6 Area Formazione

Nicola Galotta

Privacy: Situazione normativa, sanzioni e Vademecum all'applicazione del GDPR

In occasione della giornata conclusiva del Campus estivo di formazione, nella sala dei Baroni del Maschio Angioino di Napoli si è svolto il mio intervento che ha inteso offrire una panoramica delle principali novità riguardanti la privacy, ai sensi del Regolamento Europeo 679/2016, suggerendo possibili approcci operativi e gestionali in merito agli adempimenti da adottare per la piena applicazione del Regolamento.

Di seguito si riportano ulteriori approfondimenti sull'argomento trattato.

Legislazione attuale

L'Unione Europea (UE), a seguito di alcuni spiacevoli accadimenti relativi al furto ed alterazione di dati personali aventi lo scopo di influenzare le elezioni nazionali di alcuni Stati, l'opinione pubblica e polarizzare le scelte dei cittadini, ha deciso di regolare la materia attraverso il Regolamento Europeo 2016/679, a cui oggi facciamo riferimento indicandolo sinteticamente con il nome di "Regolamento Privacy" ovvero "GDPR". Il Regolamento ha l'obiettivo di proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il Regolamento abroga e sostituisce la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) – inizialmente recepita dal legislatore italiano con la legge 675/96, successivamente sostituita dal D.lgs. 196/03, l'attuale "Codice Privacy". Inoltre, rende uniforme ed armonizza a livello europeo la legislazione in materia di protezione dei dati personali.

Il nuovo Regolamento è a carattere più generale, e non entra nel merito di alcuni aspetti regolamentati, o che dovranno essere regolamentati, dalla legislazione locale. Ha lasciato

agli Stati membri ed alle Autorità competenti in materia un margine operativo per mantenere o adottare, in conformità al Regolamento, norme specifiche di settore.
Essendo un Regolamento europeo, è di immediato recepimento ed attuazione da parte di tutti i Paesi membri della Comunità Europea, quindi è in essere già dal maggio 2016. Tuttavia, i Titolari del trattamento hanno avuto due anni dalla pubblicazione del testo definitivo per mettersi in regola con gli adempimenti da esso previsti.
Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR), è stato da poco aggiornato con alcune rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea n. 127 del 23 maggio 2018. Si tratta essenzialmente di correzioni e rettifiche che non introducono alcuna novità significativa e quindi non alterano il quadro d'insieme attualmente conosciuto.

La privacy in Italia è stata da tempo regolata attraverso le disposizioni del Decreto Legislativo 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali") a cui oggi si fa riferimento indicandolo sinteticamente "Codice Privacy". La legge italiana, così come concepita nel 2003, è stata di fatto precorritrice del GDPR, anticipando moltissimi dei tratti fondamentali del Regolamento. La differenza fondamentale tra il Codice Privacy del 2003 ed il Regolamento del 2016 è essenzialmente legata alla visione sovranazionale del trattamento, al trasferimento dei dati ed alla presenza di una nuova figura professionale (DPO – Data Protection Owner), in alcuni casi obbligatoria mentre in altri facoltativa. Il DPO ha il compito di garantire l'applicazione del Regolamento da parte di ogni Titolare del trattamento, un vero e proprio organismo di vigilanza per la Privacy. Anche l'idea della valutazione del rischio per la perdita di privacy dei dati personali durante le varie fasi del trattamento (DPIA) era già presente nella versione iniziale del Codice della Privacy italiano ed in particolare si fa riferimento al documento programmatico della privacy (DPS). Nel tempo, dal 2003 ad oggi, il D.lgs. 196/2003 è stato profondamente rivisto e modificato. L'ultima modifica è avvenuta attraverso il D.lgs. del 10 agosto 2018, n. 101, attraverso la quale il legislatore italiano ha

inteso integrare ed armonizzare i dettami del Codice Privacy con il Regolamento Europeo.

Essenzialmente oggi in Italia la Privacy è regolata contemporaneamente dal Regolamento Europeo 2016/679 (Regolamento) e dalle disposizioni del Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. (Codice). Conseguentemente, la rivisitazione o la produzione di nuova documentazione e di procedure inerenti la Privacy dovrà essere fatta in forza di entrambe le leggi. I testi aggiornati e coordinati del Regolamento e del Codice sono disponibili sul sito del Garante per la protezione dei dati (www.garanteprivacy.it).

Il Regolamento ed il Codice privacy hanno come oggetto i soli dati personali di persone fisiche. In particolare si applicano al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi. Il Regolamento ed il Codice non si applicano ai trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.
Inoltre i principi di protezione dei dati non si applicano a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato e non si applica ai dati personali delle persone decedute.

Si ricorda che un dato personale è qualsiasi informazione riguardante una persona fisica («interessato») identificata o identificabile, direttamente o indirettamente.

