REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

DI CARMELA MIRANDA

1. PREMESSA

Nella cornice dell'ordinamento comunitario la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale ("dati personali") costituisce un diritto fondamentale. A sancirlo espressamente non è soltanto la Carta dei diritti fondamentali dell'Unione Europea (art. 8, par. 1), ma anche il Trattato sul funzionamento dell'Unione europea (art. 16, par. 1): entrambe le fonti stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

L'effettiva tutela del diritto in parola, onde non residuare a mera affermazione teorica, si trova oggi ad affrontare una nuova sfida: stare al passo con un'evoluzione tecnologica che, connessa al fattore globalizzazione, ha condotto ad un considerevole aumento dei dati personali scambiati in tutta l'Unione tra attori pubblici e privati.

La tecnologia attuale, infatti, consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare, nello svolgimento delle loro attività, dati personali, come mai in precedenza, Sempre più di frequente, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano.

In un simile contesto storico, garantire un elevato standard di protezione dei dati personali senza, tuttavia, arginare la libera circolazione di quest'ultimi all'interno dell'Unione e il loro trasferimento verso Paesi terzi e/o organizzazioni internazionali, è diventato, nell'agenda del Legislatore comunitario, un obiettivo prioritario, pur passando, necessariamente, attraverso la revisione o, in alcuni casi l'abrogazione, dei precedenti strumenti giuridici di tutela.

La direttiva 95/46/CE, infatti, aveva determinato la compresenza, entro i confini europei, di differenti normative nazionali e, dunque, la sussistenza di una disciplina giuridica, in materia di protezione dei dati personali, che, lungi dall'apparire omogenea, risultava, al contrario, estremamente frammentaria.

Il timore che il divario così creatosi fungesse da freno all'esercizio delle attività economiche nello spazio del mercato interno e, nell'ottica di offrire un quadro normativo confacente ai cambiamenti in essere, ha indotto l'Unione europea a prediligere un regolamento, e non più una direttiva,

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

DI CARMELA MIRANDA

quale fonte giuridica più idonea ad assicurare un meccanismo di protezione dei dati personali che si rivelasse equivalente in tutti gli Stati membri.
Nel dar seguito a tali coordinate e, abrogando la precedente direttiva 95/46/CE, il Reg. (UE) 2016/679 si propone, da un lato, di rispondere all'esigenza di certezza del diritto e trasparenza sollevata dagli operatori economici, dall'altro di offrire alle persone fisiche, in tutti gli Stati membri, il medesimo coefficiente di diritti azionabili nonché di obblighi e responsabilità a carico dei titolari e/o responsabili del trattamento.
Nella cornice testuale del Regolamento gli ambiziosi obiettivi si traducono in semplici e chiare disposizioni atte a delineare un "sistema" che, lungi dal costituire un meccanico memorandum di adempimenti, trova il suo fondamento in un principio fattuale, c.d. di responsabilizzazione, dapprima sconosciuto, che lascia ai titolari del trattamento ampia discrezionalità nell'individuazione delle misure tecniche ed organizzative più adeguate a garantire la protezione dei dati personali dei soggetti interessati.

A tale proattiva flessibilità, di cui il principio in parola (c.d. accountability) costituisce espressione, fa da contropartita un insieme di sanzioni, di non lieve entità, che punisce severamente la violazione delle disposizioni regolamentari.

2. PRINCIPIO DI RESPONSABILIZZAZIONE (ACCOUNTABILITY)
Espressamente sancito dall'art. 5, quello di responsabilizzazione (anche detto "accountability") è un principio che permane l'intero tessuto regolamentare.
Rappresentando una rilevante novità in materia di protezione dei dati personali, tale principio attribuisce ai titolari e responsabili del trattamento autonomia sull´adozione di comportamenti proattivi e tali da dimostrare la concreta applicazione di misure finalizzate ad assicurare il rispetto del Regolamento. Ad orientare le scelte del titolare o responsabile del trattamento soccorrono una serie di criteri espressamente individuati in alcune delle disposizioni normative.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

