LA TUTELA DELLA PRIVACY NELLE STRUTTURE SANITARIE (IL REGOLAMENTO UE 2016/679, COSIDDETTO GDPR, E IL DLGS ITALIANO 101/2018 DI ARMONIZZAZIONE)

a cura di Barbara Rizzato

Normativa di riferimento

Il 1° gennaio 2004 entrava in vigore il D.Lgs. 196/2003 denominato "Codice in materia di protezione dei dati personali".

L'intento del Legislatore è stato quello di garantire il diritto alla riservatezza sotto un duplice profilo:

1) l'interessato deve poter esprimere il proprio consenso all'utilizzo dei suoi dati personali e deve essere preventivamente informato circa finalità, modalità e tempi di trattamento degli stessi;

2) deve essere tutelata la sicurezza dei dati personali oggetto di trattamento, dal rischio:

- di conoscenza da parte di altri soggetti non autorizzati;
- di distruzione o perdita anche accidentale dei dati stessi.

Il 25 maggio 2018 è entrato poi in vigore il nuovo Regolamento UE 679/2016 (cosiddetto GDPR).

La sua operatività non è stata subordinata ad alcuna iniziativa da parte dei singoli Stati, con la conseguenza che le disposizioni nazionali in contrasto con la normativa comunitaria risultano comunque abrogate. L'obiettivo del Regolamento è infatti quello di garantire un sistema unitario in materia di privacy, superando la frammentazione delle normative nazionali.

L'Italia ha intrapreso un percorso di armonizzazione della nuova legislazione comunitaria culminato con l'approvazione del D.Lgs 101/2018 in vigore dal 19 settembre 2018. Il quadro normativo complessivo è quindi ormai oggi definito nella sua interezza, ciononostante i prossimi mesi saranno comunque significativi atteso che si attende l'approvazione di una serie di regole deontologiche specifiche differenziate per tipologie di dati e di trattamenti, la cui osservanza costituirà – per espressa previsione normativa – condizione essenziale per la liceità e correttezza del trattamento dei dati personali.

Glossario

Il trattamento dei dati

Il trattamento è qualsiasi operazione, svolta manualmente o in modo automatizzato, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.

Il trattamento deve inoltre essere:

- lecito
- finalizzato a scopi determinati, espliciti e legittimi
- relativo a dati esatti, aggiornati e non eccedenti lo scopo (nel rispetto della cosiddetta minimizzazione)
- limitato nel tempo (la conservazione è infatti consentita per un arco temporale definito comunque non eccedente il conseguimento delle finalità per le quali i dati sono trattati)

I dati personali. Ambito soggettivo ed oggettivo di applicazione del GDPR

I **dati personali** sono quei dati che consentono un'identificazione anche indiretta del soggetto (persona fisica) interessato dal trattamento. Si parla di **dati sensibili** quando i dati personali trattati sono idonei a rivelare – tra l'altro – lo stato di salute.

I **dati anonimi**, proprio in quanto tali, sono invece esclusi dagli obblighi imposti dalla normativa sulla Privacy. Sono anonimi i dati che non possono in alcun modo essere associati al soggetto cui si riferiscono.

Atteso che sotto il profilo soggettivo il GDPR si preoccupa solo della tutela dei dati delle persone fisiche, va sottolineato che sono conseguentemente esclusi dall'ambito di applicazione delle disposizioni del Regolamento i trattamenti dei dati relativi alle persone giuridiche.

Sotto il profilo oggettivo, invece, vale la pena sottolineare che la tutela interessa tutti i dati personali, ma in particolare quelli oggetto di trattamento *"interamente o parzialmente automatizzato"* nonché il *"trattamento non automatizzato di dati personali contenuti in un archivio".*

Il titolare del trattamento

Il titolare del trattamento è il soggetto (persona fisica, giuridica, pubblica amministrazione o qualsiasi altro ente) cui competono le decisioni in ordine alle finalità e alle modalità del trattamento dei dati dei pazienti.

Il responsabile del trattamento

Il responsabile del trattamento è il soggetto (persona fisica o giuridica) preposto dal titolare al trattamento dei dati. Non si tratta di un mero esecutore delle indicazioni fornitegli dal titolare, queste saranno infatti integrate da un punto di vista pratico e tecnico dal responsabile stesso.

