vedi anche
Notiziario della Sezione Ligure dell'Associazione Italiana Biblioteche
Vol. 29 N° 1 (2019) - ISSN 2281-0617

Appunti su GDPR e biblioteche

Giuseppe Pavoletti

Introduzione

Il regolamento UE 2016/679, generalmente citato come GDPR o RGPD (rispettivamente da *General Data Protection Regulation* e *Regolamento Generale per la Protezione dei Dati*)[1], disciplina in tutta l'Unione Europa il trattamento dei dati di persone fisiche. In Italia inoltre è ancora in vigore, anche se fortemente rimaneggiato, il precedente Decreto Legislativo 196/2003 generalmente noto come *Codice della privacy*[2], il quale disciplina aspetti che il regolamento europeo lascia alla legislazione nazionale.

Queste norme non contengono specifiche disposizioni sulle biblioteche, ma poiché queste ultime evidentemente trattano numerosi dati personali sono soggette alle disposizioni generali.

Il presente articolo non è un'esposizione sistematica del GDPR, né tantomeno un approfondimento giuridico di tutta la casistica, ma solo una modesta raccolta di considerazioni pratiche utile a mettere in evidenza alcuni effetti della norma sull'attività quotidiana delle biblioteche e – si spera – ad aiutare a non incorrere almeno nelle violazioni più grossolane: ci sono quindi molte nozioni che qui non verranno trattate. I lettori sono fortemente invitati ad esaminare direttamente il testo della norma.

In quanto segue si presuppone sempre che il trattamento non riguardi le categorie particolari di dati personali di cui all'art. 9 comma 1 del GDPR: *dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, [...] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona* né i dati relativi a condanne penali e reati di cui all'art. 10[3].

L'articolo è incentrato sul trattamento dei dati degli utenti, che è indubbiamente il più rilevante ma non l'unico: ci sono infatti i dati del personale e – anche se spesso non ci si pensa – quelli degli autori presenti nel catalogo, soprattutto nei record di autorità che in genere contengono informazioni biografiche.

---

1 https://www.garanteprivacy.it/il-testo-del-regolamento (oltre al testo della norma il sito contiene ampia documentazione aggiuntiva ivi compresa un'utile guida sintetica scritta in linguaggio facilmente comprensibile: https://www.garanteprivacy.it/web/guest/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali)

2 *https://www.garanteprivacy.it/codice*

3 Si tratta evidentemente di quelli che in precedenza venivano chiamati dati sensibili e sensibilissimi

vedi anche
Notiziario della Sezione Ligure dell'Associazione Italiana Biblioteche
Vol. 29 N° 1 (2019) - ISSN 2281-0617

Principi fondamentali

La nozione da cui partire è certamente quella di dati personali, così definiti dall'art. 4 del GDPR: *qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»).*

Strettamente connessa è la nozione di trattamento, che sempre l'art. 4 definisce come *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.*

I principi fondamentali del GDPR potrebbero essere sintetizzati come segue (cfr. art. 5):

- il trattamento dei dati personali deve essere autorizzato dall'interessato (la persona a cui i dati si riferiscono) oppure lecito per altri motivi espressamente definiti dalla legge (ad esempio svolto dall'amministrazione pubblica per scopi istituzionali)
- la sua esistenza e le sue caratteristiche devono essere rese note all'interessato
- devono essere raccolti e registrati solo i dati necessari per gli scopi del trattamento
- i dati devono essere accessibili solo agli addetti al trattamento e non possono essere resi noti ad altri
- responsabilizzazione (accountability) del titolare (v. sotto per la definizione): *il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento* (art. 24, v. anche art. 25).

Il principio della responsabilizzazione comporta una conseguenza importantissima, cioè che è onere del titolare dimostrare di aver agito in modo regolare.

Due soggetti fondamentali che entrano in gioco nel GPDR sono i seguenti, definiti dall'art. 4:

- 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*
- responsabile del trattamento: l*a persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*; si noti che il responsabile non c'è se il titolare effettua direttamente tutto il trattamento.

Benché la nozione non sia espressamente definita, il GDPR fa riferimento anche alle *persone autorizzate* al trattamento, che sono come ovvio le persone fisiche che concretamente effettuano il trattamento su incarico del titolare o del responsabile.

