Luigino Bottini
Dottore Commercialista – Revisore Legale
info@luiginobottini.com - *www.luiginobottini.com*

Contitalia S.r.l.
Centro Elaborazione Dati ed Elaborazione Paghe per conto terzi.
Via Nino Bixio 18/4 – Chiavari (Ge) – Tel. 0185.322469 - Fax 0185.313184
Via Strada Privata n. 2/A - Santa Maria del Taro - Tornolo (Pr)- Tel. 0525.80100
contital@contitalia.191.it

Circolare informativa 07/2018. **Chiavari, 4 maggio 2018.**

Ai gentili Clienti

SPECIALE PRIVACY

Come noto, la disciplina in materia di Privacy è contenuta nel D.Lgs. n. 196/2003. Con il Regolamento 27.4.2016, n. 679 (GDPR) il Legislatore comunitario ha "uniformato" la disciplina in esame applicabile negli Stati membri **a decorrere dal 25.5.2018**.

L'art. 13, Legge n. 163/2017 ha delegato il Governo all'emanazione di un apposito Decreto di adeguamento del quadro normativo nazionale alle disposizioni contenute nel citato Regolamento n. 679/2016. In data 21.3.2018 è stata approvata dal Consiglio dei Ministri la bozza del predetto Decreto.

In sintesi lo schema di Decreto prevede l'abrogazione del citato D.Lgs. n. 196/2003 e la costituzione del nuovo Codice della Privacy richiamando le disposizioni del Regolamento UE n. 679/2016 e inserendo specifiche disposizioni, tra cui le sanzioni penali.

DEFINIZIONI

L'art. 4, Regolamento UE n. 679/2016 fornisce tra l'altro le seguenti definizioni.

Dato personale	**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.

Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Titolare del trattamento	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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Responsabile del trattamento	La persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Consenso dell'interessato	**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.
Violazione dei dati personali	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati relativi alla salute	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

FINALITÀ DEL REGOLAMENTO UE

L'introduzione del citato Regolamento UE n. 679/2016 sul trattamento dei dati ha, come scopo principale, l'armonizzazione delle regole sul trattamento dei dati in tutta l'Unione Europea.

Precedentemente all'emanazione delle nuove norme, la protezione del dato personale, considerato una parte fondante della personalità dell'individuo, era minacciata dalla differenza di regole che presiedevano al trattamento del dato.

L'armonizzazione dei principi su tutto il territorio comunitario e l'obbligo per i soggetti che tratteranno dati dei cittadini comunitari di adeguarsi ai dettami del Regolamento, si prefigge lo scopo di eliminare le lacune di protezione che incombevano sui dati allorquando questi ultimi circolavano tra i diversi titolari. Il Legislatore ha inteso limitare la potenziale portata negativa per le libertà degli interessati nata dalla rapida diffusione e pervasività delle nuove tecnologie che hanno notevolmente ristretto le distanze tra i diversi Stati.

Infatti, se precedentemente all'introduzione del Regolamento l'applicabilità della legge era definita considerando la sede del Titolare, con la nuova normativa si dovrà considerare la residenza del cittadino all'interno dei confini europei.

Un approccio di questo tipo consentirà di imporre ai Titolari del trattamento, anche residenti al di fuori dell'UE, il rispetto del Regolamento e quindi garantirà un maggior grado di protezione ai cittadini quandanche dovessero utilizzare beni e servizi offerti da soggetti non comunitari.

Oltre a ciò, l'introduzione dei principi di **data protection by design** e **data protection by default** mira, in ultima analisi, a far si che la protezione della sfera privata dell'interessato venga considerata fin dalla progettazione dei trattamenti, imponendo ai titolari la minimizzazione della raccolta, comunicazione e utilizzo dei dati.

La limitazione della raccolta in termini qualitativi e quantitativi, infatti, deve essere valutata in funzione delle finalità per cui è stata prevista, senza indulgere nella tentazione di assicurarsi un maggior numero di informazioni rispetto allo scopo previsto.

APPROCCIO BASATO SUL RISCHIO E PRINCIPIO DI ACCOUNTABILITY

La nuova impostazione, in riferimento all'utilizzo di dati ed informazioni, si basa sostanzialmente su un approccio che vuole arrivare alla **massima riduzione del rischio per la libertà e la dignità del cittadino**.

