INTRODUZIONE
AL
REGOLAMENTO 679/2016/UE
Azienda Socio Sanitaria Territoriale di Cremona

SOMMARIO

INTRODUZIONE AL REGOLAMENTO 679/2016/UE

1. Contestualizzazione Regolamento 679/2016/UE

Il Regolamento 679/2016/UE del Parlamento Europeo (L. 119), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) del 4 maggio 2016. Il testo è disponibile alla risorsa di seguito indicata:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

Il Regolamento Europeo (di seguito indicato come "Regolamento UE" o come "GDPR") è stato approvato il 27 aprile 2016 ed è entrato in vigore il 24 maggio dello stesso anno con piena attuazione dal 25 maggio 2018, data a partire dalla quale questo Regolamento ha abrogato a tutti gli effetti la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. Direttiva Madre).
In Italia, in data 4 settembre 2018, è stato pubblicato in Gazzetta Ufficiale il Decreto Legislativo 101/2018 di armonizzazione al Regolamento UE, che coordina la normativa nazionale con il Regolamento europeo sulla privacy: tale decreto legislativo è entrato in vigore il 19 settembre 2018.

Il Regolamento Europeo è direttamente applicabile e vincolante rispetto a tutti gli Stati membri dell'Unione e non richiede una legge di recepimento nazionale, fatta eccezione per alcuni ambiti sui quali rimanda, deroga o richiede l'integrazione regolatoria dei singoli Stati membri. La diversa forma dell'atto – da Direttiva a Regolamento – risponde alla primaria volontà del Legislatore europeo di porre sullo stesso piano tutti gli Stati membri, garantendo medesimi diritti e doveri, assicurando uniformità alla protezione dei dati personali e certezza del diritto rispetto ai cittadini dell'Unione europea.

2. Campo di applicazione del Regolamento UE

Le norme interessano tutti quei soggetti (anche extraeuropei) che sono chiamati a trattare (in maniera automatizzata o meno) i dati relativi, per esempio, a clienti, dipendenti, studenti, utenti, fornitori, ecc. In sostanza, viene introdotto il principio dell'applicazione del diritto dell'Unione europea anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni o sevizi a cittadini UE o tali da comportare il monitoraggio dei loro comportamenti.

Il Regolamento UE, come espressamente affermato anche nei relativi Considerando al testo, si applica anche al trattamento di dati identificativi prodotti da dispositivi, applicazioni, strumenti e protocolli, quali gli indirizzi IP, i cookies e i tag di identificazione a radiofrequenza, salvo il caso in cui tali identificativi non si riferiscano ad una persona fisica identificata o identificabile. Le aziende e le istituzioni pubbliche sono tenute, pertanto, ad adottare politiche ed attuare misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato sia conforme - fin dalla fase embrionale - a tutte le disposizioni del Regolamento UE.

3. Sanzioni

Di importanza non secondaria, è l'impianto sanzionatorio. Al fine di rendere punibile chiunque, persona di diritto pubblico o di diritto privato, non ottemperi alle disposizioni del Regolamento, quest'ultimo ha richiesto agli Stati membri di garantire sanzioni efficaci, proporzionate e dissuasive e di adottare tutte le misure necessarie per la loro applicazione.

L'Autorità di Controllo può arrivare ad imporre sanzioni amministrative pecuniarie fino a 20 milioni di Euro o fino al 4% del fatturato mondiale annuo (se superiore) nel caso di un'impresa.

4. Novità introdotte dal Regolamento UE

Il Regolamento UE cambia profondamente la prospettiva in cui si colloca la protezione dei dati personali, sebbene ad una prima lettura possa rispecchiare un'impostazione simile a quella della Direttiva Madre rispetto al costrutto portante (informativa, finalità, consenso), ai ruoli, ai diritti degli interessati e ai doveri del Titolare e del Responsabile esterno del trattamento ex art. 28 GDPR.

Il GDPR consacra il diritto alla protezione dei dati personali come diritto fondamentale e costituzionale configurandolo come diritto all'autodeterminazione informativa. Questo è un principio portante fondato dalla Direttiva, che il Regolamento UE eredita, ma di cui ne ridisegna radicalmente l'implementazione, passando dalla logica dell'adempimento prevalentemente formale ad un approccio regolatorio fortemente sostanziale e centrato sulla responsabilità di assicurare/mantenere la conformità al Regolamento nonché di tutelare i diritti e la dignità degli interessati, cioè coloro ai quali si riferiscono le informazioni personali.

Il Regolamento UE, inoltre, traccia il passaggio da un diritto alla protezione dei dati personali di tipo nazionale/individuale ad un diritto di tipo europeo/sociale.

