Il Regolamento europeo sulla protezione dei dati personali 2016/679 (GDPR acronimo di General Data Protection Regulation) riprende e sviluppa la Direttiva 95/46/CE inserendosi nel solo della più ampia *Digital Single Market Policy* adottata dalla UE fin dal 2015 per consentire ai cittadini di tutelare in modo appropriato i loro dati personali, alla luce delle nuove tecniche (*Internet of Things, big-data,* profilazione dei dati…) sviluppate dalla tecnica. In questa prospettiva il GDPR non va visto come un ulteriore intralcio formale al normale svolgimento dell'attività d'impresa ma, al contrario, come un utile strumento che consente all'azienda, mediante il riordino sistematico dei dati in suo possesso, di porsi in modo più consapevole sul mercato locale e globale. Al posto di soluzioni *pret-à-porter* il GDPR ha il merito di aver sostituito le prescrizioni formali con precise assunzioni di responsabilità che impongono a ciascuna azienda di sviluppare *best practices* che non saranno uguali per tutti, bensì *tailor made* in ragione della natura, qualità e quantità dei dati trattati nonché della attività imprenditoriale concretamente svolta.

Il Reg. UE 279/2016 sul trattamento, la raccolta e la protezione di dati personali

Analisi e suggerimenti per essere in compliance alla normativa europea.

A cura dell'Avv. Giampaolo Naronte, socio GN Lex Studio Legale – Associazione Professionale

GN Lex STUDIO LEGALE

"Il Regolamento Ue/2016/679 sulla General Data Protection Regulation (GDPR): nuove regole comunitarie e precisazioni in materia di protezione dei dati personali"

Corso di formazione ed aggiornamento

a cura dell'Avv. Giampaolo Naronte

1. Premessa ed inquadramento normativo

Il 24 maggio 2016 è entrato in vigore il ***Regolamento (UE) 2016/679*** emanato il 27 aprile 2016 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati (noto come **GDPR, acronimo inglese di "*General Data Protection Regulation*"**): tale Regolamento abroga la direttiva 95/46/CE e trova applicazione diretta a partire dal 25 maggio 2018 in tutti i Paesi facenti parte dell'Unione Europea.

Nonostante la diretta applicabilità e vincolatività del GDPR in tutti i suoi elementi, in Italia l'art. 13 della Legge 25 ottobre 2017, n. 163 (cd. "*Legge di delegazione europea 2016-2017*") ha delegato il Governo ad adottare uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni ivi contenute.

Il ***Codice Privacy*** in materia di trattamento dei dati personali, dunque, dovrà essere modificato in ossequio ai criteri di delega indicati dalla Legge di delegazione europea che impongono:

i) l'espressa abrogazione delle disposizioni del Codice incompatibili con quelle contenute nel regolamento;
ii) la modifica del Codice stesso limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (più specificamente, nell'ambito delle suddette modifiche, dovrà prevedersi l'adeguamento del sistema sanzionatorio penale e amministrativo vigente alle disposizioni del GDPR, introducendo sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse);
iii) il coordinamento delle disposizioni vigenti in materia di protezione dei dati personali con quelle recate dal regolamento (UE) 2016/679 ([1]).

La delega, inoltre, abilita il governo a prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previste dal regolamento.

A tale ultimo riguardo, si segnala che la recente Legge di bilancio 2018 (Legge 27 dicembre 2017, n. 205, pubblicata in G.U. n. 302 del 29.12.2017) all'art. 1, commi da 1020 a 1025, attribuisce al

[1] Unitamente al GDPR sono state accolte il 4 Maggio 2016 due direttive UE costituenti il *Data Protection Compact* (pacchetto protezione dati) che perseguono essenzialmente la tutela dei dati personali nell'ambito del mercato digitale e, nel contempo, regolano i trattamenti dei medesimi dati per scopi di prevenzione e contrasto alla commissione di reati ed alla lotta al terrorismo.

Garante, a tutela dei diritti fondamentali e delle libertà dei cittadini, determinati poteri di carattere regolamentare, di vigilanza e inibitori, e introduce direttamente alcune modifiche e innovazioni in materia di protezione dei dati personali, in relazione a determinati trattamenti, in vista della piena applicazione del GDPR.

Oltre a comportare l'abrogazione della direttiva 95/46/CE, il regolamento GDPR trova diretta applicazione a partire dal 25 maggio 2018 prevalendo sul diritto interno, eventualmente ancora vigente, che dovesse risultare incompatibile con le disposizioni previste dal regolamento medesimo.

Un primo tentativo di uniformazione della disciplina interna alle disposizioni del GDPR è stato compiuto dalla cd. ***Legge europea del 2017*** (*Legge 20 novembre 2017, n. 167*), la quale ha modificato soltanto alcune disposizioni del Codice della privacy, in tema di responsabile del trattamento, di riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici, di conservazione dei dati relativi al traffico telefonico e telematico e di ruolo organico del personale alle dipendenze del Garante. Peraltro, il Garante ha recentemente ribadito che non sono possibili proroghe rispetto alla data di piena e diretta applicazione del GDPR.

2. Ambito di applicazione materiale e territoriale del GDPR

Il regolamento GDPR eleva ad oggetto di tutela il trattamento dei soli dati personali, al fine di assicurare la protezione dei diritti e delle libertà delle persone fisiche in maniera equivalente in tutti gli Stati membri e la libera circolazione dei dati, disciplinando, conseguentemente, i principi e le condizioni per procedere al legittimo trattamento di tali dati.

Sono, pertanto, esclusi dall'ambito di applicazione delle disposizioni del regolamento i trattamenti dei dati relativi alle persone giuridiche: è evidente che in tal caso le disposizioni del GDPR troveranno applicazione con riferimento al trattamento dei dati personali del rappresentante legale.

La definizione di dato personale assunta dal GDPR risulta particolarmente ampia. L'art. 4 del GDPR stabilisce che per ***dato personale*** debba intendersi "*qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

Gli obiettivi che il regolamento persegue richiedono una sensibile estensione dell'ambito di applicazione delle sue disposizioni. In tal senso opera l'art. 2 del GDPR che, quanto all'ambito di applicazione materiale, specifica che il regolamento si applica al trattamento "*interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali [che siano] contenuti in un archivio o destinati a figurarvi*".

Quanto all'ambito di applicazione territoriale, il par. 1 dell'art. 3 accoglie come criterio generale il cd. ***principio di stabilimento*** ([2]). Di conseguenza, il regolamento si applica ai trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento stabiliti nel territorio dell'Unione Europea, a prescindere dalla circostanza che il trattamento sia o meno ivi concretamente effettuato e a prescindere dalla nazionalità o dal luogo di residenza dei soggetti

[2] Il C22 precisa che *stabilimento* implica *l'effettivo e reale svolgimento di un'attività nel quadro di una stabile organizzazione*, a prescindere dalla forma giuridica da esso assunta (sia una succursale o una filiale, purché fornita di personalità giuridica).

(noti in Italia come "interessati" e così definiti dal GDPR) cui si riferiscono i dati personali trattati.

Sono espressamente esclusi dallo spettro applicativo del GDPR i *trattamenti che non rientrano nell'ambito di applicazione del diritto UE* ([3]), *quelli effettuati da Stati membri in materia di politica estera e di sicurezza comune* nonché *quelli effettuati da persone fisiche nell'ambito di un'attività personale* ([4]).

Ulteriormente, il *par. 2 dell'art. 3 del GDPR rende vincolanti le sue norme anche al trattamento effettuato da titolari del trattamento e responsabili del trattamento non stabiliti nell'Unione europea*, in due casi:

a) quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi nell'Unione europea, indipendentemente dall'obbligatorietà di un pagamento da parte dell'interessato;

b) quando il trattamento è riferito al monitoraggio ([5]) del comportamento degli interessati nella misura in cui tale comportamento ha luogo all'interno dell'Unione europea ([6]).

La *ratio* posta alla base del GDPR, volta a consentire la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei loro dati personali, ha condotto all'adozione di un approccio "garantista" dei diritti degli interessati: in altre parole, nell'ipotesi in cui sorga il dubbio se ad una determinata fattispecie si applichi o meno il regolamento, è preferita l'opzione positiva.

3. Principi applicabili al trattamento dei dati personali e condizioni di liceità del trattamento

Il GDPR ribadisce i principi che devono trovare applicazione al trattamento dei dati personali, parte dei quali risultano ben noti e definiti, in quanto già previsti sia dall'attuale Codice privacy sia dalla direttiva 95/46/CE (*liceità, correttezza e trasparenza del trattamento, minimizzazione, limitazione della conservazione, finalità del trattamento*) ([7]).

[3] Tra le attività che *non rientrano* nel diritto UE rileva il fenomeno della *Brexit* per effetto del quale (salvo intervengano diversi accordi *in itinere*) il 30 marzo 2019 il Regno Unito cesserà di far parte della UE e sarà quindi considerato un *Paese terzo* anche agli effetti dell'applicazione del GDPR. Per ovviare alle intuibili difficoltà connesse con tale uscita dalla UE, il Regno Unito sta elaborando un *Data Protection Bill* che sostanzialmente ricalca il GDPR e si propone la (comprensibile e condivisibile) finalità di non creare alcuna frattura rispetto alla normativa europea.

[4] Il C18 spiega che l'attività personale, per non rientrare nella sfera applicativa del GDPR, *non dovrà avere alcuna connessione con altre attività commerciali o professionali* svolte dalla persona fisica: si citano, a titolo esemplificativo, la corrispondenza e gli indirizzari o l'uso di *social network*. Così le foto, informazioni etc… che le persone scambiano via email o utilizzando i *social network* usuali non rientrano nel GDPR mentre, ovviamente, sono soggetti a tale Regolamento i titolari nonché i responsabili di tali mezzi di comunicazione (es. *Facebook* fornisce il proprio *account* per scambiare foto e messaggi oppure *Google* fornisce un *account* di posta elettronica….).

[5] Si considera *monitoraggio* (secondo il C24) *qualunque attività che traccia le persone su internet, compresa la successiva profilazione* (cioè ogni forma di trattamento automatizzato di dati personali consistente nell'uso di tali dati per valutare determinati aspetti personali di una persona fisica, prevedendo – attraverso l'uso ed il trattamento dei dati – il rendimento professionale, la situazione economica, gli interessi, l'affidabilità, il comportamento e gli spostamenti). Il C30 specifica ulteriormente che le persone fisiche possono essere associate ad identificativi *on-line* attraverso i dispositivi che utilizzano (es. indirizzi IP) o dai marcatori temporanei (*cookies*) e ogni altro strumento in grado di lasciare tracce che, combinate con identificativi e dati forniti dal *server*, possono giungere fino ad identificare le persone fisiche.

[6] La dizione del Regolamento non è chiarissima: la norma si applica ad ogni interessato che "*si trova*" nel territorio della UE: a parte la presenza fisica, dal momento che si parla di strumenti automatizzati, *non è chiaro se l'articolo in commento NON si applichi alle ipotesi di presenza "virtuale" sul territorio della UE*: si pensi al caso, affatto inusuale, che un cittadino extra UE "*entri*" attraverso una piattaforma web all'interno di un archivio di una società operante in Italia.

[7] Rinviando ai successivi paragrafi per una dettagliata disamina, qui è sufficiente sinteticamente esporre il contenuto di tali principi come segue: ***a)*** liceità, correttezza e trasparenza implica che i dati devono essere trattati *nei confronti dell'interessato* in modo lecito (cioè *secundum legem*) ed utilizzando un linguaggio chiaro e comprensibile; ***b)*** la limitazione della finalità comporta che la raccolta ed il trattamento *sono esclusivamente autorizzati* per o scopo che connota *ab origine* la raccolta stessa, scopo che dev'essere ovviamente determinato, esplicito e legittimo (nonché ovviamente noto al soggetto interessato); ***c)*** la minimizzazione è forse l'elemento più difficile da soddisfare perché implica che possano essere raccolti dati *per qualità e quantità* adeguate e strettamente pertinenti alla finalità del trattamento; ***d)*** l'esattezza comporta che i dati raccolti, oltre ad essere esatti, devono essere aggiornati; a tale requisito si collega il diritto di rettifica che il GDPR

A questi ultimi si aggiunge, tra le varie novità, l'inedito principio di "***responsabilizzazione***" o "***accountability***", in forza del quale il titolare del trattamento è tenuto a porre in essere tutte le misure tecniche e organizzative adeguate a garantire ed essere in grado di dimostrare che il trattamento dei dati personali degli interessati è effettuato nel rispetto dei principi dettati dall'art. 5, par. 1 e delle altre norme del GDPR.

Costituiscono attuazione concreta dei principi di cui al predetto art. 5, par. 1 del GDPR le disposizioni successive dedicate ai diritti dell'interessato, trattati dall'intero Capo III del GDPR (artt. da12 a 23).

Il GDPR conferma poi la regola per cui *ai fini della sua liceità ogni trattamento deve trovare fondamento in un'idonea base giuridica che, oltre al consenso*, è individuata nella sussistenza delle seguenti ipotesi:

a) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

b) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del medesimo;

c) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

d) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

e) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del medesimo o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

È possibile cogliere traccia delle predette basi giuridiche nella disciplina dettata dal Codice della privacy, in particolare da quanto previsto nell'art. 24.

4. Come garantire la "trasparenza" della raccolta e trattamento dei dati

Ciascun interessato deve conoscere quali sono i propri dati personali oggetto di trattamento, da chi sono trattati, per quale finalità e per quanto tempo. Solo così, infatti, sarà davvero possibile controllare il rispetto del proprio diritto alla protezione dei dati ed eventualmente intervenire per bloccare un utilizzo illecito.

La ***trasparenza*** è perciò uno dei presupposti fondamentali di ogni corretto trattamento di dati personali ed è richiamata espressamente dall'art. 5 del GDPR, ove si afferma che "*i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato*". Il principio di trasparenza risulta così strettamente correlato a quello di equità e a quello di responsabilizzazione (principi fondanti del Regolamento) e il titolare (o il responsabile) dovrà, pertanto, essere in grado di dimostrarne la conformità nell'ambito delle attività di trattamento effettuate. La trasparenza

riconosce agli interessati (consistente, appunto, nel rettificare dati erronei o non aggiornati che lo riguardano); ***e)*** i dati possono essere conservati solamente per un periodo di tempo che non superi il termine occorrente per raggiungere la finalità in vista della quale è stato eseguito il trattamento (es. i dati delle telecamere di videosorveglianza non possono essere conservati, di regola, per periodi superiori alle 72 ore); ***f)*** la raccolta dei dati dev'essere supportata da un'adeguata sicurezza e protezione mediante l'adozione di misure tecniche ed informatiche che prevengano e/o impediscano sia i trattamenti non autorizzati sia la perdita e/o distruzione dei dati medesimi (questo obiettivo è oggetto del *data breach* nonché della valutazione di impatto di rischio – DPIA – su cui si rinvia *infra*); ***g)*** infine il principio di *accountability* consiste nel responsabilizzare il soggetto titolare del trattamento dei dati, ponendo in capo allo stesso specifici oneri di controllo e l'adozione di misure che gli permettano di dimostrare di essere in *compliance* alla normativa UE.

infatti è uno strumento indispensabile per garantire che i dati personali siano trattati nel rispetto dei diritti e delle libertà fondamentali degli interessati, poiché pone le basi per consentire la conoscenza e il controllo effettivi da parte delle persone fisiche coinvolte nel trattamento.

La trasparenza è un obbligo trasversale del GDPR che si esplica, in particolare, in tre aspetti:

I. l'informativa resa agli interessati circa il trattamento di dati,
II. le informazioni date dai titolari agli interessati sui loro diritti; e
III. le modalità con cui viene consentito e facilitato l'esercizio dei diritti agli interessati.

Il principio di trasparenza trova, dunque, la sua principale espressione nell'***informativa*** che deve essere rilasciata agli interessati: ciò vuol dire che i titolari del trattamento devono revisionare le proprie privacy policy in modo tale che il loro contenuto preveda tutte le informazioni necessarie per rispettare ed assicurare effettività al principio di trasparenza (e i requisiti pratici sono indicati, come vedremo nell'apposita sezione, dagli articoli 12, 13 e 14 del GDPR). Importanza centrale nel rispetto del GDPR assume quindi l'informativa nei confronti degli interessati, nella quale andranno esplicitate tutte queste informazioni, dall'identità del titolare alle finalità del trattamento, dalla possibilità di accesso a quella di ricevere informazioni dirette.

La trasparenza, inoltre, va garantita sempre, indipendentemente dalle finalità per le quali viene effettuato il trattamento, ed in tutte le sue fasi (vale a dire: prima che vengono raccolti i dati personali, durante l'intero processo di elaborazione dei dati ed al verificarsi di circostanze particolari, come in caso di violazioni dei dati). Ciò significa, a livello pratico, che tutte le informazioni relative al trattamento di dati effettuate devono sempre essere rese accessibili agli interessati ed essere fornite con modalità ed espressioni chiare e facilmente comprensibili da chiunque.

Il concetto di trasparenza, come visto, va inteso con una portata molto ampia e va applicato anche alle modalità con cui vengono effettuate le operazioni di trattamento, alle tipologie ed alla quantità di dati trattati.

Le regole fondamentali al riguardo sono disciplinate dal Capo III del GDPR, dedicato ai Diritti degli Interessati, ma la trasparenza non viene direttamente definita dal Regolamento. Una chiara esplicazione del suo significato può essere, peraltro, ricavata dall'art. 12, comma 1, GDPR, il quale prevede, in particolare che le comunicazioni rese agli interessati siano fornite (i) "*in forma concisa, trasparente, intellegibile e facilmente accessibile*" e (ii) "*con un linguaggio semplice e chiaro*" ("*Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato*" 12, comma 1, GDPR).

Ne consegue che le informazioni relative alla privacy dovrebbero essere date separatamente rispetto ad altre informazioni non connesse al trattamento dei dati ed utilizzando una formulazione diretta, efficace e comprensibile. A tal fine, i titolari possono avvalersi anche di strumenti di visualizzazione particolari (immagini o icone) e devono altresì rapportare le espressioni alla tipologia media di interessato a cui le stesse sono rivolte, rendendo comunque tutte le informazioni direttamente disponibili agli interessati, senza necessità di effettuare ricerche o richieste particolari.