Per ottenere questo scopo, il Legislatore ha introdotto il **principio di accountability**, inteso quale "**responsabilizzazione**" e di un concomitante obbligo di rendicontazione delle misure intraprese per essere coerenti con il nuovo impianto normativo.

La finalità ultima dell'introduzione del nuovo principio parte dall'assunto che l'obbligo di dimostrare il rispetto della normativa, posto in capo al Titolare del trattamento, è già, di per sé stesso, una garanzia di rispetto della norma imponendo un passaggio da una protezione meramente formale ad una protezione sostanziale generata dalla necessità di dover dimostrare, nel corso del tempo, l'adozione di misure realmente efficaci.

INFORMATIVA E CONSENSO

Nella previgente disciplina l'Informativa non doveva avere particolari requisiti, ma solo dei contenuti specifici, elencati nell'art. 13, D.Lgs. n. 196/2003.

Il Regolamento UE n. 679/2016, invece, oltre a **definirne i contenuti**, fissa anche le regole necessarie a rendere effettiva la comprensione ed efficacia dell'Informativa.

Ispirandosi direttamente al principio di trasparenza (art. 5, par. 1, lett. a) il Legislatore impone al Titolare la predisposizione di Informative accessibili, **concise e scritte con un linguaggio chiaro e semplice**, di facile comprensione.

La ratio sottesa a questo principio è quella di consentire all'Interessato una comprensione realmente efficace dei trattamenti a cui saranno sottoposti i propri dati, così da poter decidere con cognizione di causa se concedere o meno il proprio consenso.

L'Informativa, infatti, è l'elemento che permette di **fornire un consenso valido** poiché i requisiti richiesti per acconsentire al trattamento dei dati, fin dalla formulazione contenuta nell'art. 23, D.Lgs. 196/2003, erano la libertà, la specificità e l'informazione resi mediante un atto documentabile.

I requisiti di validità del consenso rimangono sostanzialmente invariati anche nella formulazione dell'art. 4. par. 11, Regolamento UE n. 679/2016, ma viene aggiunto il **requisito di validità**. Il consenso sarà **valido** solo se la volontà dell'interessato è **espressa in modo inequivocabile** per ogni singolo trattamento.

INFORMATIVA ALL'INTERESSATO

Il contenuto dell'Informativa deve rispettare quanto previsto dagli artt. 13, par. 1 e 14, par. 1, Regolamento n. 679/2016. In particolare deve essere specificata la base giuridica del trattamento, il trasferimento dei dati in Stati terzi e, in caso positivo, tramite quali canali, **il periodo di conservazione dei dati, le finalità del trattamento** nonché i diritti dell'interessato.

Come sopra accennato l'Informativa deve avere **forma concisa, trasparente, intelleggibile per l'interessato e facilmente accessibile** (occorre utilizzare un linguaggio chiaro e semplice). L'Informativa, in linea di principio, è data **per iscritto** e preferibilmente in formato elettronico.

CONSENSO DELL'INTERESSATO

Con riferimento ai dati "sensibili" è previsto il consenso "esplicito". In tutti i casi deve essere libero, specifico, informato e inequivocabile (non è ammesso il consenso tacito o presunto).

Non necessariamente deve essere "documentato per iscritto", ne è richiesta la "forma scritta", anche se ciò è considerata una modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili). Deve essere manifestato attraverso una "*dichiarazione o azione positiva inequivocabile*".

FIGURE DEL TRATTAMENTO

Per consentire un'efficace catena di protezione del dato personale durante le attività di trattamento è necessario procedere ad un tracciamento della catena di custodia e utilizzo dell'informazione attraverso la definizione di ruoli e compiti all'interno della struttura del Titolare.

In quest'ottica, il D.Lgs. n. 196/2003 aveva già introdotto l'obbligo di individuare l'organigramma dei soggetti coinvolti nelle attività di trattamento del dato.

Principalmente la struttura si fondava sulle figure del Titolare, del Responsabile (interno od esterno) e degli Incaricati.

