Regolamento Europeo in materia di trattamento dati personali

FormezPA

Questo materiale didattico è stato realizzato da Formez PA nell'ambito del Progetto OpenRAS, in convenzione con la Regione Sardegna.

Il Progetto OpenRAS è finanziato dal POR FSE 2014-2020 (Decisione C 2014 N 10096 del 17/12/2014), Asse 4 - Capacità istituzionale e amministrativa, a valere sull'azione 11.1.1 "Interventi mirati allo sviluppo delle competenze per assicurare qualità, accessibilità, fruibilità, rilascio, riutilizzabilità dei dati pubblici".

Autore: Gianfranco Andriola

Creatore: Formez PA

Data: Ottobre 2017

Regolamento Europeo in materia di trattamento dati personali

La gestione delle informazioni sui propri utenti è una parte centrale delle attività per qualunque organizzazione che eroga servizi. Da un lato conoscere i propri utenti attraverso le informazioni che li riguardano è una della condizioni indispensabili per offrire servizi che siano sempre più tarati sulle reali esigenze dei propri utenti, dall'altro però - proprio in virtù del valore che questi dati hanno - la loro conservazione e archiviazione pone una rilevante responsabilità da parte di chi li gestisce. Nel momento in cui gli utenti affidano le proprie informazioni a un soggetto terzo, che sia la propria banca, il proprio gestore di posta elettronica o la palestra che frequentano, per forza di cose si instaura un rapporto di fiducia tra la persona fisica cui si riferiscono quei dati e il soggetto responsabile della loro gestione.

La pubblica amministrazione per proprio mandato istituzionale raccoglie gestisce e in alcuni casi certifica le informazione dei cittadini, però - al contrario di quello che avviene con i servizi gestiti da privati - lo fa in un regime di monopolio. L'ufficio anagrafe del proprio Comune di residenza infatti è l'unico soggetto che può fornire ai propri utenti il Certificato di stato di famiglia o la Carta di Identità. Allo stesso modo la Polizia di stato è l'unico che può rilasciare il Passaporto o così come solo la Motorizzazione civile rilascia e rinnova la Patente di guida. Questa condizione del tutto peculiare degli enti pubblici rispetto alle organizzazioni private ha sempre posto la pubblica amministrazione in una condizione di forte rigore nella gestione dei dati personali dei cittadini. La sicurezza dei dati personali degli utenti e la riservatezza del loro trattamento deve quindi essere è una parte essenziale del lavoro della pubblica amministrazione, una condizione indispensabile per l'erogazione dei servizi sia allo sportello che online.

Se da un lato l'evoluzione delle nuove tecnologie ha portato enormi vantaggi in termini di economicità ed efficienza nella gestione dei dati personali degli utenti, dall'altro pone nuove sfide alla loro sicurezza e riservatezza. Grazie a internet, trasferire enormi quantità di dati diventa sempre più immediato, aumentando esponenzialmente i rischi di furto dei dati stessi, così' come la possibilità di integrare banche dati collocate in posti differenti attraverso internet espone i dati stessi a nuovi rischi di violazione. La stessa identità degli utenti passa sempre più di frequente attraverso la rete, basti pensare a quanto diffusi siano oggi i login ai siti attraversi i propri profili Facebook o Google o allo stesso SPID, il sistema pubblico d'identità digitale che consente di accedere attraverso un'unica procedura di autenticazione ai servizi online esposti da tutte le pubbliche amministrazioni italiane.

Il contesto normativo italiano

Il legislatore italiano ha reagito alla necessità di regolare la disciplina in materia di dati personali sin dal 1996, con l'approvazione della Legge 675/96 sulla Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Subito dopo l'approvazione della Legge 675/96 si sono succeduti una serie di provvedimenti legislativi minori, volti a regolare il tema del trattamento dei dati personali adattandolo di volta in volta al contesto storico in forte evoluzione a causa della repentina diffusione di internet e delle nuove tecnologie della comunicazione.

Anche a causa della forte frammentazione di norme relative alla tutela dei dati personali, nel 2003 si è sentita l'esigenza di raccogliere in un testo unico tutti i riferimenti normativi in materia, che ha portato all'emanazione del Codice in materia di protezione dei dati personali, attuale testo di riferimento per tutto quello che concerne la protezione dei dati personali. Oltre alla chiara valenza normativa, il Codice in materia di protezione dei dati personali, chiamato anche Codice della privacy, riveste un'importanza fondamentale nel definire il ruolo cardine del Garante per la protezione dei dati personali quale autorità amministrativa indipendente volta ad assicurare la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali dei cittadini italiani e, insieme, nel dare una definizione puntuale ed esaustiva di cosa siano i dati personali e di quali siano le figure coinvolte nel trattamento.