Ancora, il GDPR richiede, per il rispetto del principio di trasparenza, che le informazioni siano date "*per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le* *informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi [n.d.r: non orali] l'identità dell'interessato*" (art. 12, co. 1, GDPR). Le linee guida al riguardo hanno precisato che la forma di default deve essere quella scritta e che per non "appesantire" eccessivamente le comunicazioni, i responsabili possono avvalersi di informative su più livelli (in forma abbreviata con rinvio immediato a quella estesa, ad esempio) od utilizzare strumenti elettronici come avvisi pop-up contestuali "just-in-time", notifiche touch o hover-over e apposite dash-board. La comunicazione in forma orale, invece, è sempre opportuno che sia accompagnata anche da idoneo avviso per iscritto.

Per garantire il rispetto della trasparenza, è fondamentale, ad ogni modo, che le informazioni siano fornite in modo tale che l'interessato possa capire in anticipo quali sono le finalità del trattamento, qual è il suo ambito e quali sono le conseguenze per i propri diritti se non si oppone ad esso.

Infine, sempre all'art. 12, il GDPR precisa anche che le informazioni e le eventuali comunicazioni devono essere date gratuitamente agli interessati. Solo in pochi casi eccezionali, come ad esempio, se le richieste da parte dell'interessato sono manifestamente eccessive o assolutamente ripetitive, il titolare potrà chiedere un rimborso spese, ragionevole e rapportato agli eventuali costi amministrativi sostenuti per raccogliere le informazioni (comma 5: "*Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può: a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure b) rifiutare di soddisfare la richiesta. Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta*").

5. La "liceità" del trattamento dei dati personali

I dati personali devono essere trattati, in primo luogo, in modo lecito. Ma cosa significa concretamente ***liceità di un trattamento***?

Sul punto interviene l'art. 6 del GDPR che stabilisce che il trattamento di dati personali è effettuato in modo lecito soltanto al ricorrere di almeno una delle condizioni espressamente previste dallo stesso articolo di seguito elencate:

a) il consenso esplicito rilasciato dall'interessato al trattamento per finalità determinate dei propri dati;
b) l'adempimento di obblighi assunti con un contratto di cui l'interessato è parte o l'esecuzione di attività precontrattuali dallo stesso richieste;
c) l'adempimento di obblighi imposti dalla legge in capo al titolare;
d) la tutela di interessi essenziali per la vita dell'interessato o di soggetti terzi (si pensi, ad esempio, a casi di trattamento a fini umanitari o in caso di epidemie);
e) rilevanti motivi di interesse pubblico correlati all'esercizio di pubblici poteri;
f) il perseguimento di un interesse legittimo del titolare o di un'altra persona fisica ritenuto prevalente sui diritti e sulle libertà fondamentali dell'interessato, realizzabile attraverso il trattamento di dati personali ([8]).

[8] E' interessante notare che il C47 espressamente specifica che il trattamento allo scopo di *marketing* diretto può essere considerato un *interesse legittimo* ai fini dell'applicazione della norma in commento anche se tale attività dovrà rispettare le regole del GDPR in tema di profilazione dei dati raccolti.

Quando si parla di liceità del trattamento viene dunque in gioco, in primo luogo, il consenso che il titolare deve acquisire dalla persona a cui i dati personali trattati si riferiscono: consenso affinché i suoi dati personali siano raccolti ed utilizzati secondo le procedure, per le finalità e per il periodo riportati chiaramente nell'informativa. L'applicazione del Regolamento non comporterà in automatico l'illiceità del consenso acquisito in precedenza sotto il Codice della Privacy: il consenso già ricevuto rimarrà valido qualora rispetti tutti i requisiti richiesti dal GDPR.

Vediamo allora quali sono gli elementi rilevanti.

Per prima cosa, ***il consenso*** ([9]) ***ai sensi del GDPR***, *come richiesto già dal Codice della Privacy,* ***deve sempre essere specifico*** ([10])***, libero e inequivocabile*** [11]: non è corretto e comporta una violazione del GDPR, quindi, l'utilizzo di caselle pre-spuntate sui moduli – siano cartacei o informatici – o di un'unica casella comprensiva di trattamenti aventi diverse finalità (ad esempio, adempimento del contratto e invio di newsletter). L'interessato infatti deve avere la possibilità di fare una scelta veramente autonoma e di poter rifiutare (o eventualmente revocare) il consenso senza subire conseguenze negative. In particolare, la richiesta di consenso deve essere chiara e facilmente identificabile e non deve confondersi con altre comunicazioni rivolte all'interessato (deve, cioè, essere chiaramente distinguibile da altre richieste) ([12]).

Il GDPR, inoltre, richiede espressamente che per il trattamento di dati sensibili (come previsto dall'art. 9 GDPR: "*È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona […] a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche*") e in caso di trattamenti automatizzati il ***consenso debba essere esplicito***. Si noti che questa seconda categoria ricomprende anche le operazioni di profilazione (ai sensi dell'art. 22 GDPR: "*1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: […] c) si basi sul consenso esplicito dell'interessato*") ([13]).

[9] Il consenso (cfr. Art.4 n. 11 GDPR) consiste in "*qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato con cui lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di un trattamento*".

[10] La *specificità* del consenso implica che se il trattamento dei dati si propone *diverse finalità*, il consenso dell'interessato deve essere espressamente prestato per ciascuna di esse e queste diverse finalità devono essere *chiaramente* espresse al soggetto in modo che costui possa liberamente scegliere se/a quale scopo acconsentire al trattamento dei suoi dati personali. Si parla in questo caso di *consenso non granulare*: es. uno stesso modulo precisa che i dati raccolti potranno essere usati sia per scopi di marketing (es. comunicare nuove attività o promozioni) sia per essere condivisi con altre aziende facenti parte dello stesso gruppo a cui appartiene il soggetto che ha predisposto il modulo: siamo in presenza di due finalità diverse che richiedono *due manifestazioni di consenso autonome*.

[11] Il C32 precisa che *non si considera consenso* la mera inattività, il silenzio così come la preselezione di caselle su un sito web effettuate dal soggetto interessato.

[12] E' interessante segnalare che il C47, occupandosi di un consenso collegato all'esecuzione di un contratto, specifica che *non è legittimo* condizionare l'esecuzione di un contratto o la prestazione di un servizio al consenso dell'interessato se il contratto o la prestazione siano eseguibili comunque mentre è perfettamente lecito *richiedere il consenso qualora ciò sia necessario all'esecuzione di un contratto o alla prestazione di un servizio* (ad es. acquisto *on line* di un bene: per perfezionare il contratto l'acquirente deve prestare il consenso a fornire i propri dati della carta di credito).

[13] La **profilazione** indica qualunque trattamento automatizzato di dati che utilizzi gli stessi per valutare determinati aspetti relativi ad una persona fisica e, in modo particolare, per analizzare o prevedere alcuni suoi aspetti quali il rendimento professionale, la situazione economica, la salute, gli interessi, le preferenze personali, il comportamento, gli spostamenti o l'affidabilità. L'Art. 22 GDPR stabilisce che l'interessato ha ***diritto a non essere sottoposto a profilazione o decisioni basate su processi automatizzati*** quando ciò possa "produrre effetti giuridici" o "incidere significativamente sulla sua persona". Gli effetti giuridici (secondo il WP29) sono quelli che incidono sui diritti fondamentali dell'interessato: es. il diritto di voto, l'acquisizione dello *status* di rifugiato, il diniego di un beneficio o dell'autorizzazione ad entrare in un certo Stato…. Pertanto nessun processo decisionale automatizzato o profilazione potranno trattare i dati personali di un soggetto allo scopo di emettere una decisione vincolante nei suoi confronti (a meno che ciò non avvenga con il previo

Un'altra novità è introdotta con riguardo all'***età dell'interessato***. L'art. 8 del GDPR, infatti, precisa che il consenso rilasciato dall'interessato è valido (e, di conseguenza, il trattamento su di esso fondato è lecito) a partire dai 16 anni di età. Questa regola comporta che, in presenza di un soggetto di età inferiore ai 16 anni, i titolari dovranno ricevere il consenso al trattamento dai genitori o da chi fa le veci del minore ([14]).

Infine, il GDPR non pretende che ***il consenso sia rilasciato in forma scritta***. D'altra parte, questa sarà in linea di massima la modalità più idonea ed opportuna per raccogliere il consenso dell'interessato, non solo quando si richiede che lo stesso sia esplicito (come in caso di profilazione), ma anche perché è comunque il titolare a doverne dimostrare la non equivocabilità e la specialità (avere traccia scritta del consenso rilasciato sarà sicuramente d'aiuto a tal fine).

Un'altra condizione di liceità che ricorre di frequente nella prassi è dato dall'interesse legittimo di un titolare o di un terzo che prevale sui diritti e sulle libertà fondamentali dell'interessato (ipotesi prevista dall'art. 6, co. 1, lett. f, GDPR). E qui il Regolamento introduce una novità particolarmente rilevante: difatti, il bilanciamento tra interesse del terzo e diritti dell'interessato spetta direttamente al titolare del trattamento e non all'Autorità pubblica. Poiché garantire e dimostrare il rispetto delle condizioni di liceità stabilite dal GDPR è onere del titolare, è a quest'ultimo che spetta anche il compito di effettuare i dovuti bilanciamenti con altri diritti, eventualmente rilevanti, dell'interessato o di terzi e di provare su tali basi la liceità dei trattamenti svolti.

6. Il consenso dell'interessato

Ai fini che qui interessano non vi è dubbio che, a seguito dell'entrata in vigore del GDPR, assumono particolare rilievo le nuove disposizioni dedicate al consenso dell'interessato.

Si è già visto che lart. 4 del GDPR definisce il ***consenso dell'interessato*** come una "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

Tale definizione apre la strada alla possibilità che la dichiarazione di consenso non risulti necessariamente da una documentazione resa per iscritto, purché tale dichiarazione sia stata prestata in maniera inequivocabile.

Il Considerando 32 del Regolamento infatti specifica che "*il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale (principio di libertà delle forme). Potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Se il consenso dell'interessato è*

consenso dell'interessato o si basi su motivi di interesse pubblico per la UE). Pur in assenza di una specifica previsione normativa a riguardo, il WP29 *ritiene che i processi decisionali automatizzati* e la *profilazione* NON possano MAI riguardare soggetti minori (ponendosi tale ipotesi come eccezione alla regola posta dall'Art. 22 GDPR – *su cui si rinvia infra* – che ammette la possibilità di raccogliere e trattare i dati di minori di età superiore a 16 anni).

[14] La responsabilità e gli adempimenti del soggetto che tratta i dati devono essere tenuti distinti dalla normativa civilistica (Artt. 1425 ss c.c.) in tema di minori che riconosce la capacità giuridica di concludere validamente un contratto solo in capo a soggetti *non minori* di anni 18 (nonché interdetti, inabilitati etc…). Se, ad esempio, un minore conclude via internet un contratto *occultando con artifizi e raggiri* la sua età e presta il consenso, il titolare del trattamento ben potrebbe chiedere l'annullamento (civilistico) del contratto *ma ciò non lo esimerebbe dal dover provare di aver agito in modo da verificare la vera età del soggetto richiedente*.

richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso".

Quanto alla libera espressione del consenso, il Considerando 42 esclude che lo stesso possa essere ritenuto liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio. In tal senso, quindi, il regolamento si pone nel solco degli orientamenti già espressi dal Garante in tema di libera espressione del consenso.

Stesso dicasi in relazione al requisito relativo alla ***specificità del consenso***, quale elemento già richiesto dal Codice della privacy. Il requisito della specificità è soddisfatto nel momento in cui il consenso sia applicato a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Differentemente, qualora il trattamento sia effettuato per la realizzazione di più finalità, il consenso dovrebbe essere prestato per ciascuna di esse.

Le condizioni che devono essere soddisfatte affinché la prestazione del consenso possa ritenersi legittima sono ulteriormente specificate dall'art. 7 del GDPR, il quale si riferisce a situazioni che assumono particolare interesse e sulle quali occorre, pertanto, soffermarsi.

Nello specifico la norma in esame esplicita la regola generale in base alla quale, in linea con il principio di accountability, il titolare del trattamento deve essere sempre in grado di dimostrare che l'interessato ha prestato – inequivocabilmente – il proprio consenso al trattamento dei suoi dati personali, con la conseguenza che è necessario porre particolare attenzione a tale "onere probatorio" nell'ipotesi in cui il consenso non venga acquisito per iscritto.

Qualora, al contrario, il consenso sia prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del GDPR è vincolante.

Quando il trattamento è basato sul consenso, l'interessato ha il diritto di revocare (*con efficacia ex nunc*) il proprio consenso in qualsiasi momento. Tuttavia, la revoca non è idonea a pregiudicare la liceità del trattamento già effettuato e basato sul consenso precedentemente prestato. Il diritto di revocare il consenso prestato deve essere indicato nell'informativa comunicata all'interessato prima di esprimere il consenso medesimo.

Particolare rilevanza riveste poi la regola in base alla quale "*il consenso è revocato con la stessa facilità con cui è accordato*", comportando l'obbligo di prevedere le medesime forme e/o misure tecniche per la revoca del consenso già utilizzate al momento della raccolta del medesimo.

Il GDPR detta nuove e più stringenti regole per ciò che riguarda le informazioni che devono essere fornite all'interessato da parte del soggetto titolare del trattamento dei dati personali e che vengono riportate in un documento comunemente denominato "***informativa privacy***".

Le norme che vengono in considerazione sono innanzitutto gli artt. 13 ("*Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato*") e 14 ("*Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato*") del GDPR, i quali delineano in modo tassativo i contenuti di una corretta informativa. Le informazioni richieste dal GDPR peraltro risultano essere più ampie rispetto a quelle finora necessarie ai sensi del Codice Privacy: questo comporta che le informative predisposte nel rispetto del Codice, a partire dal 25 maggio us non saranno più valide e dovranno essere integrate con gli ulteriori elementi necessari ([15]).

La ***informativa privacy in base all'Art. 13*** (*dati raccolti presso l'interessato*) deve contenere i seguenti elementi:

1. i dati di contatto del titolare del trattamento, nonché, se presente, del suo rappresentante sul territorio europeo e (se nominati) del responsabile e del DPO (*Data Protection Officer*): l'interessato infatti deve essere messo nelle condizioni di identificare chiaramente e poter contattare i soggetti a cui spetta il trattamento dei propri dati personali (e a cui spetta garantirne la legittimità);
2. la base giuridica del trattamento (quindi, le condizioni di liceità su cui il trattamento si basa: consenso, interesse legittimo del terzo, interesse pubblico, ecc.) e le finalità (lo scopo della raccolta o dell'elaborazione dei dati) ([16]);
3. i destinatari o le categorie di destinatari dei dati personali: quindi, a chi saranno comunicati quei dati o con chi verranno condivisi, anche semplicemente per poter effettuare un servizio richiesto dallo stesso interessato;
4. se vi sia l'intenzione del titolare del trattamento di trasferire i dati personali a un paese terzo (cioè extra europeo) o a un'organizzazione internazionale: in poche parole, bisogna far sapere all'interessato se i suoi dati verranno diffusi al di fuori del territorio dell'Unione Europea;
5. il periodo di conservazione dei dati o i criteri utilizzati per determinarlo: periodo che sarà strettamente correlato allo scopo perseguito con il trattamento: quando la finalità sarà stata raggiunte, i dati non potranno più rimanere in possesso del titolare. E, come è facilmente intuibile, si tratta di una valutazione che non è sempre possibile fare con certezza a priori: in questi casi, però, si dovrà quanto meno comunicare all'interessato al verificarsi di quali condizioni i dati raccolti saranno cancellati, in modo che lo stesso possa successivamente verificare la correttezza del trattamento effettuato;
6. l'esistenza, in capo all'interessato, di una serie di diritti che dovrebbero permettergli di controllare e gestire consapevolmente il flusso dei propri dati e, in particolare: (i) diritto di accesso ai dati, (ii) il diritto di chiederne la rettifica, la cancellazione, o la limitazione del trattamento, (iii) il diritto di opporsi al trattamento, (iv) il diritto alla portabilità dei dati ([17]), (v) il diritto di revocare il consenso al trattamento, in qualsiasi momento e (vi) il diritto di proporre reclamo all'autorità di controllo: è infatti compito del titolare far conoscere all'interessato quali siano questi diritti e come procedere per esercitarli concretamente (oltre a predisporre delle procedure semplici ed efficaci per darvi esecuzione);
7. se la comunicazione dei dati personali sia un obbligo legale, contrattuale, oppure un requisito necessario per la conclusione di un contratto e se l'interessato abbia l'obbligo di fornire

[15] In base ad una lettura ontologica dell'Art. 7 GDPR l'*informativa privacy* dovrebbe essere separata rispetto al *consenso* al trattamento nonché dai documenti che non hanno nulla a che fare con la *data protection* (es. il formulario contrattuale…).
[16] La base giuridica del trattamento dei dati che sta alla base della *informativa privacy* varia a seconda che si tratti di *dati personali "comuni"* (quelli oggetto del GDPR) oppure dati "*particolari*" (che comprendono oltre ai vecchi *dati sensibili,* quelli *biometrici, genetici* e *sulla salute* dell'interessato nonché quelli relativi a condanne penali).
[17] Il ***diritto alla portabilità*** (*data portability*) di cui all'Art. 20 GDPR rappresenta una delle maggiori novità del GDPR: esso prevede che in caso di trattamenti *basati sul consenso o sul contratto* e quelli effettuati *con mezzi automatizzati*, il titolare – su richiesta dell'interessato – deve mettere a disposizione di costui tutti i dati su un formato di uso comune e leggibile anche da un dispositivo automatico. La richiesta dell'interessato *non deve essere supportata da una giustificazione* ma occorre che il titolare sia certo dell'identità del richiedente con l'interessato. La norma del GDPR presenta alcuni coni d'ombra, ad esempio nella parte in cui afferma che *sono esclusi dalla portabilità la maggior parte dei documenti cartacei* non essendo dato sapere cosa significhi "*maggior parte*" e, soprattutto, *quali documenti cartacei possano essere trasferiti* su un formato richiesto dall'interessato. Il Working Party 29 (organismo nato in base all'Art. 29 GDPR che riunisce le autorità di protezione dei dati personali dei Paesi UE) *precisa opportunamente che il responsabile dovrebbe indicare (già nella informativa privacy) quali sono i dati "portabili" e quali sono quelli "accessibili"* in quanto i primi possono essere oggetto, appunto, di "portabilità" mentre i secondi sono esclusivamente oggetto del diritto di accesso ma non sono "portabili". Una volta ricevuta la richiesta di portabilità, il titolare deve ottemperare entro il termine massimo di 3 mesi (in realtà il termine ordinario per rispondere alla richiesta è di 1 mese, ma il GDPR prevede che il responsabile possa – con *adeguata motivazione* a riguardo – chiedere una proroga di 2 mesi; ovviamente tale richiesta di proroga deve essere inviata all'interessato).

i dati oltre alle conseguenze dell'eventuale mancata comunicazione: il titolare quindi deve dire all'interessato se la raccolta di quei dati sia necessaria o meno per poter fornire un servizio o dare esecuzione a una richiesta rivolta dall'interessato stesso oppure se sia direttamente la legge ad imporla. Inoltre, occorre spiegare all'interessato cosa succede nell'ipotesi in cui lo stesso non voglia comunicare i dati richiesti (il che, per lo più, consisterà nell'impossibilità di fornire il servizio in oggetto): ad esempio, per un servizio di newsletter il titolare richiederà l'indirizzo di posta elettronica all'interessato; bisognerà quindi informarlo che, se non darà questa informazione, quel servizio non potrà essergli eseguito;

8. l'esistenza di un processo decisionale automatizzato, compresa la profilazione, aggiungendo in questo caso informazioni che consentano all'interessato di capire in cosa consista nella pratica quel trattamento: quindi, ad esempio, informazioni sugli strumenti utilizzati, sulla portata del trattamento così effettuato, sulla diffusione dei dati che ne può conseguire e così via;

9. le categorie di dati personali in questione (ad esempio, se sono raccolti dati sensibili) e, nel caso in cui i dati personali non siano stati ottenuti direttamente dall'interessato, la fonte da cui arrivano e l'eventualità che provengano da fonti accessibili al pubblico (ad esempio, elenchi pubblici a cui chiunque può avere accesso) ([18]).