Si tratta di una figura per lo più esterna alla struttura organizzativa del titolare, non soggetta alla sua autorità. Qualora nominato il responsabile, deve obbligatoriamente essere un soggetto che, per esperienza, capacità ed affidabilità, fornisca idonea garanzia del pieno rispetto delle disposizioni vigenti in materia di trattamento dei dati.

Gli incaricati al trattamento

Gli incaricati sono i soggetti (necessariamente persone fisiche) autorizzati dal titolare o dal responsabile a compiere specifiche operazioni di trattamento dei dati, sotto il controllo del titolare e/o del responsabile.

La legge impone al titolare di verificare ed aggiornare annualmente l'ambito di trattamento dei soggetti incaricati.

Il Data protection officer (DPO) – nuova figura introdotta dal GDPR

Si tratta di un organo indipendente di vigilanza del sistema di conformità al GDPR.

La nomina di tale figura è obbligatoria per le PA, nonché in presenza di circostanze di maggior rischio. Il ruolo può essere rivestito sia da persone interne che esterne all'azienda, purché siano garantite competenza specifica e indipendenza di giudizio.

Vale la pena in questa sede di sottolineare come la corretta individuazione dei soggetti del trattamento appaia particolarmente rilevante per quanto concerne l'aspetto sanzionatorio; le responsabilità connesse al trattamento dei dati gravitano infatti attorno alla figura del "titolare", soggetto preposto all'assunzione degli obblighi connessi al trattamento; tali responsabilità sono

però condivise con il "responsabile" qualora questi abbia violato gli obblighi del Regolamento specificamente diretti a lui o comunque le istruzioni che gli sono state impartite dal titolare.

Obblighi in capo al titolare del trattamento

Il principio dell'accountability e la soppressione degli obblighi di comunicazione preventiva

Il principio ispiratore del nuovo GDPR è quello dell'accountability, ovvero della responsabilizzazione del titolare del trattamento dei dati, che passa per una serie di iniziative che tale figura è chiamata ad assumere fattivamente all'interno della propria struttura, e che per converso esime il titolare stesso da tutte quelle comunicazioni preventive al Garante prima previste dal D.Lgs 196/2003 in specifici casi. Il risultato è quindi l'abrogazione degli obblighi preventivi di notificazione, comunicazione, autorizzazione (ivi comprese le autorizzazioni generali collettive) prima disciplinati dagli artt. dal 37 al 41 del codice sulla privacy.

Il GDPR impone quindi al titolare del trattamento di adottare modelli organizzativi e misure idonee a garantire la riservatezza dei dati trattati e la conformità del trattamento alle previsioni regolamentari. Non solo: il principio dell'accountability presuppone che il titolare sia in grado di dimostrare (in sede di verifica a suo carico) l'adeguatezza delle iniziative assunte.

Informativa al paziente

L'informativa (art. 13 D.Lgs. 196/03 e artt. 12-13-14 GDPR) è sempre obbligatoria, la stessa si arricchisce tra l'altro di nuovi contenuti per effetto dell'entrata in vigore del GDPR. Ne deriva che il titolare del trattamento, è tenuto ad adeguare il contenuto delle informative in uso nella propria struttura, non solo con riferimento ai nuovi trattamenti, ma anche con riferimento a quelli in corso.

Il titolare del trattamento di dati personali, dovrà preventivamente informare l'interessato circa:

a) l'esistenza del trattamento;
b) le finalità del trattamento (nel caso in cui durante il corso del trattamento dei dati, vari la finalità del trattamento stesso, deve esserne data comunicazione all'interessato);
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto;
d) il periodo di conservazione dei dati (oppure, ove non sia possibile definirlo, i criteri utilizzati per determinare il periodo di conservazione);
e) l'individuazione dei suoi diritti;
f) gli estremi identificativi del titolare, la presenza di eventuali soggetti responsabili ed eventualmente del DPO con i relativi dati di contatto.

Il GDPR impone anche che l'informativa sia resa con un linguaggio semplice e chiaro e che la stessa sia oggetto di un documento *ad hoc*, separato rispetto ad altri documenti che regolino i rapporti tra titolare e interessato. In tale previsione emerge in tutta la sua evidenza la volontà del legislatore comunitario di far sì che l'interessato sia messo nelle condizioni di realmente comprendere la portata del trattamento dei suoi dati e l'ampiezza dei suoi diritti.