DI CARMELA MIRANDA

2.1. PROTEZIONE DEI DATI "BY DEFAULT" E "BY DESIGN"

Tra i criteri sopra citati merita menzione, in primo luogo, quello sintetizzato dall´espressione inglese "data protection by default and by design" (art. 25), intendendosi con essa: 1) la necessità che il titolare metta in atto, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso (by design) misure tecniche ed organizzative tali assicurare il rispetto dei principi di protezione (ad esempio la pseudonimizzazione); 2) il monito a che siano trattati, per impostazione predefinita (by default) solo i dati personali necessari per ogni specifica finalità del trattamento. L'impegno applicativo da parte dei titolari (e responsabili) deve, pertanto, sostanziarsi in una serie di attività specifiche e dimostrabili, per la cui gestione diventa fondamentale l'approccio basato sull'analisi del rischio inerente allo specifico trattamento.

2.2. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Elemento tra quelli di maggiore rilevanza nel nuovo contesto normativo, la valutazione di impatto rappresenta un'emblematica applicazione del principio di responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati. Come più volte indicato, infatti, i titolari sono tenuti non soltanto a garantire l'osservanza delle disposizioni del Regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza.

Più nel dettaglio, attraverso un apposito processo, rispetto al quale l'art. 35 descrive i punti fondamentali, il titolare avrà modo di valutare se un determinato trattamento è idoneo a produrre impatti negativi sulle libertà e i diritti degli interessati. L'analisi, infatti, verrà svolta tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All´esito di questa valutazione di impatto sarà il titolare a decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l´autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l´autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà,

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

DI CARMELA MIRANDA

ove necessario, adottare tutte le misure correttive ai sensi dell´art. 58: dall ´ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

2.3. MISURE DI SICUREZZA

Rappresentando il principio di responsabilizzazione, e la correlativa autonomia dei titolari (e responsabili) del trattamento, uno dei pilastri portanti del nuovo sistema di governance dei dati personali, il Regolamento non contiene un catalogo di misure "minime" di sicurezza bensì rimette al titolare e al responsabile di individuare, caso per caso, le misure di sicurezza più opportune a "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, par. 1). La lista di cui al par. 1 dell´art. 32, contenente alcune di tali possibili misure (come la pseudonimizzazione e la cifratura) non deve, pertanto, intendersi esaustiva, come dimostra l'utilizzo dell'espressione "tra le altre, se del caso".

2.4. VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Nell'ottica di rimettere pur sempre al titolare la valutazione del "rischio" circa un determinato trattamento, il Regolamento prevede che il titolare, venuto a conoscenza di una violazione di dati personali, sia tenuto a notificare tale violazione all'autorità di controllo, soltanto nell'ipotesi in cui egli ritenga probabile che da tale violazione derivino rischi per i diritti e lelibertà degli interessati. Pertanto, la notifica all´autorità dell´avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Qualora prevista, la notifica andrà svolta entro 72 ore o, comunque, "senza ingiustificato ritardo". Inoltre, se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, ugualmente "senza ingiustificato ritardo" (art. 33). La disposizione normativa prescrive il contenuto "minimo" della notifica, la quale dovrà contenere, ad esempio, una descrizione circa la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione e le probabili conseguenze della violazione avvenuta, oltre a dover indicare le misure adottate o di cui il titolare si propone l'adozione al fine di porre rimedio alla

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

DI CARMELA MIRANDA

violazione o, se del caso, per attenuarne i possibili effetti negativi

3. IL RESPONSABILE DELLA PROTEZIONE DEI DATI O DATA PROTECTION OFFICER

Delineando un rinnovato quadro di riferimento in termini di compliance per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (o accountability), il Regolamento introduce il "Responsabile della protezione dei dati" (d'ora in avanti RPD) elevandolo ad elemento chiave del nuovo sistema e prevedendo una serie di condizioni in rapporto alla nomina, allo status e ai compiti specifici (att. 37-39).

Pur incoraggiando i titolari e/o responsabili del trattamento ad adottare un approccio propositivo (nominare il RPD su base volontaria, anche laddove non espressamente richiesto), l'obbligo di designazione di tale figura viene rapportato a determinati casi specifici: sono tenuti a nominare un RPD tutte le amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie; tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Il RPD può far parte del personale del titolare del trattamento o del responsabile del trattamento ovvero assolvere i suoi compiti in base a un contratto di servizi. In quest'ultimo caso il RPD sarà esterno e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica.