Una seconda modalità di raccolta è poi prevista dall'Art. 14 GDPR che riguarda l'***informativa privacy di dati raccolti da fonti diverse dall'interessato***: le categorie di dati personali sono diverse rispetto a quelle dell'Art. 13 e soprattutto *manca l'informativa circa l'obbligo legale o l'esecuzione di un contratto per la cui esecuzione sono stati raccolti i dati personali*. Anche in questo caso il titolare deve fornire la informativa entro 1 mese dalla data in cui ha raccolto i dati che, nello stesso termine, devono essere comunicati *anche* all'interessato.

Un secondo punto sul quale il GDPR si è soffermato è quello dei ***termini entro i quali bisogna fornire l'informativa ovvero quando queste informazioni devono essere comunicate agli interessati***. In particolare, nel caso in cui si tratti di dati raccolti direttamente presso l'interessato (cioè forniti dall'interessato e non ottenuti da altre fonti, come può avvenire, ad esempio, quando l'interessato dà il consenso affinché i propri dati siano utilizzati per finalità di marketing da partner commerciali del titolare), l'informativa dovrà essere fornita prima che quei dati vengano raccolti. Nel caso in cui, invece, i dati personali non siano stati ottenuti presso l'interessato, ma ricevuti da terzi, l'informativa dovrà essere resa non più all'atto della registrazione dei dati come previsto dal Codice Privacy, ma entro un termine ragionevole (a seconda delle particolari circostanze e della tipologia di dati e di trattamento) dall'ottenimento dei dati stessi (e che comunque non può essere superiore a un mese), oppure al momento della prima comunicazione dei dati all'interessato o al terzo ([19]). Ad esempio, se ho in precedenza acconsentito all'utilizzo dei dati per finalità di marketing da soggetti terzi, quando riceverò la loro prima comunicazione promozionale, ad essa dovrà essere accompagnata una adeguata informativa riguardante il trattamento che questi soggetti terzi stanno effettuando dei miei dati.

[18] Si evidenzia che molti dei dati che il titolare deve riportare nella informativa privacy sono gli stessi che devono essere indicati nel Registro del Trattamento dei Dati (cfr. Art. 30 GDPR) e, ancor prima, valutati nella DPIA *data protection impact assessment* di cui all'Art. 35 GPDR. Anzi, nell'ottica del *risk management* che informa l'intero impianto della GDPR si può sostenere che la *informativa privacy* sia il prodotto della DPIA svolta in precedenza che, a sua volta, per individuare i rischi avrà dovuto "mappare" i processi, i trattamenti, i soggetti responsabili etc… cioè l'insieme dei dati e informazioni che sono contenute nel Registro del Trattamento dei Dati.

[19] A seguito della ricezione di richiesta di accesso da parte dell'interessato, in base all'Art. 12 (3) GDPR il titolare deve fornire le informazioni richieste *senza ingiustificato ritardo* e comunque *entro un mese dal ricevimento della richiesta* (il termine di 40 gg previsto dalla Direttiva 96/45 UE è stato quindi abbreviato). Il titolare può prorogare *fino a due mesi* il termine ma per fare ciò *deve rispondere all'interessato fornendo precise motivazioni a riguardo* (deve comunque trattarsi di circostanze oggettive – es. necessità di espletare un numero elevato di richieste – e non di fattori meramente soggettivi). Nel caso in cui il titolare *non voglia* rispondere alla richiesta, deve darne comunicazione scritta all'interessato (sempre entro e non oltre il termine di 1 mese) *specificando i motivi del rifiuto o della impossibilità di soddisfare la richiesta* e indicando nel contempo *la possibilità per l'interessato di proporre reclamo davanti al Garante ovvero in sede giudiziaria*.

Non meno importanti, infine, sono le modalità con cui l'informativa dovrà essere fornita agli interessati, espressamente richiamate dal GDPR. Come emerge dall'art. 12, paragrafo 1, infatti, le informazioni da trasmettere all'interessato dovranno essere date in forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro (ad es. utilizzando immagini, icone standardizzate o informative brevi, in modo da fornire un quadro d'insieme facilmente comprensibile).

7. Contenuto e modalità di attuazione del "diritto di accesso"

Il ***diritto di accesso*** consiste, come previsto dall'art. 15, paragrafo 1 del GDPR, nel diritto in capo al soggetto interessato "*di ottenere dal titolare del trattamento la conferma che sia in corso o meno un trattamento dei dati personali che lo riguardano*". In questa ipotesi l'interessato ha il diritto di ottenere l'accesso ai propri dati personali raccolti ed elaborati nell'ambito di quel trattamento e di ricevere dal titolare una serie di informazioni ad esso relative, per capire come quei dati sono stati ricevuti, per quale scopo e come vengono utilizzati. Siccome lo stesso titolare potrebbe trattare anche una notevole quantità di informazioni dello stesso interessato (ad esempio perché i dati sono trattati per numerose finalità distinte), gli è consentito, in questi casi, chiedere delle precisazioni all'interessato così da identificare, prima di procedere, a quali informazioni o a quali attività lo stesso vuole avere accesso.

Il GDPR prevede, in particolare, che l'interessato abbia il diritto di conoscere:

a) le finalità del trattamento;
b) le categorie dei dati personali di cui il titolare è in possesso;
c) i destinatari cui i dati sono stati o saranno comunicati, specificando in particolare se si tratta di soggetti che si trovano in paesi terzi rispetto all'Unione Europea o se si tratta di organizzazioni internazionali. In particolare, qualora ricorra una di queste ultime ipotesi, l'interessato ha anche il diritto di essere informato sull'esistenza di adeguate garanzie concernenti il trasferimento dei suoi dati personali (uscendo in questi casi, almeno parzialmente dalla copertura del GDPR), come precisato nel Capo V del GDPR, dedicato proprio ai trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali;
d) se possibile, la durata prestabilita del periodo di conservazione dei dati o quanto meno i criteri cui il titolare fa riferimento per determinare tale durata;
e) l'esistenza del suo diritto: (I) a chiedere la rettifica o la cancellazione dei dati (quindi la modifica, ad esempio, se i dati raccolti sono errati o sono cambiati rispetto al momento del loro ottenimento oppure la loro eliminazione, come nel caso in cui sia decorso il periodo di conservazione previsto o i dati siano detenuti illegittimamente dal titolare), (II) a chiedere la limitazione del trattamento dei dati personali (quando ne viene fatto un utilizzo che va oltre quanto consentito dall'interessato, ad esempio, perché eccedente rispetto allo scopo comunicato nell'informativa al momento della raccolta o semplicemente perché l'interessato ha avuto un ripensamento – come può accadere quando viene chiesto di non ricevere più determinate comunicazioni commerciali) e (III) ad opporsi al loro trattamento, perché ritenuto illegittimo;
f) il diritto di proporre un reclamo all'autorità di controllo (ovvero al Garante per la protezione dei dati personali) quando l'interessato ritiene che vi sia stata violazione dei propri diritti o delle proprie libertà;
g) tutte le informazioni disponibili sull'origine dei dati nel caso in cui non siano stati raccolti presso l'interessato, ma ricevuti da soggetti terzi (ai quali l'interessato potrebbe aver dato il consenso anche a tal fine) oppure ottenuti tramite elenchi pubblici;
h) infine, la logica su cui è basato un processo automatizzato, come ad esempio la profilazione, e il funzionamento di tali meccanismi e le possibili conseguenze del loro utilizzo (ovvero in cosa consistono sostanzialmente, quali dati e come vengono elaborati).

Vista la varietà di informazioni e considerato che alcune di esse possono variare nel corso del tempo (si pensi al periodo di conservazione, se non predeterminato fin dall'inizio del trattamento o all'utilizzo di meccanismi di profilazione), il diritto d'accesso può essere esercitato anche più volte e persino con una cadenza periodica, perché solo mediante un controllo costante l'interessato sarà davvero consapevole delle attività che riguardano i propri dati personali. Addirittura, nella logica del GDPR viene consigliato ai titolari di creare un sistema per consentire all'interessato l'accesso remoto a un sistema sicuro che gli permetta di verificare direttamente i propri dati

Come puntualizzato poi dall'art. 12, paragrafo 3, l'interessato ha il diritto di ricevere dal titolare le informazioni richieste esercitando il proprio diritto di accesso il prima possibile e, comunque, al massimo entro un mese. Soltanto in casi particolari, ad esempio quando le richieste siano molto numerose oppure le informazioni da fornire siano particolarmente complesse, il titolare potrà estendere questo termine ad un periodo massimo di due mesi, informando però, sempre entro un mese dalla sua richiesta, l'interessato della necessità di proroga e dei relativi motivi che l'hanno resa necessaria (per esempio, i tempi tecnici necessari al titolare per reperire le informazioni e per preparare la documentazione).

Si configura in questo modo l'obbligo per il titolare (o per il responsabile, se presente) di riscontrare sempre la richiesta dell'interessato entro un mese dalla ricezione, anche nel caso in cui non intenda ottemperare (il comma 4 dell'art. 12 GDPR prevede infatti che "*Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale*").

Le informazioni dovranno essere date a titolo gratuito all'interessato, salvo il caso eccezionale in cui il titolare debba sostenere delle spese tecniche rilevanti per adempiere (ad esempio, qualora siano state richieste più copie, art. 15, co. 3, GDPR) oppure le richieste dell'interessato siano risultate infondate o eccessive (art. 12, co. 5, GDPR): in presenza di simili condizioni, il titolare potrà, quindi, addebitare, entro limiti ragionevoli all'interessato una parte delle spese e richiedergli il versamento di un contributo.

Di norma, poi, la risposta dovrà essere data in forma scritta, assecondando però, per quanto possibile, le eventuali modalità richieste specificamente dall'interessato (ad esempio, se l'interessato chiede che le informazioni siano fornite oralmente). Lo stesso Regolamento, poi, precisa che quando l'interessato avanza delle richieste utilizzando mezzi elettronici, anche le risposte da parte del titolare dovranno fare ricorso alle medesime modalità (art. 15, co. 3, GDPR: "*Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune*").

Infine, due precisazioni sono necessarie: per prima cosa, il titolare è tenuto ad adottare anche in questo contesto tutte le misure di sicurezza adeguate, prime tra tutte quelle atte a verificare l'identità di chi chiede l'accesso, con particolare attenzione ai casi in cui ciò avvenga direttamente online. In secondo luogo, l'esercizio del diritto in esame non deve creare delle violazioni a diritti di altri soggetti: il Considerando n. 63, al riguardo, a titolo esemplificativo, fa riferimento ai segreti industriali e ai diritti di proprietà industriale (si pensi alla tutela dei diritti d'autore relativi a software).

8. Il "diritto all'oblio"

Il ***diritto all'oblio*** con l'entrata in vigore del nuovo Regolamento Generale sulla Protezione dei Dati Personali riceve finalmente un'espressa disciplina che ne indica portata e limiti.

Questo diritto, che non ha carattere assoluto in quanto dev'essere inevitabilmente contemperato con altri interessi (primo fra tutti il diritto alla libertà di espressione e di informazione), può essere definito come l'interesse di un singolo ad essere dimenticato. La sua esplicazione consiste infatti nella cancellazione dei propri dati personali e nella pretesa che tali informazioni non vengano più fatte oggetto di trattamento: in particolare, qualora si rientro nell'ambito di un trattamento on line, tale diritto si realizza attraverso la rimozione dei contenuti, dalle varie pagine web, di precedenti informazioni relative ad un interessato.

Il diritto all'oblio oggi riceve dunque un'espressa e precisa regolamentazione nell'art. 17 (intitolato "Diritto alla cancellazione («diritto all'oblio»), secondo il quale: "*1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1. 2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. 3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria*"),che ne specifica la portata, i presupposti e le limitazioni.

In primo luogo questo diritto si configura come diritto alla cancellazione dei dati personali: in sostanza, al ricorrere di una delle condizioni previste dal GDPR, i soggetti interessati potranno esigere la cancellazione dei propri dati personali da parte del titolare del trattamento, sul quale ricade l'obbligo di attivarsi in tal senso senza ritardo.

Ad esempio, l'interessato può richiedere la cancellazione dei dati personali che lo riguardano quando:

- i dati non sono più necessari rispetto alle finalità per le quali furono raccolti o trattati: ad esempio, se ordino un prodotto online e comunico il mio indirizzo soltanto per questo scopo, il titolare non potrà poi utilizzare questo dato per inviarmi dei dépliant pubblicitari. Qualora lo faccia, potrò chiedere che proceda a cancellare tali informazioni, non essendo più legittimato a conservarne traccia;
- l'interessato ha revocato il consenso e non sussiste altro fondamento giuridico per il trattamento. Anche in questo caso la situazione è semplice: se prima acconsento, ad esempio, all'invio di materiale pubblicitario e poi cambio idea, oppure se non ha più efficacia un contratto

precedentemente in essere, il titolare non può legittimamente continuare a trattare i miei dati e io posso chiederne la cancellazione;

- l'interessato si oppone al trattamento dei dati (sul tema si invita a leggere l'apposito approfondimento a seguire) e non sussiste alcun motivo legittimo prevalente per proseguire tale trattamento;
- i dati sono stati trattati illecitamente: in presenza di una qualsiasi violazione della normativa in tema di protezione di dati personali, il titolare non può continuare ad utilizzare tali informazioni e ciascun interessato può chiederne quindi la cancellazione;

A questo diritto si associa, ovviamente, l'obbligo in capo al titolare del trattamento di cancellare i dati ma anche - e questo può risultare problematico - di comunicare la richiesta di cancellazione agli altri titolari che stiano trattando quelle informazioni. Si capisce, infatti, che se l'obiettivo è interrompere definitivamente ogni trattamento relativo a quei dati (e abbiamo visto che sostanzialmente l'interessato può farlo quando mancano i presupposti per un trattamento legittimo) ed impedirne un futuro utilizzo, è necessario che sia eliminato qualsiasi link, copia o riproduzione dei dati oggetto della richiesta. Diversamente il diritto dell'interessato potrebbe essere agevolmente eluso dai vari titolari in possesso di quelle informazioni.

Il diritto all'oblio non può peraltro essere esercitato in modo assoluto: come precisato infatti in alcune ipotesi eccezionali risulteranno prevalenti altri diritti. L'esercizio di tale diritto potrà, in particolare, essere limitato o impedito nel caso in cui il trattamento dei dati sia necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'esercizio del diritto di difesa in sede giudiziaria;
- per motivi di interesse pubblico generale di tutela della salute pubblica;
- per l'adempimento di un obbligo di legge o per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri.

Si intuisce già che i problemi principali, anche in assenza di un'espressa previsione, si presenteranno per effettuare un bilanciamento tra il diritto all'oblio e il diritto all'informazione. Resterà sul punto da vedere come questa norma verrà applicata concretamente dalle Autorità nazionali: è probabile, peraltro, che un grosso aiuto verrà dall'interpretazione complessiva dei principi a fondamento del GDPR, in particolare dal rispetto dei principi di esattezza dei dati e di liceità del trattamento. Una violazione di tali norme spingerà infatti verso una prevalenza della protezione di dati personali, in quanto il trattamento effettuato sarà da considerare illegittimo.

Infine un'altra ipotesi specifica prevista dal GDPR al ricorrere della quale il diritto all'oblio è destinato a soccombere si verifica quando i dati siano necessari a fini di archiviazione, di ricerca storica o scientifica o di analisi statistica: si noti, però, che in questo caso i dati potranno essere utilizzati una volta resi anonimi.

Come previsto poi dall'art. 19 ("*Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda*"), il titolare del trattamento dovrà comunicare l'avvenuta cancellazione dei dati personali anche ai destinatari ai quali tali dati siano stati trasmessi, a meno che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Inoltre, se c'è la richiesta dell'interessato, il titolare del trattamento gli dovrà comunicare informazioni relative a tali destinatari per rendere possibile un controllo diretto ed una verifica particolare da parte dello stesso interessato.

9. *Rettifica, limitazione ed opposizione*

Gli artt. 16, 18 e 21 del GDPR prevedono altri importanti diritti in capo al soggetto interessato quali: il diritto di rettifica dei dati; il diritto di limitazione del trattamento e il diritto di opposizione.

