Aprile 2018

GDPR: valutazione di impatto sui dati personali e dimostrazione dell'affidabilità aziendale. La DPIA come strumento di creazione di valore.

Avv. Stefano Maria Zappalà e Avv. stabilito Maria Juan - Abogado, Studio Legale EIPF

Il Regolamento Europeo n. 679/2016 o *General Data Protection Regulation* (**GDPR**) sarà applicabile a partire dal prossimo 25 maggio. Entro tale data **ogni soggetto** che effettui un trattamento dei dati personali dovrà poter dimostrare la propria osservanza alla disciplina introdotta dal GDPR.

Il GDPR si applica:

- a tutte le società con **sede in uno stato membro dell'UE**; e anche
- alle **società estere con sede fuori dal territorio dell'UE** qualora: (a) offrano beni o servizi ai soggetti che si trovano nel territorio dell'UE; oppure; (b) svolgano attività di monitoraggio di comportamenti di soggetti che si trovano nel territorio dell'UE.

L'inosservanza degli obblighi concernenti il Regolamento può comportare l'applicazione delle seguenti **sanzioni pecuniarie:**

- fino a € 10 M, o fino al 2% del fatturato consolidato dell'anno precedente, se superiore; e, nei casi più gravi
- fino a € 20 M, o fino al 4% del fatturato consolidato dell'anno precedente, se superiore.

Uno degli elementi di grande rilevanza che emerge dal nuovo quadro normativo introdotto dal GDPR è la procedura per la valutazione di impatto sulla protezione dei dati personali trattati dalle aziende, la *Data Protection Impact Assessment* (**DPIA**). La DPIA si configura come una procedura che obbligatoriamente dovranno condurre tutte quelle aziende che effettuano:

- trattamenti valutativi o di assegnazione di punteggi, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);

- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche)[1];
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i *Big Data*);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

Data Mapping - passi per condurre una verifica preliminare

La necessità di verificare se occorra effettuare una valutazione d'impatto dovrebbe fare parte del normale processo di organizzazione aziendale. Di seguito indichiamo una serie di domande che possono essere di ausilio per le aziende onde verificare sei i dati personali trattati devono, o meno, essere sottoposti a una verifica e all'adozione di misure compensative per mitigare i possibili rischi di violazione. Giova sin d'ora evidenziare come i rischi di violazione possono provenire da fonti esterne alla propria organizzazione ma anche, e molto frequentemente, da soggetti interni. I meccanismi di protezione e mitigazione che consentiranno quindi alle aziende di poter invocare l'esenzione da

[1] Cfr. considerando (75) GDPR "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*."

responsabilità in caso di violazione dovranno necessariamente prendere in considerazione tali due fattori (interni ed esterni).

Passando ora alla fase che precede l'eventuale verifica, il primo passo sarà di effettuare una "**mappatura dei dati**" identificando i seguenti elementi:

a) il tipo di dati personali trattati (nome, e-mail, indirizzi, etc) e in quale categoria essi ricadono (dati sulla salute, dati di natura criminale, dati di localizzazione geografica etc.);

b) le modalità di trattamento: i dati personali vengono trattati unicamente in azienda? Per quali scopi? Sono conservati in archivi elettronici oppure anche in formato cartaceo? dove sono custoditi? Cloud? in *cloud* fuori dall'UE?

c) l'organizzazione aziendale: chi è il titolare o il responsabile del trattamento? Esistono altre figure che hanno accesso ai dati? Ho recentemente acquistato una nuova azienda senza aver condotto una *due diligence* sulla protezione dei dati?

d) il flusso dei dati: i dati personali sono condivisi con terzi fornitori alla propria organizzazione? Verranno trattati fuori dall'UE? Esistono accordi di protezione dati (*data protection agreements*) con terzi fornitori o collaboratori che stabiliscano le cd. *standard contractual terms* per garantire la protezione dei dati? Oppure la mia azienda adotta misure per la protezione dei dati solo internamente, ma quando questi vengono trasferiti (anche mediante la semplice conservazione in cloud esterni) non vengono adottate misure per garantire la protezione degli stessi?.

Questo ultimo elemento è di importanza fondamentale. Infatti, uno dei principi basilari del GDPR è quello per cui le misure per garantire la protezione dei dati personali devono coprire l'intero flusso dei dati non dovendo mai interrompersi. È pertanto necessario descrivere il ciclo completo del trattamento dei dati, dal suo conferimento da parte del soggetto interessato, fino a coprire l'intero ciclo di vita (distruzione, periodo di conservazione, etc.), ivi inclusa la previsione di futuri trattamenti; solo in questo modo si potranno determinare correttamente i rischi e adottare le misure di salvaguardia (*privacy by design*) sin dall'inizio del trattamento.

Solo dopo avere risposto alle predette domande e avere effettuato una mappatura dei dati personali trattati, l'azienda può decidere che la propria organizzazione non ha bisogno di condurre una valutazione (DPIA) perché il trattamento dei dati ha un basso impatto sulla *privacy*. In questo caso sarà comunque utile conservare traccia della procedura di mappatura per poter dimostrare la propria esenzione da responsabilità, qualora in un futuro si dovessero verificare casi di violazione.

Qualora invece venisse accertata la necessità di una DPIA, sarà necessario coinvolgere il *management* aziendale nel processo di verifica di impatto. Ricordiamo

che il titolare del trattamento, qualora si verificasse una violazione dei dati personali (*data breach*) e lo stesso non potesse dimostrare di avere adoperato tutte le misure imposte dal GDPR sarà considerato come l'unico responsabile; il GDPR in questo senso esonera da responsabilità figure come il DPO. Questa responsabilità appena descritta corrisponde al cd. principio di *accountability;* essa rovescia completamente la disciplina della *privacy*, incentrandosi il quadro normativo sulla **responsabilizzazione del «titolare»**[2], che dovrà essere in grado di dimostrare di essersi conformato al Regolamento attraverso l'adozione di misure tecniche ed organizzative relative al trattamento.