Di solito titolare e responsabile sono facilmente individuabili, ma come vedremo possono esserci dubbi nel caso di servizi gestiti tramite l'accordo di numerosi soggetti.

vedi anche
Notiziario della Sezione Ligure dell'Associazione Italiana Biblioteche
Vol. 29 N° 1 (2019) - ISSN 2281-0617

Scopi e necessità del trattamento

A questo punto, conviene partire dai fondamenti della liceità del trattamento, analizzando il suo rapporto con gli scopi della biblioteca. Il trattamento deve essere quello necessario per tali scopi, mentre non può essere esteso a piacere, a meno che non abbia anche altre giustificazioni. Ad esempio, se si raccolgono dati utili per attività e servizi culturali diversi dalla biblioteca, questo va considerato un trattamento distinto e deve avere una giustificazione distinta.

Anche nell'ambito della biblioteca vanno distinti i servizi essenziali, come il prestito, che comportano la raccolta di un certo insieme di dati minimi indispensabili , cioè quelli utili ad identificare l'utente e poterlo contattare (nome, cognome, data di nascita, codice fiscale, residenza, telefono, email) e attività diverse come elaborazioni statistiche o fornitura di servizi quali l'invio di news personalizzate e simili, che richiedono la raccolta di ulteriori dati (ad esempio titolo di studio, professione, preferenze di lettura ecc.).

Quelli elencati vanno considerati trattamenti distinti: si noti che alcuni dati vengono utilizzati per tutti i trattamenti (come l'anagrafica degli utenti), altri dati solo per alcuni trattamenti (ad esempio la professione, che è inutile per fornire il prestito ma può servire per le statistiche o per altri servizi).

Deve quindi essere sempre ben chiaro il collegamento tra i dati raccolti e i trattamenti che vengono eseguiti (dei quali, come vedremo, l'utente deve essere informato).

Proteggere i dati nella pratica

Poiché l'oggetto del regolamento è la protezione dei dati, occorre considerare come questi di fatto, nella pratica vengono protetti, anche perché la mancata protezione può determinare gravi sanzioni per i responsabili. Non basta infatti scrivere nei documenti che si persegue la protezione dei dati personali, bisogna che la protezione ci sia anche nella pratica!

I dati devono essere protetti contro l'accesso e la diffusione illeciti (cioè da parte di chi non ne ha diritto per lo svolgimento dei trattamenti leciti, o per trattamenti non autorizzati dall'utente o a lui non comunicati), nonché contro l'alterazione e la distruzione. Ne consegue che ai sistemi informatici devono essere applicate le misure di sicurezza volte ad impedire il loro uso abusivo, come: uso di password adeguate, custodia delle password atta ad impedire che non vengano a conoscenza di chi non ne ha diritto, protezione della rete tramite firewall, separazione della rete a cui sono collegate le postazioni del pubblico da quella a cui sono collegate le postazioni del personale, aggiornamento regolare del sistema operativo e dei software applicativi, uso di antivirus e antimalware, adozione di comportamenti sicuri (ad esempio prudenza con l'installazione dei programmi e con gli allegati alle email). Assolutamente da evitare (anche indipendentemente dal GPDR!) il login automatico senza immissione della password e il salvataggio della password nel browser.

L'accesso ai dati personali non deve essere consentito a tutto il personale, ma solo a quello che ne ha realmente bisogno per la sua attività. Ad esempio, un catalogatore

Vol. 29 N° 1 (2019) - ISSN 2281-0617

esterno normalmente dovrà essere abilitato solo alla procedura di catalogazione, e non alla gestione dei servizi che comporta l'accesso all'anagrafica degli utenti.

La protezione però non riguarda solo i dati informatizzati, ma anche quelli su carta, che devono anch'essi essere conservati in sicurezza.