Il ***diritto di rettifica***, pur essendo già in precedenza riconosciuto sia nel diritto europeo che nell'ordinamento italiano, trova nel GDPR una più forte affermazione (art. 16: "*L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa*"). Rientra infatti tra gli obiettivi di fondo del Regolamento permettere all'interessato di mantenere un controllo costante e attivo sui propri dati e sull'utilizzo che ne viene fatto: da questa prospettiva si intuisce che la possibilità di far correggere o modificare i dati quando gli stessi risultino errati, non aggiornati o insufficienti è una condizione imprescindibile, anche per evitare che da eventuali trasferimenti ed attività conseguano gravi pregiudizi per l'interessato, ma anche per il titolare (si pensi ad esempio alle conseguenze di un'operazione di profilazione effettuata su dati errati). In particolare, quindi, attraverso il riconoscimento di questo diritto l'interessato avrà la possibilità di ottenere dal titolare del trattamento la correzione senza ritardo dei dati inesatti che lo riguardano. Inoltre, tenuto conto delle finalità del trattamento, l'interessato potrà ottenere l'integrazione dei propri dati incompleti, anche fornendo una dichiarazione integrativa.

È opportuno che anche per l'esercizio di questo diritto siano predisposti strumenti e sistemi in grado di facilitare l'accesso diretto dell'interessato alle informazioni che lo riguardano, così da permettergli di intervenire prontamente e, per quanto possibile, autonomamente per modificare dai dati inesatti.

Il ***diritto di limitazione*** del trattamento è invece stato introdotto *ex novo* dal GDPR, anche se per certi versi poteva ricavarsi in via interpretativa dalle precedenti disposizioni. Tale diritto presenta, ad ogni modo, caratteri innovativi e più ampi rispetto a quelli già delineati dalle regole in materia, come può emergere dal confronto con l'art. 7, comma 3 del Codice Privacy, che non conteneva alcun riferimento alla "limitazione" (secondo tale articolo, infatti: "*L'interessato ha diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato*").

In particolare, il riconoscimento di questo diritto consente all'interessato di pretendere una limitazione dell'uso che il titolare fa dei propri dati. Una simile richiesta peraltro trova fondamento al ricorrere di determinate condizioni che l'art. 18 elenca specificamente:

a) qualora l'interessato contesti l'esattezza dei dati personali, per il periodo necessario al fine di verificarne l'esattezza (ovvero il trattamento è "congelato" nel tempo tecnico richiesto per verificare se i dati siano esatti o meno, dopodiché si agirà di conseguenza, correggendo o integrando i dati);
b) quando il trattamento dei dati sia illecito e l'interessato si opponga alla loro cancellazione, preferendo che ne sia disposta una limitazione d'utilizzo;
c) quando il titolare non abbia più bisogno di conservare i dati ai fini del trattamento, ma essi sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) infine, quando l'interessato si sia opposto al trattamento nell'attesa delle necessarie verifiche sulla prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Come si evince dal termine stesso, in queste ipotesi i dati non vengono cancellati ma ne viene ridotto l'utilizzo consentito da parte del titolare. In linea di massima, quindi, i dati potranno essere trattati solo ai fini della loro conservazione, a meno che vi sia il consenso dell'interessato o il trattamento sia necessario per l'esercizio o la difesa di un diritto in sede giudiziaria, per la tutela dei diritti di un'altra persona o per ragioni di interesse pubblico rilevante. La limitazione potrà essere in seguito revocata e in questo caso, prima che ciò avvenga, il titolare del trattamento dovrà informare specificamente l'interessato.

Per quanto riguarda le modalità per limitare il trattamento dei dati, tra le possibili soluzioni suggerite ai titolari vi è il trasferimento temporaneo dei dati selezionati verso un altro sistema di trattamento o la rimozione provvisoria dei dati pubblicati da un sito web o l'inaccessibilità per gli utenti.

Il Considerando 67 precisa, in particolare, che "*negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato*".

Come previsto dall'art. 19 (in forza del quale "*Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda*") nel caso in cui sia fatto valere il diritto di rettifica o di limitazione del trattamento dei dati personali il titolare del trattamento dovrà comunicare le eventuali correzioni o limitazioni del trattamento ai destinatari cui i dati siano stati trasmessi, a meno che risulti essere impossibile o implichi uno sforzo sproporzionato. Inoltre, anche in questo caso in presenza di una richiesta dell'interessato, il titolare del trattamento gli dovrà comunicare informazioni relative a tali destinatari (al riguardo si veda anche l'articolo dedicato al diritto all'oblio).

Infine il GDPR sancisce, all'art. 21, che l'interessato ha il ***diritto di opporsi*** in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni.

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

Nel caso in cui l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità. Il diritto di cui sopra è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Il diritto di opposizione che per definizione consiste nel diritto dell'interessato di opporsi in qualsiasi momento, e per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano. Conseguenza dell'esercizio di tale diritto è l'obbligo, in capo al titolare, di astenersi dal trattamento dei dati. Questo particolare diritto riguarda però situazioni in cui il titolare sta lecitamente trattando dei dati personali: pertanto, è riconosciuta la facoltà per il titolare di dimostrare che i suoi interessi specifici connessi al trattamento prevalgono su quelli evidenziati dall'interessato.

Nel caso in cui i dati personali siano trattati con finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento e gratuitamente al trattamento, anche (e soprattutto) nel caso in cui questo avvenga mediante attività di profilazione. Questa previsione è particolarmente innovativa e di grande tutela per l'interessato, al quale infatti tale possibilità deve essere resa nota dal titolare in maniera chiara, esplicita e separatamente rispetto alle altre informazioni: non potrà, ad esempio, ritenersi corretto un generico riferimento nell'informativa ai diritti riconosciuti dal GDPR, ma sarà necessario evidenziare in modo facilmente intellegibile per l'interessato l'esistenza e la portata del diritto di opposizione.

10. Il Titolare del Trattamento dei Dati Personali

Il GDPR delinea la figura del ***titolare del trattamento*** negli stessi termini previsti dalla Direttiva 95/46/CE e dal Codice Privacy. Come risulta infatti dall'art. 4, paragrafo 1, n. 7) del GDPR, il titolare del trattamento è definito come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*". Ciò che consente di individuare il soggetto titolare del trattamento è, pertanto, il potere decisionale a lui imputabile in ordine al trattamento dei dati personali.

In particolare, come precisato anche dal Garante per la protezione dei dati personali (Provvedimento del 29 aprile 2009, che tuttora si può ritenere appropriato), il titolare del trattamento dei dati è individuabile come quella figura che ha il potere di:

a) prendere decisioni in relazione alle finalità del trattamento;
b) impartire istruzioni e direttive;
c) svolgere funzioni di controllo.

La norma prosegue poi precisando che, nei casi in cui le finalità e i mezzi del trattamento siano determinati direttamente dal diritto dell'Unione o degli Stati membri, anche il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti a monte a livello legislativo (europeo o nazionale).

Sotto il profilo soggettivo è opportuno precisare, come risulta anche dall'art. 28 del Codice Privacy, che nel caso in cui il trattamento dei dati sia effettuato da una persona giuridica, titolare del trattamento dovrà essere considerata l'entità nel suo complesso, e non i singoli soggetti - persone fisiche- che amministrano o rappresentano la persona giuridica in questione.

A tale proposito, il Garante per la protezione dei dati personali con una circolare del 13 novembre 1997, e riferendosi all'abrogata L. 675/1996, ebbe già a suo tempo modo di chiarire che "*qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il "titolare" è l'entità nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.), anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono,* *in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno (ad esempio, l'amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.)*"

Per quanto riguarda le novità introdotte dal GDPR, l'art. 30, comma 1, prevede in capo al Titolare del trattamento (e anche al suo rappresentante, se presente) l'obbligo di tenere il ***registro delle attività di trattamento*** svolte sotto la sua responsabilità. Si tratta di un registro che deve essere redatto in forma scritta, *anche in formato elettronico*, ed è obbligatorio quando l'organizzazione ha più di 250 dipendenti (anche se il Garante suggerisce che tale registro sia tenuto pure dalle strutture che hanno dimensioni inferiori).

In particolare, il registro dei trattamenti (su cui si rinvia *infra* al paragrafo 18 del presente documento) deve contenere una serie di informazioni, quali:

1. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
2. le finalità del trattamento;
3. una descrizione delle categorie di interessati e delle categorie di dati personali;
4. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
5. i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
6. i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
7. una descrizione generale delle misure tecniche e organizzative adottate per garantire la sicurezza dei dati.

Un altro elemento di novità che il GDPR introduce consiste nella possibile ***contitolarità del medesimo trattamento da parte di due o più titolari*** (art. 26: "*1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati. 2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato. 3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento*").

Il Regolamento prescrive che, in questa circostanza, i titolari dovranno definire specificamente le rispettive sfere di responsabilità e i rispettivi compiti, con particolare riferimento all'osservanza degli obblighi derivanti dal GDPR, all'esercizio dei diritti dell'interessato, e alle rispettive funzioni di comunicazione delle informazioni da fornire all'interessato. Questi elementi dovranno essere parte di un apposito accordo interno tra i contitolari del trattamento, i cui contenuti essenziali dovranno essere messi a disposizione dell'interessato stesso.

Nel caso in cui si configuri un'ipotesi di contitolarità, il soggetto interessato avrà inoltre, secondo quanto disposto dall'art. 26, paragrafo 3, la facoltà di esercitare i diritti che il Regolamento gli riconosce (quali, ad esempio, il diritto di accesso, il diritto all'oblio, il diritto alla limitazione del trattamento, il diritto all'opposizione e il diritto alla portabilità dei dati) nei confronti di ciascun titolare del trattamento, indifferentemente.

Un'ipotesi particolare presa in considerazione dal GDPR è poi quella in cui ***il titolare del trattamento (o il responsabile del trattamento, se nominato) non siano stabiliti nel territorio dell'Unione Europea***. Come previsto infatti dall'art. 3, paragrafo 2, infatti, il Regolamento si applica anche "*al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*

I. *l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure*
II. *il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione*".

In questi casi il Regolamento stabilisce, all'art. 27, che il titolare del trattamento è tenuto ad individuare per iscritto un suo rappresentante all'interno dell'Unione.

Questo obbligo tuttavia non si applica in due ipotesi, in cui il GDPR presume che i diritti dell'interessato siano comunque sufficientemente tutelati, che si verificano:

- quando il trattamento è occasionale, non implica il trattamento di dati "sensibili" (quali: i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, biometrici o relativi allo stato di salute o all'orientamento sessuale della persona), o di dati personali relativi a condanne penali o a reati consistenti nell'illiceità del trattamento dei dati, ed è improbabile che comporti un rischio per i diritti e le libertà delle persone tenendo anche in considerazione la natura, il contesto, l'ambito di applicazione e le finalità del trattamento stesso; oppure
- quando titolare del trattamento è un'autorità pubblica o comunque un organismo pubblico.

Quando, invece, il rappresentante deve esserci, lo stesso dovrà essere stabilito in uno degli Stati membri in cui si trovano i soggetti interessati i cui dati personali sono trattati nel contesto di un'offerta di beni o servizi o il cui comportamento è monitorato.

Al fine di agevolare la comunicazione con i soggetti interessati e con le autorità è infine previsto che il rappresentante possa essere incaricato dal titolare del trattamento (o, se nominato, dal responsabile) a fungere da interlocutore -in aggiunta o anche in sostituzione al titolare stesso- con le autorità di controllo e con gli interessati per tutte le questioni relative al trattamento dei dati personali.

Ad ogni modo, anche nel caso in cui sia stato nominato un rappresentante del titolare straniero, rimane sempre salva la possibilità di agire legalmente direttamente nei confronti del titolare del trattamento.

11. Il Responsabile del Trattamento dei Dati

Come nel caso del titolare del trattamento, anche la figura del ***responsabile del trattamento dei dati*** - sotto il profilo delle sue caratteristiche soggettive e delle sue responsabilità - è definito dal GDPR negli stessi termini già previsti dalla Direttiva 95/46/CE e dal Codice Privacy.

In particolare, con il termine "responsabile del trattamento" il GDPR si riferisce alla "*persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*" (art. 4, paragrafo 1, n. 8). Si tratta quindi del soggetto preposto ed al quale viene affidato, da parte del titolare, il trattamento dei dati personali.

Per quanto riguarda i requisiti soggettivi che il responsabile del trattamento deve possedere, il GDPR prevede che si tratti di una figura in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato (art. 28, co. 1, GDPR: "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*").

A questo proposito, come specificato dal Considerando 81, le garanzie che il responsabile del trattamento deve essere in grado di fornire si sostanziano in: una conoscenza specialistica della materia, affidabilità e possesso di risorse che permettano di attuare misure tecniche e organizzative in grado di soddisfare tutti i requisiti stabiliti dal Regolamento per il trattamento dei dati personali, anche sotto il profilo della sicurezza.

Il Responsabile del trattamento dovrà quindi avere una competenza qualificata, che potrà essere comprovata da apposita documentazione (rilasciata, ad esempio, in seguito alla frequentazione di corsi qualificati, benché non esistano attualmente particolari abilitazioni o il possesso di specifiche certificazioni). Per quanto riguarda invece il profilo dell'affidabilità, questo requisito dovrà essere fondato su aspetti etico-deontologici, che potrebbero essere dimostrati, ad esempio, con semplici autocertificazioni, anche per escludere eventuali condanne che possano essere rilevanti al riguardo.

A questo proposito, si ricorda che già il Codice della Privacy prevede, all'art. 29, comma 2, che "*Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza*".

Non si ravvisano quindi particolari novità nel GDPR, se non per il fatto che il Responsabile deve disporre di sufficienti risorse per mettere in atto le misure tecniche ed organizzative che soddisfino quanto richiesto dal Regolamento. Il Responsabile deve, pertanto, avere a disposizione sufficienti disponibilità sia economiche, sia di personale, e più in generale deve poter disporre di tutti i mezzi necessari allo svolgimento dei compiti affidati dal Titolare. Nel caso in cui il Responsabile del trattamento dei dati sia un soggetto interno all'organizzazione, sarà lo stesso Titolare del trattamento a dover fornire tali risorse; se invece il servizio viene affidato all'esterno, sarà autonomamente il Responsabile nominato a prevedere adeguate risorse per lo svolgimento dell'incarico nel rispetto del GDPR.

Il Responsabile del trattamento dei dati potrebbe, come anticipato, essere tanto una figura interna all'azienda, quanto esterna. A questo proposito, il Garante della Privacy, alla luce della disciplina interna aveva precisato che: "*è necessario precisare chi svolgerà l'eventuale ruolo di "responsabile del trattamento*". Conseguentemente, l'Amministrazione deve decidere se prevedere tale figura ed attribuirne la responsabilità o alla struttura esterna cui è affidata l'attività in concessione, oppure ad un dipendente di quest'ultima, o a un proprio ufficio o dipendente dell'Amministrazione stessa (quest'ultima opzione presuppone che l'ufficio o il funzionario pubblico abbiano poteri effettivi di ingerenza sulle attività e sull'organizzazione dell'impresa concessionaria: cosa, in realtà, poco frequente). In concreto, la nomina del responsabile, che deve essere effettuata in forma scritta, potrebbe essere inserita in un apposito articolo della convenzione, oppure essere oggetto di un distinto provvedimento amministrativo o atto di diritto privato.

In realtà, altri Stati membri hanno sempre individuato questo ruolo come spettante a soggetti esterni rispetto al titolare del trattamento e l'assenza di specificazioni all'interno del GDPR sta dando luogo ad alcune divergenti interpretazioni al riguardo. D'altra parte, in assenza di ulteriori precisazioni, è opportuno ritenere che rimanga valida la facoltà di scelta, come fino ad oggi prevista dal nostro ordinamento.

Il Responsabile del trattamento è obbligato (come previsto dall'art. 28, comma 3 del GDPR), in forza del contratto stipulato con il titolare, a:

I. trattare i dati personali solo sulla base di un'istruzione documentata del titolare del trattamento, anche nel caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale a meno che lo richieda il diritto dell'Unione Europea o nazionale cui è soggetto il responsabile del trattamento. In quest'ultimo caso, il responsabile del trattamento dovrà informare il titolare dell'esistenza di un tale obbligo giuridico prima del trattamento, a meno che ciò sia giuridicamente vietato per rilevanti motivi di interesse pubblico;
II. garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
III. adottare tutte le misure richieste dall'art. 32 GDPR, ovvero le misure tecniche e organizzative necessarie al fine di garantire un livello di sicurezza adeguato al rischio (ad esempio, la pseudomizzazione dei dati o la cifratura)
IV. rispettare tutte le condizioni previste per l'eventuale nomina di un sub-responsabile;
V. assistere il titolare del trattamento con misure tecniche e organizzative adeguate, e tenuto conto della natura del trattamento, al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (quali il diritto di accesso ai dati personali, il diritto di rettifica, il diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati, il diritto di opposizione);
VI. assistere il titolare del trattamento nel garantire il rispetto degli obblighi in materia di tutela della sicurezza dei dati, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
VII. cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento (su indicazione del titolare del trattamento), nonché cancellarne le eventuali copie esistenti; e infine
VIII. mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto dei suoi obblighi, nonché contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da lui incaricato. Il responsabile deve, inoltre, informare immediatamente il titolare del trattamento ritenga che un'istruzione violi il Regolamento o altre disposizioni nazionali o di diritto europeo relative alla protezione dei dati.

Il Titolare deve scegliere il Responsabile *solo se in possesso di garanzie sufficienti per porre in essere le misure tecniche ed organizzative adeguate* al rispetto del GDPR ed alla tutela dei diritti dell'interessato sicché in caso di *data breach* imputabile a colpa del Responsabile, sarà il Titolare a rispondere di tale violazione (a titolo di *culpa in eligiendo*): si crea, in sostanza, un sistema piramidale in base al quale il Responsabile è (si scusi il gioco di parole) *responsabile* verso il Titolare il quale, a sua volta, è responsabile verso gli interessati e verso il Garante. Per questa ragione il contratto (o altro atto giuridico) che vincola il Responsabile al Titolare deve avere un contenuto *minimo* consistente nell'indicare: a) la materia oggetto del trattamento; b) la durata, natura e finalità del trattamento; c) i tipi dei dati degli interessati soggetti al trattamento; d) gli obblighi ed i diritti del Titolare nei confronti del Responsabile.

