sui vari server.

Nel caso un cliente lo richieda, può essere dato un accesso riservato via FTP sicuro per scaricare copie dei backup aggiornati in modo autonomo. Esiste un sistema di backup di tali dati usando chiavi crittografiche per garantire l'apertura di tali backup solo al personale autorizzato dell'ente.

Accesso ai dati

Cloud storage

È possibile integrare servizi di terze parti (come StorageBox o Blackblaze) per la gestione di spazio di archiviazione cloud. Questi servizi possono essere utilizzati, ad esempio, per il salvataggio di digitalizzazioni o per la conservazione di ulteriori copie di backup dei dati degli applicativi. Grazie a questi servizi aggiuntivi è possibile pianificare una copia periodica dei dati degli applicativi o richiedere estrazioni una tantum dell'intero database.

Accesso diretto al database

Per consentire agli Amministratori di sistema attività di estrazione dati autonoma, è possibile abilitare un accesso diretto ai database di produzione degli applicativi. Tale accesso può essere definito in modalità sola lettura, o in modalità lettura/scrittura. L'utilizzo di tale accesso è



agevolato da un'interfaccia amichevole, che permette di effettuare qualsiasi query sul DB ed impostare le relative esportazioni in vari formati.

Per tale attività Comperio mette a disposizione per gli amministratori interessati incontri formativi su tecniche di interrogazione del DB e di estrazione dei dati.

Misure antispam per l'invio mail

Comperio ha realizzato una integrazione nei propri applicativi, volta ad attenuare il più possibile le misure antispam messe in atto dai principali fornitori del servizio di posta elettronica. In questo senso è stato implementato un sistema di invio mail *transazionale*, tale cioè da consentire la tracciatura affidabile e puntuale dello stato degli invii di posta elettronica da parte dell'applicativo. Questo sistema permette la gestione di record DNS di tipo SPF (Sender Policy Framework) per verificare che il server di posta mittente sia autorizzato ad inviare mail per conto di uno specifico dominio, e di tipo DKIM (DomainKey Identified email), per aggiungere una *firma crittografica* ad ogni invio ed aumentare di conseguenza la reputazione dei messaggi, riducendo ulteriormente le probabilità che siano interpretati come SPAM da parte dei clienti di posta elettronica.

Lo stato delle notifiche inviate agli utenti viene opportunamente aggiornato in base al risultato della consegna delle email al destinatario e vengono inoltre gestiti i diversi tipi di errore: hard bounce e soft bounce.

- **Hard bounce:** è un errore grave in genere causato da un indirizzo email di destinazione errato o inesistente. Quindi la notifica, non potendo essere consegnata, viene conseguentemente associata ad uno stato di errore e l'email dell'utente destinatario viene impostata come non valida.
- **Soft bounce:** riguarda email che sono rifiutate in genere per problemi temporanei del tipo "casella email piena" oppure quando si verifica il raggiungimento delle quote di invio settimanali o mensili che diversi provider applicano. In questo caso la singola notifica viene messa in errore ma un servizio batch può provare a inoltrarla dopo qualche giorno nell'ipotesi che il problema sia stato nel frattempo risolto.

Certificati di sicurezza e privacy

Comperio detiene una serie di certificazioni integrate per:

- la gestione della qualità (ISO 9001:2015);
- la gestione della sicurezza delle informazioni, cybersecurity e protezione della privacy (SO/IEC 27001:2024), integrata dalle prassi sui controlli per la sicurezza delle informazioni per i servizi in cloud (ISO/IEC 27017:2021) e dalle prassi per la protezione dei dati personali trattati in cloud pubblici da responsabili del trattamento (ISO/IEC 27018:2020);
- la gestione della continuità operativa (ISO 22301:2019).

Inoltre, operando all'interno dell'Unione Europea, rispetta i requisiti del regolamento generale sulla protezione dei dati (GDPR).

In questo senso i Servizi Cloud e l'infrastruttura Comperio implementano una serie di funzionalità e policy volte a:

- rispettare e far rispettare la normativa vigente in materia di privacy;
- prevenire, identificare e risolvere i potenziali rischi alla sicurezza dei dati trattati;
- intervenire tempestivamente nella risoluzione di incidenti legati alla sicurezza informatica.

