diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 19/01/2016

All'indirizzo http://www.diritto.it/docs/37732-una-panoramica-sugli-aspetti-sanzionatori-nel-nuovo-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

Autore: Marcoccio Gloria

Una panoramica sugli aspetti sanzionatori nel nuovo Regolamento europeo in materia di protezione dei dati personali

Una panoramica sugli aspetti sanzionatori nel nuovo Regolamento europeo in materia di protezione dei dati personali

Gloria Marcoccio - gloria.marcoccio@glory.it

19 Gennaio 2016

Introduzione

il Parlamento Europeo, il Consiglio dell'Unione Europea e la Commissione Europea, dopo tre anni di intense e complesse revisioni e negoziazioni, a Dicembre 2015 hanno raggiunto l'accordo finale sul testo del nuovo Regolamento Generale Europeo sulla protezione dei dati personali (Regolamento[1]): si tratta del più importante cambiamento che riguarderà le leggi in materia di protezione dati personali della Unione Europea, in arrivo dopo 20 anni dalla direttiva europea sulla privacy 95/46/EC. Il Regolamento porta con se il riconoscimento di maggiori tutele per le persone, un generale innalzamento dei livelli di protezione per i dati personali con l'introduzione di nuove misure di sicurezza, nuovi adempimenti, nonché previsione di consistenti sanzioni in caso di violazione delle prescrizioni. Il Regolamento è atteso in Gazzetta Ufficiale Europea dopo la sua approvazione da parte del Parlamento Europeo in sessione plenaria, evento previsto entro Primavera 2016, e dovrà essere implementato entro due anni in tutti i 28 paesi membri UE (a differenza delle Direttive, che devono essere trasposte nei sistemi legislativi nazionali, i Regolamenti sono direttamente applicabili in tutti i singoli paesi dell'Unione). Il Regolamento inciderà in modo significativo sulle imprese di tutti i settori industriali e richiederà un' attenta revisione di quanto in essere ed un pronto adeguamento alle nuove misure di natura tecnica, organizzativa e procedurale.

Molteplici sono le novità portate dal Regolamento e tra queste assumono una particolare rilevanza quelle che riguardano le sanzioni, oggetto di questa breve nota e relative considerazioni.

Regole comuni per le sanzioni amministrative

In primo luogo occorre considerare che la nuova normativa europea, con la sua natura di Regolamento, delinea un quadro sanzionatorio unico a livello UE, pensato per uniformare il più possibile l'approccio per la gestione delle sanzioni in caso di violazioni delle regole previste per il trattamento dati personali, tema finora inevitabilmente e totalmente ancorato a quanto stabilito in proposito dai sistemi legislativi dei singoli Stati Membri UE. Ad oggi, in conseguenza di quanto previsto dalla direttiva 95/46/CE con il suo articolo 28[2], entità delle sanzioni, prescrizioni oggetto delle stesse, nonché modalità e criteri adottati da parte dei Garanti privacy europei per la loro applicazione, mostrano importanti differenze e particolarizzazioni a livello di singolo Stato Membro. Qualche esempio: in Inghilterra per gravi violazioni rispetto a quanto previsto dal Data Protection Act il Garante privacy inglese può imporre una sanzione pecuniaria fino a 500.000 sterline (circa 661.000 euro) mentre invece nel caso della Romania, l'entità delle sanzioni è di fatto a discrezione del Garante privacy rumeno, nel caso Italiano la situazione è assai variegata e comunque, prendendo come riferimento l'inosservanza di provvedimenti emessi dall'Autorità, art162 comma 2-ter del D.Lgs 196/03, il Garante privacy italiano può arrivare ad imporre sanzioni fino a 180.000 euro, cifra che può anche essere aumentata fino al quadruplo, qualora risulti inefficace in ragione delle condizioni economiche del contravventore (art. 164-bis del D.Lgs 196/03).