Anche in capo al Responsabile del trattamento il GDPR pone l'obbligo di tenere il registro dei trattamenti svolti per conto del titolare del trattamento (art. 30, comma 2, GDPR), nel quale vanno riportate dettagliatamente una serie di indicazioni relative ai trattamenti di dati effettuati.

12. Responsabilità ed obblighi del Titolare e del Responsabile

Come stabilito dall'art. 82, comma 1 del GDPR: "*Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*".

È previsto quindi il diritto dell'interessato (in quanto danneggiato) di ottenere il risarcimento del danno, sia patrimoniale sia non patrimoniale, nel caso in cui sia stata posta in essere una condotta, attiva o omissiva, che integri una violazione del Regolamento. E sono tenuti al risarcimento del danno sia il titolare che il responsabile del trattamento.

In particolare, il titolare del trattamento risponderà per il danno cagionato dal trattamento dei dati personali realizzato in violazione del regolamento (come previsto dall'art. 82, comma 2, GDPR: "*Il soggetto titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento*").

Il responsabile del trattamento risponderà, invece, per il danno causato dal trattamento solo se non ha adempiuto correttamente agli obblighi sanciti nel GDPR in capo ai responsabili del trattamento, oppure se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

È stato osservato che questa norma sembra configurare profili di responsabilità molto ristretti in capo al titolare ed al responsabile del trattamento. Questa considerazione non è tuttavia corretta se si pensa che deve essere interpretata anche alla luce del Considerando n. 146, per quanto riguarda la figura del titolare del trattamento e dell'art. 28, comma 3, per quanto riguarda invece il responsabile del trattamento.

In sostanza, in questo modo si stabilisce che il titolare sarà responsabile non solo in caso di violazione delle disposizioni del GDPR, ma anche nel caso di inosservanza delle altre disposizioni previste dalle norme attuative, dagli atti delegati, dagli atti di esecuzione del Regolamento e dalle altre disposizioni dei singoli stati membri (il Considerando n. 146 stabilisce infatti che le violazioni del regolamento non pregiudicano "*[…] le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito […]*").

Quanto al responsabile del trattamento, la sua responsabilità sembrerebbe essere circoscritta alle sole azioni od omissioni in relazione all'osservanza delle disposizioni del GDPR, nonché al rispetto delle indicazioni e delle direttive del titolare del trattamento. In realtà, il responsabile del trattamento ha anche un dovere generale, nel senso che è suo compito anche quello di avvisare il titolare del trattamento delle eventuali condotte che risultano non correttamente disciplinate dallo stesso titolare. Sarà quindi possibile configurare a suo carico una responsabilità per omessa informazione nei confronti del titolare del trattamento.

Il titolare del trattamento o il responsabile del trattamento saranno, però, esonerati dalla responsabilità se riescono a dimostrare che l'evento dannoso non è in alcun modo imputabile alla loro condotta, e quindi che il danno è scaturito da una fonte "estranea" al loro raggio d'azione, oppure se dimostrano di aver adottato tutte le misure idonee al fine di evitare il danno stesso.

Qualora più titolari o responsabili del trattamento siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato per effetto del trattamento, ogni titolare o responsabile sarà responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento integrale del danno subito dall'interessato. L'art. 82, comma 4 prevede, a questo proposito, che "*Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato*".

Nel caso in cui, poi, un titolare o un responsabile abbia pagato l'intero risarcimento del danno, avrà il diritto di reclamare dagli altri titolari o responsabili - coinvolti nello stesso trattamento - la parte del risarcimento corrispondente alla loro parte di responsabilità.

La norma è interessante in quanto disciplina le conseguenze patrimoniali derivanti dal danno, nei rapporti interni tra titolare/i e responsabile/i del trattamento dei dati: una responsabilità che si configura "per quote", ossia sulla base delle diverse "porzioni" di responsabilità che possono essere delineate in capo alle diverse figure coinvolte.

Questo è quanto è stabilito dall'art. 82, comma 5 che dispone: "*Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2*".

13. Il Data Protection Officer

Il ***responsabile della protezione dei dati*** è un consulente, esperto e qualificato, che affianca il titolare nella gestione delle questioni connesse al trattamento dei dati personali e lo aiuta a rispettare la normativa vigente. Il DPO viene introdotto per la prima volta nel nostro ordinamento dal GDPR: il ruolo di tale figura è da tenere ben distinto da quello del responsabile del trattamento, che, come detto sopra, è il soggetto che affianca per compiti e responsabilità il titolare stesso (per facilitare questa distinzione ed evitare confusione si preferisce, e si è maggiormente diffuso, l'utilizzo del termine inglese ***Data Protection Officer*** e del relativo acronimo ***DPO***) ([20]).

Analizzando la nuova disciplina, emerge che il DPO è una figura nominata dal titolare o dal responsabile del trattamento che può essere selezionata tra gli stessi dipendenti del titolare del trattamento o può essere un libero professionista, esterno e autonomo, appositamente incaricato di svolgere questo ruolo in forza di un contratto di servizi.

In ogni caso, come previsto dall'art. 38, commi 1 e 2 del GDPR, il DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni relative alla protezione dei dati, e pertanto il titolare o il responsabile del trattamento dovranno assicurarsi che abbia a disposizione tutte le risorse (umane ed economiche) necessarie per lo svolgimento dei suoi compiti. Le norme appena richiamate così stabiliscono: "*1. Il titolare del trattamento e il responsabile*

[20] Il DPO viene nominato dal Titolare e dal Responsabile e deve svolgere i compiti assegnati dall'Art. 39 GDPR: sebbene molti commentatori abbiano profuso grandi energie in relazione a questa figura, trattasi di un soggetto marginale in quanto la sua nomina è *obbligatoria* solo per i trattamenti dati eseguiti da PA o da organismi pubblici (fatta eccezione per quelli di natura giurisdizionale), i Titolari ed i Responsabili la cui attività *principale* sia un trattamento che richiede un monitoraggio sistematico degli interessati *su larga scala* nonché quelli la cui attività *principale* sia il trattamento *su larga scala* di *dati particolari e condanne penale o reati*. Se il concetto di *attività principale* non crea problemi (es. un ospedale rispetto al trattamento dei dati dei pazienti) il concetto di *larga scala* implica un riferimento (ancorché vago, in quanto legato al comune sentire) alla *quantità* dei dati ed al *numero* degli interessati (sicché il singolo trattamento eseguito da un medico di un ospedale non vi rientra). Sono sicuramente parametri significativi (oltre alla quantità dei dati ed al numero degli interessati) anche la *durata e la sistematicità* dei trattamenti nonché l'*estensione geografica* degli stessi.

del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica".

Il DPO, per poter essere nominato, deve poi essere in possesso di alcuni requisiti, in particolare:

I. deve avere un'idonea competenza e conoscenza della normativa e della prassi in materia di gestione dei dati personali, anche con riferimento alle misure tecniche e organizzative necessarie per garantire la sicurezza dei dati personali. Non è necessario che sia in possesso di attestazioni formali, né che sia iscritto in un apposito albo professionale, ma la frequentazione di un corso di perfezionamento o di un master può essere uno strumento adeguato a dimostrare il raggiungimento di un livello adeguato di conoscenza. Non esistono attualmente delle abilitazioni né delle certificazioni particolari o necessarie: certo, rivolgersi ad un soggetto che possa garantire e dimostrare seriamente una competenza qualificata nella materia è, prima di tutto, interesse dello stesso titolare, sul quale, in ultimo, si ripercuotono le effettive capacità del DPO;
II. deve essere una figura autonoma e indipendente e deve svolgere le sue funzioni in assenza di conflitto di interesse, quindi non potrà essere un soggetto che prende decisioni sulle finalità o sugli strumenti da utilizzare per il trattamento dei dati personali. Tale ruolo non potrà quindi essere svolto da soggetti che si trovano ai vertici di un'azienda e che possono gestire o influenzare le soluzioni e le scelte concretamente adottate in tema di trattamento di dati personali.

Questa indicazione risulta specificata anzitutto dal comma 3 dell'art. 38 del GDPR, laddove è previsto che il DPO non debba ricevere alcuna istruzione relativamente all'esecuzione dei suoi compiti e che si riferisca direttamente ai vertici aziendali, quindi non al titolare o al responsabile del trattamento. La norma prevede infatti: "*Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento*". In secondo luogo, il comma 6 dell'art. 38 stabilisce che il DPO possa svolgere anche altri compiti e funzioni, ma questi non devono dar luogo a un conflitto d'interessi.

Emerge chiaramente il fatto che il legislatore europeo, attraverso l'introduzione di questa figura professionale specifica, abbia voluto innanzitutto spostare da un soggetto (il titolare o il responsabile del trattamento) ad un altro (il DPO) una serie di compiti in ambito di protezione dei dati personali, ferma restando la responsabilità in capo al titolare del trattamento.

In secondo luogo, attraverso la previsione di questa figura, sarà possibile garantire che un soggetto specializzato ed esperto in materia si occupi esclusivamente della protezione dei dati personali, rimanendo sempre aggiornato sui rischi, sui problemi e sulle misure di sicurezza necessarie al fine di garantire un livello di tutela adeguato. Tutto questo è stato stabilito tenendo conto della sempre maggiore diffusione e complessità (e della conseguente attenzione e cautela da dedicare) che il settore della protezione e del trattamento dei dati personali sta avendo, anche in considerazione del ruolo del web, sempre più importante ed invasivo.

14. Le responsabilità del DPO

Il DPO ha, innanzitutto, il compito di vigilare sull'osservanza del GDPR da parte dei titolari che gli affidano tale incarico. Come emerge dall'art. 39, comma 1, lettera b), infatti, il DPO viene incaricato, tra gli altri compiti, anche di: "*sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo*".

Fanno parte di questi compiti di controllo svolti dal DPO:

I. la raccolta di informazioni per individuare i trattamenti svolti;
II. l'analisi e la verifica della conformità dei trattamenti;
III. l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile. Come precisato dall'art. 39, comma 1, lettera a).

Attenzione, però: il controllo del rispetto del Regolamento non significa che il DPO sia personalmente responsabile in caso di inosservanza degli obblighi in materia di protezione dei dati personali. Il GDPR, all'art. 24, comma 1, chiarisce infatti che è compito del titolare (e non del DPO) mettere in atto le misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento. La responsabilità di garantire il rispetto della normativa in materia di protezione dei dati ricade quindi sul titolare del trattamento o sul responsabile del trattamento.

Altro ruolo di grande importanza attribuito al DPO è poi quello di assistere il titolare del trattamento dei dati nello svolgimento della "*valutazione d'impatto sulla protezione dei dati*" che, come previsto dall'art. 35, comma 1 del GDPR, è un onere posto direttamente in capo al titolare del trattamento. L'art. 35, comma 2, prevede infatti in modo specifico che il titolare "si consulti" con il DPO quando svolge una valutazione d'impatto sulla protezione dei dati, e allo stesso tempo, l'art. 39, comma 1, lettera c) affida al DPO il compito di "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35".

Il *Gruppo di Lavoro Ex art. 29* (gruppo di esperti che ha elaborato, in base all'Art. 29 GDPR, una serie di linee guida per l'applicazione pratica del Reg. UE) ha precisato nelle "*Linee Guida sui responsabili della protezione dei dati*" che è opportuno che il titolare del trattamento si consulti con il DPO su una serie di argomenti, quali, a titolo esemplificativo, se condurre o meno una valutazione d'impatto, quale metodo adottare per effettuarla, se svolgerla utilizzando risorse interne o esterne all'organizzazione e quali misure adottare per attenuare i rischi per i diritti e gli interessi delle persone interessate. Si noti bene, peraltro, che, nel caso in cui il titolare del trattamento non concordi con le indicazioni fornite dal DPO, il suo dissenso dovrà essere appositamente motivato e documentato.

Altro aspetto importante è quello che emerge dall'art. 39, comma 1, lettere d) ed e), secondo i quali il DPO deve "cooperare con l'autorità di controllo" e "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione".

Il DPO opera quindi come punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei suoi compiti, nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi.

Aspetto importante è anche che il DPO nello svolgimento delle sue funzioni ha l'obbligo di rispettare le norme in materia di segreto o riservatezza, in base a quanto stabilito dal diritto dell'Unione Europea o degli stati membri.

In base all'art. 39, comma 2, il DPO deve poi -nell'esecuzione dei suoi compiti- considerare "*debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo*". Ciò che si richiede al DPO è, in sostanza, un'attenzione particolare verso quelle che sono le questioni che presentino maggiori rischi in termini di protezione dei dati. La norma appena richiamata sottolinea quindi l'opportunità di dedicare un'attenzione maggiore verso gli ambiti che presentino rischi più elevati, sulla base di valutazioni specifiche e concrete effettuate per ciascuna realtà di trattamento.

L'art. 30 del GDPR prevede che sia compito del titolare del trattamento o del responsabile del trattamento, e non del DPO, quello di tenere un registro delle attività di trattamento svolte, o un registro di tutte le categorie di trattamento svolte per conto del titolare del trattamento. In realtà, il Gruppo di Lavoro ex art. 29 ha rilevato come sia una prassi consolidata (fondata sulle disposizioni di numerose leggi) quella di attribuire proprio al DPO il compito di realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite dai vari uffici che trattano i dati personali. Tuttavia, spetterà al titolare e al responsabile, i quali rimangono onerati di tale adempimento e responsabili nei confronti degli interessati e delle Autorità di controllo per eventuali violazioni, fornire tutte le informazioni necessarie e ad approvare quanto riportato dal DPO nel registro dei trattamenti.

Va comunque tenuto presente che l'elenco di compiti affidati al DPO previsto dall'art. 39, comma 1 del GDPR non esaustivo, ma meramente esemplificativo. Il titolare del trattamento ha quindi la possibilità di affidargli anche altre funzioni, tra cui appunto quella di tenere il registro delle attività di trattamento, benché si tratti sempre di attività svolte sotto la responsabilità del titolare stesso o del responsabile.

Il DPO potrà, in conclusione, rispondere di eventuali responsabilità correlate allo svolgimento dei suoi obblighi di consulenza e assistenza (contrattuali o disciplinari, a seconda che si tratti di un soggetto interno o esterno all'azienda) nei confronti del titolare del trattamento, il quale rimane (eventualmente in solido con il responsabile) l'unico soggetto responsabile del rispetto della normativa vigente.

15. Strumenti da adottare per essere in compliance con il GDPR

Il GDPR lascia un certo margine di discrezionalità ai titolari del trattamento nel decidere le concrete modalità da adottare al fine di conformarsi alle sue disposizioni. A questa maggiore libertà si contrappone, tuttavia, l'onere di dimostrare le ragioni a fondamento delle decisioni prese, attraverso le quali si ritiene di poter raggiungere un livello di conformità alla normativa.

Come previsto infatti dal Considerando n. 78 del GDPR, "*La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate a garantire il rispetto delle disposizioni del presente regolamento*".

Questo tipo di approccio andrà sicuramente ad incidere sugli strumenti che i titolari del trattamento dovranno concretamente adottare al fine di ottemperare agli obblighi previsti e dimostrare così la loro conformità al GDPR.

Innanzitutto, al fine di poter dimostrare la conformità al regolamento, il titolare del trattamento dei dati personali dovrà predisporre delle politiche interne e delle misure tecniche che consentano di dimostrare, nello specifico, il rispetto del principio della "*protezione dei dati fin dalla progettazione e della protezione dei dati di default*".

Misure idonee per raggiungere un tale obiettivo potrebbero essere, ad esempio:

I. una riduzione al minimo indispensabile del trattamento dei dati personali;
II. la pseudonimizzazione dei dati personali da realizzare già nelle prime fasi del trattamento;
III. un approccio trasparente in relazione alle funzioni e al trattamento dei dati;
IV. il mettere l'interessato nella condizione di poter controllare come viene effettuato il trattamento dei suoi dati personali;
V. realizzare e migliorare le caratteristiche di sicurezza per il trattamento dei dati personali.

Da un punto di vista operativo, un importante strumento di compliance è sicuramente la predisposizione di un "***registro dei trattamenti***" di cui si è già fatto cenno in precedenza.

Come precisato infatti dal Considerando n. 82, al fine di dimostrare la conformità al GDPR, il titolare o il responsabile del trattamento dei dati dovrebbero tenere un apposito registro dei trattamenti posti in essere, nel quale documentare ogni elemento connesso all'utilizzo di dati personali.

La norma che viene in riferimento è il più volte citato art. 30 del GDPR, il quale afferma appunto che ogni titolare o responsabile del trattamento (se previsto) tengano un registro delle attività di trattamento svolte sotto la propria responsabilità.

Il GDPR prevede un contenuto specifico per il registro dei trattamenti su cui si rinvia *infra* al paragrafo 18.

La tenuta del registro viene incentivata dal legislatore europeo, perché la sua predisposizione dovrebbe essere concepita come qualcosa di più di un mero obbligo legale, potendo costituire uno strumento estremamente utile e vantaggioso per le aziende.

Il suo corretto utilizzo infatti potrebbe configurare un mezzo di pianificazione e di controllo fondamentale al fine di garantire la correttezza del trattamento dei dati personali nel rispetto delle prescrizioni del GDPR, ma anche per documentare tutte le relative attività e trovarsi pronti ad affrontare eventuali controlli dell'Autorità.

Oltre alla tenuta del registro, al fine di dimostrare la conformità al dettato normativo del nuovo Regolamento, l'adozione di opportune misure da parte del titolare o del responsabile del trattamento dovrà fondarsi sulle indicazioni contenute in appositi codici di condotta che potrebbero essere disposti, sulla necessità di acquisire particolari certificazioni, sulle linee guida emanate dalle Autorità garanti europee o da appositi gruppi di studio, oltre che, ovviamente, sulle istruzioni e sui consigli forniti dal responsabile della protezione dei dati (DPO).

Attraverso un impiego integrato di questi strumenti, il titolare potrà essere in grado di garantire il pieno rispetto e la corretta applicazione del Regolamento, trovandosi in condizione di 1) individuare i rischi connessi al trattamento dei dati personali, 2) svolgere un'analisi del rischio sotto il profilo dell'origine, della natura, della probabilità e della gravità e 3) identificare i mezzi più adeguati al fine di attenuare un tale rischio e garantire elevati livelli di protezione.