E' senz'altro opportuno fornire le suddette informazioni per iscritto, facendo sottoscrivere al paziente la presa visione dell'informativa; quest'ultima, infatti, può essere fornita anche in forma

verbale, ma ciò comporta evidenti svantaggi sotto il profilo probatorio.

L'informativa deve essere resa nel momento in cui i dati vengono raccolti per la prima volta; nel caso in cui i dati vengano raccolti da un'altra fonte (quindi non direttamente dall'interessato) l'informativa va resa entro 30 giorni dalla raccolta.

Consenso al trattamento

Il consenso (art. 23 D.Lgs. 196/03 e art. 4 GDPR) è sempre obbligatorio, fatta eccezione per:
- i trattamenti derivanti dalla necessità di dare esecuzione ad un contratto;
- i trattamenti necessari per adempiere un obbligo previsto per legge;
- i trattamenti necessari per la salvaguardia di interessi vitali;
- i trattamenti giustificati dalla sussistenza di un legittimo interesse del titolare (sempre che non prevalgano interessi o diritti dell'interessato degni di maggiore tutela);
- i trattamenti ad opera di enti, associazioni ed ONLUS relativi ai dati degli associati;
- i dati relativi ai dipendenti per attività connesse al rapporto di lavoro.

Va altresì detto che la normativa introduce una semplificazione per i professionisti iscritti in albi relativi a professioni sanitarie, stabilendo che gli stessi sono esonerati dal richiedere il consenso al trattamento per finalità di cura e diagnosi, purchè sia correttamente assolto l'obbligo dell'informativa. Tale semplificazione investe però solo i singoli professionisti, non invece le strutture sanitarie organizzate in altra forma, inoltre il rilascio del consenso espresso rimane necessario in tutti i casi in cui il professionista intenda trattare i dati anche per scopi ulteriori rispetto alla cura e alla diagnosi, fosse anche solo per l'invio ai pazienti di comunicazioni di carattere informativo/promozionale rispetto all'attività svolta.

Ciò premesso, qualora il trattamento sia basato sul consenso (che si suggerisce comunque di considerare la regola generale nell'ambito delle strutture sanitarie), è necessario che il titolare sia in grado di dimostrare che l'interessato ha effettivamente inteso prestarlo. In tale contesto va detto che il GDPR introduce una specifica definizione di consenso stabilendo che quest'ultimo deve essere frutto di una *"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".*

Nel caso di trattamento di dati sensibili, è quindi opportuno che il consenso sia fornito per iscritto direttamente dall'interessato (mediante l'apposizione della firma). Il consenso per le persone incapaci e per i minori è reso da chi ne esercita legalmente la potestà.

Diritti dell'interessato

L'obbligo dell'informativa si interfaccia con il diritto dell'interessato ad avanzare specifiche istanze al titolare. I diritti dell'interessato escono ampliati dall'approvazione del GDPR, con la conseguenza che i diritti scaturenti dal nuovo assetto normativo risultano essere oggi i seguenti:
- diritto all'informativa (completa dei contenuti più sopra esplicitati)
- diritto di accesso ai dati
- diritto di chiederne la rettifica
- diritto di cancellazione (cosiddetto diritto all'oblio)
- diritto di limitazione del trattamento (raccolta di dati non eccedenti lo scopo e per periodi di tempo definiti)
- diritto alla portabilità (ovvero di ottenere in formato strutturato i propri dati per trasferirli ad

altro titolare)
- diritto di opposizione
- diritto alla profilazione

Nomina degli incaricati al trattamento

La figura dell'incaricato non è espressamente prevista dal GDPR, che fa però riferimento a *"persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile"*. Si tratta sostanzialmente di dipendenti e collaboratori interni alla struttura soggetti all'autorità del titolare.

Si deve ritenere che la nomina degli incaricati vada (come in passato) fatta per iscritto e che debba contenere la puntuale definizione dell'ambito entro cui il soggetto è legittimato a trattare i dati.

Va altresì precisato che l'obbligo di formazione degli incaricati e di vigilanza sull'operato degli stessi è condiviso da titolare e responsabile ed incide in maniera significativa sulla portata della loro responsabilità sotto il profilo sanzionatorio.

