IL QUADRO DELLA TUTELA DEI DATI PERSONALI NELLA DISCIPLINA DEL GDPR

Avv. Francesco Anastasi

SOMMARIO: ***1****. Premessa;* ***2****. Codici di condotta;* ***3.*** *Certificazioni;* ***4.*** *Data Breach;* ***5.*** *Diritto alla portabilità dei dati;* ***6.*** *Responsabile del trattamento;* ***7****. Responsabilità e quadro sanzionatorio.*

1. Premessa

Con il regolamento Europeo in materia di protezione dei dati personali (regolamento 2016/679 detto anche GDPR secondo l'acronimo anglosassone), approvato in data 14 aprile 2016 dal Parlamento Europeo e pubblicato sulla Gazzetta Ufficiale Europea del 4 maggio 2016 inizia una nuova stagione per i diritti dei cittadini europei nei rapporti con le pubbliche amministrazioni e le imprese.

Con il regolamento Europeo in materia di protezione dei dati personali (regolamento 2016/679), approvato in data 14 aprile 2016 dal Parlamento Europeo e pubblicato sulla

AmbienteDiritto.it - Rivista Giuridica Telematica - ISSN 1974-9562 - (BarCode 9 771974 956204)

Gazzetta Ufficiale Europea del 4 maggio 2016 inizia una nuova stagione per i diritti dei cittadini europei nei rapporti con le pubbliche amministrazioni e le imprese.

Il regolamento costituisce un prezioso tentativo di armonizzazione delle regole privacy dei vari Stati ed è finalizzato a sviluppare il mercato unico digitale attraverso la creazione e la promozione di nuovi servizi, applicazioni, piattaforme e software[1].

Il regolamento costituisce con la direttiva Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati il c.d. "*pacchetto protezione dati personali*".

Il testo del regolamento abroga la direttiva la Direttiva 95/46/CE in materia di protezione dei dati personali - privacy, concepita in un periodo nel quale solo una minima parte della popolazione europea (nella percentuale del 1%) utilizzava internet e non esistevano social media, tablet, app e gli scenari e gli effetti della moderna e l'attuale società della sorveglianza elettronica nella quale sono gli stessi cittadini che pubblicano, più o meno inconsapevolmente i propri dati personali sulle piattaforme on line e social media.

Tra le principali novità introdotte dal regolamento va segnalato il principio di "responsabilizzazione" (cd. *accountability*), che attribuisce 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 (art. 5).

In quest'ottica, la nuova disciplina impone alle amministrazioni un diverso approccio nel trattamento dei dati personali, prevede nuovi adempimenti e richiede un'intensa attività di adeguamento, preliminare alla sua definitiva applicazione a partire dal 25 maggio 2018.

Al fine di fornire un primo orientamento il Garante per la protezione dei dati personali suggerisce alle Amministrazioni pubbliche di avviare, con assoluta priorità.

[1] Franco Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018 pp. 5 e ss.

2. Codici di condotta

Sicuro elemento di grade interesse e novità apportato dal regolamento 27 aprile 2016, n. 2016/679, è l'elaborazione di **codici di condotta**. Quest'ultimi dovrebbero essere redatti dalle associazioni e dalle organizzazioni che rappresentano categorie di titolari del trattamento o di responsabili del trattamento e dovrebbero tenere conto delle caratteristiche specifiche dei settori di riferimento e delle diverse esigenze connesse alle dimensioni aziendali.

In particolare, secondo l'art. 40 del regolamento, i codici di condotta dovrebbero concernere:

- Il trattamento corretto e trasparente dei dati;
- I legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
- La raccolta dei dati personali;
- La pseudonimizzazione;
- L'informazione fornita al pubblico e agli interessati;
- L'esercizio dei diritti degli interessati;
- La protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
- Le misure di sicurezza;
- La notifica dei *data breach* e la relativa comunicazione agli interessati;
- Il trasferimento di dati personali verso paesi terzi;
- Le procedure stragiudiziali di composizione delle controversie.

Il progetto di codice deve essere sottoposto all'Autorità garante nazionale e questa esprimerà un parere sul progetto. Se il parere è positivo e l'applicazione del codice riguarda solamente lo Stato membro in cui è presentato, l'Autorità registrerà e pubblicherà il codice realizzato.

4. Certificazioni

Accanto ai codici tra le principali novità si collocano le cd **certificazioni**. L'art. 42 del Regolamento UE 2016/679 le riconosce come uno strumento volontario, che si affianca a tutti quelli obbligatori e a quelli consigliati indicati nel regolamento. L'applicazione

AmbienteDiritto.it - Rivista Giuridica Telematica - ISSN 1974-9562 - (BarCode 9 771974 956204)

di un codice di condotta approvato o di un meccanismo di certificazione approvato può essere utilizzata come uno degli elementi in grado di dimostrare la conformità e il rispetto degli obblighi da parte del titolare del trattamento.