La DPIA: misure ed elementi di valutazione

Il documento di valutazione di impatto sui dati personali dovrà essere in grado di identificare per ciascun dato o categoria di dati (ricordiamo che i dati possono essere raggruppati in categorie qualora presentino delle caratteristiche simili) i rischi e le relative misure di mitigazione (può essere utile, ad esempio, assegnare un certo colore a quei trattamenti che presentano un alto rischio per la protezione dei dati e un altro colore a quelli per i quali il trattamento non presenta rischi). La DPIA dovrà contenere inoltre una valutazione circa la necessità e proporzionalità dei trattamenti in relazione alle finalità per cui sono effettuati, compreso, ove applicabile, il legittimo interesse del titolare del trattamento.

I rischi devono poi essere distinti in (i) rischi per l'interessato e, (ii) rischi per l'azienda, in caso di mancato adeguamento (ivi inclusa l'indicazione delle relative sanzioni) incluso il rischio reputazionale (si pensi se una violazione dei diritti divenisse di pubblico dominio, ad esempio per un fornitore di servizi *cloud*). Alcuni rischi possono provenire, ad esempio, dalla condivisione dei dati personali con altre aziende, interne o esterne all'organizzazione dell'azienda che procede al trattamento; per mitigare tale rischio, si potrebbe proporre l'adozione di adeguate procedure per rendere anonimi i dati personali.

Da ultimo occorre ricordare quanto affermato dal Gruppo Europeo Garanti Privacy (UE WP29): "*Carrying out a DPIA is a continual process, not a one-time exercise"*; ciò si traduce nel concetto che l'analisi e l'adozione delle misure di protezione è e deve essere un processo in continuo svolgimento.

[2] Cfr. art. 24 GDPR (responsabilità del titolare del trattamento) "1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, 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"

Data e Big Data – una nuova valuta del core business aziendale

Già nel 2009 Meglena Kuneva, Commissario Europeo per la politica dei consumatori, affermava: "*i dati personali sono il nuovo motore di internet e la nuova valuta del mondo digitale*"[3]. Nove anni più tardi il valore dei dati personali continua a crescere rapidamente, parallelamente alla crescita della capacità di raccoglierli analizzarli.

I dati personali costituiscono una fonte di profitto per le aziende ed è proprio in questo ambito che l'UE e il Garante sulla *privacy* hanno evidenziato come la garanzia della *privacy* e la regolamentazione nel flusso delle informazioni sono quanto mai oneri fondamentali per gli enti che trattano dati.

I dati personali correttamente trattati e protetti, generano un valore per l'azienda e, a sua volta, generano altri dati, creando così un circolo virtuoso. Questo avviene già dopo aver condotto la mappatura dei dati aziendali. Pensiamo ad esempio al caso di una azienda che produce e vende un determinato prodotto. Attraverso l'analisi delle abitudini dei propri clienti, o della domanda degli stessi può sicuramente migliorare il proprio processo interno di produzione onde offrire servizi personalizzati ai propri clienti, nonché migliorare la sicurezza della propria organizzazione o la gestione efficiente dell'energia, generando con questo processo altri ulteriori dati, che possono favorire terze parti e così via, creando il circolo virtuoso cui si accennava.

I *Big Data*, ossia tutte le informazioni di cui dispone una azienda (interne ma anche quelle ottenute attraverso fonti esterne, quali ad esempio *social media*, etc.) che sono analizzati, nel rispetto dei principi del GDPR e della relativa normativa applicabile, attraverso l'utilizzo di algoritmi, possono aiutare le imprese ad avere un quadro storico della *performance* aziendale, in grado ad esempio di elaborare dati previsionali (*forecasting*) o proporre ai vertici aziendali delle soluzione strategiche sulla base dei dati analizzati che diventano quindi una fonte sicura di valore e di profitto.

La procedura di DPIA, quindi, può essere letta anche in questa ottica, quasi fosse un investimento aziendale.

Alle stesse conclusioni, limitatamente all'ambito delle istituzioni finanziarie, sembra raggiungere anche il rapporto sui Big Data elaborato dal *Joint Committee*, organo coordinatore delle *European Supervisory Authorities* (ESAs) formato dall'EBA (*European Banking Authority*), ESMA (*European Securities and Markets Authority* e dall'EIOPA (*European Insurance and Occupational Pensions Authority*), pubblicato il 15 marzo scorso. Molte delle istituzioni che hanno partecipato al questionario hanno evidenziato come le regole contenute nel GDPR per la protezione dei dati personali nel contesto delle decisioni automatizzate, così come le regole contenute nella MiFID II sulla consulenza e la adeguatezza delle dichiarazioni, sono dei buoni strumenti per mitigare i

[3] *Personal data is the new oil of the internet and the new currency of the digital world* (http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm)

rischi derivanti dall'utilizzo dei Big Data, ad esempio nel campo della consulenza su prodotti finanziari. L'ESAs inoltre raccomanda[4] di sviluppare buone pratiche ("*good practices*") per promuovere da parte delle istituzioni finanziarie il trattamento dei dati dei consumatori in modo corretto ("*fair*"), trasparente ("*transparent*") e non discriminatorio ("*non* discriminatory") allorché detti dati siano utilizzati tramite tecnologie basate sui Big Data.

[4] Cfr. considerando 136 del "Joint Commitee Final Report on Big Data" (JC/2018/04).