A differenza di quanto previsto dal D.Lgs. n. 196/2003 che assegnava formalmente un ruolo all'Incaricato, la nuova disciplina del Regolamento UE n. 679/2016 fa riferimento a "***chiunque** agisca sotto la responsabilità*" del Titolare o del Responsabile o alle "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*" è tuttavia stato chiarito che il personale dipendente può accedere e trattare i dati solo se ha ricevuto un **inquadramento formale e solo entro i limiti delle istruzioni ricevute**.

Questa impostazione fa rimanere attuale l'obbligo di procedere ad un atto di **nomina formale** per i soggetti autorizzati al trattamento dei dati personali.

Per quel che riguarda la figura del Responsabile del trattamento, come sopra accennato, l'art. 4, par. 8, Regolamento UE n. 679/2016 lo definisce "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

La prassi italiana, fino ad ora, ha sempre individuato la figura del responsabile interno e quella del responsabile esterno del trattamento.

Questa impostazione non sembra trovare continuità nel Regolamento UE n. 679/2016 che sostanzialmente divide nettamente i ruoli interni (soggetti autorizzati) da quelli esterni (responsabili) all'organizzazione del Titolare.

Un valido sostegno a questa impostazione è ravvisabile nel testo dell'art. 29, Regolamento UE n. 679/2016 che sembra delineare una **chiara distinzione tra i ruoli interni** (coloro che agiscono sotto l'autorità del titolare) **ed esterni** (coloro che agiscono sotto l'autorità del Responsabile).

Di contro, l'art. 4, par. 8, nel definire il Responsabile, laddove introduce il concetto di "servizio", sembra lasciare aperta la strada anche ad una ripartizione interna. Quest'ultimo aspetto, però, potrebbe nascere da un equivoco di traduzione, lasciando quindi aperta la strada all'interpretazione più orientata alla distinzione tra ruoli interni ed esterni.

Una novità importante dal punto di vista organizzativo viene introdotta dalla possibilità di **nomina di sub responsabili** che consentirà una migliore mappatura dei flussi di dati esterni all'organizzazione del Titolare.

Sempre nell'ottica della tracciabilità dei flussi di dati e delle garanzie per gli interessati, il Regolamento comunitario introduce anche la figura del **Co-titolare**.

L'art. 26, Regolamento UE n. 679/2016 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, 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*".

RESPONSABILE DEL TRATTAMENTO DATI

È designato dal Titolare del trattamento, **tramite contratto** nel quale dovranno essere specificate tassativamente almeno le materie di cui all'art. 28, par. 3, Regolamento UE n. 679/2016. Allo stesso sono imputabili **specifici obblighi** distinti da quelli di pertinenza del Titolare.

In particolare deve:

- tenere il **Registro dei trattamenti** svolti (non richiesto per i soggetti con meno di 250 dipendenti che non effettuano "trattamenti a rischio" ex art. 30, par. 5, Regolamento UE n. 679/2016) contenente un quadro aggiornato dei trattamenti in essere all'interno dell'azienda "indispensabile per ogni valutazione e analisi del rischio";
- adottare misure tecniche e organizzative per **garantire la sicurezza dei trattamenti**;
- designare, nel caso in cui sia necessario, il **Responsabile per la protezione dei dati** (RPD / Data Protection officer – DPO).

RESPONSABILE DELLA PROTEZIONE DEI DATI

Rappresenta una nuova figura non prevista dalla previgente disciplina, finalizzata a facilitare l'attuazione della disciplina in materia di Privacy da parte del Titolare / Responsabile.

Il RPD assolve **funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento UE n. 679/2016**.

È una **figura obbligatoria** per i soggetti le cui attività consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala** o un trattamento su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati.

Come desumibile dalle specifiche FAQ disponibili sul sito Internet del Garante della Privacy, sono tenuti alla normativa, ad esempio: istituti di credito, imprese assicurative, società finanziarie, società di revisione controllo, CAF e patronati, società operanti nel settore della cura della salute, della prevenzione / diagnostica / diagnostico sanitaria.

