ALLEGATO D

ACCORDO DI CONTITOLARITÀ TRA GLI ENTI SOTTOSCRITTORI E GLI ENTI ADERENTI AL POLO MOD SBN EX ART. 26 DEL REGOLAMENTO UE N. 2016/679 "REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI" (GDPR)

Art. 1 - Oggetto

1. Il presente Accordo, quale parte integrante e sostanziale della Convenzione a cui è allegato, regola il rapporto di contitolarità tra gli Enti sottoscrittori e gli Enti aderenti del Polo Bibliotecario Modenese SBN per i trattamenti dei dati personali necessari allo sviluppo e alla gestione di un sistema informativo bibliografico e documentale territoriale e alla definizione di un servizio bibliotecario regionale quale strumento di cooperazione interbibliotecaria, diffusione di servizi anche digitali ai lettori, articolazione del Servizio Bibliotecario Nazionale e partecipazione ad eventuali iniziative europee, così come previsto nella sopra citata convenzione di Polo sottoscritta tra le Parti.

Art. 2 - Ruoli e attività di trattamento di dati personali

1. Gli Enti sottoscrittori e gli Enti aderenti - d'ora innanzi anche "Contitolari" - agiscono in regime di contitolarità dei trattamenti di dati personali, ai sensi e per gli effetti di cui all'art. 26 del Regolamento UE n. 679/2016 "Regolamento generale sulla protezione dei dati", d'ora in avanti "Regolamento UE" o "GDPR".

2. I trattamenti di dati personali in regime di contitolarità sono quelli che afferiscono ai servizi bibliotecari integrati e riguardano i dati personali degli utenti delle biblioteche (dati anagrafici, codice fiscale, residenza/domicilio, telefono/cellulare, indirizzo di posta elettronica, professione, titolo di studio, estremi di un documento di riconoscimento, firma, ecc.) al fine di

- condividere le risorse bibliotecarie per una più ampia accessibilità dei documenti all'utenza;
- condividere le anagrafiche e altre informazioni sugli utenti con lo scopo di massimizzare l'efficienza e l'efficacia dei servizi bibliotecari erogati, in aderenza ai principi della Convenzione di Polo;
- svolgere attività statistica in forma anonima.

3. I dati sono trattati dagli Enti sottoscrittori e dagli Enti aderenti limitatamente alle finalità sopra descritte.

4. I Contitolari curano in sinergia gli adempimenti derivanti dalla normativa in materia di protezione dei dati personali. È compito di ciascun Contitolare verificare l'osservanza degli obblighi in materia di protezione dei dati personali presso le proprie sedi, formare e autorizzare al trattamento il personale.

5. Nei casi in cui soggetti terzi concorrano al trattamento di dati personali oggetto di contitolarità, ciascuno dei Contitolari designa per iscritto gli stessi quali Responsabili del trattamento di dati personali, in aderenza a requisiti, compiti e funzioni stabiliti dall'art. 28 del GDPR.

6. Ciascuno dei Contitolari si impegna altresì, ai sensi dell'art. 26, comma 2, del GDPR, a mettere a disposizione il contenuto essenziale del presente accordo con la sua pubblicazione sul proprio sito istituzionale.

7. È definito Gestore Tecnologico il Soggetto che gestisce uno o più dei servizi di seguito indicati:

- i servizi sistemistici;
- servizi infrastrutturali;
- servizi applicativi riferiti ai servizi bibliotecari integrati.

8. I Contitolari possono avvalersi di uno o più gestori tecnologici, secondo quanto disposto dal Comitato di Gestione.

9. Tutte le interazioni in materia di protezione dei dati personali tra i Contitolari sono effettuate a mezzo posta elettronica tramite lista di distribuzione privacy@bibliomo.it.

10. Alla suddetta lista di distribuzione sono abilitati almeno due referenti per ciascun Contitolare e un referente di ciascun Gestore Tecnologico. In caso di problematiche particolari o di violazioni di dati

personali sarà cura di ciascun Contitolare coinvolgere anche il proprio Responsabile della protezione dei dati personali (DPO).

Art. 3 - Ruolo della Regione

1. In quanto comproprietaria del Sistema Informativo Condiviso (d'ora in avanti SIC), alla Regione compete l'onere di curare con il Fornitore dei servizi manutentivi del SIC (di seguito anche solo "Fornitore del SIC") l'attività di progettazione, sviluppo e manutenzione evolutiva del software, in aderenza ai principi di privacy by design e privacy by default.