---

[1] Questo articolo fa riferimento al testo del Regolamento sul quale è stato raggiunto l'accordo del 15.12.2015 documentato dal comunicato stampa: http://www.consilium.europa.eu/it/press/press-releases/2015/12/18-data-protection/

[2] Direttiva 95/46/CE - Articolo 24 Sanzioni "*Gli Stati membri adottano le misure appropriate per garantire la piena applicazione delle disposizioni della presente direttiva e in particolare stabiliscono le sanzioni da applicare in caso di violazione delle disposizioni di attuazione della presente direttiva."*

Caratteristiche principali delle sanzioni previste dal Regolamento

Allo scopo di rafforzare ed uniformare a livello UE le sanzioni amministrative in caso di violazione del Regolamento, alle autorità Garanti privacy europee è esplicitamente conferito il potere di imporre sanzioni amministrative, per specifiche prescrizioni del Regolamento, di un determinato valore massimo pecuniario, attenendosi ad un apposito criterio per stabilire la sanzione da applicare in ogni singolo caso in esame. Tale criterio tiene in considerazione diversi fattori tra i quali: la natura, gravità e durata della violazione, il numero dei soggetti coinvolti ed il livello di danno da loro subito, le categorie di dati oggetto della violazione, le misure adottate dal trasgressore per prevenire o attenuare le conseguenze della violazione stessa ed il grado della sua cooperazione con il Garante privacy, aspetti aggravanti o mitiganti applicabili al singolo specifico caso di violazione.

Riguardo l'entità massima delle sanzioni pecuniarie è prevista una articolazione in termini di tipologia del trasgressore (persona, impresa) nonché tipo di prescrizione oggetto di violazione, che il legislatore europeo ha suddiviso in due classi separate. In sintesi il quadro derivante per le sanzioni amministrative previste dal Regolamento è così schematicamente rappresentabile:

Sanzione fino a 10 milioni di euro, in caso di imprese fino al 2% del fatturato annuo totale a livello mondiale se superiore a 10 milioni di euro, per violazione delle prescrizioni in materia di:

Consenso per il caso dei minori, Sicurezza, Accountability[3], rispetto dei principi di Privacy by Design e Privacy by Default, Consultazione Preventiva del Garante privacy, adempimenti in generale del Titolare del Responsabile e del Rappresentante (di Titolare non UE), Data Breach, Privacy Impact Assessment, Data Protection Officer, rispetto delle prescrizioni che riguardano le Certificazioni (quest'ultima è una delle importanti novità portate dal Regolamento, vedasi prossimo paragrafo)

Sanzione fino a 20 milioni di euro, in caso di imprese fino al 4% del fatturato annuo totale a livello mondiale se superiore a 20 milioni di euro, per violazione delle prescrizioni in materia di:

Requisiti per espressione e documentazione del Consenso, principi di correttezza e liceità dei trattamenti, diritti degli interessati (tra cui la Portabilità dei dati[4] ed il Diritto all'oblio[5]), trasferimenti di dati all'estero, rispetto degli ordini e provvedimenti emessi dal Garante privacy, comunicazione di Data Breach agli interessati, rispetto di specifici divieti di trattamenti, rispetto degli obblighi per specifici casi di trattamento come quelli che riguardano i dati dei lavoratori nel contesto del rapporto del lavoro,...

Ben evidente il forte inasprimento previsto per le sanzioni di carattere pecuniario e l' ampia casistica di prescrizioni del Regolamento alle quali si riferiscono. Sarà dunque essenziale che l'applicazione di tale aspro regime

[3] con il termine 'Accountability' si intende la disposizione del Regolamento per cui il Titolare e il Responsabile devono documentare i trattamenti effettuati secondo un determinato schema di riferimento (tipologia di dati, di trattamento, di soggetti cui i dati si riferiscono, misure di sicurezza, trasferimenti di dati extra UE,...) e rendere tale documentazione disponibile a richiesta del Garante privacy. La disposizione non si applica ad imprese con meno di 250 lavoratori a meno che il trattamento non comporti rischi per i diritti e le libertà degli interessati, se si tratta di trattamento non occasionale o se il trattamento include particolari categorie di dati o dati relativi a condanne penali e reati.