Bisogna verificare attentamente se non sia in uso qualche pratica contraria alle disposizioni della normativa. In particolare, stupisce che ci siano ancora biblioteche che conservano nel libro la scheda col nome di tutti i lettori che l'hanno preso in prestito: questa pratica rende un dato personale visibile a chiunque, senza che ciò sia in alcun modo necessario per la gestione del prestito, ed è quindi assolutamente illecita, a maggior ragione perché è facilmente evitabile. Basta, ad esempio, sostituire il nome con un codice utente (a condizione, ovviamente, che l'archivio degli utenti sia adeguatamente custodito, in modo che solo gli operatori autorizzati possano associare il codice all'identità della persona).

Anche nei comportamenti quotidiani, inclusi i contatti informali con gli utenti, bisogna aver cura di non rivelare sbadatamente dati personali di qualcuno.

Consenso dell'interessato

Un ulteriore elemento fondamentale è il consenso dell'interessato. In linea generale, il consenso non è necessario per i trattamenti effettuati da enti pubblici a fini istituzionali (art. 6 comma 1 lettera e): *il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*). Anche se in Italia il D.Lgs 196/2003 richiede che il trattamento sia basato su norme di legge, non sembra che sia necessaria una legge che preveda espressamente ogni tipo di trattamento. Non è comunque vietato chiedere ugualmente il consenso esplicito, che è invece necessario per gli enti privati[4]. L'art. 6 prevede altri casi in cui il consenso non è necessario, ma raramente o mai essi potranno riguardare l'attività delle biblioteche[5].

Durata del trattamento e conservazione archivistica

Piuttosto complesso è il tema della durata del trattamento. Il trattamento infatti è lecito non per sempre, ma finché è necessario per le sue finalità. È evidente quindi che è lecito trattare i dati di un lettore che ha dei prestiti in corso, ma che dire dei dati di prestiti chiusi da anni, o di lettori che da anni non frequentano la biblioteca? In questo caso non c'è più la giustificazione originaria del trattamento, ma la loro pura e semplice cancellazione impedirebbe di utilizzarli per analisi statistiche e ricerche storiche, creando di conseguenza un danno. Anche il GDPR prevede che i dati possano essere conservati proprio in quanto documenti archivistici anche dopo che sia esaurita

[4] In realtà ci si potrebbe appellare anche alla lettera b) del comma 1 dell'art. 6: *il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso*, tuttavia per evitare dubbi e contestazioni probabilmente è in pratica più consigliabile richiedere il consenso.

[5] Il caso di cui alla lettera e): *il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato* è però rilevante per i record di autorità dei cataloghi.

Vol. 29 N° 1 (2019) - ISSN 2281-0617

la finalità del trattamento originario: la loro utilità per la ricerca determina una nuova finalità che ne rende ancora lecito il trattamento.

Sulle modalità di tale trattamento però non tutti concordano. Secondo alcuni essi possono essere considerati dati archivistici da conservare nella forma originale (per lo più separatamente dal sistema gestionale di origine, dove non sono più utili per l'attività ordinaria e sarebbero quindi esposti a rischi inutili) e da rendere consultabili secondo le norme generali sugli archivi e secondo le Regole deontologiche emanate dal Garante per la protezione dei dati personali[6]. Secondo altri è necessario, o quanto meno più opportuno, anonimizzare i dati, cioè eliminare i riferimenti a specifiche persone mantenendo tutte le altre informazioni. I dati anonimizzati rimangono utili per studi statistici: ad esempio, è possibile sapere se in un certo anno la biblioteca è stata frequentata più da medici o da agricoltori, oppure quali sono stati i libri più prestati, ma senza ricostruire le informazioni su specifiche persone.

Non è possibile qui arrivare ad una conclusione definitiva. Poiché le ricerche che richiedono i dati nella forma originaria sono piuttosto rare, l'anonimizzazione è sufficiente a soddisfare la maggior parte delle esigenze, anche se gli archivisti generalmente non vedono bene l'alterazione di documenti[7].

Informativa

Tutti gli elementi indicati sopra vengono inclusi nell'informativa sul trattamento che deve sempre essere resa agli interessati, anche quando non è necessario il consenso. I contenuti dell'informativa sono minuziosamente specificati dall'art. 13 del GDPR, quindi non li ripetiamo qui. Bisogna avere molta cura affinché l'informativa sia chiara, completa e veritiera. In rete sono facilmente reperibili numerose informative riferite proprio a biblioteche: ciò non significa che sia sufficiente sceglierne una qualunque e copiarla ciecamente. È invece indispensabile confrontare il testo da una parte con i propri trattamenti, e dall'altro con la norma, per verificare se sia adeguato[8].