2. Con Sistema Informativo Condiviso si identificano sia il modulo di front office che quello di back office del software gestionale in uso presso il Polo Mod SBN. Le funzionalità di front office permettono agli utenti lettori di accedere al catalogo e ad alcuni servizi come, ad esempio, controllare la propria situazione lettore, richiedere la prenotazione o la proroga dei prestiti, salvare le proprie ricerche bibliografiche, ecc. Le funzionalità di back office sono, invece, di carattere gestionale e permettono agli operatori bibliotecari di accedere a servizi che concernono, ad esempio, la visualizzazione delle schede degli utenti lettori, l'autorizzazione di prenotazione o la proroga dei prestiti, le estrazioni di dati a fini statistici, ecc.

Art. 4 - Ruolo del Fornitore del SIC

1. Il Fornitore del SIC, ai fini della ripartizione di compiti e responsabilità in materia di protezione dei dati personali, è Responsabile del trattamento, ai sensi e per gli effetti dell'art. 28 del GDPR.

2. Il Fornitore del SIC:

a. effettua l'attività di progettazione, sviluppo e manutenzione evolutiva, secondo le specifiche funzionali adottate d'intesa con la Regione, in aderenza alle Linee Guida di sicurezza nello sviluppo delle applicazioni pubblicate da AGID e, in ogni caso, garantendo misure di sicurezza adeguate ai rischi correlati ai trattamenti;
b. nella sua qualità di Responsabile del trattamento ex art. 28 del GDPR, tratta i dati personali solo ai fini dell'esecuzione dell'oggetto del contratto di affidamento delle attività di progettazione, sviluppo e manutenzione evolutiva
c. non trasferisce i dati personali a soggetti terzi, se non a fronte di quanto disciplinato nel presente accordo;
d. adotta procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta del Polo dei dati personali di ogni interessato e/o a conformarsi alle istruzioni fornite dal Polo in materia;
e. assicura la massima collaborazione al fine dell'esperimento delle valutazioni di impatto ex art. 35 del GDPR che il Polo intenderà esperire sui trattamenti che rivelano, a suo insindacabile giudizio, un rischio elevato per i diritti e le libertà delle persone fisiche;
f. implementa appropriate misure di sicurezza, sia tecniche che organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati;
g. conserva, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema del SIC;
h. dà attuazione alla prescrizione di cui al punto 2, lettera e), "Verifica delle attività" del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
i. adotta misure tecniche ed organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti al Polo, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema di propria competenza;
j. assicura massima cooperazione e assistenza al fine di dare effettività alle azioni di mitigazione previste dal Polo per affrontare rischi correlati al trattamento;
k. garantisce competenze e affidabilità dei propri dipendenti e collaboratori autorizzati al trattamento dei dati personali;

l. è autorizzato sin d'ora, previa informazione al Committente alla designazione di altri responsabili del trattamento (d'ora in poi anche "sub-responsabili"), imponendo agli stessi condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute nel presente Accordo;
m. in tutti i casi, si assume la responsabilità nei confronti degli enti contitolari per qualsiasi violazione o omissione realizzati da un sub-responsabile o da altri terzi soggetti incaricati dallo stesso, indipendentemente dal fatto che il Responsabile del trattamento abbia o meno rispettato i propri obblighi contrattuali, ivi comprese le conseguenze patrimoniali derivanti da tali violazioni o omissioni;
n. non effettua trasferimenti dei dati personali oggetto di trattamento al di fuori dell'Unione Europea;
o. provvede, su scelta dei Contitolari, alla restituzione o cancellazione dei dati personali trattati per l'esecuzione delle attività sopra indicate al termine dell'affidamento;
p. si rende disponibile a specifici audit in tema di privacy e sicurezza informatica da parte del Polo;
q. in virtù di quanto previsto dall'art. 33 del GDPR e nei limiti di cui al perimetro delle attività affidate, deve comunicare all'indirizzo di cui all'art. 2, punto 9 del presente Accordo, a mezzo di posta elettronica certificata, nel minor tempo possibile, e comunque non oltre 24 (ventiquattro) ore da quando ne abbia avuto notizia, qualsiasi violazione di sicurezza che abbia comportato accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, ivi incluse quelle che abbiano riguardato i propri sub-fornitori. Tale comunicazione deve contenere ogni informazione utile alla gestione del data breach, oltre a:
    - descrivere la natura della violazione dei dati personali
    - le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
    - i recapiti del DPO nominato o del soggetto competente alla gestione del data breach;
    - la descrizione delle probabili conseguenze della violazione dei dati personali;
    - una descrizione delle misure adottate o che si intende adottare per affrontare la Violazione della sicurezza, compreso, ove opportuno, misure per mitigare i suoi possibili effetti negativi;
r. fornisce tutto il supporto necessario ai fini delle indagini e sulle valutazioni in ordine alla violazione di dati, anche al fine di individuare, prevenire e limitare gli effetti negativi della stessa, conformemente ai suoi obblighi ai sensi del presente articolo e per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa;
s. amministra il database curandone tutti gli aspetti che non attengono la gestione sistemistica (es: progettazione logica, integrità dei dati, ecc.) e all'applicazione dei principi di privacy by design e privacy by default;
t. cura la gestione delle password (a titolo esemplificativo: le attività di reset, cifratura, caratteristiche di robustezza della password), salvo il caso in cui gli enti sottoscrittori utilizzino un sistema di federazione.