Al RPD spetta il compito di "sorvegliare" l'osservanza del disposizioni regolamentari: tale controllo trova specificazione in una serie di concrete attività operative, tra le quali rientrano, ad esempio, la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile nonché dei dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

DI CARMELA MIRANDA

Con riguardo all'attività di consulenza, il ruolo di RPD acquista particolare rilievo in materia di valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo inglese). Sebbene, infatti, il Regolamento attribuisca al titolare del trattamento l'incarico di svolgere, ove necessario, una DPIA, si prevede espressamente che questi debba consultarsi con il RPD quanto alla decisione sul se condurre o meno una DPIA ovvero su quale metodologia adoperare. Laddove richiesto, il RPD dovrà fornire un parere in merito alla DPIA, manifestando, ad esempio, se quest'ultima sia stata svolta correttamente e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi alle disposizioni regolamentari.

Chiamato a cooperare con l'autorità di controllo su questioni attinenti al trattamento dei dati, il RPD funge, inoltre, da punto di contatto per facilitare l'accesso, da parte di quest'ultima, ai documenti e alle informazioni necessarie per l'adempimento dei compiti attribuitile nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi che le spettano.

Il RPD deve poter operare in piena autonomia e indipendenza: a tal fine non potrà ricevere nessuna istruzione da parte del titolare del trattamento o del responsabile del trattamento per quanto riguarda lo svolgimento dei suoi compiti né, relativamente a questi, potrà essere penalizzato o rimosso dall'incarico. Emerge con particolare rilevanza, inoltre, l'assenza di conflitto di interessi con eventuali ulteriori compiti e funzioni svolti dal RPD.

Posto che l'elencazione normativa dei compiti attribuiti al RPD non è da ritenersi esaustiva, nulla vietando al titolare o responsabile del trattamento al RPD ulteriori attività (ad esempio la tenuta del registro delle attività di trattamento), ai fini del loro espletamento e, a monte, della sua designazione, è ad egli richiesto il possesso, sia di qualità personali (integrità e aderenza elevati standard deontologici) che di qualità professionali atte a comprovare la capacità di assolvere a tali compiti.

In particolare, indice della sussistenza di idonee qualità professionali è la conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati. Non trovando risposta in una definizione tassativa, il livello di conoscenza richiesto dovrà essere

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

DI CARMELA MIRANDA

proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento (per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto). Sebbene non siano richieste attestazioni formali o l'iscrizione ad appositi albi professionali, la partecipazione a master e corsi di studio/professionali potrà rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze. Non da meno, costituirà utile criterio la conoscenza, da parte del RPD, dello specifico settore di attività e della struttura organizzativa del titolare del trattamento.

4. CONSENSO

Indicato tra le basi giuridiche in cui ogni trattamento deve poter trovare fondamento (art.6), il consenso, nel tessuto delle disposizioni regolamentari, non muta i suoi principali connotati (libero, specifico, informato e inequivocabile) salvo che per alcune tipologie di dati personali.

L'art. 9, infatti, postula il consenso esplicito dell'interessato ai fini del trattamento dei c.d. dati sensibili, ricomprendendosi in tale categoria i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione, di cui all' art. 22).

Qualora il trattamento sia basato sul consenso, grava sul titolare l'obbligo di dimostrare che l'interessato abbia effettivamente prestato il proprio consenso al trattamento dei propri dati personali.

Sebbene non debba necessariamente essere documentato per iscritto - anche se la forma scritta costituisce una modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili)- laddove il consenso dell'interessato venga prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, occorre che la richiesta di consenso sia presentata in modo chiaramente distinguibile dalle altre, in forma

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

DI CARMELA MIRANDA

comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nulla vieta all'interessato di poter revocare, in qualsiasi momento, il proprio consenso, senza in tal modo pregiudicare la liceità del trattamento basata sul consenso prima della revoca (art.7)
Di maggiori cautele è circondata la manifestazione del consenso da parte dei minori: il Regolamento, infatti, reputa validamente prestato il consenso del minore a partire dai 16 anni (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età si renderà necessario raccogliere il consenso dei genitori o di chi ne fa le veci. (art.8).