[4] con il termine 'Portabilità dei dati' si intende il diritto per l'interessato di poter richiedere al Titolare di un trattamento di ricevere indietro i propri dati in un formato tale ("*in a structured and commonly used and machine readable format*") per cui l'interessato possa trasmettere i dati ad un altro Titolare senza dover subire ostacoli in questa operazione (tipicamente applicabile in casi di servizi on line, ad esempio 'hosting' dei dati).

[5] con il termine 'Diritto all'Oblio' si intende il diritto dell'interessato di ottenere dal Titolare la cancellazione dei dati che lo riguardano, senza indebito ritardo, per determinati casi di trattamento. Questo diritto è stato recentemente già oggetto di attenzione con la vigente normativa privacy, vedasi il caso della sentenza contro Google Spain ed i suoi risvolti anche in ambito Italiano (a titolo di esempio: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3623678#1)

sanzionatorio avvenga in modo realmente uniforme e che non diventi invece fonte di nuove disparità tra Stati Membri UE, per cui il coordinamento tra i Garanti privacy europei, espressamente previsto dal nuovo Regolamento, sul fronte sanzionatorio assumerà un valenza fondamentale per il successo e l'efficacia della nuova regolamentazione europea per la protezione dei dati personali, con l'auspicio che possa evitare squilibri che sarebbero davvero difficili da giustificare da tutti i punti di vista, e con ovvi impatti sul business delle imprese oltre che per le responsabilità dei singoli.

Le sanzioni penali

Per quanto concerne gli aspetti penali, il Regolamento prevede che saranno gli Stati Membri UE a stabilire quali dovranno essere le misure da adottare ed in modo tale che le sanzioni siano effettivamente applicate, efficaci, proporzionate e dissuasive. Con riferimento al caso Italiano si potrà probabilmente assistere, in linea di massima, al mantenimento dell'attuale quadro sanzionatorio per illeciti penali delineato con quanto previsto dagli artt 167-172 del D.Lgs 196/03, con le necessarie modifiche in funzione del nuovo quadro di obblighi e requisiti previsti dal Regolamento.

L'applicabilità delle sanzioni a particolari figure, e il caso del settore pubblico

A differenza della direttiva 95/46/EC, il Regolamento individua, come destinatari delle sue prescrizioni, altre figure oltre a quella del Titolare del trattamento.

In primo luogo il Responsabile (persona fisica o giuridica che effettua i trattamenti di dati per conto del Titolare, è tipicamente un fornitore di servizi che comportano trattamento dati personali), ruolo privacy già definito dalla direttiva 95/46/EC, le cui responsabilità ora sono largamente accresciute in quanto esplicitamente destinatario di obblighi in termini di: necessità di definire un Rappresentante nella UE ai fini della normativa in oggetto (qualora il Responsabile sia stabilito in paese estero rispetto la UE), obblighi di informare il Titolare e di ottenere il suo consenso qualora il Responsabile intenda a sua volta coinvolgere subfornitori nelle operazioni di trattamento dati (anch'essi saranno dei Responsabili) ed obblighi di vincolare tali ulteriori Responsabili al rispetto delle istruzioni fornite da Titolare per il trattamento dei dati personali, mantenimento di apposita documentazione in merito ai trattamenti svolti (il concetto di Accountability), obblighi di cooperazione con il Garante privacy quando richiesto, obblighi di approntamento delle misure di sicurezza, obblighi di comunicazione senza indebito ritardo al Titolare dei casi di Data Breach, obblighi di designare il Data Protection Officer in determinate condizioni - le stesse valide per il Titolare, rispetto delle regole qualora il Responsabile adotti una certificazione ai fini del trattamento dati personali, adempimenti richiesti nel caso di trasferimento di dati verso paesi esteri rispetto la UE.

Tali accresciute responsabilità comporteranno evidentemente una maggiore esposizione al rischio sanzioni anche per i Responsabili oltre che per i Titolari di trattamento.

