Allegato 3. Disciplinare di responsabile del trattamento Comuni, Regione Emilia Romagna e biblioteche specialistiche, in qualità di contitolari, e la Provincia di Reggio Emilia, in qualità di responsabile del trattamento di dati personali

1. Premesse.

Il presente Accordo si compone delle clausole di seguito rappresentate e dall'Allegato: Glossario.

2. Trattamento dei dati nel rispetto delle istruzioni fornite

2.1 Il Responsabile del trattamento, relativamente a tutti i Dati personali che tratta per conto dei Contitolari garantisce che:

2.1.1 tratta tali Dati personali solo ai fini dell'esecuzione della convenzione di cui il presente disciplinare costituisce allegato, parte integrante e sostanziale, agendo pertanto, esclusivamente sulla base delle istruzioni documentate e fornite dai Contitolari;

2.1.2 non trasferisce i Dati personali a soggetti terzi, se non nel rispetto delle condizioni di liceità assolte dai Contitolari e a fronte di quanto disciplinato nel presente accordo;

2.1.3 non tratta o utilizza i Dati personali per finalità diverse da quelle per cui è conferito incarico dai Contitolari, financo per trattamenti aventi finalità compatibili con quelle originarie;

2.1.4 prima di iniziare ogni trattamento e, ove occorra, in qualsiasi altro momento, informerà i contitolari qualora una qualsiasi istruzione si ponga in violazione di Normativa applicabile;

2.2 Al fine di dare seguito alle eventuali richieste da parte di soggetti interessati, il Responsabile del trattamento si obbliga ad adottare:

- procedure idonee a garantire il rispetto dei diritti e delle richieste formulate ai Contitolari dagli interessati relativamente ai loro dati personali e/o a conformarsi alle istruzioni fornite dai Contitolari in materia;
- procedure atte a garantire l'aggiornamento, la modifica e la correzione dei dati personali di ogni interessato su richiesta di ciascun Ente che effettua la nomina ex art. 28 del GDPR e/o a conformarsi alle istruzioni fornite dai Contitolari in materia;

- procedure atte a garantire la cancellazione o il blocco dell'accesso ai dati personali a richiesta dai Contitolari e/o a conformarsi alle istruzioni fornite dai Contitolari in materia;
- procedure atte a garantire il diritto degli interessati alla limitazione di trattamento, su richiesta dei Contitolari e/o a conformarsi alle istruzioni fornite dai Contitolari in materia.

o Il Responsabile del trattamento deve garantire e fornire ai Contitolari cooperazione, assistenza e le informazioni che potrebbero essere ragionevolmente richieste per consentire di adempiere ai propri obblighi ai sensi della normativa applicabile, ivi compresi i provvedimenti e le specifiche decisioni del Garante per la protezione dei dati personali.

o Il Responsabile del trattamento, anche nel rispetto di quanto previsto all'art. 30 del Regolamento, deve mantenere e compilare e rendere disponibile, un registro dei trattamenti dati personali che riporti tutte le informazioni richieste dalla norma.

o Il Responsabile del trattamento assicura la massima collaborazione al fine dell'esperimento delle valutazioni di impatto ex art. 35 del GDPR che ciascun contitolare intenderà esperire sui trattamenti che rivelano, a Suo insindacabile giudizio, un rischio elevato per i diritti e le libertà delle persone fisiche.

3. Le misure di sicurezza

3.1 Il Responsabile del trattamento deve adottare e mantenere 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.

3.2 Nei casi in cui il Responsabile effettui trattamenti di conservazione dei dati personali del Titolare nel proprio sistema informativo, garantisce la separazione di tipo logico di tali dati da quelli trattati per conto di terze parti o per proprio conto.

3.3. Il Responsabile del trattamento conserva, nel caso siano allo stesso affidati servizi di amministrazione di sistema, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

3.5 Il Responsabile del trattamento deve adottare misure tecniche ed organizzative adeguate per salvaguardare la sicurezza di qualsiasi rete di comunicazione elettronica o dei servizi forniti ai Contitolari, con specifico riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema.

3.6 Conformemente alla disposizione di cui all'art. 28 comma 1 del Regolamento e alla valutazione delle garanzie che il Responsabile del trattamento deve presentare, lo stesso Responsabile attesta, a mezzo della sottoscrizione del presente accordo, la conformità della propria organizzazione almeno ai parametri di livello minimo di cui alle misure di sicurezza individuate da Agid la circolare n. 2/2017.

4. Analisi dei rischi, privacy by design e privacy by default

4.1 Con riferimento agli esiti dell'analisi dei rischi effettuata dai Contitolari sui trattamenti di dati personali cui concorre il Responsabile del trattamento, lo stesso assicura massima cooperazione e assistenza al fine di dare effettività alle azioni di mitigazione previste dai Contitolari per affrontare eventuali rischi identificati.