La certificazione ai sensi del GDPR non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti. In particolare, nel caso in cui debba essere erogata una sanzione amministrativa pecuniaria e fissare l'ammontare della stessa sono previsti degli sconti sanzionatori in relazione all'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42.

5. Data Breach

Altro profilo di rilevo introdotto dal regolamento europeo è rappresentato dall'obbligo di comunicazione delle violazioni di dati personali - il cd. ***Data Breach*** - (non previsto nella precedente direttiva 95/46/CE) a tutti i trattamenti di dati personali effettuati dalle pubbliche amministrazioni e imprese.

La "violazione dei dati personali" è da intendersi, secondo quanto disciplinato dal regolamento europeo, come "*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*".

Il regolamento riconosce, in particolare, due ipotesi di data breach: la comunicazione delle violazioni di dati all'autorità nazionale di protezione dei dati personali (*ex* art.33) e la comunicazione ai soggetti a cui si riferiscono i dati, nei casi più gravi (c.d. soggetti "interessati), di cui all'art. 34.

Il regolamento europeo individua il soggetto tenuto a notificare, le tempistiche, le modalità ed il contenuto della notificazione della violazione dei dati personali, nonché le eventuali responsabilità e sanzioni nel caso di violazione degli obblighi previsti.

La previsione di obbligo di data breach comporta che le pubbliche amministrazioni e le imprese sono tenute ad accertare e controllare affinché siano state messe in atto adeguate misure tecnologiche e organizzative di protezione.

AmbienteDiritto.it - Rivista Giuridica Telematica - ISSN 1974-9562 - (BarCode 9 771974 956204)

6. Diritto alla portabilità dei dati

Altra importante novità apportata dal GDPR, è il riconoscimento del cosiddetto **diritto alla portabilità dei dati**[2]. Si tratta di un diritto innovativo, previsto dall'articolo 20 del GDPR, che consente all'interessato di ricevere i dati personali forniti a un titolare, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli ad altro titolare del trattamento senza impedimenti. L'obiettivo di tale diritto è quello di accrescere il controllo degli interessati sui propri dati personali, facilitandone la circolazione, la copia o la trasmissione da un ambiente informatico all'altro.

Per l'interessato, **la portabilità dei propri dati** implicherà non solo di ricevere un sottoinsieme dei dati personali che lo riguardano e di conservarli in vista di un utilizzo ulteriore per scopi personali, ma anche di ottenere la trasmissione degli stessi da un titolare ad un altro, «senza impedimenti» da parte del primo. Ciò, infatti, è volto principalmente ad evitare fenomeni di dipendenza forzata dell'interessato da un determinato fornitore di servizi (il cosiddetto *lock-in*).

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[3] delle attività di trattamento (art. 30 e cons. 171).

Le amministrazioni pertanto sono tenute nel rispetto del GDPR a effettuare 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.

[2] Cfr. Franco Pizzetti (a cura di), Intelligenza artificiale, protezione dei dati personali e regolazione, Giappichelli, 2018 p. 25 e ss..
[3] Ivi p. 83 e ss.

AmbienteDiritto.it - Rivista Giuridica Telematica - ISSN 1974-9562 - (BarCode 9 771974 956204)

La ricognizione è pertanto necessaria 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).

7. Responsabile del trattamento

Una importante figura introdotta dal GDPR è il **responsabile del trattamento**[4]. Questa figura consiste in una persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento.
In base all'art. 28 del nuovo regolamento generale europeo, la **nomina deve avvenire tramite contratto o altro "*atto giuridico* a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento**".

Questa figura deve essere individuata in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati: il DPO costituisce il cardine del processo di attuazione del principio di "*responsabilizzazione*".

Sotto il profilo delle responsabilità da illecito amministrativo, il DPO non ha responsabilità dirette, tuttavia, permangono certamente responsabilità in via di rivalsa sul piano risarcitorio a favore del titolare e del responsabile che abbia subito un danno derivante da colpa grave o inadempienze gravi riferibili ai compiti previsti per il DPO.

Inoltre, il DPO come noto dovrà effettuare una supervisione complessa in ordine alla conformità al regolamento e dovrà anche garantire l'esercizio dei diritti dell'interessato con tempi prestabiliti.

Quest'ultimo è tenuto inoltre a collaborare e fungere da contatto con l'Autorità garante mostrando il lavoro svolto in termini di documentazione (c.d. principio di

[4] Cfr. WP, Guidelines on Data Protection Officers (DPOs).

accountability o di responsabilizzazione) delle misure di sicurezza adeguate alle esigenze dell'organizzazione di riferimento.

Di recente il Gruppo Articolo 29 si è interrogato sulla necessità di garantire l'assenza di conflitto di interessi riconducile al DPO. In particolare si è ritenuto che possa sussistere conflitto di interesse del DPO con i seguenti ruoli: l'amministratore delegato, il responsabile del personale, il responsabile del sistema informativo, il direttore sanitario, il direttore marketing.

8. Responsabilità e quadro sanzionatorio

Il GDPR, da ultimo, tratteggia anche un importante quadro di responsabilità e un quadro sanzionatorio che entrerà in vigore dopo il 25 maggio 2018.