Nomina del responsabile del trattamento e la figura del contitolare

La sua nomina deve passare attraverso un contratto o comunque un atto giuridico il cui contenuto è disciplinato dall'art. 28 del GDPR. Quest'ultimo lo definisce come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

La nomina del responsabile va fatta per iscritto e deve contenere le istruzioni relative al trattamento affidatogli. La stessa deve garantire un certo grado di autonomia al responsabile atteso che questi condivide con il titolare le responsabilità connesse al trattamento; tale condivisione di responsabilità implica che il soggetto designato debba manifestare l'accettazione della nomina mediante sottoscrizione della stessa.

Una novità importante del GDPR è data dalla possibilità di nominare soggetti sub responsabili, facoltà quest'ultima che consente una migliore organizzazione soprattutto con riferimento al trattamento affidato a soggetti esterni all'organizzazione del Titolare. Va precisato però che il responsabile non può mai ricorrere ad altro responsabile senza aver previamente acquisito autorizzazione

Perseguendo la medesima logica, il Regolamento comunitario introduce anche la figura del contitolare. L'art. 26 del GDPR specifica infatti che *"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".*

Il responsabile della protezione dei dati – RDP o DPO

Si tratta di una figura nuova rispetto alle previgenti disposizioni del D.Lgs 196/2003. Tale figura è disciplinata dagli artt. 37. 38 e 39 del GDPR, la sua nomina è obbligatoria solo in specifici casi, in particolare lo è:

- per i soggetti pubblici, a prescindere dal tipo di dati trattati;

- per gli altri soggetti, che come attività principale effettuino un monitoraggio costante e su larga scala delle persone fisiche o di particolari dati sensibili.

Dalle FAQ diffuse dal Garante Privacy emerge il chiaro pensiero che le società operanti nel settore della cura della salute, della prevenzione e della diagnosi sanitaria siano tenute alla nomina del DPO; la necessità di procedere a tale nomina pare invece meno sentita negli studi mono-professionali (in tal senso anche il decreto di armonizzazione 101/2018), pur restando però necessaria una valutazione specifica che tenga conto di volta in volta del caso concreto. Ciò premesso, va altresì detto che, anche ove il Regolamento non imponga la designazione di un DPO, la sua nomina su base volontaria è comunque incoraggiata, atteso che lo stesso funge da interfaccia tra i soggetti coinvolti. In tal caso è necessario che – se nominato – il DPO rispetti i requisiti previsti dagli art. 37 e 39 del Regolamento. Va altresì considerato che la nomina del DPO, attribuendo comunque dei compiti di consulenza e di vigilanza, costituisce evidentemente un costo aggiuntivo per il titolare che può essere giustificato solo in casi di effettiva esigenza.

Il responsabile della protezione dei dati non risponde personalmente in caso di inosservanza del GDPR, i soggetti tenuti ad assicurare il rispetto della normativa sono infatti il titolare e il responsabile del trattamento. E' inoltre auspicabile che questi ultimi documentino le valutazioni compiute per stabilire se si applichi o meno l'obbligo di nomina di un DPO nel caso di specie.

Specifiche linee guida sui **responsabili della protezione dei dati** sono state adottate dal gruppo di lavoro art. 29 WP 243 il 13 dicembre 2016 e revisionate il 5 aprile 2017. Le stesse, precisando ed integrando i contenuti di massima fissati dal GDPR, affrontano in dettaglio requisiti e compiti del DPO che possiamo brevemente riassumere come segue:

Requisiti del DPO
È designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e della capacità di assolvere i compiti di cui all'art.39. La nomina deve garantire indipendenza e assenza di conflitto di interessi, in particolare il DPO non può quindi rivestire un ruolo che comporti la definizione delle finalità o delle modalità di trattamento (che spettano invece al titolare e al responsabile).

Compiti del DPO
Deve informare e fornire consulenza al titolare e/o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal regolamento comunitario, nonché sorvegliare sulla sua osservanza.
Partecipa altresì con titolare e responsabile a tutte le questioni riguardanti la protezione dei dati, formulando pareri, in particolare nello svolgimento della valutazione d'impatto sulla protezione dei dati (cosiddetta DPIA).
Infine coopera nell'attività di controllo, è punto di contatto e facilitatore in caso di violazioni o di esercizio dei propri diritti da parte degli interessati al trattamento.

Il Regolamento UE e l'ineludibile adeguamento dei sistemi IT aziendali

Il quadro normativo che esce dal Regolamento UE 679/2016 induce a soffermarsi sull'esigenza per tutti gli operatori economici di investire in innovazione e in sicurezza informatica.