Regolamento europeo in materia di protezione dei dati personali

Buona parte della recenti sollecitazioni sul tema della privacy derivano dalla estrema facilità con cui è possibile oggi raccogliere, archiviare e conservare i dati personali degli gli utenti. Il modo in cui internet è diventato perno su cui ruota la quotidianità della vita di ogni giorno ha per forza di cosa cambiato il modo in cui le informazioni riguardanti ogni aspetto della vita degli utenti vengono conservate in maniera costante e pervasiva. Il tracciamento dei dati personali degli utenti da parte dei gestori dei servizi online avviene in maniera così naturale e costante che nella maggior parte dei casi gli interessanti quasi non ci fanno più caso. Certamente questo aspetto solleva innanzitutto una questione culturale, volta a sensibilizzare tutti gli utenti dei servizi online sui nuovi rischi per la privacy e su un utilizzo consapevole dei nuovi mezzi di comunicazione e - successivamente - pone la necessità di un intervento regolatorio da parte dei Governi, volto a riconoscere l'immenso valore che questa particolare tipologia di informazioni costituisce tutelando sia per gli utenti proprietari dei dati che le aziende che proprio su questi stessi dati producono servizi e fanno innovazione. Si rende necessario quindi un cambiamento di natura soprattutto culturale rispetto al modo in cui pensiamo ai dati personali degli individui. Tutelare e difendere i dati personali, significa innanzitutto difendere le persone,

l'unicità della loro l'identità e la libertà delle stesse.

Queste in parte le premesse con cui l'Unione europea ha dato inizio all'iter legislativo che nel 2016 ha portato all'approvazione del Regolamento Europeo in materia di protezione dei dati personali (Regolamento UE 2016/679), pubblicato sulla Gazzetta Ufficiale Europea del 4 maggio 2016. Con il Regolamento UE cambia in maniera sostanziale il rapporto tra utenti e gestori dei dati personali, siano essi imprese private che pubbliche amministrazioni.

Per queste ultime in particolare, il Regolamento UE introduce il principio di "responsabilizzazione" (accountability) della Pubblica amministrazione, attribuendo direttamente ai titolari del trattamento il compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicabili al trattamento dei dati personali, adottando approcci e politiche che tengano conto costantemente del rischio che un qualunque trattamento di dati personali intrapreso da un ente pubblico può comportare per i diritti e le libertà degli interessati.

Il regolamento è entrato in vigore il 24 maggio 2016 e trova applicazione in tutti gli Stati appartenenti all'Unione europea a partire dal 25 maggio 2018.

Nuove definizioni per nuove esigenze normative

Tra le principali innovazioni portate dal Regolamento UE la prima è certamente rappresentata dalla ridefinizione dei termini utili a descrivere tutte le figure interessate dal trattamento dei dati personali, le azioni da essi compiute e le condizioni in cui possono trovarsi. Di seguito le più rilevanti:

- **dato personale**: 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
- **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;

- **limitazione di trattamento**: il contrassegno dei dati personali conservati con l'obiettivo di limitare il trattamento in futuro
- **profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizi 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;
- **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;
- **destinatario**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- **terzo**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- **consenso dell'interessato**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **violazione dei dati personali**: la violazione di sicurezza che comporta 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;

Le esigenze a cui il Regolamento risponde

Il Regolamento europeo in materia di protezione dei dati personali nasce come risposta puntuale del legislatore europeo a una serie di criticità riguardanti la privacy degli utenti relativamente ai seguenti aspetti:

- **Armonizzare le norme per tutti gli Stati dell'Unione europea**. Il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri dell'Unione europea e non richiede una legge di recepimento nazionale. Inoltre, si applica integralmente alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione europea. Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le regole fissate nell'Ue. Fra le principali novità del Regolamento c'è il cosiddetto «sportello unico» (one stop shop), che semplificherà la gestione dei trattamenti e garantirà un approccio uniforme.
- **Semplificare le Informazioni sul trattamento dei dati personali**. L'informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti. Per facilitare la comprensione dei contenuti, nell'informativa si potrà fare ricorso anche a icone, identiche in tutta l'Unione europea. Gli interessati dovranno sapere se i loro dati sono trasmessi al di fuori dell'Ue e con quali garanzie
- **Garantire il diritto all'oblio**. Grazie all'introduzione del cosiddetto «diritto all'oblio», gli interessati potranno ottenere la cancellazione dei propri dati personali anche online da parte del titolare del trattamento qualora ricorrano alcune condizioni previste dal Regolamento: se i dati sono trattati solo sulla base del consenso; se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti; se i dati sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento. A questo diritto si accompagna l'obbligo per il titolare del trattamento che ha pubblicato i dati di comunicare la richiesta di cancellazione a chiunque li stia trattando, nei limiti di quanto tecnicamente possibile.
- **Portabilità dei dati**. Liberi di trasferire propri dati in un mercato digitale più aperto alla concorrenza Il Regolamento introduce il diritto alla «portabilità» dei propri dati personali per trasferirli da un titolare del trattamento ad un altro. Ad esempio, si potrà cambiare il provider di posta elettronica senza perdere i contatti e i messaggi salvati. Ci saranno però alcune eccezioni che non consentono l'esercizio del diritto: in particolare, quando

si tratta di dati contenuti in archivi di interesse pubblico, come ad esempio le anagrafi.