Descrizione delle attività e cronoprogramma per l'avvio dei servizi

Fase 1: Analisi delle specificità del cliente per una idonea migrazione ed integrazione delle procedure

Obiettivo	Precisare l'architettura generale del catalogo e dei servizi di rete.
Operatori coinvolti nell'attività	Comperio, Responsabili biblioteca/Sistema
Metodo di lavoro	Riunioni con redazione di verbali/documenti conclusivi
Vincoli	L'attività deve essere conclusa prima dell'avvio della Fase 3
Durata prevista	1 settimana

Protocolli operativi o documenti disponibili al termine di questa fase:

Documento 1: Verifica della struttura generale dei dati catalografici

Il documento ha lo scopo di condividere e precisare ulteriormente il progetto di migrazione dati catalografici descritto nel punto 1 del presente Progetto tecnico.

In modo particolare per ciascun elemento del catalogo saranno concordati eventuali interventi automatici di modifica o sistemazione dei dati da verificare in fase di importazione.

Documento 2: Caratteristiche salienti della base dati

1. Eventuale elenco di fondi speciali o di basi dati particolari a cui è riservato un trattamento particolare ai fini della gestione e della circolazione.
2. Definizione dei parametri di circolazione condivisi nella rete per tipologia di materiali.

Documento 3: Definizione dei profili di accesso e loro organizzazione nel sistema

La verifica consiste nel definire i profili degli operatori a cui associare le permissions all'interno degli applicativi (operatori, catalogatori, responsabili, ecc.). E' anche possibile definire per i catalogatori un ulteriore livello di autorità per la gestione della correzione delle notizie, qualora lo si ritenga utile.

A tal fine è opportuno produrre in questa fase:

1. elenco dei profili di accesso e delle relative funzioni autorizzate/negate
2. elenco degli operatori con associato profilo di accesso (ed eventualmente per i catalogatori anche il livello di autorità su creazione/modifica notizie).

Fase 2: Analisi dei dati da migrare e verifica della loro disponibilità

Obiettivo	Individuare e descrivere in modo analitico le basi dati da importare, la loro disponibilità e la loro struttura. Preparazione del server di test.
Operatori coinvolti nell'attività	Comperio, Responsabili biblioteca/Sistema
Metodo di lavoro	Predisposizione server di test e verifica del suo funzionamento. Analisi di dati con redazione di documento conclusivo.
Vincoli	L'attività deve essere conclusa prima dell'avvio della Fase 3
Durata stimata	1 settimana



Attività svolte durante questa fase:

1. Definizione delle modalità, dei referenti e delle tempistiche di restituzione dei dati del precedente gestore
2. Predisposizione di un ambiente di test
3. Estrazione dei dati dal database da importare
4. Analisi dettagliata dei dati e predisposizione di un piano analitico di migrazione

Fase 3: Migrazione di prova, verifiche ed eventuali procedure di correzione

Obiettivo	Realizzare una migrazione di prova dei dati in un ambiente di test
Operatori coinvolti nell'attività	Comperio, Responsabili biblioteca/Sistema
Metodo di lavoro	Importazione dati nell'ambiente di test. Riunioni di verifica.
Vincoli	L'attività presuppone la conclusione delle Fasi 1 e 2 e deve essere conclusa prima dell'avvio della Fase 4
Durata stimata	3 settimane

Durante questa fase viene fatta sull'ambiente di test la prima migrazione dei dati (che non implica alcun blocco e nessuna limitazione delle attività della Rete). L'ambiente viene quindi messo a disposizione dei responsabili della rete o dei bibliotecari preposti all'attività di test. Eventuali errori o incompletezze nella migrazione vengono segnalate e si procede ad ulteriori migrazioni, per verificare l'effettiva correzione delle procedure.

Attività svolte al termine di questa fase:

1. Disponibilità di un ambiente di test.
2. Comunicazione dell'indirizzo internet di test per l'attività di formazione.

Fase 4: Formazione degli operatori del sistema

Obiettivo	Realizzare l'attività di formazione per gli operatori dei singoli bacini
Operatori coinvolti nell'attività	Operatori delle biblioteche, Comperio
Metodo di lavoro	Incontri formativi
Vincoli	L'attività è opportuno che avvenga dopo la Fase 3 cioè avendo a disposizione l'ambiente di prova con i dati della rete, e può protrarsi fino all'avvio del sistema.
Durata stimata	1 settimana

Attività svolte al termine di questa fase:

1. Comunicazione a tutti gli operatori dell'indirizzo di test e dell'indirizzo dell'Help Center Comperio
2. Comunicazione a tutti gli operatori dei protocolli operativi e delle eventuali "precisazioni" (vademecum) sull'uso del software di rete.
3. Realizzazione degli incontri formativi all'interno della biblioteca.
4. Comunicazione a tutti gli operatori delle modalità per l'assistenza di primo livello.