Muovendo sempre dal principio ispiratore della cosiddetta "accountability", il GDPR stabilisce che il titolare del trattamento dei dati è responsabile dell'individuazione e dell'attuazione dei principi di "data protection", nonché della capacità di dimostrarne la conformità al Regolamento stesso.

Si stabilisce quindi un principio generale, che si svincola dalle precedenti formalità dettate del codice sulla privacy per prediligere un approccio sostanziale: è il titolare del trattamento che deve adottare un sistema di gestione e controllo che garantisca la conformità delle proprie operazioni di trattamento dei dati personali al GDPR. Egli dovrà quindi poter dimostrare che l'assetto organizzativo prescelto e l'insieme delle procedure operative adottate sono adeguati a garantire il rispetto della normativa, secondo un approccio basato sul rischio.

Della correttezza delle valutazioni fatte in autonomia circa l'impianto di misure da adottare, il titolare risponde innanzi al Garante della Privacy (che riveste un ruolo di autorità di supervisione) e innanzi al giudice ordinario.

Un'adeguata valutazione "data protection" è quindi la base di partenza essenziale della responsabilizzazione (accountability). Il titolare risulterà responsabilizzato se il processo valutativo è stato sviluppato in modo corretto in funzione della pericolosità del trattamento dei dati. E' quindi indispensabile dedicare risorse e procedure interne fin dalla fase della valutazione preventiva, avendo cura di monitorare costantemente nel tempo le eventuali modifiche alle operazioni di trattamento che possano richiedere l'adozione di procedure diverse (si pensi al caso in cui lo sfruttamento dei dati personali avviene per finalità diverse da quelle originarie).

La dimostrazione di aver posto in essere un processo di valutazione adeguato passa poi necessariamente per l'individuazione di procedure che impongano ad ogni operatore che compia operazioni di trattamento dei dati di rispettare specifiche istruzioni o vincoli contrattuali imposti dal titolare medesimo. Va da sé che il titolare, nel conferimento di incarichi specifici, dovrà fornire istruzioni dettagliate agli operatori incaricati al trattamento e dovrà altresì verificare che i comportamenti di questi ultimi siano conformi alle linee guida diffuse, se del caso anche nominando un DPO – Data Protection Officer (di cui si è detto al paragrafo precedente).

Manifestazione documentale del rispetto del principio di accountability sarà poi l'istituzione e il periodico aggiornamento del Registro dei Trattamenti e semmai della valutazione d'impatto (cosiddetta DPIA), da effettuare nel caso di trattamento di dati a potenziale rischio elevato che richiedono una valutazione, per così dire, rafforzata.

Dalle evidenze fin qui esposte, emerge chiaramente che - in caso di verifica o di insorgenza di un problema con un soggetto interessato al trattamento - la prova di aver adottato misure sufficienti alla tutela dei dati trattati (sul cui significato torneremo diffusamente nel prossimo paragrafo) non potrà che essere di natura documentale. Va però precisato che il DLgs 101/2018 si è espresso nel senso di ritenere sovrabbondante (e quindi non obbligatorio) il Registro dei Trattamenti negli studi monoprofessionali, atteso che il pre-requisito della sussistenza di trattamenti di dati sensibili su larga scala pare difficilmente realizzarsi in strutture monoprofessionali.

Le misure di sicurezza sufficienti

Se facciamo riferimento a quanto disciplinato dal D.lgs 196/2003, le misure di sicurezza venivano definite come il complesso di misure tecniche, organizzative, logistiche e procedurali atte a ridurre al minimo i rischi di perdita o di distruzione anche accidentale dei dati, di accesso non autorizzato, di trattamento illecito.

Il codice sulla privacy individuava, nell'ambito delle misure di sicurezza, delle misure minime, illustrate nel disciplinare tecnico (allegato B del codice).

L'approccio del nuovo GDPR è differente: quest'ultimo non richiede più l'adozione delle misure minime di sicurezza puntualmente previste dal disciplinare tecnico, ma richiede invece l'adozione

di **misure sufficienti** al rispetto degli obblighi, senza dare indicazioni specifiche, ma ponendo l'obiettivo generale dell'adeguatezza delle misure adottate. Spetta quindi al titolare del trattamento di individuare gli interventi necessari per adeguarsi alla normativa comunitaria, mettendo a punto procedure e affidando specifici incarichi agli operatori, tenendo conto di quali trattamenti vengono effettuati, su quali dati e con quali finalità, con un approccio che garantisca prevenzione ed efficacia. L'adozione di misure sufficienti passa poi per la chiarezza e la prevenzione: l'impianto di regole, procedure e documenti da utilizzare, la definizione di organigrammi e ruoli deve essere *in primis* chiaro e funzionale a prevenire e contenere un potenziale problema.