Art. 5 - Ruolo degli Enti aderenti

1. Gli Enti aderenti, ai fini della ripartizione di compiti e responsabilità in materia di protezione dei dati personali, sono Contitolari del trattamento, ai sensi e per gli effetti dell'art. 26 del GDPR.

2. L'esecuzione dei trattamenti da parte degli Enti aderenti è disciplinata dall'apposita convenzione stipulata con uno degli Enti sottoscrittori, previa approvazione del Comitato di Gestione e parere positivo della Commissione tecnica, ed esplicita adesione dell'Ente aderente al presente Accordo di contitolarità

Art. 6 - Informativa per il trattamento dei dati personali

1. I Contitolari stabiliscono, in sede di Comitato di gestione, le informazioni di cui agli artt. 13 e 14 del GDPR.

2. Nei casi in cui i dati siano raccolti in presenza fisica dell'interessato, l'informativa per il trattamento dei dati personali, come definita dai Contitolari, è fornita dalla biblioteca presso la quale il dato è stato raccolto.

3. In ogni caso l'informativa per il trattamento dei dati personali è messa a disposizione degli utenti con modalità telematiche.

4. Gli Enti sottoscrittori e aderenti possono utilizzare i dati personali degli utenti per finalità ulteriori compatibili, ai sensi e nei limiti del Considerando 50 e dell'art. 6, comma 4, del GDPR.

Art. 7 - Esercizio dei diritti da parte degli interessati

1. Gli interessati possono esercitare i diritti loro riconosciuti dalla normativa in materia di protezione dei dati personali, presentando istanza nei confronti della propria biblioteca di riferimento, direttamente in sede o tramite modalità telematiche.

2. L'Ente destinatario dell'istanza, entro 7 (sette) giorni dalla ricezione, propone agli altri Contitolari un'ipotesi di riscontro alla stessa a mezzo d'invio di comunicazione di posta elettronica all'indirizzo privacy@bibliomo.it.

3. Decorsi 10 (dieci) giorni senza aver ricevuto proposte di rettifica, il riscontro viene trasmesso all'interessato nei termini proposti che si assumono condivisi da tutti i Contitolari.

4. I Contitolari possono addebitare all'interessato un contributo spese ragionevole basato sui costi amministrativi solo nel caso in cui siano richieste più copie di dati in formato cartaceo.

5. I Contitolari conservano i dati personali degli interessati, conformemente ai principi di cui all'art. 5 del GDPR, per un arco di tempo non superiore al conseguimento delle finalità e con specifico riguardo al principio di limitazione della conservazione di cui all'art. 5, lett. e), del medesimo Regolamento, e comunque fino a quando non perviene la richiesta di cancellazione da parte dell'utente, fatti salvi ulteriori obblighi di conservazione previsti da disposizioni di legge o per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

6. Nei casi in cui l'utente richieda la cancellazione dei propri dati personali, l'Ente destinatario dell'istanza, dopo avere esperito la procedura di cui ai punti precedenti, elimina dalla banca dati ogni dato personale ad esso riferito dandone comunicazione agli altri Contitolari.

Art. 8 - Misure di sicurezza

1. I Contitolari utilizzano sistemi affidabili che garantiscano la sicurezza dei procedimenti.

2. Gli stessi implementano misure adeguate a prevenire ogni possibile contraffazione, nonché idonee anche a garantire la riservatezza, l'integrità e la sicurezza del procedimento e delle attività di generazione delle credenziali di accesso.

3. L'assegnazione e revoca delle credenziali di accesso alla base dati Sebina del Polo Mod SBN è in capo al Comune di Modena in qualità di Ente gestore, previa richiesta scritta da parte dei responsabili delle biblioteche partner da trasmettere via PEC all'indirizzo biblioteche@cert.comune.modena.it.