Valutazione di impatto

Una previsione di un certo rilievo contenuta del GDPR è la Valutazione di impatto sulla protezione dei dati (art. 35), con la quale il titolare valuta quale sia l'impatto del trattamento sulla protezione dei dati: in pratica deve valutare quali siano i rischi connessi al trattamento in considerazione della natura dei dati e degli effetti del loro uso illecito, e delle caratteristiche del trattamento. La Valutazione di impatto non è sempre obbligatoria, tuttavia non sempre è chiaro (anche utilizzando le linee guida del Garante[9]) se uno specifico trattamento rientri o no nell'obbligo.

---

6 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069661

7 Come ovvio, l'anonimizzazione è in pratica realizzabile solo su dati informatizzati

8 Molto importante anche questa guida predisposta dal Garante: https://www.garanteprivacy.it/web/guest/regolamentoue/informativa.

9 https://www.garanteprivacy.it/web/guest/regolamentoue/dpia.

Vol. 29 N° 1 (2019) - ISSN 2281-0617

In linea di massima, è difficile affermare che rientrino nell'obbligo i trattamenti effettuati da piccole e medie biblioteche civiche, mentre nel caso di grandi biblioteche o sistemi bibliotecari e poli SBN sarà quanto meno più prudente effettuare la valutazione, che comunque può sempre essere effettuata anche quando palesemente non obbligatoria.

Servizi in cooperazione

I servizi realizzati tramite la collaborazione di numerosi soggetti, e quindi in particolare i poli SBN, pongono problemi particolari per l'individuazione del titolare e del responsabile, perché il GDPR non si adatta molto bene a queste situazioni.

Limitando il discorso ai poli SBN, essi possono avere organizzazione diversa: alcuni fanno interamente capo ad un solo soggetto, che sarà ovviamente il titolare, altri derivano dall'accordo di soggetti diversi sullo stesso piano, altri ancora – in particolare quelli regionali – sono istituiti e gestiti da un solo soggetto, ma molti altri sono quelli che vi partecipano. Senza analizzare in dettaglio tutta la casistica, spesso la soluzione migliore è prevedere che tutti i partecipanti siano contitolari, stipulando però un apposito accordo che delimiti ruoli e responsabilità di ciascuno. In assenza di tale accordo, tutti i contitolari sarebbero responsabili di tutto, mentre è evidente – ad esempio - che se in una biblioteca aderente ad un polo SBN regionale le password non vengono tenute in sicurezza non ne sono responsabili le altre biblioteche o la regione. La ditta incaricata della gestione informatica del polo, che ha accesso a tutti i dati, sarà normalmente responsabile del trattamento, in quanto incaricata dal titolare[10].

Conclusione

In conclusione, il GDPR nel suo insieme è certo una normativa molto complessa, ma nella maggior parte dei casi gli adempimenti necessari sono abbastanza semplici. La cosa fondamentale è che la protezione dei dati avvenga nella realtà, cioè che essi siano davvero mantenuti al sicuro da accessi e usi illeciti: solo a questa condizione hanno senso autorizzazione, informativa, accordi tra i titolari ecc. Se invece manca la sicurezza reale, tutta la modulistica e le scritture non alleggeriscono la responsabilità del titolare, anche se si tratta solo di negligenza e non di dolo[11].

[10] Altre soluzioni possibili, riferite ad un polo regionale, sono: regione titolare, tutti gli altri responsabili, o anche tutti contitolari tranne la regione che è responsabile (per il fatto che mantiene il polo come servizio alle biblioteche, e quindi in un certo senso su loro incarico)

[11] Le sanzioni previste dall'art. 83 possono essere pesantissime, anche più di 20 milioni di euro. È giusto preoccuparsene, ma è ovvio che il massimo della sanzione sarà riservato a violazioni dolose su vasta scala. Tuttavia anche superficialità e approssimazione ("tanto cosa vuoi che succeda" ecc. ecc.) sono sufficienti a incorrere in qualche sanzione