Lo stesso Garante specifica che nei **casi diversi** da quelli sopra richiamati, la designazione del RPD non è obbligatoria (ciò si riscontra, ad esempio, in relazione ai trattamenti effettuati da **liberi professionisti operanti in forma individuale**, agenti / rappresentanti / mediatori operanti non su larga scala, imprese individuali / familiari / piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti).

Il ruolo di RPD può essere ricoperto **da un dipendente del Titolare o del Responsabile** (non in conflitto di interessi) che conosce la realtà operativa in cui avvengono i trattamenti; L'incarico può essere affidato **anche a soggetti esterni**, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento UE n. 679/2016 assegna a tale figura.

DIRITTI DEGLI INTERESSATI

I diritti riconosciuti all'interessato sono elencati negli articoli da 12 a 29 del Regolamento UE n. 679/2016. Molti di questi diritti erano già riconosciuti dall'art. 7, D.Lgs n. 196/2003; il Regolamento comunitario introduce garanzie ulteriori.

Le più rappresentative sono il **diritto alla portabilità** del dato ed il **diritto all'oblio**.

La logica ispiratrice del diritto alla portabilità del dato è quella di consentire all'interessato di poter disporre e, di conseguenza, controllare, il proprio dato utilizzandolo per scopi diversi evitando pratiche scorrette tese, soprattutto, ad impedire la portabilità del dato ed a creare una fidelizzazione "forzata" dell'utente di un servizio.

Il diritto all'oblio vuole tutelare l'interessato quando, la circolazione di informazioni che lo riguardano, essendo venuto meno l'interesse pubblico a conoscerle, diventa lesiva della sua onorabilità.

Viene quindi riconosciuto che il bilanciamento dell'interesse del cittadino alla riservatezza con l'interesse pubblico all'informazione, possa, nel tempo, subire delle modificazioni. Va in ogni caso precisato che la valutazione in ordine al bilanciamento di interessi non può essere fondata solamente su un fattore cronologico, ma va legata anche ad altri fattori quali la gravità degli eventi, il valore sociale dell'informazione e molti altri.

COME APPROCCIARE IL CAMBIAMENTO

La migrazione verso i nuovi concetti di tutela e riduzione del rischio può essere alquanto laboriosa ed onerosa sia dal punto di vista organizzativo che economico.

Fondamentale, nell'ottica dell'organizzazione dei processi è individuare un percorso strutturato che conduca alla piena attuazione dei principi contenuti nel Regolamento UE n. 679/2016.

Dando per scontata la necessaria conoscenza della normativa, la prima attività da compiere è una **ricognizione ed identificazione** dei trattamenti di dati personali, che potrà, poi sfociare nella predisposizione del registro dei trattamenti svolti.

Dopo la classificazione delle categorie di trattamenti di dati, sarà necessario individuare le unità aziendali che se ne occupano con la mappatura dei **soggetti da autorizzare**.

L'operazione più importante, però, sarà l'individuazione dei **rischi che incombono sui dati**, che potrà eventualmente sfociare nella predisposizione di una valutazione di impatto dei trattamenti (DPIA) e la conseguente adozione di contromisure adeguate.

Il Regolamento UE n. 679/2016, però, introducendo il principio di accountability, intende responsabilizzare il Titolare imponendogli il mantenimento della sicurezza dei trattamenti nel tempo, anche in ragione dell'evoluzione tecnologica.

Non sarà quindi più sufficiente intendere la protezione del dato come sistema statico, ma sarà necessario procedere a **valutazioni periodiche** dell'esistente e ad analisi preventive in caso di introduzione di nuove tipologie di trattamento.

Ciò implica non solo una costante attenzione e verifiche periodiche dell'efficacia delle misure individuate, ma anche una costante valutazione del contesto in cui avviene il trattamento perché non è necessariamente detto che ciò che andava bene prima debba andare bene anche dopo.

In conclusione, va segnalato che sarà di fondamentale importanza la documentazione e rendicontazione di tutte le attività svolte per la tutela della riservatezza del dato.

Sarà quindi necessario dotarsi di **procedure interne organizzate e standardizzate** che consentano il monitoraggio di ogni fase di trattamento nell'ottica della riduzione del rischio e l'organizzazione di momenti formativi per i soggetti autorizzati (obbligatori ex art. 29, Regolamento UE n. 679/2016).