4.2 Il Responsabile del trattamento dovrà consentire ai Contitolari, tenuto conto dello stato della tecnica, dei costi, della natura, dell'ambito e della finalità del relativo trattamento, di adottare, sia nella fase iniziale di determinazione dei mezzi di trattamento, che durante il trattamento stesso, ogni misura tecnica ed organizzativa che si riterrà opportuna per garantire ed attuare i principi previsti in materia di protezione dati e a tutelare i diritti degli interessati.

4.3 In linea con i principi di privacy by default, dovranno essere trattati, per impostazione predefinita, esclusivamente quei dati personali necessari per ogni specifica finalità del trattamento, e

che in particolare non siano accessibili dati personali ad un numero indefinito di soggetti senza l'intervento di una persona fisica.

4.4 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle policy di privacy by design e by default adottate dai Contitolari e specificatamente comunicate dai Contitolari, anche successivamente alla stipula del presente accordo.

5. Soggetti autorizzati ad effettuare i trattamenti - Designazione

5.1 Il Responsabile del trattamento garantisce competenze ed affidabilità dei propri dipendenti e collaboratori autorizzati al trattamento dei dati personali (di seguito anche incaricati) effettuati per conto dei Contitolari .

5.2 Il Responsabile del trattamento garantisce che gli incaricati abbiano ricevuto adeguata formazione in materia di protezione dei dati personali e sicurezza informatica, consegnando ai Contitolari le evidenze di tale formazione.

5.3 Il Responsabile del trattamento, con riferimento alla protezione e gestione dei dati personali, impone ai propri incaricati obblighi di riservatezza non meno onerosi di quelli previsti nel Contratto di cui il presente documento costituisce parte integrante. In ogni caso il Responsabile del trattamento è direttamente ritenuto responsabile per qualsiasi divulgazione di dati personali dovesse realizzarsi ad opera di tali soggetti.

6. Sub-Responsabili del trattamento di dati personali.

6.1 Nell'ambito dell'esecuzione del contratto, il Responsabile del trattamento è autorizzato sin d'ora, alla designazione di altri responsabili del trattamento (d'ora in poi anche "sub-responsabili"), dandone informazione ai Contitolari, ed imponendo agli stessi condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute nel presente disciplinare.

6.2 In tutti i casi, il Responsabile del trattamento si assume la responsabilità nei confronti dei 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.

7. Trattamento dei dati personali fuori dall'area economica europea

7.1 I Contitolari non autorizzano il trasferimento dei dati personali oggetto di trattamento al di fuori dell'Unione Europea.

8. Cancellazione dei dati personali

8.1 Il Responsabile del trattamento, a richiesta di ciascun Titolare, provvede alla restituzione o cancellazione dei dati personali trattati per l'esecuzione del presente contratto al termine dell'affidamento o del periodo di conservazione e in qualsiasi circostanza in cui sia richiesto dai Contitolari, compresa l'ipotesi in cui la stessa debba avvenire per dare seguito a specifica richiesta da parte di interessati.

9. Indagini dell'Autorità e reclami

9.1 Nei limiti della normativa applicabile, il Responsabile del trattamento o qualsiasi Sub-Responsabile informa senza alcun indugio i Contitolari di qualsiasi

- richiesta o comunicazione promanante dal Garante per la protezione dei dati personali o da forze dell'ordine
- istanza ricevuta da soggetti interessati

Il Responsabile del trattamento fornisce, in esecuzione del contratto e, quindi, gratuitamente, tutta la dovuta assistenza ai Contitolari per garantire che possano rispondere a tali istanze o comunicazioni nei termini temporali previsti dalla normativa e dai regolamentari applicabili.

10. Violazione dei dati personali e obblighi di notifica

10.1 Il Responsabile del trattamento, 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 ai Contitolari 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

10.2 Il Responsabile del trattamento deve fornire tutto il supporto necessario ai Contitolari 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, previo accordo con i Contitolari, per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa. Il Responsabile del trattamento non deve rilasciare, né pubblicare alcun comunicato stampa o relazione riguardante eventuali data breach o violazioni di trattamento senza aver ottenuto il previo consenso scritto dei Contitolari.

GLOSSARIO

“Garante per la protezione dei dati personali”: è l’autorità di controllo responsabile per la protezione dei dati personali in Italia;

“Dati personali ”: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

“GDPR” o “Regolamento”: si intende il Regolamento UE 2016/679 sulla protezione delle persone fisiche relativamente al trattamento dei dati personali e della loro libera circolazione (General Data Protection Regulation) che sarà direttamente applicabile dal 25 maggio 2018;

“Normativa Applicabile”: si intende l’insieme delle norme rilevanti in materia protezione dei dati personali, incluso il Regolamento Privacy UE 2016/679 (GDPR) ed ogni provvedimento del Garante per la protezione dei dati personali e del WP Art. 29.

“Titolare del Trattamento”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

“Trattamento”: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

“Responsabile del trattamento”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.