Come noto già il Codice della Privacy conteneva alcune sanzioni amministrative. In particolare l'art. 161 del Codice della Privacy prevedeva una **sanzione pecuniaria da tremila a diciottomila euro**, **nel caso che l'omessa o inidonea informativa** si riferisca a dati personali identificativi, ma in alcuni casi è previsto anche un aggravio della pena da cinquemila a trentamila euro.

L'apparato sanzionatorio del GDPR solitamente colpisce per le rilevanti cifre previste **dall'articolo 83, che arrivano a colpire Titolari e Responsabili con sanzioni amministrative fino a 20 milioni di euro o fino al 4 % del fatturato mondiale totale annuo**[5].

In realtà, il quadro sanzionatorio previsto dal regolamento europeo, come previsto dall'art. 84 del regolamento europeo, demanda la materia penale alla competenza di ciascuno Stato Membro, e solo le sanzioni amministrative pecuniarie sono armonizzate nel rispetto di criteri di effettività, proporzionalità e dissuasività.

In particolare, l'art. 83 specifica che le sanzioni devono essere applicate in funzione del singolo caso e tenendo conto della natura, della gravità e della durata della violazione, delle finalità del trattamento, del numero di interessati lesi e del livello del danno, oltre ad altri elementi come il carattere doloso o colposo della violazione, le misure adottate.

In termini molto generali, sebbene le sanzioni previste nel regolamento siano di importi molti elevati fino al 20 milioni di euro o il 4% del fattura mondiale annuale, il principio generale è che una violazione del regolamento potrebbe comportare una imposizione

[5] Cfr. Giusella Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, 2017, p. 595 e ss.

di sanzioni equivalente in tutti gli Stati membri. A tale scopo le recenti linee guida pubblicate il 3 ottobre dal Gruppo articolo 29 analizzano i vari parametri in base ai quali determinare l'ammontare della sanzione che, in casi irrisori e che non hanno rischi significativi per gli interessati, potrà anche corrispondere una mera diffida amministrativa. Tuttavia, tenendo conto delle circostanze specifiche, una violazione dei dati potrebbe anche comportare una sanzione pecuniaria superiore ai 10 mln di euro se dovessero ricorrere delle circostanze di maggiore gravità ed inosservanza delle prescrizioni dell'Autorità di controllo.

È chiaro che la speculazione circa la futura applicazione del GDPR è ancora allo stato embrionale, e solo la concreta attuazione potrà farci comprendere e valutare quali sono le direttrici che le Autorità nazionali ed europee tenderanno a seguire.

Bibliografia

Franco Pizzetti, *Data protection, ecco cosa cambia con le linee guida sulla DPIA*, 27 Ott 2017, agendadigitale.eu

Manuela Bianchi, *GDPR: cosa cambia con il nuovo regolamento privacy europeo?*, cyberlaws.it, 25 gennaio 2018.

Fabio Di Resta, *GDPR, scegliere il responsabile trattamento dati: interno o esterno all'azienda?*, 28 Feb 2018, agendadigitale.eu

Luca Homberger, *Il Gdpr in 10 passi il nuovo regolamento europeo sulla privacy*, CWS Digital solution,

Franco Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018.

Giusella Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, 2017.

Giusella Finocchiaro e Laura Greco, *Gdpr e notifica delle violazioni: tutto ciò che bisogna sapere*, 15 Set 2017, agendadigitale.eu

Raffaella Natale, *GDPR, tutto ciò che c'è da sapere per essere in regola*, 16 Apr 2018, agendadigitale.eu

Franco Pizzetti, *Dati sanitari, i due pericoli nascosti nella Legge europea 2017*, 04 Dic 2017, agendadigitale.eu

Giusella Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 1.

D'Acquisto G. Naldi M., *Big Data e privacy by design, Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli, Torino, 2017.

PUBBLICATO SU AMBIENTEDIRITTO.IT - 26 APRILE 2018 – ANNO XVIII

AmbienteDiritto.it - Rivista Giuridica Telematica - Electronic Law Review - Via Filangeri, 19 - 98078 Tortorici ME - Tel +39 0941 421391 - Fax digitale +39 1782724258 Mob. +39 3383702058 - info@ambientediritto.it - Testata registrata presso il Tribunale di Patti Reg. n. 197 del 19/07/2006 - ISSN 1974-9562

www.ambientediritto.it

La rivista Giuridica AMBIENTEDIRITTO.IT 1974-9562 è riconosciuta ed inserita nell'Area 12 - Riviste Scientifiche Giuridiche. ANVUR: Agenzia Nazionale di Valutazione del Sistema Universitario e della Ricerca (D.P.R. n.76/2010). Valutazione della Qualità della Ricerca (VQR); Autovalutazione, Valutazione periodica, Accreditamento (AVA); Abilitazione Scientifica Nazionale (ASN). Repertorio del Foro Italiano Abbr. n.271 www.ambientediritto.it