In questa fase Comperio mette a disposizione un proprio operatore per definire alcune attività specifiche quali:

1. Stampa etichette e codici a barre ed eventuale fornitura di attrezzatura dedicata questa attività.
2. Eventuali attività di apposizione dei codici a barre al patrimonio pregresso, se richiesto.
3. Studi di fattibilità per l'uso di tecnologie RFID in biblioteca.
4. Studi di fattibilità per l'uso di reti wifi e/o strumenti per la navigazione controllata per gli utenti integrata nei Servizi Cloud Comperio.

Fase 5: Attività di verifica della configurazione dei dispositivi presso le biblioteche

Obiettivo	Assicurarsi che ciascuna postazione di lavoro sia configurata in modo ottimale per l'utilizzo dell'applicativo. Installare il nuovo software sulla postazione di autoprestito. Configurare la modulistica e i testi dei messaggi automatici.
Operatori coinvolti nell'attività	Comperio, Operatori della biblioteca
Metodo di lavoro	Verifica in remoto, installazioni in remoto o in locale
Vincoli	Realizzazione della Fase 3
Durata stimata	2 settimane

Attività svolte al termine di questa fase:

1. Comunicazione agli operatori relativa al controllo della configurazione delle postazioni di lavoro su cui si lavorerà con gli applicativi
2. Installazione presso le biblioteca del software per la gestione dell'autoprestito direttamente connesso agli applicativi.
3. Eventuale configurazione della modulistica speciale

Fase 6: Migrazione definitiva ed avvio del sistema in produzione

Obiettivo	Realizzazione della migrazione definitiva e avvio del sistema
Operatori coinvolti nell'attività	Comperio
Metodo di lavoro	Migrazione dati, Startup sistema
Vincoli	Realizzazione della Fase 3
Durata stimata	9 giorni consecutivi (2 giorni di blocco delle attività gestionali)

Per la migrazione definitiva sono necessari 9 giorni, tuttavia questo non comporta necessariamente il blocco delle attività di circolazione. Il blocco dei prestiti e dell'iscrizione utenti è limitato a due giorni (lunedì e martedì).

Il modello di cronoprogramma per la migrazione definitiva è il seguente:

Lunedì mattina	Blocco delle catalogazioni (al catalogo non vengono più aggiunti record bibliografici e record di copia). Viene effettuata l'esportazione definitiva del
----------------	--

	catalogo bibliografico. In questa fase le attività di prestito e iscrizioni utenti procedono normalmente sul vecchio software. Comperio provvede alla migrazione del catalogo grafico, all'arricchimento delle schede con i dati suppletivi (copertine, indici, ecc.), all'attività di schiacciamento concordata.
Da lunedì pomeriggio a venerdì	In questa fase le attività di prestito e iscrizioni utenti procedono normalmente sul vecchio software.
Sabato	Il sabato (ad orario da stabilire) si blocca l'attività di prestito e iscrizione utenti. Vengono esportati i dati gestionali.
Da lunedì a martedì	Comperio procede alla migrazione dei dati gestionali (utenti, prestiti, prenotazioni ecc.) e alla configurazione finale del sistema e all'apertura del nuovo OPAC.
Mercoledì mattina	La nuova base dati viene messa a disposizione dei bibliotecari. Si consiglia di destinare il mattino alle ultime attività di controllo e verifica.
Mercoledì pomeriggio	Avvio delle attività utilizzando i Servizi Cloud Comperio

Schema riassuntivo del cronoprogramma

Durata complessiva dell'intervento: **70 giorni solari (10 settimane)**

Attività	Settimane									
	1	2	3	4	5	6	7	8	9	10
Fase 1: Analisi delle specificità del cliente per una idonea migrazione ed integrazione delle procedure	X									
Fase 2: Analisi dei dati da migrare e verifica della loro disponibilità		X								
Fase 3: Migrazione di prova, verifiche ed eventuali procedure di correzione			X	X	X					
Fase 4: Formazione degli operatori del sistema						X				
Fase 5: Attività di verifica della configurazione dei dispositivi presso le biblioteche							X	X		
Fase 6: Migrazione definitiva ed avvio del sistema in produzione									X	X

Piano di gestione delle fasi conclusive del contratto

Comperio, entro 2 mesi dalla conclusione del contratto, su richiesta del Cliente, propone al cliente il Piano di gestione delle fasi conclusive del contratto. In tale piano saranno messe in evidenza le attività che Comperio si impegna ad effettuare per escludere strategie di lock-in ed agevolare la trasparenza della trasmissione dei dati e delle infrastrutture.