Allegato 2. Accordo di contitolarità tra gli enti aderenti alla convenzione del sistema bibliotecario

Art. 1. Ruoli e attività di trattamento di dati personali

1.1 Gli Enti sottoscrittori 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.

1.2 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.

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 dal sistema di gestione bibliotecario. Il corretto trattamento delle categorie di dati sopra elencate ricade nella responsabilità di ogni singolo Titolare il quale è tenuto a fornire precise disposizioni ai propri operatori sulle modalità di trattamento dei dati che rispettino i principi di cui agli artcioli 5 e 6 del Regolamento europeo 679/2016.

1.3 I dati sono trattati dagli enti sottoscrittori e dai soggetti aderenti limitatamente alle finalità sopra descritte e ricade nell'ambito di responsabilità di ciascun Titolare vigilare affinché i propri operatori trattino i dati solo ed esclusivamente per le finalità dichiarate.

1.4 Nei casi in cui Soggetti terzi concorrano al trattamento di dati personali oggetto di contitolarità, ciascuno dei Contitolari autonomamente designa per iscritto gli stessi quali Responsabili del trattamento di dati personali. I contitolari devo essere informati della nomina di soggetti terzi a Responsabili del trattamento da parte dei singoli titolari attraverso comunicazioni generali a cadenza annuale che diano conto delle nomine effettuate.

1.5 Le Parti si impegnano altresì, ai sensi dell'art. 26, comma 2, del Regolamento (EU) 2016/679, a mettere a disposizione dell'interessato il contenuto del presente Accordo con le modalità di comunicazione che riterrà più opportune e confacenti al modello di privacy policy adotatto.

1.6 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.

1.7 È definito Gestore Tecnologico il soggetto che gestisce uno o più dei servizi di seguito indicati:

- i servizi sistemistici;
- servizi infrastrutturali;
- l'assegnazione credenziali e l'assistenza tecnica agli utenti del SIC;
- servizi applicativi riferiti ai servizi bibliotecari integrati.

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

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

1.10 Alla suddetta lista di distribuzione sono abilitati almeno due referenti per ciascun Contitolare, i Responsabili della protezione dei dati personali dei Contitolari e un referente di ciascun Gestore Tecnologico.

Art. 2. Il ruolo della Regione Emilia Romagna

1.1 Poiché la Regione Emilia Romagna è comproprietaria del SIC sullo Stesso grava 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.

Art. 3 Il ruolo del Fornitore del SIC

1.1. 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 Regolamento UE n. 679/2016.

Il Fornitore del SIC:

a. effettua l'attività di progettazione, sviluppo e manutenzione evolutiva, secondo le specifiche funzionali adottate d'intesa con la Regione Emilia Romagna, 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 Regolamento UE 2016/679, 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 e a seguito di accordo con i contitolari, 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" dando evidenza ai Contitolari delle nomine degli Amministratori di sistema effettuate in conformità al sopracitato Provvedimento del Garante per la protezione dei dati personali;

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, affidabilità ed adeguata formazione in materia di protezione di dati personali dei propri dipendenti e collaboratori autorizzati al trattamento dei dati;

l. previa informazione ai contitolari è autorizzato sin d'ora, 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 od 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 od omissioni;

n. non effettua trasferimenti dei dati personali oggetto di trattamento al di fuori dell'Unione Europea;

o. provvede alla restituzione o cancellazione dei dati personali trattati per l'esecuzione delle attività sopra indicate al termine dell'affidamento; in caso di richiesta di cancellazione dovrà attenersi alle modalità di distruzione dei dati stabilite dai contitolari al momento della scadenza contrattuale;

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 Regolamento e nei limiti di cui al perimetro delle attività affidate, deve comunicare 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:

a) descrivere la natura della violazione dei dati personali

b) le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

c) i recapiti del DPO nominato o del soggetto competente alla gestione del data breach;

d) la descrizione delle probabili conseguenze della violazione dei dati personali;

e) 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

a. 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.

b. amministra il database curandone tutti gli aspetti che non attengono la gestione sistemistica e collabora con i contitolari nell'applicazione dei principi di privacy by design e privacy by default;

c. 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 Il ruolo dei Soggetti aderenti

1.1 I soggetti aderenti, ai fini della ripartizione di compiti e responsabilità in materia di protezione dei dati personali, sono Responsabili del trattamento, ai sensi e per gli effetti dell'art. 28 del Regolamento UE n. 679/2016.

1.2 L'esecuzione dei trattamenti da parte dei Soggetti Aderenti è disciplinata dall'Allegato A, che vincola tali responsabili del trattamento ai Contitolari e che disciplina durata, natura, finalità del trattamento, ivi compresi i tipi di dati personali e le categorie di interessati, i compiti e responsabilità specifici dei responsabili del trattamento, nonché gli obblighi e i diritti dei Contitolari.