4. Per la richiesta si dovrà compilare un apposito modulo predisposto dal Comitato di gestione, che dovrà contenere tra l'altro nome, cognome e dati anagrafici dell'operatore da abilitare, ruolo (es. dipendente TD/TI, appalto, libero professionista, servizio civile), profilazione richiesta (es. addetto prestito, catalogatore, ILL, ecc.), biblioteche da associare e dichiarazione attestante l'incarico al trattamento dati.

5. I Contitolari incaricano e formano adeguatamente i soggetti autorizzati al trattamento di dati personali.

6. I Contitolari, nell'ambito della gestione tecnologica del servizio, effettuano attività di monitoraggio della sicurezza degli strumenti informatici.

7. I Contitolari si impegnano inoltre a comunicare con sollecitudine all'ente gestore eventuali variazioni degli operatori in modo da poter provvedere tempestivamente alla revoca delle credenziali o alla modifica delle abilitazioni.

Art. 9 - Disservizi, incidenti di sicurezza e data breach

1. I Contitolari comunicano immediatamente alla lista di distribuzione di cui all'art. 2, punto 9, del presente Accordo, qualsiasi sospetta distruzione, perdita, alterazione, divulgazione o accesso non autorizzato ai dati e alle informazioni trattate di cui vengono a conoscenza.

2. I Gestori Tecnologici e il Fornitore del SIC comunicano tempestivamente alla predetta lista di distribuzione eventuali malfunzionamenti e/o interruzioni di servizio (programmate e non). Per malfunzionamento si intende un disservizio che non consenta l'ordinaria fruibilità del SIC. Per Interruzione di Servizio si intende la non disponibilità del SIC per un tempo superiore a 20 minuti consecutivi o nell'arco di un'ora.

3. I Gestori Tecnologici e il Fornitore del SIC comunicano a mezzo di posta elettronica certificata all'indirizzo di posta di cui all'art.2.9, nel minor tempo possibile, e comunque non oltre 24 (ventiquattro) ore da quando ne abbia avuto notizia, qualsiasi violazione di sicurezza che abbia comportato accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, ivi incluse quelle che abbiano riguardato i propri sub-Fornitori.

4. Nel caso di ricezione di informazioni inerenti una presunta violazione, gli Enti sottoscrittori, in aderenza agli artt. 33 e 34 del Regolamento UE, valutano congiuntamente la probabilità che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche e procedono all'eventuale notifica al Garante per la protezione dei dati personali ed eventualmente agli interessati.

5. La valutazione congiunta viene effettuata entro 48 ore dalla contezza della sussistenza della violazione di dati personali, convocando una riunione d'urgenza del Comitato di Gestione, con l'eventuale partecipazione dei Responsabili per la protezione dei dati degli Enti stessi; non è richiesto un numero minimo di partecipanti e le decisioni assunte sono prese a maggioranza semplice per conto di tutti gli Enti sottoscrittori. In tale sede è, altresì, individuato il Soggetto delegato alla notifica della violazione al Garante per la protezione dei dati personali ed eventualmente agli interessati.

6. I Gestori Tecnologici, anche alla luce delle indicazioni fornite dai Contitolari

- preparano il personale ad affrontare situazioni anomale e non codificate;
- minimizzano i danni relativi agli incidenti di sicurezza e ne impediscono la propagazione;
- gestiscono correttamente il processo di ripristino dei sistemi e delle applicazioni;
- acquisiscono le eventuali evidenze digitali di reato.

Art. 10 - Registro delle attività di trattamento

1. I Contitolari, in aderenza all'art. 30 del Regolamento UE con riferimento ai trattamenti di dati personali effettuati di cui all'art. 2.1, riportano, nel proprio registro dei trattamenti, tutte le informazioni richieste dalla norma.

2. Nel registro dei trattamenti deve specificatamente essere riportato che tali trattamenti di dati personali sono effettuati in regime di contitolarità.

Art. 11 - Durata dell'accordo

1. La durata del presente accordo è correlata alla durata della somministrazione dei servizi bibliotecari integrati del Polo.

2. Il presente accordo deve intendersi risolto nel caso di cessazione della somministrazione del servizio.

Art. 12 - Disposizioni conclusive

1. Il presente Accordo verrà revisionato periodicamente per assicurarne l'attualità e la conformità alle disposizioni legislative vigenti

2. Rimane inteso che, tra le Parti, ogni Contitolare sarà responsabile per i danni che dovessero derivare da proprio esclusivo inadempimento, manlevando e tenendo indenne le altre Parti dalle conseguenze del danno causato dal suddetto trattamento non conforme

3. L'invalidità, anche parziale, di una o più delle clausole del presente Accordo non pregiudica la validità delle restanti clausole.

4. Per quanto non espressamente previsto dal presente Accordo si rinvia alla Convenzione di Polo.