E' pertanto fondamentale individuare un percorso strutturato che conduca alla piena attuazione dei principi contenuti nel GDPR, che potremmo così schematizzare:

- ricognizione e classificazione dei trattamenti di dati personali
- l'individuazione dei rischi che incombono sui dati ed eventuale predisposizione della valutazione d'impatto - DPIA
- mappatura dei soggetti da autorizzare (incaricati) o ai quali conferire nomine specifiche di natura contrattuale (responsabili)
- individuazione delle misure sufficienti a garantire la sicurezza e la riservatezza dei dati e programmazione sistematica di verifiche periodiche dell'efficacia delle misure adottate, in modo da garantirne l'adeguatezza nel tempo anche in ragione delle mutate tecnologie o dei mutati tipi di trattamento o di finalità
- formazione degli operatori e programmazione di un'attività di vigilanza costante ed eventuale nomina del DPO

La realizzazione di tale percorso va comprovata dalla rendicontazione sistematica e standardizzata di tutte le attività svolte, che potrà se del caso essere contenuta nel registro dei trattamenti, ma ben potrà essere esposta anche in un documento privo di requisiti di forma specifici, laddove vengono enucleate le procedure di sicurezza adottate.

Il registro dei trattamenti (art. 30)

Una delle misure centrali è il registro dei trattamenti, obbligatorio per i titolari con oltre 250 dipendenti e nel caso di trattamento di dati sensibili su larga scala. Questo registro, se istituito, per sua natura e contenuti, ben si adatta alla necessità di provare quanto si è fatto per la tutela della privacy.

Il registro conterrà infatti l'indicazione del titolare, del responsabile e del ruolo rivestito dai vari operatori, nonché dei dati di contatto di tutte le figure privacy; si soffermerà sulle caratteristiche del trattamento nel caso di specie, individuando finalità, categorie di dati, sistemi e misure adottati a tutela degli interessati, modi di trasferimento dei dati, ecc….

La valutazione d'impatto – DPIA (art. 35)

Si tratta di una valutazione che ha carattere preventivo rispetto al trattamento dei dati, richiesta obbligatoriamente:

per trattamenti su larga scala
per trattamenti che contemplano la profilazione dei soggetti interessati
per la sorveglianza di zone accessibili al pubblico su larga scala

La DPIA ha lo scopo di individuare in via preventiva le misure tecnico-organizzative atte a ridurre il rischio a livelli contenuti.

Data Breach (art. 33 e 34)

Il GDPR impone al titolare l'obbligo di notifica al Garante degli eventuali casi di violazione dei dati. Tale notifica deve avvenire entro 72 ore dall'avvenuta conoscenza, in caso di ritardo nella notifica, vanno esplicitati i motivi del ritardo.

La notifica deve contenere:

- la descrizione della natura della violazione
- le categorie di dati violati
- gli interessati o le categorie dei dati violati
- il numero approssimativo di registrazioni di dati personali

- comunicazione dei dati di contatto delle figure privacy
- descrizione delle probabili conseguenze
- possibile risoluzione o attenuazione degli effetti negativi

La notifica della violazione deve essere fatta anche all'interessato ma solo nei casi in cui la violazione può determinare un rischio elevato ai diritti e alle libertà della persona fisica.

Strumenti di compliance volontaria per attenuare la pericolosità e formazione dei soggetti preposti al trattamento

Il GDPR introduce la possibilità per le associazioni e gli organismi di rappresentanza delle varie categorie di titolari del trattamento, di introdurre dei codici di condotta allo scopo di dettare linee guida uniformi per la corretta applicazione del Regolamento.

Analogamente viene anche introdotta la possibilità di acquisire certificazioni finalizzate a dimostrare la conformità dell'assetto privacy al GDPR. In tale contesto, i titolari del trattamento possono infatti sottoporsi volontariamente ad un'attività di audit (un iter di esami e controlli) che, se svolta da parte di enti certificatori, culmina per l'appunto nel rilascio di un certificato avente validità triennale. La certificazione non elimina le responsabilità in capo a titolari e responsabili e lascia d'altro canto impregiudicata l'attività di controllo e quella sanzionatoria, ma è evidente che l'adozione di una procedura di audit (sfociante o meno nell'ottenimento di una certificazione) è di per sé dimostrazione che il titolare ha inteso adottare strumenti di compliance volontaria con lo scopo di ridurre la pericolosità dei trattamenti posti in essere.