REGIME SANZIONATORIO

L'art. 83, par. 3 e 4, Regolamento UE n. 679/2016 prevede 2 distinte categorie di sanzioni amministrative pecuniarie a seconda della natura della violazione. In particolare, sono previste le seguenti sanzioni:

- **fino al 2% del fatturato** dell'esercizio precedente per le sanzioni relative agli obblighi:
  - del Titolare / Responsabile del trattamento;
  - dell'Organismo di certificazione;
  - dell'Organismo di controllo;
- **fino al 4% del fatturato** dell'esercizio precedente per le violazioni relative: ai principi base del Trattamento, comprese le condizioni di consenso;
  - ai diritti degli Interessati;
  - ai trasferimenti dei dati personali a un destinatario di uno Stato terzo o un'organizzazione internazionale;
  - a qualsiasi obbligo ai sensi della legislazione nazionale adottata a norma del Capo IX;
  - all'inosservanza di un ordine, di una limitazione provvisoria / definitiva di trattamento o di un ordine di sospensione dei flussi di dati all'Autorità di controllo o il negato accesso.

Merita infine sottolineare che, con il recente Comunicato 19.4.2018, il Garante della Privacy è intervenuto **smentendo** la notizia circolata su Internet, circa **un possibile differimento** dello svolgimento delle funzioni ispettive e sanzionatorie e affermando che

> "*Nessun provvedimento del Garante, peraltro, potrebbe incidere sulla data di entrata in vigore del Regolamento europeo, fissata al 25 maggio 2018.*"

PRINCIPALI ADEMPIMENTI

Si fa presente ai Signori Clienti che per la specificità e la complessità della materia, nonché per le relative sanzioni, lo Studio non si potrà occupare degli adempimenti relativi al GDPR, si invitano pertanto tutte le aziende e i lavoratori autonomi a prendere contatto con imprese e professionisti del settore al fine di rispettare le nuove disposizioni in materia di Privacy.

Ai fini puramente indicativi e non esaustivi si individuiamo di seguito i principali adempimenti che le imprese e gli enti pubblici dovranno attuare per dare corretta applicazione alla nuova normativa, già in vigore dal 24 maggio 2015, ma ufficialmente obbligatoria a partire dal 25 maggio 2018.

Il consenso

Per i dati "sensibili" il consenso **DEVE** essere "esplicito".

Lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione). La diretta conseguenza è l'inammissibilità di un consenso tacito o presunto, come potrebbe avvenire nei casi delle caselle pre-spuntate. Resta immutato il concetto che il consenso deve sempre essere libero, informato e specifico.

Il consenso **NON** deve essere necessariamente "documentato per iscritto", nonostante spesso questa modalità venga considerata la più idonea per il suo essere esplicito.
Il titolare **DEVE** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Il consenso dei minori è valido a partire dai **16 anni**.

Prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Le modalità dell'informativa

Sono state stabilite nuove caratteristiche dell'informativa: **DEVE** essere di forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee. Deve essere data, in linea di principio, per iscritto e preferibilmente in formato elettronico, anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente.

Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione dei dati.

Il regolamento **AMMETTE**, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa; queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

I diritti riconosciuti agli interessati

Il diritto di accesso dell'interessato: l'interessato ha diritto di ottenere dal titolare l'accesso ai dati che lo riguardano. Il titolare può rendere disponibile la consultazione di dati in modo sicuro da remoto. L'interessato ha il diritto di conoscere le **finalità** perseguite con il trattamento avente ad oggetto i propri dati, i **destinatari** a cui verranno comunicati i suoi dati personali, ove possibile, la **durata** del trattamento ed infine, le eventuali **conseguenze** di un trattamento basato sulla profilazione. Fra le informazioni che il titolare deve fornire non rientrano le "modalità" del trattamento.

Il diritto all'oblio: l'interessato ha il diritto di ottenere la cancellazione dei propri dati personali se non pertinenti o non più pertinenti, o se inadeguati rispetto alle finalità del trattamento, o se l'interessato abbia revocato il proprio consenso, o qualora i dati siano trattati in modo illecito. Sarà obbligatorio per il titolare del trattamento informare eventuali altri titolari del trattamento in merito alla richiesta di cancellazione da parte dell'interessato.