Vi è poi il caso della figura del Certificatore. Il Regolamento introduce infatti un importante novità: la (volontaria) certificazione ed adozione di 'marchi privacy' allo scopo di dimostrare conformità al Regolamento nelle attività di trattamento dati condotte sia da Titolari che da Responsabili. L'introduzione della certificazione ai fini della normativa privacy è destinata senz'altro a suscitare grande interesse:

- in termini positivi in quanto si apre un mercato decisamente innovativo ed importante come numeri; al contempo per le aziende, l'aver conseguito una tale certificazione, porterà vantaggi quantomeno sotto il profilo dei minori oneri burocratici (che sono ridotti, ma ancora inevitabilmente presenti nel Regolamento)

- come elemento di perplessità da vari punti di vista, in virtù del legame che si viene a creare tra adempimento richiesto come obbligo di legge ed una attestazione a tal fine basata su una certificazione rilasciata da ente terzo, il che potrebbe presentare qualche falla 'logica' e comportare anche conseguenze negative tali da compromettere la stessa impostazione del sistema di certificazione privacy

Il Regolamento individua specifici compiti ed obblighi per gli enti coinvolti nel meccanismo di certificazione e relativa manutenzione (enti certificatori e relativi organismi di controllo), in violazione dei quali prevede a carico di tali enti la sanzione fino a 10 milioni di euro (o fino al 2% del fatturato in caso di impresa, se questo è superiore ai 10 milioni di euro).

Relativamente invece alle autorità ed enti pubblici, il Regolamento rimanda agli Stati Membri UE la facoltà di stabilire se e in quale misura possano essere imposte le sanzioni amministrative a tali autorità ed enti: su questo punto è notevole la differenza di impostazione rispetto alla direttiva 95/46/EC il cui considerando 55 prevedeva che "....*sanzioni debbono essere applicate nei confronti di qualsiasi soggetto di diritto privato o di diritto pubblico che non rispetti le norme nazionali di attuazione della presente direttiva*" e l'articolo 24 relativo alle Sanzioni non introduceva infatti alcuna specificità per il caso di sanzioni per violazioni commesse da parte della pubblica amministrazione (vedasi nota 2 in piè di pagina).

L'ampio ambito territoriale dell'applicabilità del Regolamento e conseguente numerosità dei soggetti destinatari di sanzioni in caso di inosservanza delle sue disposizioni

Una delle maggiori caratteristiche del Regolamento, sulla quale si sono accentrate numerose critiche e richieste di modifica da parte dei maggiori operatori internazionali di servizi basati sul trattamento di dati personali (social network, vendita di beni e servizi tramite internet, fornitori extra UE di vari servizi quali 'hosting' dei dati, aziende pubblicitarie...) è senz'altro quella del suo ampio ambito di applicabilità: infatti, oltre ad essere applicabile alle società (Titolari o Responsabili) stabilite con le loro attività di business nella UE, le prescrizioni del Regolamento si applicano anche alle aziende (Titolari e Responsabili) non stabilite nella UE che:

- trattano dati personali di persone fisiche che si trovano nella UE (non necessariamente solo i residenti in paesi UE) e il trattamento è in relazione ad offerte di beni o servizi, indipendentemente dal fatto che sia richiesto o meno un pagamento per essi,
  e/o
- effettuano attività di monitoraggio sul comportamento di tali persone (comportamento on line su internet ma anche monitoraggio di altro tipo, ad esempio nell'uso di beni e servizi) nella misura in cui il comportamento oggetto di monitoraggio avviene all'interno della UE

Pur tenendo presente l'esistenza di margini per l' interpretazione letterale della disposizione riguardo l'ambito di applicabilità del Regolamento (si pensi ad esempio alla modalità con cui circoscrivere, in modo documentato ed opponibile a terzi, un *'comportamento all'interno della UE'* o meno, in caso di attività svolta via internet dalla persona) il novero dei destinatari delle sanzioni in caso di violazioni delle prescrizioni del Regolamento sarà decisamente ben più ampio rispetto a quanto in essere con l'attuale normativa: da vedere. tra circa due anni e nella realtà pratica, come le autorità competenti potranno effettivamente essere nelle condizioni di rilevare violazioni ed imporre sanzioni in questo ambito, più che ampio, sterminato.