I principi che stanno alla base del Regolamento UE si traducono, sia per le imprese che per le pubbliche amministrazioni, in indicazioni fortemente operative, volte ad assicurare la massima tutela nel trattamento dei dati personali dei cittadini.

Cosa devono fare le PA per adeguarsi al Regolamento UE

Subito dopo l'approvazione del Regolamento UE, il Garante per la protezione dei dati personali italiano ha reso disponibili alcuni suggerimenti rivolti alle amministrazioni pubbliche di avviare, con assoluta priorità per arrivare preparati al 25 maggio 2018, data in cui il Regolamento UE avrà piena operatività:

1. la designazione del Responsabile della protezione dei dati – RPD (artt. 37-39). Questa nuova figura, che il regolamento richiede sia individuata in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati, costituisce il fulcro del processo di attuazione del principio di "responsabilizzazione". Il diretto coinvolgimento del RPD in tutte le questioni che riguardano la protezione dei dati personali, sin dalla fase transitoria, è sicuramente garanzia di qualità del risultato del processo di adeguamento in atto. In questo ambito, sono da tenere in attenta considerazione i requisiti normativi relativamente a: posizione (riferisce direttamente al vertice), indipendenza (non riceve istruzioni per quanto riguarda l'esecuzione dei compiti) e autonomia (attribuzione di risorse umane e finanziarie adeguate);

2. l'istituzione del Registro delle attività di trattamento (art. 30 e cons. 171). Essenziale avviare quanto prima la ricognizione dei trattamenti svolti e delle loro principali caratteristiche (finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione, misure di sicurezza, tempi di conservazione, e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte) funzionale all'istituzione del registro. La ricognizione sarà l'occasione per verificare anche il rispetto dei principi fondamentali (art. 5), la liceità del trattamento (verifica dell'idoneità della base giuridica, artt. 6, 9 e 10) nonché l'opportunità dell'introduzione di misure a protezione dei dati fin dalla progettazione e per impostazione (privacy by design e by default, art. 25), in modo da assicurare, entro il 25 maggio 2018, la piena conformità dei trattamenti in corso (cons. 171);

3. la notifica delle violazioni dei dati personali (cd. data breach, art. 33 e 34). Fondamentale

appare anche, nell'attuale contesto caratterizzato da una crescente minaccia alla sicurezza dei sistemi informativi, la pronta attuazione delle nuove misure relative alle violazioni dei dati personali, tenendo in particolare considerazione i criteri di attenuazione del rischio indicati dalla disciplina e individuando quanto prima idonee procedure organizzative per dare attuazione alle nuove disposizioni.

4. Informazioni sul trattamento da fornire agli utenti (art. 13). Prima di raccogliere i dati degli utenti un ente pubblico deve fornire, pubblicando sul proprio sito web, le seguenti informazioni:

- l'identità e i dati di contatto del titolare del trattamento;
- i dati di contatto del responsabile della protezione dei dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

Una volta che i dati personali sono stati acquisiti, alle informazioni precedenti vanno aggiunte le seguenti, necessarie per garantire un trattamento corretto e trasparente:

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- il diritto di proporre reclamo all'autorità di controllo;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Nello sviluppo di tutti e quattro i passaggi appena esposti è opportuno che le Pubbliche amministrazioni impegnate ad implementare le attività di adeguamento al Regolamento europeo in materia di protezione dei dati personali tengano presente che principio chiave alla base è il cosiddetto privacy by design, ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, adottando da subito comportamenti che consentano di prevenire possibili problematiche.

Il Regolamento UE ha introdotto inoltre l'obbligo per il titolare del trattamento di effettuare valutazioni di impatto (privacy impact assessment) prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone.

È bene ricordare ancora che, qualora si dovessero verificare dei casi di violazioni dati personali dei cittadini, il Regolamento UE sancisce il diritto dei cittadini stessi di essere avvertiti (data breach notification) dalle pubbliche amministrazioni e dalle imprese entro le 72 ore successive all'accaduto.

In fine è opportuno che le pubbliche amministrazioni abbiano chiaro sin da subito che, oltre a prevedere un rafforzamento dei poteri delle Autorità Garanti nazionali, il Regolamento UE porta un forte inasprimento delle sanzioni amministrative. Nel caso di violazioni dei principi e disposizioni previste dal Regolamento, le sanzioni possono arrivare fino a 10 milioni di euro.