In generale il GDPR, collocandolo in questa premessa e provando a dimensionarlo su diritti-doveri-controllo:

- muta l'approccio regolatorio da "formale e re-attivo" a "sostanziale e pro-attivo": il trattamento e la protezione dei dati personali evolvono fino ad acquisire una propria e autonoma rilevanza all'interno dei processi organizzativi e gestionali di un'Organizzazione o di un'azienda;
- consolida le garanzie e i diritti azionabili dall'interessato per il controllo delle proprie informazioni e l'esercizio dell'autodeterminazione ereditati dalla Direttiva riaffermandone molti (diritto all'accesso, rettifica, cancellazione, limitazione, revoca e opposizione), rafforzandone altri (in primis la disciplina del consenso, rispetto alla quale introduce

un vera e propria definizione dell'istituto del consenso esplicito, ma anche della trasparenza, rispetto alla quale perfeziona il catalogo delle informazioni da esporre nell'informativa) e introducendone di nuovi (diritto alla portabilità, all'oblio e all'opposizione verso il trattamento di profilazione);

- accresce le responsabilità del Titolare e del Responsabile esterno del trattamento ex art. 28 GDPR con la positivizzazione del principio di accountability, con la finalità di porre chi tratta i dati personali in una posizione di ridurre i rischi di operazioni non conformi o non consentite inducendo e motivando, in tal senso, il Titolare e il Responsabile esterno del trattamento ex art. 28 GDPR a tenere comportamenti e prassi virtuose;
- centralizza la governance e il controllo sul rispetto e sulla conformità dei trattamenti alla normativa tramite la cooperazione e la valorizzazione delle Autorità di Controllo nazionali verso il Comitato europeo per la protezione dei dati (in inglese European Data Protection Board o "EDPB"), incoraggiando meccanismi di certificazione, ampliando il sistema di vigilanza e rafforzando quello sanzionatorio.

4.1. Dovere di documentazione e di informazione

È divenuto necessario elaborare un sistema documentale di gestione della privacy contenente tutti gli atti, regolarmente aggiornati ed elaborati per soddisfare i requisiti di conformità al Regolamento UE. È l'applicazione operativa del principio di rendicontazione (che rientra nel concetto di "accountability"), secondo cui il Titolare del trattamento deve conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente - per ognuno di essi - una serie "nutrita" di informazioni tali da assicurare e comprovare la conformità di ciascuna operazione alle disposizioni del Regolamento UE (qualcosa di simile al Documento Programmatico sulla Sicurezza, ma di portata più ampia).

In tal senso, acquisisce ancora più importanza il principio di trasparenza e di informazione nei confronti dell'interessato, che il Titolare del trattamento fa valere sia attraverso l'adozione di politiche concise, trasparenti, chiare e facilmente accessibili, sia mediante la resa di informazioni e comunicazioni con un linguaggio semplice e chiaro (in particolare se le informazioni sono destinate ai minori). Inoltre, ancora più rilevante diviene l'obbligo di resa dell'informativa privacy e dell'acquisizione "granulare" dei consensi (specifici per ogni tipologia di trattamento), quando dovuti. Il Regolamento UE amplia il contenuto da inserire nell'informativa rispetto al dettato dall'art. 13 del D.Lgs. 196/2003.

4.2. Accresciuta responsabilità del Titolare e del Responsabile esterno del trattamento

La responsabilità del Titolare (artt. 24 e 25 GDPR) e del Responsabile esterno del trattamento (art. 28 GDPR) - possono anche essere più di uno - si configura come una sostanziale assunzione di rischio, atteso che il Titolare del trattamento deve mettere in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare la conformità del trattamento al Regolamento UE, tenendo conto, inoltre, della natura, dell'obbligo, del contesto e delle finalità di trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Al Titolare del trattamento ed al Responsabile esterno del trattamento si affianca una nuova figura obbligatoria - tra le altre - per le Pubbliche Amministrazioni: il Responsabile della Protezione dei Dati personali (cd. "Data Protection Officer" o "DPO"). Il Data Protection Officer è obbligatorio nei casi previsti dall'art. 37, comma 1, del GDPR, che dispone che "Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un Responsabile della Protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".

Prioritariamente, rientrano tra le responsabilità del Titolare e del Responsabile esterno del trattamento: l'attuazione dei princìpi di privacy by design e by default, la Valutazione d'impatto, la definizione e il mantenimento delle procedure di sicurezza e valutazione dei rischi, la tenuta dei rispettivi registri delle attività di trattamento e la valutazione prudenziale sulla violazione dei dati personali, sul coefficiente di gravità e sulle relative ricadute sul soggetto interessato.