Sanzioni

Le sanzioni amministrative pecuniarie previste dal GDPR (art. 83), sono inflitte in funzione delle circostanze di ogni singolo caso. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa, in ogni singolo caso, si tiene debito conto dei seguenti elementi:

- la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- il carattere doloso o colposo della violazione;
- le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto;
- eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- le categorie di dati personali interessate dalla violazione;

- la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- qualora siano stati precedentemente disposti provvedimenti nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- l'adesione ai codici di condotta approvati o ai meccanismi di certificazione approvati.

La violazione delle disposizioni relative agli obblighi del titolare del trattamento e del responsabile del trattamento, agli obblighi dell'organismo di certificazione e agli obblighi dell'organismo di controllo, sono soggetti a sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Sempre in riferimento al GDPR (art. 83), la violazione delle disposizioni relative ai principi di base del trattamento (comprese le condizioni relative al consenso, i diritti degli interessati, i trasferimenti di dati personali a un destinatario in un Paese terzo o un'organizzazione internazionale, l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo o il negato accesso, sono soggetti a sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

DATO PERSONALE

È qualsiasi informazione (ad esempio nome, codice fiscale, immagine, voce, impronta digitale, traffico telefonico) che riguardi persone fisiche identificate o identificabili tramite ulteriori dati quali un numero o un codice identificativo. La persona a cui si riferiscono i dati soggetti al trattamento si definisce ***"interessato"****. A titolo indicativo e non esaustivo, le Istituzioni AGIDAE sono titolari (ovvero determinano le finalità e/o i mezzi del trattamento) di dati personali:*

- ✓ *degli studenti;*
- ✓ *dei pazienti assistiti;*
- ✓ *degli ospiti delle strutture ricettive;*
- ✓ *dei dipendenti subordinati;*
- ✓ *dei propri fornitori.*

Mentre le sanzioni penali previste dal Codice della Privacy, D.lgs. 30 giugno 2003 n. 196 coordinato con il D.lgs. 10 agosto 2018 n. 101, sono:

- il **Trattamento illecito di dati personali** (Art. 167 c 1) è punito con la *reclusione da sei mesi a un anno e sei mesi*;
- il **Trattamento illecito di particolari categorie di dati personali** (Art. 167 c 2) è punito con la *reclusione da uno a tre anni*;

- **comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala** (Art. 167- bis) è punito con la *reclusione da uno a sei anni*;
- **acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala** (Art. 167- ter) è punito con la *reclusione da uno a quattro anni*;
- **falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante** (Art. 168) è punito con la *reclusione da sei mesi a tre anni*.

Vademecum all'applicazione del GDPR

A fronte del Regolamento sulla Privacy quale è l'elenco operativo (checklist) di cose da fare per adeguarsi, avendo come prerequisito di base la precedente applicazione del Codice della Privacy italiano?

La risposta a questa domanda è nei passaggi logici e gli adempimenti da espletare elencati di seguito:

1 **Individuare i dati trattati, i soggetti interessati e la base giuridica.**
La prima attività da svolgere è la compilazione del Registro dei Trattamenti (GDPR, art. 30). Si tratta di una mappatura che consente di avere contezza dei soggetti interessati, delle tipologie di dati trattati e della loro provenienza.
L'obbligo del registro (art. 30) non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati o i dati personali relativi a condanne penali e a reati.
Nonostante che in alcuni casi non ci sia l'obbligo del registro dei trattamenti, il Garante raccomanda comunque la tenuta del registro dei trattamenti chiarendo che non costituisce un adempimento formale bensì è parte integrante di un sistema per una corretta gestione dei dati personali. Per tale motivo, invita tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche, ove già non condotta.

2 **Verificare l'esistenza/necessità di eventuali trasferimenti di dati verso Paesi terzi o verso organismi internazionali.**
Il trasferimento, verso Paesi terzi, dei dati trattati richiede un'attenta valutazione dei rischi e la predisposizione di accorgimenti tecnici ed organizzativi idonei a mitigarne eventuali impatti (GDPR, art. 44 e 45).

3 **Verificare le possibili fonti di rischio derivanti dalla presenza/uso di sistemi tecnologici.**
Quasi tutti gli strumenti tecnologici sono oggi collegati o collegabili in rete.
Questo rappresenta un potenziale pericolo che deve essere adeguatamente gestito.

4 **Valutare i rischi di violazione privacy.**

Una volta in possesso della mappa dei trattamenti, sarà più facile valutare i possibili rischi di violazione, tenendo anche conto delle misure di mitigazione già messe in atto e delle eventuali misure da implementare (GDPR, art. 32).
Come ausilio alla valutazione dei rischi è possibile seguire le indicazioni del Garante sulla valutazione del rischio
(https://www.garanteprivacy.it/web/guest/regolamentoue/dpia/gestione-del-rischio).

5 **Verificare la necessità della redazione della DPIA (Data Protection Impact Assessment).**
In base a quanto disposto dall'art. 35 del Regolamento, il documento riportante la DPIA si rende necessario in presenza di rischi elevati nel trattamento e per la presenza di particolari tipi di dati. La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi di:
a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati;
c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
Il Garante Francese distribuisce gratuitamente un software di supporto alla redazione della DPIA (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil).