1.3 I Soggetti aderenti sono autorizzati alla designazione di altri responsabili del trattamento (d'ora in poi anche "sub-responsabili"), a condizione che siano imposti agli stessi condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute nell'Allegato 2.

1.4 In tutti i casi, il Responsabile del trattamento si assume la responsabilità per qualsiasi violazione od omissione realizzati da un Sub-Responsabile o da altri terzi soggetti autorizzati 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 od omissioni.

Art. 6. Informativa per il trattamento dei dati personali

6.1 I Contitolari stabiliscono, in sede di Comitato di gestione, le informazioni di cui all'art. 13 del Regolamento (UE)n. 679/2016 e si assumono l'onere, singolarmente e per il proprio bacino di utenza, di rendere disponibile l'informativa agli interessati.

6.2 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.

6.3 In ogni caso l'informativa per il trattamento dei dati personali è messa a disposizione degli utenti ovvero resa permanentemente disponibile sia in formato cartaceo nelle sedi bibliotecarie, che in formato telematico sui siti web istituzionali delle singole biblioteche.

6.4 Gli Enti possono utilizzare i dati personali degli utenti per finalità ulteriori compatibili, ai sensi e nei limiti del Considerando 50 e dell'art. 6 par. 4 del Regolamento UE 679/2016 tenendo conto *"tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti,in particolare le ragionevoli aspettative dell'interessatoin base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto"*.

Art. 7. L'esercizio dei diritti da parte degli interessati

7.1 Gli interessati possono esercitare i diritti loro riconosciuti dalla normativa in materia di protezione dei dati personali, presentando istanza nei confronti di qualsiasi Ente aderente al Polo, direttamente nelle biblioteche o tramite modalità telematiche.

7.2 L'Ente destinatario dell'istanza di cui al comma 1 propone, entro 7 giorni dalla ricezione, agli altri Contitolari un'ipotesi di riscontro alla stessa a mezzo d'invio di comunicazione di posta elettronica all'indirizzo poloXXXprivacy@dominio.it.

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

7.4 Al fine di semplificare le modalità di inoltro e di ridurre i tempi per il riscontro, nell'informativa per il trattamento dei dati personali viene suggerito agli interessati di utilizzare un unico punto di contatto.

7.5 Le Parti 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.

7.6 Le parti conservano i dati personali degli interessati, conformemente ai principi di cui all'art. 5 del GDPR, per un periodo non superiore a quello necessario per il perseguimento delle finalità istituzionali degli enti secondo quanto concordato nel Comitato di Gestione del Polo, e con specifico riguardo al principio di limitazione della conservazione di cui all'art. 5, paragrafo 1, lett. e) GDPR). Nei casi in cui l'utente richieda la cancellazione dei propri dati personali le Parti eliminano ogni dato personale in proprio possesso ad esso riferito, dandone comunicazione agli altri contitolari.

Art. 8. Le misure di sicurezza

8.1 I Contitolari utilizzano sistemi affidabili che garantiscano la sicurezza dei procedimenti, in conformità ai criteri riconosciuti in ambito europeo o internazionale, allineando le proprie procedure di sicurezza agli standard internazionali.

8.2 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.

8.3 I Contitolari formano adeguatamente i soggetti autorizzati al trattamento di dati personali in conformità a quanto disposto dal precedente articolo 1.2.

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

Art. 9 Disservizi, incidenti di sicurezza e data breach

1.1 Gli Enti aderenti al Polo e i Contitolari comunicano immediatamente alla lista di distribuzione di cui all'art. 1.9 qualsiasi sospetta distruzione, perdita, alterazione, divulgazione o accesso non autorizzato ai dati e alle informazioni trattate.

1.2 I Gestori Tecnologici e il Fornitore del SIC comunicano e agli Enti sottoscrittori 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.

1.3 Nel caso di ricezione di informazioni inerenti una presunta violazione, i Contitolari, in aderenza agli artt. 33 e 34 del Regolamento (UE) 2016/679, valutano congiuntamente la probabilità che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche e procede all'eventuale notifica al Garante per la protezione di dati personali ed eventualmente agli interessati.

1.4 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 ed informando i Responsabili della protezione dei dati dei singoli titolari; non è richiesto un numero minimo di partecipanti e le decisioni assunte sono prese a maggioranza semplice per conto di tutti i Contitolari. 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.

1.5 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

10.1 I Contitolari, in aderenza all'art. 30 del Regolamento (UE) 2016/679 con riferimento ai trattamenti di dati personali effettuati di cui all'art. 1.2, riportano, nel proprio registro dei trattamenti, tutte le informazioni richieste dalla norma.

10.2 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

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

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

Art. 12 Miscellanea

12.1 Le eventuali modifiche al presente Accordo sono apportate per iscritto.

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

12.3 Per quanto non espressamente previsto dal presente Accordo si rinvia alla Convenzione di Polo, nonché alle norme vigenti in materia di protezione dei dati personali.