16. Livelli di tutela e protezione dei rischi

Un preciso compito del titolare del trattamento dei dati personali sarà dunque quello di effettuare una valutazione preliminare dei rischi che ciascun trattamento che il titolare andrà ad effettuare potrebbe comportare per la protezione dei dati personali.

Simile valutazione è necessaria per capire se un trattamento potrebbe presentare un rischio particolarmente elevato per i diritti e le libertà delle persone fisiche e per predisporre misure tecniche ed organizzative adeguate ai rischi prospettati.

Questo è quanto previsto infatti dall'art. 35, par. 1 del GDPR, che così stabilisce: "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*".

Ma è preliminare a ciò capire quali sono, nelle intenzioni del legislatore europeo, le situazioni in cui un trattamento può determinare un rischio elevato e richiedere, quindi, che sia realizzata una valutazione d'impatto sulla protezione dei dati.

Da questo punto di vista il punto di partenza è sempre l'analisi del contesto specifico di riferimento, tenendo conto, in particolare, di una serie di elementi quali, ad esempio:

1. la presenza di big data;
2. la presenza di dati sensibili (si pensi, ad esempio, al trattamento di dati sanitari su larga scala);
3. l'utilizzo di strumenti di decisione altamente automatizzati;
4. l'impiego di meccanismi di profilazione degli interessati;
5. il trasferimento dei dati verso Stati non appartenenti all'UE (e non tutelati quindi dalla sua regolamentazione)

Questi sono elementi che dovrebbero far suonare un campanello d'allarme per i titolari e i responsabili.

Dopo aver fatto una stima di quelli che possono essere i rischi prevedibili per i diritti e le libertà degli interessati derivanti da ciascun trattamento che si vorrebbe effettuare, il titolare del trattamento dovrà individuare le misure concrete che, caso per caso, possano consentire di raggiungere un livello di tutela che sia adeguato a quegli specifici rischi previsti.

In particolare, le misure così determinate dovranno essere idonee a minimizzare i rischi individuati, assestandoli ad un livello tollerabile, anche con l'obiettivo di dimostrare la conformità alla disciplina dettata dal GDPR.

A questo proposito, come sottolineato nelle Linee guida concernenti la valutazione d'impatto sulla protezione dei dati, le misure che dovranno essere concretamente adottate dai titolari al fine di controbilanciare in modo efficace i rischi individuati come probabili, dipenderanno dal singolo e specifico caso, quindi dal contesto particolare, in relazione a quella precisa situazione e a quel preciso trattamento dei dati.

Di conseguenza, strumenti come la pseudonimizzazione o la cifratura dei dati personali, previsti dal GDPR all'art. 32, par. 1, lett. a) come alcune delle misure che possono essere poste in essere al fine di garantire un adeguato livello di sicurezza del trattamento dei dati, non saranno necessariamente appropriate o idonee o sufficienti per garantire la protezione dei dati personali.

Il GDPR si limita, infatti, a fornire un'elencazione esemplificativa delle misure di sicurezza, ma l'unica soluzione accettabile consisterà in decisioni concrete, prese caso per caso.

Quando, poi, il titolare del trattamento non riesca ad individuare strumenti che consentano di trattare i dati in maniera tale da controbilanciare in modo sufficiente i rischi individuati, cioè quando i rischi "residui" si mantengono particolarmente elevati, il titolare o il responsabile dovranno consultarsi con l'Autorità di controllo per capire se e come sia possibile procedere ad effettuare quel particolare trattamento. Questo è previsto, in particolare, dall'art. 36, par. 1 del GDPR (la norma, a questo proposito, dispone che "*Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio*").

Un'ipotesi di questo tipo potrebbe concretizzarsi nel caso in cui si preveda che potrebbero verificarsi, in capo agli interessati, delle conseguenze negative o irreversibili, oppure nel caso in cui sia altamente probabile che un tale rischio si concretizzerà in futuro.

Questa eventualità potrebbe ricorrere, ad esempio, nel caso in cui un accesso illegittimo ai dati personali potrebbe comportare un rischio per la vita o la sicurezza degli interessati, oppure concretizzare un grave rischio di tipo finanziario, o ancora nel caso in cui non sia possibile dare una soluzione soddisfacente ad una criticità o vulnerabilità nota, perché, ad esempio, il numero di persone aventi accesso ai dati personali non può essere diminuito.

In aggiunta a questo, il titolare del trattamento dovrà poi interpellare l'Autorità di vigilanza qualora sia lo stesso diritto dello Stato membro che viene in rilievo nel caso particolare a stabilire che i titolari del trattamento debbano necessariamente consultarsi, oppure ottenere un'autorizzazione preliminare, come potrebbe essere previsto, ad esempio, qualora il titolare del trattamento debba eseguire un compito di interesse pubblico (ad esempio in materia di pubblica sicurezza o di sanità pubblica). Questo è quanto prevede l'art. 36, par. 5 del GDPR che così dispone: "*Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica*".

Le Linee guida sopra richiamate precisano poi anche la circostanza che una tale valutazione di impatto non sarà richiesta, in particolare, per quei trattamenti in corso che erano già stati autorizzati dalle competenti autorità e che non presentino modifiche significative prima del 25 maggio 2018.

17. Come si dimostra la compliance

Il Regolamento pone fortemente l'accento sulla responsabilizzazione dei titolari e dei responsabili del trattamento, affinché adottino autonomamente una serie di comportamenti che permettano di dimostrare l'adozione di misure idonee al rispetto del Regolamento stesso.

Questo obbligo emerge con evidenza dall'art. 24 del Regolamento, che infatti stabilisce che "*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. Dette misure sono* *riesaminate e aggiornate qualora necessario. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento*".

Automatica conseguenza di questo nuovo approccio è, peraltro, il fatto che l'intervento delle Autorità di controllo sarà successivo, cioè avverrà, da un punto di vista cronologico, solo quando il titolare abbia autonomamente assunto le sue decisioni e posto in essere quanto dallo stesso ritenuto necessario per essere in *compliance*.

Proprio per queste ragioni, a partire dal 25 maggio 2018 sono aboliti alcuni istituti in vigore nella precedente normativa, come la notifica preventiva dei trattamenti all'autorità di controllo e la verifica preliminare (previsti dal Codice della Privacy, il d.lgs. 196/2003).

Questi sono infatti sostituiti, in una logica inversa, da istituti quali il registro dei trattamenti, lo svolgimento della valutazione d'impatto sul trattamento dei dati e, appunto, l'adozione di idonee e concretamente adeguate misure di sicurezza.

La logica di base è infatti quella per cui prima si dovrà realizzare un'organizzazione adeguata alla tutela della privacy e solo in un secondo momento il Garante si esprimerà sulla correttezza e adeguatezza delle scelte realizzate.

I titolari e responsabili del trattamento dei dati dovranno poi cooperare con l'Autorità competente (quindi, nel caso dell'Italia, il Garante della privacy) per lo svolgimento di controlli mettendo prontamente a sua disposizione, su sua richiesta, tali registri in modo tale da agevolare il controllo sui trattamenti stessi e la verifica del rispetto della normativa.

In secondo luogo, al fine di garantire la sicurezza dei dati trattati e assicurare che il trattamento degli stessi sia posto in essere in modo conforme al Regolamento, il titolare e il responsabile dovranno innanzitutto valutare quali sono i possibili rischi che si potrebbero verificare per la protezione dei dati personali, ad esempio la distruzione illegale o accidentale degli stessi, la loro perdita, modifica o rivelazione, oppure l'accesso non autorizzato che potrebbero dar luogo a possibili danni, materiali o immateriali, a carico dei soggetti interessati.

Dopo aver fatto questo, il titolare o il responsabile dovranno adottare, ed essere in grado di dimostrare di aver attuato delle misure di sicurezza adeguate, in relazione al singolo caso di volta in volta considerato, al fine di minimizzare tali rischi, come ad esempio la cifratura dei dati.

Nel caso in cui poi il trattamento possa, nel caso di specie, rappresentare un rischio elevato per i diritti e le libertà delle persone, il titolare dovrà effettuare un'apposita valutazione d'impatto sulla protezione dei dati in modo tale da specificare, anzitutto, l'origine, la natura e la gravità del rischio.

L'esito di questa valutazione dovrà poi essere posto a fondamento della decisione relativa alle opportune misure di sicurezza che dovranno essere adottate, al fine di dimostrare -in un momento successivo- che il trattamento dei dati personali posto in essere è conforme alle disposizioni ed ai principi alla base del regolamento.

Qualora ancora emerga che il rischio per la protezione dei dati sia tanto elevato da non poter essere tenuto sotto controllo attraverso le misure previste, anche laddove i costi di attuazione delle misure idonee siano eccessivamente elevati, e anche in base alla tecnologia a disposizione, il titolare non potrà porre comunque in essere quel trattamento, ma dovrà rinunciarvi oppure consultare il Garante per valutare la possibilità di individuare una soluzione soddisfacente in termini di sicurezza dei dati, che consenta di proseguire con tale trattamento nonostante gli elevati rischi individuati a monte.

Concretamente, occorre poi ricordarsi che la forma più idonea per dimostrare la *compliance* alla disciplina del Regolamento è sicuramente quella scritta.

Anche laddove tale forma non sia espressamente richiesta per i vari adempimenti previsti dal GDPR, sarà quindi interesse (e vantaggio concreto) dello stesso titolare quello di documentare quante più attività possibili in modo chiaro e completo, e di prepararsi a produrre tali documenti al Garante o all'interessato, a seconda dei casi, in tempi rapidi e in un formato adeguato.

Ad esempio, se il consenso dell'interessato venga rilasciato in forma orale, ferma restando la validità in termini teorici di tale consenso, sarà il titolare a doversi attivare al fine di procurarsi comunque una prova scritta di tale conferimento, da poter presentare in caso di eventuali successivi controlli dell'Autorità di controllo, oppure anche su richiesta dell'interessato, al fine ultimo di dimostrare di aver effettuato un trattamento legittimo.

18. Le procedure obbligatorie

Il GDPR introduce una serie di obblighi che derivano essenzialmente dal più generale principio di responsabilizzazione (***accountability***) posto a fondamento della struttura del Regolamento europeo e del rispetto dei principi essenziali in tema di privacy (l'art. 5, co. 2, GDPR, infatti, dopo aver elencato i principi applicabili al trattamento di dati personali, afferma che "*Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo – responsabilizzazione*").

In particolare, come si è avuto modo di precisare in più occasioni, il titolare e il responsabile del trattamento sono sotto diversi aspetti incentivati ad adottare provvedimenti finalizzati a dare concreta ottemperanza alle disposizioni del GDPR.

Si ricorda infatti che l'approccio che viene incoraggiato dal nuovo Regolamento europeo è focalizzato principalmente sulla concreta protezione dei dati ed è fondato su una valutazione preliminare del rischio (si parla per questo di *sistema risk-based*) a una volta basata su un'opportuna considerazione della natura, della portata, del contesto e delle finalità del trattamento, sulla probabilità e sulla gravità dei rischi per i diritti e libertà degli utenti. In relazione a tale complessa e globale valutazione si determinerà poi la misura della eventuale responsabilità del titolare e del responsabile del trattamento.

Un approccio incentrato sul rischio ha sicuramente, da un lato, il vantaggio di pretendere l'ottemperanza di una serie di obblighi più generali che possono andare al di là di una mera e superficiale conformità al dettato normativo.

Dall'altro lato, si tratta di un sistema che si presta ad una maggiore flessibilità ed elasticità, essendo in grado di adattarsi al mutamento delle esigenze e degli strumenti tecnologici. Infine, non di può ignorare che il fatto che un simile approccio deleghi sostanzialmente ai titolari ogni valutazione, si presenta come un'arma a doppio taglio: maggiore libertà di scelta, ma maggiore impegno da parte dei titolari e più difficile contestare eventuali provvedimenti sanzionatori da parte del Garante.

Cercando di sintetizzare, ove possibile, gli oneri e gli obblighi imposti al Titolare del Trattamento dei Dati si ricava quanto di seguito esposto:

Adozione di misure tecniche ed organizzative adeguate; *privacy policies* proporzionate alle attività di trattamento; codici di condotta e certificazioni

oneri ed obblighi del Titolare del Trattamento Dati

Misure di sicurezza del trattamento; valutazione impatto rischi e *data breach*; controllo dell'accesso ai dati; *data breach notification* e conseguenze; controllo della *valutazione di impatto privacy* (DPIA) quando il trattamento preveda l'uso di nuove tecnologie e comporti un rischio elevato per i diritti e per le libertà delle persone fisiche

Registro del Trattamento (per società con più di 250 dipendenti, per trattamenti che presentino rischi per i diritti e le libertà degli interessati, per trattamenti che riguardano dati sensibili particolari – es. condanne penali – nonché infine per i trattamenti dati non occasionali)

In conseguenza di ciò, per poter essere in linea con le prescrizioni e gli obblighi sanciti dal GDPR, è necessario che le aziende realizzino una revisione completa dei dati e delle informazioni che raccolgono e che gestiscono, verificando anche quelle che sono le basi normative a giustificazione di tali trattamenti nonché le conseguenze che il trattamento dei dati effettuato può comportare per gli interessati.

Tra gli adempimenti che dovranno quindi essere realizzati troviamo:

I. la verifica dei dati che saranno oggetto di trattamento, con identificazione delle varie tipologie di dati e delle categorie di appartenenza e la verifica della finalità di ogni trattamento e della base giuridica sul quale ciascuno di essi si fonda, anche al fine di rendere adeguata informativa ai soggetti interessati, come previsto dagli artt. 13 e 14 del GDPR (dedicati, rispettivamente, alle informazioni da fornire qualora i dati personali siano raccolti – art. 13 – o meno – art. 14 – presso l'interessato);
II. la predisposizione dell'informativa (o il suo aggiornamento) che deve essere fornita agli interessati nel rispetto di tutti gli elementi indicati agli artt. 13 e 14 del GDPR, in particolare gli interessati dovranno essere messi a conoscenza dei diritti che il Regolamento riconosce loro (diritto di accesso, diritto all'oblio, diritto di rettifica, diritto di limitazione e di opposizione al trattamento, diritto alla portabilità dei dati – sul punto si vedano le apposite sezioni dedicate dello Speciale);
III. la predisposizione del registro delle attività di trattamento dei dati personali, qualora esso risulti necessario in base al disposto dell'art. 30 del GDPR, ossia nel caso in cui l'impresa o l'organizzazione che effettua il trattamento dei dati abbia più di 250 dipendenti. Tale registro dovrà, del resto, essere redatto anche nel caso in cui l'impresa od organizzazione abbia meno di 250 dipendenti, ma ponga in essere un trattamento dei dati che presenta un potenziale rischio per i diritti e libertà degli interessati (l'art. 30, co. 5, GDPR prevede infatti che "*Gli obblighi di cui ai paragrafi 1 e 2 non si applicano 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 di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10*");
IV. l'instaurazione di una procedura da adottare in caso di eventuali violazioni dei dati (c.d. ***Data Breach***) ([21]), ad esempio al verificarsi di una divulgazione (intenzionale o meno),

[21] L'Art. 32 GDPR prevede che il Titolare (ed il Responsabile) adottino le misure tecniche ed organizzative che garantiscano un livello di sicurezza adeguato al rischio; a tal fine il Regolamento suggerisce la cifratura dei dati; la capacità di assicurare in modo permanente la riservatezza, integrità e disponibilità dei dati trattati; la capacità di ripristino tempestivo ed accesso ai dati in caso di incidente fisico o tecnico; le procedure per testare periodicamente l'efficacia e l'idoneità delle misure tecniche adottate. Il concetto di *data breach* si riferisce alla perdita, modifica, distruzione, l'accesso o la divulgazione non autorizzata dei dati che avvenga *accidentalmente* o *in modo illecito*: è opportuno precisare che la *sicurezza* che deve garantire il Titolare *non riguarda esclusivamente i dati informatici ed i sistemi automatizzati ma si estende anche ai documenti cartacei.* Sostanzialmente il *data breach* (secondo le Linee Guida elaborate dal WP29) si estrinseca in tre modalità di violazione dei seguenti principi: la *riservatezza* (divulgazione o accesso accidentale ovvero non autorizzato), la *integrità* (modifica, accidentale o illecita, dei dati) e la *disponibilità* (perdita dell'accesso o distruzione accidentale o illecita). A questi principi rinvia espressamente l'Art. 32 GDPR nella parte

della distruzione, della perdita, della modifica o dell'accesso non autorizzato ai dati personali oggetto di trattamento. Il GDPR prevede infatti degli specifici adempimenti nel caso in cui si verifichi una violazione di tal genere, a causa di un attacco informatico, di un accesso abusivo o di un incidente. In questi casi il GDPR impone, come previsto dall'art. 33, in capo al titolare del trattamento l'obbligo di comunicare all'autorità di controllo l'avvenuta violazione entro 72 ore o comunque senza ritardo (art. 33, co. 1, GDPR "*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro72 ore, è corredata dei motivi del ritardo*"). Nel caso in cui la violazione verificatasi faccia presumere che vi sia anche un elevato e attuale pericolo per i diritti e le libertà degli interessati, anche questi ultimi dovranno essere direttamente informati senza ritardo di quanto successo.

V. inoltre, come previsto poi dall'art. 35 del GDPR, si configura, in capo al titolare del trattamento (e con la possibilità di consultare il Responsabile della protezione dei dati se presente), l'obbligo di procedere ad una valutazione d'impatto sulla protezione dei dati nel caso in cui un tipo di trattamento, anche in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento stesso, presenti un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35, co. 1, GDPR "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*"). Del resto, il GDPR non sancisce un vero e proprio obbligo di svolgimento della valutazione d'impatto, ma si ricorda che il regolamento prevede un generale obbligo, in capo al titolare del trattamento, di attuare le misure idonee al fine di gestire adeguatamente i rischi per i diritti e le libertà degli interessati che possono derivare dal trattamento dei loro dati. Sarà quindi opportuno procedere all'effettuazione della valutazione d'impatto anche quando sul titolare non incombe l'obbligo normativo in tale senso.