6 **Nomina del DPO (Data Protection Officer).**
La nomina del DPO/RPD (art. 37), è obbligatoria per gli enti e organismi pubblici e per quelle organizzazioni che trattano particolari categorie di dati (come i dati sanitari) in larga scala.
Può essere nominato sia un soggetto esterno che interno all'organizzazione, senza però trovarsi in situazioni che presentino conflitti di interesse.

DPO (Data Protection Officer) o RPD

Il Responsabile della protezione dei dati personali (DPO o RDP) è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679. Il DPO ha il compito di informare e consigliare il Titolare o il Responsabile del trattamento, nonché i dipendenti, sugli obblighi previsti dalle norme in materia e verificarne l'attuazione e l'applicazione. Quindi, raccoglie informazioni sui trattamenti svolti e ne verifica la conformità alle norme. Il ruolo di DPO può essere affidato ad **uno dei dipendenti dell'azienda**, ma anche **esternalizzato ad un fornitore di servizi** (libero professionista o azienda) tramite apposito contratto. Può essere una persona fisica o un'organizzazione e può essere nominato per un gruppo di imprese al fine di ridurre i costi.

7 **Verificare l'adeguatezza dei documenti di Informativa Privacy esistenti.**
Gli artt. 13 e 14 del GDPR danno le indicazioni relative al contenuto e modalità con cui formulare l'informativa. I vecchi modelli dovranno essere adeguati al nuovo disposto.

8 Verificare/Predisporre il modello per la raccolta del consenso al trattamento dei dati da parte dei soggetti interessati.

Pur non essendo richiesta la forma scritta, bisogna poter dimostrare che il consenso è avvenuto in maniera libera, inequivocabile ed informata. L'art. 7 del GDPR, in maniera specifica, ne disciplina le caratteristiche ed i casi in cui è reso obbligatorio.

9 Predisporre le modalità di gestione del diritto di trasparenza verso i soggetti interessati.

Predisporre procedure atte a rispondere prontamente ai diritti dell'interessato [diritto all'accesso, alla rettifica (GDPR, art. 16), all'opposizione ed alla limitazione, diritto all'oblio (GDPR, art. 17) ed alla portabilità (GDPR, art. 20) dei dati].

10 La Privacy by Design e la Privacy by Default.

Si tratta di due principi cardine (GDPR, art. 25) che devono essere tenuti in considerazione sin dalla progettazione, formulazione ed organizzazione di un servizio.

11 Predisporre le procedure di comportamento per il trattamento delle informazioni.

Creare procedure che regolino particolari attività:

- l'utilizzo di internet, della posta elettronica e dei dispositivi informatici (tablet, smartphone, pendrive),
- modalità di archiviazione dei dati e loro cifratura,
- regole e limitazioni per l'accesso ai dati (chi può fare cosa).

12 Predisporre un modello di contratto/incarico per ogni figura/ruolo convolti nel trattamento.

Oltre al titolare ci sono, o ci potrebbero essere, altre figure coinvolte nella gestione dei dati: Contitolari, Responsabili esterni od interni, Addetti al trattamento.

È necessario predisporre, per ciascun soggetto, un incarico scritto che ne chiarisca competenze e responsabilità.

13 Predisporre i piani di formazione sul sistema privacy.

Il GDPR pone la formazione su un piano di assoluto rilievo (art. 39). È obbligo del titolare rendere edotti i responsabili e gli addetti delle procedure e dei rischi collegati al trattamento dei dati. Predisporre delle schede su cui registrare la formazione sostenuta da ciascun soggetto.

14 Predisporre la procedura di comportamento in caso di violazione (data breach) degli archivi.

Gli adempimenti, in caso di data breach, sono disciplinati dagli artt. 33 e 34 del GDPR.

Predisporre la procedura, in caso di violazione, che contenga:

- modello di comunicazione da inviare all'Autorità garante entro le 72 ore dall'intrusione;
- modello di comunicazione da inviare agli interessati;
- registro delle violazioni, su cui riportare le azioni intraprese o le eventuali cause di esonero;
- procedure e controlli di "Business Continuity".

15 Periodicamente …. Verificare!

Predisporre una procedura che preveda la verifica periodica della corretta attuazione di quelle che sono le disposizioni previste dal Regolamento e la rispondenza delle valutazioni contenute nel Modello Organizzativo Privacy rispetto alle esigenze dell'organizzazione.

Questo elenco rappresenta soltanto un indice delle principali ed immediate azioni da compiere. Ha il semplice obiettivo di fare da bussola operativa rispetto al Regolamento della Privacy. Molti di questi punti hanno un'applicazione articolata e complessa che merita ulteriori approfondimenti, alcuni dei quali specifici per attività e per i singoli soggetti giuridici che dovranno applicarli.

Per agevolare gli Enti nell'applicazione del GDPR, Agidae Opera mette a disposizione un servizio di consulenza che ha l'obiettivo di formare e accompagnare gli Istituti nella revisione e nella predisposizione di quanto previsto dal GDPR e dal Codice della Privacy.

Sala dei Baroni - Maschio Angioino - Napoli