Il diritto di limitazione di trattamento: il diritto è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento. Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze, come nel caso di accertamenti in sede giudiziaria.

Il diritto alla portabilità: l'interessato ha il diritto di ricevere i dati personali forniti a un titolare, in un formato di uso comune e leggibile da dispositivo informatico, e di trasferirli a un altro titolare del trattamento senza impedimenti. Questo diritto non si applica per archivi o registri cartacei: sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato e solo i dati che siano stati "forniti" dall'interessato al titolare.

Nomine di Titolari e Responsabili dei trattamenti

Il regolamento pone con forza l'accento sulla "responsabilizzazione" di **titolari e responsabili** – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. Si dovrà quindi essere in grado di fornire sempre le "garanzie sufficienti", quali la natura, durata e finalità del trattamento, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e delle disposizioni contenute nel regolamento.

Il regolamento disciplina la **contitolarità del trattamento** e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti, con particolare riguardo all'esercizio dei diritti degli interessati. Il regolamento fissa più dettagliatamente (rispetto all'art. 29 del Codice) le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti. Inoltre il regolamento consente la nomina di sub-responsabili del trattamento da parte di un responsabile, per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario.

Il regolamento prevede **obblighi specifici in capo ai responsabili** del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare la tenuta del registro dei

trattamenti svolti, l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti e la designazione di un RPD-DPO. Si ricorda, inoltre, che anche il responsabile non stabilito nell'Ue dovrà designare un rappresentante in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento.

Adempimenti da parte di Titolari e Responsabili del trattamento

Il registro dei trattamenti: Si tratta di un documento volto a tenere traccia dei trattamenti effettuati da parte del titolare e degli eventuali responsabili, e contiene: le finalità del trattamento, le categorie di interessati e dei dati personali, i destinatari, gli eventuali trasferimenti verso Paesi terzi, la durata del trattamento, l'indicazione delle modalità di raccolta dei dati e l'eventuale descrizione dell'attività di profilazione dei dati. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda, indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Definizione delle politiche di sicurezza e valutazione dei rischi: In questa fase bisogna procedere alla valutazione e all'attuazione di tutte le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR. Per raggiungere lo scopo della valutazione di sicurezza deve essere definito il risk appetite, ossia quanto l'organizzazione è disposta ad esporsi all'impatto del realizzarsi di una minaccia. Successivamente va definito per ogni minaccia un grado di probabilità potenziale di realizzazione e il suo impatto sull'organizzazione in termini di riservatezza, integrità e disponibilità.

Data Breach: Con il termine data breach si intende una "violazione della sicurezza" in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. Solitamente il data breach si realizza con una divulgazione involontaria (o talune volte volontaria) di dati riservati all'interno di un ambiente privo di misure di sicurezze come il web. In caso di accessi non autorizzati, perdita o furto di dati vi è l'obbligo di comunicare tempestivamente e, ove possibile, entro 72 ore sia agli interessati che alla competente autorità le suddette violazioni.

DPIA: Valutazione d'impatto sulla protezione dei dati personali. Al fine di assicurare trasparenza nelle operazioni di trattamento dei dati personali e adeguata protezione agli stessi, la DPIA implica che il titolare effettui precise e adeguate valutazioni d'impatto. Attraverso tale istituto è possibile, di conseguenza, valutare gli aspetti relativi alla protezione dei dati, prima che questi vengano trattati.

Generazione, stesura o modifica della documentazione contenente le risultanze dei punti precedenti, affinché sia completa ed aggiornata secondo le prescrizioni della nuova normativa. Non c'è più una scadenza di revisione annuale, ma viene richiesto che il documento sia sempre aggiornato. L'analisi dei rischi, come molti altri documenti, va aggiornata ogni volta in cui vengano introdotti nuovi trattamenti o avvengano variazioni sostanziali su quelli in essere.

Lo studio resta a disposizione per eventuali chiarimenti.

Cordiali saluti

Dott. Luigino Bottini