VI. un altro adempimento che viene richiesto al titolare del trattamento consiste nella designazione del Responsabile della protezione dei dati (per un approfondimento su tale sfigura vi invitiamo a leggere l'articolo ad esso dedicato del presente Speciale). Tale nomina è, come previsto dall'art. 37 del GDPR, obbligatoria soltanto in una serie di

---

in cui precisa che il Titolare del Trattamento deve assicurare che gli stessi non siano violati, adoperando – come detto – le idonee misure tecniche. Nel caso in cui si verifichi un *data breach* il Titolare deve darne comunicazione (mediante notifica) alla competente autorità (in Italia il Garante per la Privacy) entro un termine massimo indicato in 72 ore da quando è avvenuto il fatto (*rectius* da quanto il Titolare viene a conoscenza della violazione). La realizzazione di un *data breach* non comporta, *ipso facto*, l'obbligo del Titolare di provvedere alla notifica della violazione al Garante, in quanto la WP29 offre una serie di parametri – di seguito indicati sinteticamente – che il Titolare deve valutare e ponderare per decidere se procedere, o meno, alla notifica:

a) Il *data breach* può riguardare, come detto sopra, tre elementi (*riservatezza, integrità* e *disponibilità*): in primo luogo il Titolare deve verificare quale di questi settori è stato intaccato dalla violazione;
b) *Categorie* e *volume* dei dati oggetto della violazione: se i dati sono già pubblici (es. nome e cognome di un soggetto) il *data breach* può essere omesso; diverso è il caso in cui, ad esempio, siano divulgati gli estremi dei genitori adottivi dell'interessato.
c) *Facilità di identificazione degli interessati*: il Titolare deve considerare il grado di facilità con cui coloro che sono entrati in possesso dei dati, potrebbero identificare gli interessati (es. furto di identità…);
d) *Gravità delle conseguenze*: questo elemento deve essere ovviamente valutato caso per caso. Se, ad esempio, il furto di dati inerenti ad un minorenne si considera grave *in re ipsa*, in altre ipotesi la gravità dipende da una pluralità di fattori contingenti;
e) *Caratteristiche del Titolare*: se il Titolare è un ente che gestisce dati sanitari o altri dati sensibili, è evidente che la necessità del *data breach* si avverte con maggior cogenza rispetto all'accesso a dati puramente commerciali;
f) *Numero di persone colpite*. Come per il requisito del *volume* dei dati violati, anche il numero dei potenziali interessati incide sull'opportunità, o meno, di notificare la violazione al Garante.

ipotesi, in particolare, nel caso in cui il trattamento dei dati sia effettuato da un'autorità pubblica o da un organismo pubblico (ad eccezione per le autorità giurisdizionali quando esercitano le loro funzioni); quando le attività principali svolte del titolare o del responsabile del trattamento consistono in operazioni che, per la loro natura, l'ambito di applicazione o le finalità, richiedono un monitoraggio regolare e sistematico degli interessati su larga scala; e infine nel caso in cui le attività principali effettuate consistano nel trattamento, su larga scala, di dati sensibili o di dati relativi a condanne penali e a reati consistenti nell'illecito trattamento dei dati personali.

In tutti i restanti casi, quando il regolamento non impone specificamente la nomina di un DPO, questa figura potrà comunque essere designata dal titolare o dal responsabile del trattamento su base volontaria.

19. Il Registro delle Attività di Trattamento

Come stabilito dall'art. 30 del GDPR, tutti i titolari e i responsabili di trattamento dei dati personali, ad eccezione delle imprese e organizzazioni che hanno meno di 250 dipendenti (ma solo se non effettuano trattamenti a rischio), devono tenere un ***registro di tutte le attività di trattamento*** dei dati effettuate.

Questo registro è un documento che dovrà contenere, per legge, una serie di informazioni sulle attività riguardanti il trattamento dei dati personali, quali:

1. il nome e i dati di contatto del titolare (ed eventualmente del contitolare) del trattamento, del rappresentante del titolare e del responsabile della protezione dei dati;
2. le finalità del trattamento;
3. una descrizione delle categorie di interessati e delle categorie di dati personali trattati;
4. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi eventualmente i destinatari di paesi terzi non appartenenti all'Unione Europea od organizzazioni internazionali;
5. nel caso in cui sia previsto, l'indicazione del fatto che i dati personali saranno trasferiti verso un paese terzo o un'organizzazione internazionale, indicando anche di quale paese od organizzazione internazionale si tratta e, inoltre, la documentazione delle garanzie previste;
6. i termini ultimi stabiliti per la cancellazione delle diverse categorie di dati; e infine
7. una descrizione generale delle misure di sicurezza tecniche e organizzative individuate al fine di garantire un livello di sicurezza dei dati personali adeguato al rischio cui gli stessi sono esposti.

Per quanto concerne i soggetti obbligati alla tenuta del registro dei trattamenti, come risulta dall'art. 30, paragrafi 2 e 3 ("*Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente: a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico*") essi sono tanto il titolare quanto il responsabile del trattamento o, se presenti, i loro rappresentanti. Su entrambi incombe pertanto uno specifico dovere in tal senso, tenendo però conto che, dal punto di vista del contenuto, nel caso in cui il registro sia tenuto direttamente dal titolare del trattamento, o dal suo rappresentante, avrà una portata più estesa, invece qualora esso sia tenuto dal responsabile del trattamento, o dal suo rappresentante, dovrà indicare obbligatoriamente (ma ogni ulteriore informazione sarà sempre utile, nell'ottica del GDPR) solo:

a) i contatti del titolare, del responsabile del trattamento e dei loro rappresentanti, se presenti, nonché del responsabile della protezione dei dati;
b) le categorie di trattamenti effettuati per ciascun titolare del trattamento;
c) il trasferimento dei dati ad un paese terzo (extra-europeo) o ad un'organizzazione internazionale, specificando di quale paese o organizzazione si tratta ed evidenziando le adeguate garanzie previste per il trasferimento stesso; e infine
d) se possibile, la descrizione delle misure di sicurezza tecniche ed organizzative adeguate ai rischi preventivati.

Il registro delle attività di trattamento si configura come uno strumento fondamentale non soltanto ai fini di eventuali controlli di legittimità da parte del Garante, ma anche perché consente di avere a disposizione un quadro aggiornato dei trattamenti che vengono realizzati nell'azienda, organizzazione o soggetto pubblico. Quest'ultima circostanza sarà importante, in particolare, per poter realizzare una corretta ed efficace analisi e valutazione dei rischi.

Da un punto di vista strettamente formale, il GDPR non detta delle regole generali né individua le concrete modalità attraverso cui il registro delle attività di trattamento dovrà essere formato.

L'art. 30 si limita infatti a precisare che il registro delle attività di trattamento dei dati dovrà essere tenuto in forma scritta, su supporto tangibile oppure, e preferibilmente, in formato elettronico, e dovrà inoltre essere messo a disposizione su richiesta dell'autorità di controllo (nel caso dell'Italia, il Garante per la protezione dei dati personali).

Al contrario poi di altri adempimenti sanciti dal nuovo Regolamento europeo a titolo obbligatorio, la predisposizione di un tale registro delle attività di trattamento non è un adempimento formale. Esso si configura, piuttosto, come uno strumento che è parte integrante di quel generale sistema di corretta gestione dei dati personali che le aziende, organizzazioni o soggetti pubblici dovranno creare.

Un'adeguata predisposizione del registro delle attività di trattamento potrà essere, infatti, un elemento importante al fine di realizzare un corretto trattamento dei dati personali, in linea quindi con l'obiettivo di responsabilizzazione (*accountability*), che, come precisato in più occasioni in questo Speciale di approfondimento sul GDPR, è uno dei principi fondamentali che il legislatore europeo ha voluto incentivare maggiormente e su cui fonda l'intera disciplina del Regolamento.

La necessità di dimostrare la legittimità del trattamento dei dati, e di conseguenza la sua conformità alla disciplina dettata dal GDPR, prescinde dalle dimensioni effettive dell'organizzazione aziendale, e quindi in un panorama di questo tipo il registro diventa un valido strumento per tutte le organizzazioni.

Proprio per questa ragione, su indicazione del Garante della Privacy, tutti i titolari ed i responsabili del trattamento dei dati, a prescindere dalle dimensioni dell'organizzazione (e quindi anche qualora vi siano meno di 250 dipendenti), sono invitati a predisporre un tale registro.

In ogni caso, anche se tale registro non verrà predisposto, è necessario che i titolari e i responsabili del trattamento si impegnino per effettuare in altro modo una scrupolosa individuazione dei trattamenti posti in essere e delle loro caratteristiche principali.

D'altra parte, come visto più sopra, i contenuti del registro dei trattamenti, delineati dall'art. 30, possono essere integrati anche con altre informazioni da parte del titolare o del responsabile, i quali potranno infatti inserire ogni elemento aggiuntivo, se lo riterranno opportuno alla luce della complessiva valutazione d'impatto sulla protezione dei dati e sulla base delle attività di trattamento svolte.

20. La Valutazione di Impatto dei Rischi

L'art. 35 del GDPR sancisce, in capo al titolare del trattamento (con la possibilità di consultare il Responsabile della protezione dei dati se presente), l'obbligo di effettuare una ***valutazione d'impatto sulla protezione dei dati*** qualora un tipo di trattamento, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento stesso, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche cui i dati personali trattati si riferiscono ("*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*").

Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali4, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24). In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.

Non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento: infatti è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1); un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. La "gestione dei rischi", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

Come precisa la norma, al paragrafo 7, il contenuto minimo è indispensabile di tale valutazione consiste in:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso anche, eventualmente, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, comprese le garanzie, le misure di sicurezza e i meccanismi previsti al fine di garantire la protezione dei dati personali e dimostrare la

conformità del trattamento al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

La valutazione d'impatto sulla protezione dei dati dovrà essere necessariamente realizzata, come previsto dal GDPR, in una serie di ipotesi particolari, e in particolare nel caso in cui il titolare ponga in essere delle attività che consistono in:

a) una valutazione sistematica e globale degli aspetti personali relativi a persone fisiche, basata sul trattamento automatizzato, compresa la profilazione, e su cui si fondano decisioni che hanno effetti giuridici o incidono comunque significativamente sulle persone fisiche;
b) un trattamento, su larga scala, di categorie particolari di dati (dati sensibili), o di dati relativi a condanne penali e a reati;
c) operazioni di sorveglianza sistematica di zone accessibile al pubblico su larga scala.

Sarà comunque compito dell'autorità di controllo competente predisporre e rendere pubblico un apposito elenco relativo alle diverse tipologie di trattamenti per i quali sarà o non sarà necessario effettuare una valutazione d'impatto sulla protezione dei dati (adempimento cui il nostro Garante non ha ancora provveduto).

Tuttavia, come precisato anche nelle linee guida delineate in materia, il fatto che non sia configurabile un vero e proprio obbligo di svolgimento della valutazione d'impatto non incide affatto sul più generico obbligo -al quale sottostanno i titolari del trattamento- di attuare delle misure idonee al fine di gestire adeguatamente i rischi per i diritti e le libertà degli interessati che possono derivare dal trattamento dei loro dati.

In ogni caso, al fine di procedere ad una corretta valutazione d'impatto sulla protezione dei dati, i titolari e responsabili del trattamento dovranno tenere in considerazione anche l'osservanza dei codici di condotta eventualmente approvati, in modo tale da assicurare e contribuire alla corretta applicazione del regolamento.

Come sottolineato dalle Linee Guida, la ***valutazione d'impatto*** (detta anche ***DPIA***, acronimo di "*Data Protection Impact Assessment*") dovrebbe essere condotta in via anticipata, ovvero prima di procedere al trattamento dei dati. Essa infatti dovrebbe essere considerata proprio come uno strumento di ausilio in quel processo decisionale complessivo relativo al trattamento. Un tale approccio non dovrebbe peraltro stupire perché appare del tutto coerente con i principi della Privacy by design e Privacy by default che sono sanciti nel GDPR (art. 25 GDPR: "*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita 1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. 2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*").

Questa valutazione dovrebbe quindi essere svolta preferibilmente già nella fase di progettazione di un'attività di trattamento dei dati, anche se è normale che in quella fase così precoce non tutte le operazioni di trattamento siano già state messe a punto.

Questa considerazione si collega alla necessaria e attenta attività di aggiornamento delle informazioni contenute nella DPIA, ritenuta per il GDPR imprescindibile sviluppo di tale procedura. L'aggiornamento successivo della prima valutazione effettuata assicurerà quindi l'osservanza continuativa del quadro normativo di riferimento in materia di protezione dei dati personali.

In altre parole, la valutazione d'impatto sulla protezione dei dati non è un'attività che dovrà essere posta in essere una tantum, ma si configura piuttosto come un processo continuativo da mantenere attivo e aggiornato nel corso del tempo.

Come precisato sopra, è compito del titolare del trattamento quello di effettuare la valutazione d'impatto; tuttavia lo svolgimento materiale della stessa potrà essere affidato ad un altro soggetto, sia interno che esterno all'organismo anche se comunque, in quest'ultima ipotesi, la responsabilità ultima in ordine all'adempimento dell'obbligo ricade sul titolare del trattamento.

Al titolare del trattamento spetta assicurare che la valutazione d'impatto sulla protezione dei dati sia eseguita (articolo 35, paragrafo 2). La valutazione d'impatto sulla protezione dei dati può essere effettuata da qualcun altro, all'interno o all'esterno dell'organizzazione, tuttavia al titolare del trattamento spetta la responsabilità ultima per tale compito. Inoltre il titolare del trattamento deve consultarsi con il responsabile della protezione dei dati (RPD), qualora ne sia designato uno (articolo 35, paragrafo 2) e il parere ricevuto, così come le decisioni prese dal titolare del trattamento, debbano essere documentate all'interno della valutazione d'impatto sulla protezione dei dati. Il responsabile della protezione dei dati deve altresì sorvegliare lo svolgimento della valutazione d'impatto sulla protezione dei dati (articolo 39, paragrafo 1, lettera c)). Ulteriori orientamenti in merito sono forniti nelle "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243.

Qualora il trattamento venga eseguito in toto o in parte da un responsabile del trattamento dei dati, quest'ultimo deve assistere il titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati e fornire tutte le informazioni necessarie (conformemente all'articolo 28, paragrafo 3, lettera f).

Le Linee Guida sopra richiamate suggeriscono, infine, diversi metodi attraverso cui poter realizzare una valutazione d'impatto.

A questo proposito si rileva che è stata predisposta una specifica norma internazionale (ISO/IEC 29134 dal titolo "*Privacy Impact Assessment – Methodology*") di prossima pubblicazione che propone uno schema composto da una serie di passaggi (di cui alcuni riferiti specificamente al riesame periodico e all'attuazione di eventuali cambiamenti che si renderanno necessari), con lo scopo di fornire un valido metodo di riferimento.

Il GDPR lascia ai titolari del trattamento un margine di flessibilità per quanto riguarda la forma che tale valutazione d'impatto dovrà avere, in modo tale da consentire loro di includere un riferimento alle prassi già in essere.

Qualsiasi sia comunque la forma prescelta, la valutazione d'impatto dovrà essere impostata come una vera e propria valutazione dei rischi, in modo tale quindi da mettere i titolari in condizione di adottare le misure adeguate al fine di gestire e minimizzare tali rischi. Un'analisi efficace dovrebbe quindi tener conto correttamente del tipo di dati trattati e della loro pericolosità per la riservatezza dei soggetti cui si riferiscono, nonché del comportamento degli operatori e dei vari elementi (attinenti agli strumenti utilizzati e al contesto specifico) che vengono in considerazione.

Il WP29 ritiene che una valutazione d'impatto sulla protezione dei dati non sia richiesta nei seguenti casi:

1) quando il trattamento non è tale da "*presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (articolo 35, paragrafo 1);

2) quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 119);

3) quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate (cfr. III.C);

4) qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10), a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;

5) qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5). Tale elenco può contenere attività di trattamento conformi alle condizioni specificate da detta autorità, in particolare attraverso linee guida, decisioni o autorizzazioni specifiche, norme di conformità, ecc. (ad esempio in Francia, autorizzazioni, esenzioni, norme semplificate, pacchetti di conformità, ecc.). In tali casi e a condizione che venga eseguita una nuova valutazione da parte dell'autorità di controllo competente, non è richiesta una valutazione d'impatto sulla protezione dei dati, ma soltanto se il trattamento rientra a tutti gli effetti nel campo di applicazione della procedura pertinente menzionata nell'elenco e continua a rispettare pienamente tutti i requisiti pertinenti del regolamento generale sulla protezione dei dati.

21. Quando si rischiano le sanzioni

Il sistema sanzionatorio delineato dal nuovo Regolamento europeo in materia di protezione dei dati personali (Regolamento UE 679/2016, c.d. GDPR) si fonda principalmente sulla previsione di sanzioni amministrative pecuniarie, le quali rientrano nell'insieme degli strumenti che le autorità di controllo in ogni singolo Stato membro dell'Unione Europea hanno a disposizione, al fine di assicurare una corretta ed uniforme applicazione delle disposizioni del GDPR in tutto il territorio europeo.

In particolare, nel momento in cui venga riscontrata ed accertata la violazione delle norme sancite dal GDPR, l'autorità di controllo competente (in Italia, l'Autorità Garante per la protezione dei dati personali) potrà individuare la misura di carattere sanzionatorio più appropriata al fine di porre rimedio alla situazione.

Nello specifico, come previsto dall'art. 83, sarà possibile, per l'autorità di controllo, comminare anzitutto delle sanzioni amministrative pecuniarie in presenza di un'amplissima gamma di violazioni (anche per inadempimenti parziali della normativa) specificamente elencate dalla norma stessa. Tuttavia, come vedremo meglio in seguito, l'elencazione contenuta nel GDPR è tutt'altro che d'aiuto nel circoscrivere le possibili condotte che espongono a sanzioni: l'art. 83 fa infatti riferimento a numerosissimi articoli del Regolamento, molti dei quali per di più contengono principi e regole generali.

Peraltro, in aggiunta o in alternativa alle sanzioni pecuniarie, le Autorità garanti potranno applicare anche altre misure di tipo correttivo, previste invece dall'art. 58 del GDPR (tra cui, ad esempio, rivolgere avvertimenti e ammonimenti al titolare e al responsabile in caso di violazioni riscontrate o presunte della normativa, imporre limitazioni ai trattamenti, fino a vietarli completamente, e revocare le certificazioni se i requisiti non risultano soddisfatti). La norma in ultimo richiamata fornisce, infatti, un elenco degli strumenti e dei poteri riconosciuti all'autorità di controllo competente che vanno dai poteri di indagine a quelli di accesso ai dati e ai locali aziendali, fino a quelli correttivi e consultivi.