5. DIRITTO ALLA PORTABILITA' DEI DATI
Collocandosi tra le principali novità introdotte dal Regolamento, il diritto alla portabilità dei dati (art. 20) consente all'interessato: a) di ricevere dati personali trattati da un titolare e conservarli su un supporto personale o un cloud privato in vista di un utilizzo ulteriore per scopi personali; b) trasmettere dati personali da un titolare del trattamento ad un altro (es.: un diverso fornitore di servizi). Prevedendo specifiche condizioni ai fini del suo esercizio, la disposizione regolamentare qualifica "portabili" solo i dati trattati con il consenso preventivo dell´interessato o sulla base di un contratto stipulato con quest'ultimo ovvero quelli trattati attraverso strumenti automatizzati e solo quelli che siano stati forniti consapevolmente e in modo attivo dall'interessato (ad es., i dati di registrazione inseriti compilando un modulo online, come indirizzo postale, nome utente, età, ecc.).
Al fine di soddisfare la portabilità, i titolari dovranno utilizzare formati "interoperabili" di impiego comune, se già esistenti, oppure utilizzare formati aperti (es. XML), ovvero sviluppare formati interoperabili e strumenti informatici che consentano di estrarre i dati pertinenti.

6. REGISTRO DEI TRATTAMENTI
Lungi dal considerarsi mero adempimento formale, la tenuta del registro dei trattamenti, al contrario, si candida parte integrante di un sistema di corretta gestione dei dati personali, rappresentando uno strumento fondamentale, non soltanto ai fini dell´eventuale supervisione da parte dell'autorità di controllo, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all´interno di un ´azienda o di un soggetto pubblico.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

DI CARMELA MIRANDA

Per tale ragione, sebbene l'obbligo venga normativamente prescritto nei riguardi dei soli titolari o responsabili di trattamento con più di 250 dipendenti, la redazione del registro in parola anche da parte di enti e aziende al di sotto di tale soglia costituirebbe indice di responsabilizzazione, apprezzabile in sede di verifica di conformità al Regolamento. Ciò, precisando, che anche gli organismi con meno di 250 dipendenti, laddove effettuino trattamenti a rischio, dovranno ugualmente adeguarsi a tale previsione normativa. Posto che il registro debba avere forma scritta, anche elettronica, e debba essere esibito su richiesta all'autorità di controllo, tra i suoi contenuti rientra, ad esempio, l'indicazione del RPD, delle finalità del trattamento nonché una descrizione delle categorie di interessati e delle categorie di dati personali trattati (art. 30).
Inoltre, pur sempre sulla scia della responsabilizzazione e, nell´ottica della complessiva valutazione di impatto dei trattamenti svolti, nulla vieta a un titolare o responsabile di inserire ulteriori informazioni, laddove ritenuto opportuno.

7. SANZIONI AMMINISTRATIVE PECUNIARIE
L'impianto repressivo tratteggiato dal Regolamento attribuisce alle autorità di controllo, congiuntamente alle altre misure previste dall'art. 58, il potere di irrogare sanzione amministrative pecuniarie, il cui ammontare può spingersi sino a ventimila euro per il singolo o, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
Onde valutare sia l'opportunità di irrogare la sanzione che l'importo di quest'ultima, l'autorità di controllo dispone di alcuni criteri, normativamente sanciti dall'art. 83, par. 2: tra questi figurano a) "la natura, la gravità e la durata della violazione"; b) "il carattere doloso o colposo della violazione"; c) "le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati"; d) "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 ai sensi degli articoli 25 e 32".
Introducendo, in materia di protezione dei dati personali, un livello ben superiore di responsabilità del titolare del trattamento rispetto alla direttiva 95/46/CE, il quadro

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

DI CARMELA MIRANDA

sanzionatorio delineato dal Regolamento in esame induce l'autorità di controllo a porsi un unico e, principale, interrogativo: in che misura il titolare del trattamento ha fatto quanto ci si aspettava facesse, considerando la natura, le finalità o l'entità del trattamento, alla luce degli obblighi imposti dal Regolamento stesso?
Nel rispondere, occorrerà procedere a una valutazione che tenga conto di tutte le circostanze di ogni singolo caso, conformemente all'art. 83, sopra citato.

Dott.ssa Carmela Miranda
Addetto all'ufficio legale e Responsabile alla Protezione dei dati personali (DPO) -Bit4id S.r.l.