Sanzioni

Quanto alle **sanzioni** applicabili, queste sono disciplinate dal GDPR che prevede due diverse forme di tutela per l'interessato: una tutela giurisdizionale atta ad ottenere il riconoscimento del diritto al risarcimento del danno e una tutela amministrativa che prevede l'applicazione di pesanti sanzioni pecuniarie diversificate in funzione del tipo di violazione contestata.

Il titolare del trattamento dei dati risponde del danno nel caso in cui il suo comportamento violi il Regolamento, il responsabile risponde invece del danno in caso di violazione diretta del Regolamento (con ciò intendendo violazione degli obblighi che il GDPR pone direttamente a carico dei responsabili o in caso di mancato rispetto delle istruzioni fornite dal titolare). Ne deriva che l'azione per il risarcimento del danno patrimoniale e/o morale ex art. 2050 c.c. potrà essere promossa dall'interessato tanto nei confronti del titolare del trattamento, quanto nei confronti del responsabile (che potrà diversamente essere chiamato a rispondere del danno cagionato

anche in forma di rivalsa ad opera del titolare stesso). Si ritiene altresì che potranno essere chiamati a rispondere di eventuali danni anche gli incaricati al trattamento, ma solo nei casi di grave negligenza, imprudenza, imperizia, nonché di violazione del segreto professionale; in capo agli incaricati si potrà pertanto profilare solo un'eventuale responsabilità per fatto proprio, mai per fatto altrui.

Quanto alle sanzioni pecuniarie, queste non sono fissate nella loro entità, ma solo nel loro limite massimo (si arriva a parlare addirittura di sanzioni fino a 10 milioni di € o fino al 2% del fatturato annuo dell'impresa, se non addirittura fino a 20 milioni di € o fino al 4% del fatturato annuo per violazioni più gravi).

Le autorità preposte al controllo, pur agendo in piena indipendenza, dovrebbero garantire che in caso di violazione del regolamento comunitario saranno imposte sanzioni equivalenti. Il GDPR precisa anche che le sanzioni amministrative pecuniarie devono essere effettive, proporzionate e dissuasive. Sotto questo profilo va quindi tenuto presente che l'entità delle sanzioni è fissata tenendo conto anche di una serie di fattori attenuanti o aggravanti, così come individuati (pur in modo non esaustivo) dalle linee guida WP 253 adottate dal gruppo di lavoro art. 29 il 3 ottobre 2017. La natura della violazione, l'oggetto e la finalità del trattamento, nonché il numero di interessati lesi e il livello del danno da questi subito, sono circostanze che vanno valutate dalle autorità di controllo nella loro complessità ai fini dell'individuazione della sanzione da irrogare. In questo contesto, sarà valutata anche la durata dell'infrazione (che potrebbe essere sintomatica anche del fatto che il titolare non è in grado di attuare le misure organizzative necessarie alla tutela dei dati), nonché il carattere doloso o colposo della violazione (ravvisabile quest'ultimo anche nel caso di mancata adozione di misure preventive appropriate).

In caso di violazioni minori, tra l'altro, la sanzione può essere sostituita da un ammonimento, in particolare quando il titolare del trattamento è una persona fisica e la sanzione applicabile costituirebbe un onere sproporzionato tenendo conto delle circostanze del caso specifico.

Quanto alla responsabilità in sede penale del titolare del trattamento ed eventualmente del responsabile, si deve ritenere che la contestazione di una fattispecie di reato potrà essere mossa direttamente nei confronti del titolare del trattamento se si tratta di una persona fisica. Nel caso in cui invece si tratti di una persona giuridica (ente, società, ecc...) il procedimento penale sarà avviato a carico di coloro che (persone fisiche) ricoprono ruoli decisionali all'interno della struttura titolare del trattamento. Agli incaricati potrà invece essere ascritta una qualche responsabilità penale solo in ragione di una condotta criminosa degli stessi che non poteva essere impedita dal titolare o dal responsabile.

Documento aggiornato ad ottobre 2018