Inoltre, come specificato poi dall'art. 83, paragrafo 3, "*Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave*".

In aggiunta a quanto previsto dal GDPR, occorre tenere presente che il diritto dei singoli Stati membri dell'Unione Europea potrà anche estendere, come espressamente previsto dall'art. 83, paragrafo 7, il campo di applicazione delle misure correttive di cui all'art. 58, paragrafo 2 e delle sanzioni amministrative pecuniarie di cui all'art. 83, che potranno essere inflitte, ove previsto, non solo dal Garante, ma anche da altre autorità pubbliche dello Stato membro. L'art. 83, paragrafo 7 dispone infatti che "*Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro*".

L'ordinamento giuridico di ogni singolo Stato potrà poi anche consentire, o addirittura imporre, l'irrogazione di ulteriori sanzioni amministrative pecuniarie per la violazione di disposizioni in materia di protezione dei dati personali diverse da quelle già indicate dal GDPR all'art. 83: in altre parole, l'elencazione ivi prevista potrebbe essere ulteriormente ampliata e arricchita dai singoli ordinamenti nazionali.

Questo è quanto viene stabilito specificamente dall'art. 84 del GDPR, il quale precisa che le sanzioni dovranno in ogni caso essere effettive, proporzionate e dissuasive. In questa ipotesi, ogni Stato membro dovrà notificare alla Commissione le disposizioni normative adottate in tal senso, entro il 25 maggio 2018, data in cui il GDPR sarà pienamente applicabile in tutto il territorio dell'Unione Europea.

Dovranno, del resto, essere comunicate anche tutte le successive modifiche apportate alle misure in questione senza ritardo.

Ad ogni buon conto, il GDPR precisa che ogni caso dovrà essere valutato singolarmente e con specifico riferimento alle particolarità del contesto in cui si verifica la violazione ai fini dell'applicazione concreta delle sanzioni amministrative pecuniarie.

L'art. 83, paragrafo 2 stabilisce, a questo proposito, che al momento di decidere se infliggere una sanzione amministrativa pecuniaria, e di fissare l'ammontare della stessa, si dovrà tenere nella dovuta considerazione una serie di elementi specifici che la norma stessa provvede poi ad elencare. Tra questi, come si avrà modo di precisare nel prosieguo di questo Speciale di approfondimento sul GDPR si trovano, ad esempio: la natura, la gravità e la durata della violazione, il suo carattere doloso o colposo, le misure eventualmente adottate direttamente dal titolare o dal responsabile del trattamento al fine di attenuare il danno subito dagli interessati, le categorie di dati personali oggetto della violazione, le eventuali precedenti violazioni già commesse dal titolare o dal responsabile del trattamento, e così via.

22. Le sanzioni pecuniarie: criteri per determinarle

Le sanzioni amministrative pecuniarie previste dal GDPR dovranno essere disposte in modo tale da poter dare un'adeguata risposta in base alla natura, alla gravità e alle conseguenze della violazione che è stata realizzata.

Volendo scendere nel merito delle singole sanzioni pecuniarie previste dal GDPR, emerge anzitutto il fatto che il Regolamento, indicando due diversi massimali (€ 10.000.000 e € 20.000.000), riconosce il fatto che la violazione di alcune disposizioni sarà nettamente più grave rispetto alla violazione di altre.

In particolare, come previsto dall'art. 83, paragrafo 4, sarà "soggetta all'applicazione di sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2% del fatturato mondiale totale annuo riferito all'esercizio precedente" (se si tratta di un importo superiore ai 10 milioni di euro) la violazione, anzitutto, di una serie di obblighi che il Regolamento pone in capo al titolare e al responsabile del trattamento dei dati, tra cui, ad esempio:

a) Gli obblighi sanciti per il trattamento dei dati personali riguardanti soggetti minori di 16 anni (art. 8);
b) Gli obblighi previsti per il trattamento di dati senza necessaria identificazione dell'interessato (art. 11);
c) Gli obblighi relativi alla protezione dei dati personali fin dalla progettazione e per impostazione predefinita (ovvero il rispetto dei principi di privacy by design e privacy by default), alla tenuta dei registri delle attività di trattamento, alla cooperazione con l'autorità di controllo, nonché quelli previsti in materia di sicurezza del trattamento dei dati, di notifica delle violazioni dei dati all'autorità di controllo e all'interessato, così come gli obblighi riguardanti la valutazione d'impatto sulla protezione dei dati e la designazione del responsabile della protezione dei dati (artt. da 25 a 39);
d) Gli obblighi relativi ai meccanismi di certificazione della protezione dei dati (artt. 42 e 43).

Questa stessa sanzione potrà essere applicata poi, come previsto dall'art. 83, paragrafo 4, lett. b) e c), anche nel caso di violazione degli obblighi sanciti in capo all'organismo di certificazione della protezione dei dati dagli artt. 42 e 43 e degli obblighi dell'organismo di controllo per quanto concerne il monitoraggio della conformità dei codici di condotta approvati, di cui all'art. 41, paragrafo 4.

Darà luogo, invece, all'applicazione di "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 si tratta di un importo superiore a 20 milioni di euro) la violazione di:

→Principi fondamentali che stanno alla base di un legittimo trattamento dei dati personali, ossia:

I. In base all'art. 5, i principi di correttezza, liceità e trasparenza del trattamento, il principio di limitazione della finalità del trattamento, il principio di minimizzazione, di esattezza, di limitazione della conservazione, di integrità e riservatezza dei dati personali e, infine, di responsabilizzazione del titolare del trattamento;
II. Il principio di liceità del trattamento dei dati espresso dall'art. 6, in forza del quale un trattamento sarà lecito se fondato sul consenso dell'interessato, se necessario per l'esecuzione di un contratto o di misure precontrattuali di cui l'interessato sia parte, o ancora per adempiere ad un obbligo di legge da parte del titolare del trattamento o per la tutela di interessi vitali dell'interessato o di un soggetto terzo, come per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è

investito il titolare del trattamento, oppure per il perseguimento del legittimo interesse del titolare del trattamento o di terzi;

III. I principi che, in base all'art. 7, assicurano che la prestazione del consenso, da parte dell'interessato, al trattamento dei dati personali possa essere considerato legittimo; e infine

IV. I principi a fondamento del legittimo trattamento di categorie particolari di dati personali, quali dati sensibili e dati relativi a condanne penali, come previsto dall'art. 9 ([22]) ([23]).

→Diritti sanciti in capo ai soggetti interessati a norma degli artt. da 12 a 22 del GDPR, quali:

I. Il diritto di ricevere adeguate informazioni in ordine al trattamento dei propri dati personali (artt. da 12 a 14);
II. Il diritto di accesso (art. 15);
III. Il diritto di rettifica (art. 16);
IV. Il diritto all'oblio (art. 17);
V. Il diritto alla limitazione del trattamento dei dati (art. 18);
VI. Il diritto alla portabilità dei dati (art. 20);
VII. Il diritto di opposizione al trattamento (art. 21); e, infine
VIII. Il diritto di non essere sottoposto a una decisione fondata unicamente su di un trattamento automatizzato, compresa la profilazione, e produttiva di effetti giuridici a suo carico (art. 22).

→Disposizioni riguardanti il trasferimento di dati personali a un destinatario situato in un paese terzo o un'organizzazione internazionale (in base agli artt. da 44 a 49);

→Obblighi sanciti dagli ordinamenti giuridici dei singoli stati membri e aventi ad oggetto specifiche situazioni di trattamento dei dati, come previsto ai sensi degli artt. da 85 a 91; e infine

[22] Il quarto comma del citato Art. 9 pone numerose eccezioni al generale divieto (di cui al primo comma) di trattamento di *dati sensibili* oltre a quelli *biometrici, genetici* e *relativi alla salute* e comunque stabilisce che gli Stati membri della UE possano mantenere o introdurre ulteriori condizioni rispetto a tali categorie di dati. Più in particolare: il ***dato sensibile*** seppur estremamente rilevante NON è definito in modo espresso dal GDPR di talché occorre riferirsi alla normativa comunitaria (Direttiva 94/46/CE) che fa rientrare in questa categoria *ogni dato il cui trattamento potrebbe comportare rischi significativi per i diritti e le libertà fondamentali dell'individuo*. I ***dati genetici*** sono invece quelli relativi alle *caratteristiche genetiche ereditarie o acquisite che forniscono informazioni univoche sulla fisiologia e la salute di una persona*. Più problematica appare invece la definizione di ***dati biometrici***, tali essendo i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica tali da consentirne l'univoca identificazione (es. immagine facciale o impronte digitali). Il problema sta nel fatto che l'Art. 9 *non vieta il trattamento dei dati biometrici tout court* ma solo di quelli che *consentono in modo univoco ad identificare una persona*: così, ad esempio, una fotografia scattata mediante l'uso di una videocamera (il C51 parla di "*immagine facciale*") potrebbe non rientrare nella categoria di dato biometrico se non consente in modo univoco l'identificazione del soggetto ritratto.

[23] Venendo alle eccezioni al divieto, l'Art. 9 stabilisce che il trattamento dei dati sensibili, biometrici, genetici e relativi alla salute sia possibile nei seguenti casi:

a) Esplicito consenso rilasciato dal soggetto interessato (*salvo tale trattamento non sia, ab origine, vietato o limitato dal diritto degli Stati membri della UE*);
b) Trattamento necessario per esigenze connesse al diritto del lavoro, sicurezza e protezione sociale;
c) Il trattamento sia necessario a tutelare un *interesse vitale* dell'interessato il quale sia nell'incapacità giuridica (es. minore) o fisica (es. in coma) di prestare il consenso;
d) Il trattamento sia eseguito nell'ambito di associazioni o altri organismi senza scopo di lucro che perseguano finalità politiche, ideologiche o religiose;
e) I dati oggetto del trattamento siano resi *manifestamente pubblici* dallo stesso interessato;
f) Il trattamento sia finalizzato ad esercitare o difendere un diritto in sede giudiziaria;
g) Sussistano *motivi di rilevante interesse pubblico* al trattamento di tali categorie di dati;
h) Il trattamento sia finalizzato a scopi di medicina preventiva, medicina del lavoro, determinazione della capacità lavorativa di un dipendente, gestione o organizzazione di sistemi di servizi sanitari o sociali;
i) Il trattamento sia necessario *per motivi di interesse pubblico nel settore della sanità pubblica*;
j) Infine quando il trattamento dei dati sia correlato a finalità di archiviazione nel pubblico interesse, ricerca scientifica o scopi statistici.

→Ordini o limitazioni provvisorie o definitive di trattamento stabilite dall'autorità di controllo, come previsto dall'art. 58, paragrafo 2.

Da quanto riportato emerge che, a differenza di quanto previsto dall'attuale normativa interna, il GDPR introduce delle sanzioni effettive e particolarmente elevate per far fronte alla violazione dei principi fondamentali in materia di protezione dei dati personali. Per quanto sia vero che la concreta determinazione delle sanzioni andrà stabilita in stretto rapporto al contesto ed alla gravità della violazione, non può lasciare indifferenti il fatto che da un'informativa inadeguata resa agli interessati possano derivare sanzioni di un valore pari a 2 milioni di euro. È evidente che nell'ottica del GDPR al rispetto dei principi essenziali è riconosciuta un'importanza estrema; è altrettanto evidente, però, l'enorme portata potenziale di simili previsioni normative e la massima attenzione che i titolari dovranno porre per garantirne il rispetto.

Il GDPR precisa che ogni singola ipotesi di violazione delle disposizioni in esso sancite dovrà essere valutata singolarmente ai fini dell'applicazione delle sanzioni amministrative pecuniarie nel caso di specie.

A questo proposito, l'art. 83, paragrafo 2 stabilisce che: "*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 […]*". Segue un'elencazione delle circostanze che potranno incidere, appunto, sulla misura della sanzione che dovrà essere applicata, in modo da risultare adeguata e deterrente rispetto al contesto concreto in cui la violazione è stata realizzata.

Nel determinare la portata reale della sanzione si dovranno quindi tenere in debita considerazione:

a) la natura, la gravità e la durata della violazione con riferimento anche alla natura, all'oggetto o alla finalità del trattamento in questione, nonché al numero di interessati lesi dal danno e al livello del danno da essi subito.

L'autorità di controllo potrà quindi ritenere, innanzitutto, che le circostanze specifiche nel caso concreto oggetto di valutazione non creino un rischio significativo per i diritti degli interessati; in quest'ultimo caso la sanzione potrà anche essere sostituita da un semplice ammonimento. Occorrerà poi valutare il numero di interessati coinvolti, al fine di verificare se si tratta di un evento isolato o, piuttosto, di una violazione sistematica, la finalità del trattamento, che dovrà essere indicata specificamente e alla quale l'utilizzo dei dati dovrà essere conforme, l'entità dell'eventuale danno cagionato agli interessati e, infine, la durata della violazione.

b) Il carattere doloso o colposo della violazione. Con il concetto di "dolo" ci si riferisce, in generale, all'elemento soggettivo che qualifica una condotta posta in essere con la consapevolezza e l'intenzione di realizzare un determinato risultato illecito, mentre con il concetto di "colpa" si fa riferimento alla mancanza di consapevolezza e di intenzione dell'evento dannoso, dovuto piuttosto ad un mancato rispetto degli obblighi di diligenza stabiliti dalla legge. Una violazione dolosa è chiaramente più grave quella colposa, e di conseguenza potrà giustificare l'applicazione di una sanzione amministrativa pecuniaria.
c) Le misure adottate dal titolare o dal responsabile del trattamento per attenuare il danno subito dagli interessati. I titolari e i responsabili del trattamento devono porre in essere le misure tecniche e organizzative necessarie al fine di garantire un livello di sicurezza dei dati oggetto di trattamento che sia adeguato al rischio, effettuare valutazioni d'impatto sulla protezione dei dati e mitigare i rischi per i diritti e le libertà personali che possono derivare dal trattamento dei dati personali. In aggiunta, qualora si verifichi una violazione delle disposizioni del Regolamento tale da provocare dei danni in capo all'interessato, il soggetto responsabile dovrebbe comunque attivarsi per ridurre le conseguenze negative a carico dei soggetti coinvolti. Un tale comportamento, o l'assenza dello stesso, verrà senz'altro valutato

dall'autorità di controllo nella scelta della misura sanzionatoria da applicare nel caso specifico.

d) Il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto anche delle misure tecniche e organizzative da essi messe in atto. In particolare, a questo proposito si dovrà valutare anzitutto se il titolare o responsabile del trattamento abbiano adottato misure tecniche rispettose dei principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (privacy by design e by default), come previsto dall'art. 25, nonché misure di sicurezza adeguate al rischio come richiesto dall'art. 32.
e) Eventuali precedenti violazioni delle prescrizioni in materia di protezione dei dati personali commesse dal titolare o dal responsabile del trattamento. Per quanto riguarda questo aspetto, le autorità di controllo dovranno tenere nella giusta considerazione ogni tipo di precedente violazione del regolamento, anche se di natura diversa da quella esaminata nel caso di specie. Tali elementi potrebbero infatti essere pertinenti ai fini della valutazione, perché potrebbero fornire delle utili indicazioni su eventuale insufficiente livello di conoscenza o di indifferenza nei confronti delle norme sancite dal Regolamento per la protezione dei dati.
f) Il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione effettuata e attenuarne i possibili effetti negativi. Il GDPR non precisa, a questo proposito, in che modo l'autorità di controllo dovrà tenere conto degli sforzi dei titolari o dei responsabili del trattamento nel porre rimedio ad un'eventuale violazione già accertata. Tuttavia, nel decidere quale misura correttiva è la più adeguata nel singolo caso concreto, si dovrà prendere in considerazione anche l'eventuale attività del titolare o del responsabile del trattamento con cui siano state limitate, o addirittura annullate, le conseguenze negative a carico dei diritti e libertà degli interessati.
g) Le categorie di dati personali interessate dalla violazione. A questo proposito si dovrà valutare, ad esempio, se la violazione riguarda il trattamento di dati personali sensibili o se possa comunque causare immediati danni o disagi agli interessati.
h) Il modo in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che modo il titolare o il responsabile del trattamento hanno comunicato la violazione realizzata. Si ricorda che il titolare del trattamento ha l'obbligo di notificare all'autorità di controllo eventuali violazioni dei dati personali, quindi nel caso in cui si limiti ad adempiere, tale attività non potrà essere considerata come fattore attenuante al fine di disporre una sanzione minore. All'opposto, nel caso in cui il titolare o il responsabile del trattamento non abbia provveduto a notificare la violazione, l'autorità di controllo potrebbe ritenere di comminare una sanzione più grave
i) L'osservanza o inosservanza di eventuali altri provvedimenti o sanzioni disposti in precedenza nei confronti del titolare o del responsabile del trattamento e riguardanti lo stesso oggetto.
j) L'adesione ai codici di condotta o ai meccanismi di certificazione. Nel caso in cui il titolare o il responsabile del trattamento abbia aderito a un codice di condotta approvato, l'autorità di controllo potrebbe ritenere sufficiente che sia l'ente incaricato di gestire il codice ad intervenire direttamente nei confronti del proprio, senza quindi la necessità di imporre misure sanzionatorie aggiuntive.

Come si può notare, molteplici sono le circostanze che dovranno essere prese in considerazione per la determinazione della misura della sanzione concretamente applicabile.

Preme ribadire infatti che, come visto sopra, ciascuna ipotesi di violazione delle disposizioni sancite nel GDPR dovrà essere valutata singolarmente per la determinazione della misura della sanzione pecuniaria applicabile. Più nello specifico, si dovrà attendere l'effettiva applicazione del Regolamento per poter verificare come tali sanzioni saranno concretamente determinate, e se saranno eventualmente previsti degli scaglioni rispetto ai massimali previsti dall'art. 83 del

GDPR. Ad ogni modo, l'importo della sanzione da comminare nel caso specifico dovrà essere determinato sulla base delle circostanze che emergono nel caso concreto e non, quindi, in astratto e a priori.