4.3. Valutazione d'impatto sulla protezione dei dati (Data Protection Impact Analysis - DPIA)

Il Titolare del trattamento è tenuto ad effettuare una Valutazione degli impatti privacy (Data Protection Impact Analysis – DPIA) fin dal momento della progettazione del processo aziendale e degli applicativi informatici di supporto, nei casi in cui il trattamento alla base degli stessi, per sua natura, oggetto o finalità, presenti rischi specifici per i diritti e le libertà degli interessati. In particolare, a titolo meramente esemplificativo e non esaustivo, la DPIA va realizzata per trattamenti:

- che prevedono la valutazione sistematica di aspetti della personalità dell'interessato o volti ad analizzarne la situazione economica, l'ubicazione, lo stato di salute, l'affidabilità o il comportamento mediante un trattamento automatizzato;
- che coinvolgono dati concernenti la vita sessuale, la prestazione di servizi sanitari, lo stato di salute, la razza o l'origine etnica;
- che coinvolgono dati in archivi su larga scala riguardanti minori, dati genetici o biometrici, a sorveglianza di zone accessibili al pubblico, in particolare se effettuata mediante dispositivi ottico-elettronici (video-sorveglianza).

Stando a quanto disposto dal Considerando 70 del Regolamento UE, viene abolito l'obbligo di notificazione di specifici trattamenti all'Autorità di Controllo (il nostro attuale Garante Privacy). Tale adempimento è considerato dal Legislatore europeo come un obbligo che comporta oneri amministrativi e finanziari senza aver mai veramente contribuito a migliorare la protezione dei dati personali (in particolare per le piccole e medie imprese). È pertanto necessario (continua il testo del Regolamento UE) abolire tale obbligo generale di notificazione e sostituirlo con meccanismi e procedure efficaci che si concentrino piuttosto su quelle operazioni di trattamento che potenzialmente presentano rischi specifici per i diritti e le libertà degli interessati, per la loro natura, portata o finalità. In tali casi è necessaria una Valutazione d'impatto sulla protezione dei dati, da effettuarsi prima del trattamento, che verta, in particolare, sulle misure, sulle garanzie e sui meccanismi previsti per assicurare la protezione dei dati personali e per comprovare il rispetto del Regolamento UE.

L'Autorità di Controllo redige e pubblica l'elenco delle tipologie di trattamenti soggetti a preventiva Valutazione di impatto. La Valutazione di impatto deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti, delle finalità e l'eventuale ricorrenza di un legittimo interesse;
- la valutazione sulla necessità e la proporzionalità dei trattamenti rispetto alle predefinite finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure organizzative e tecniche (comprese quelle di sicurezza) previste e ogni meccanismo ritenuto utile per la tutela dei diritti dei soggetti interessati.

La responsabilità della Valutazione d'impatto attiene prioritariamente al Titolare del trattamento, supportato dal Data Protection Officer (DPO), ove previsto.

4.4. Introduzione dei Registri delle attività di trattamento – Considerando 82, art. 30 GDPR

Il Titolare e il Responsabile esterno del trattamento devono tenere i rispettivi Registri delle attività.

Il Registro del Titolare deve contenere:

- i riferimenti di contatto del Titolare/i, del Rappresentante del Titolare del trattamento nell'Unione (in caso di non stabilimento nell'Unione) e del Data Protection Officer (DPO);
- le finalità del trattamento;
- la descrizione degli interessati e dei destinatari dei dati;
- la categoria dei dati personali trattati;
- la presenza di trasferimenti di dati verso un Paese Terzo o un'organizzazione internazionale, unitamente alla documentazione sulle appropriate garanzie dei trasferimenti;
- la tempistica della cancellazione dei dati;
- la descrizione delle misure di sicurezza e organizzative adottate.

Il Registro del Responsabile esterno deve contenere, tra le altre, le informazioni previste ed elencate per il Registro del Titolare, inclusi:

- i riferimenti di contatto dei Responsabili, dei Titolari per conto dei quali operano, dei Rappresentanti e del Data Protection Officer (DPO);
- le categorie dei trattamenti effettuati per conto del Titolare del trattamento.

4.5. Smaltimento di dispositivi e supporti contenenti dati personali

Permane l'obbligo di garantire la protezione dei dati anche mediante un'accurata cancellazione al momento della distruzione dei supporti che li contengono. Sul tema, si segnala un provvedimento dell'Autorità Garante su "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali" - 13 ottobre 2008 - G.U. n. 287 del 9 dicembre 2008 (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1571514).

4.6. Attuazione dei requisiti di sicurezza dei dati (art. 32 GDPR)

L'attuale testo del Regolamento UE richiede la messa in atto di misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento comporta. L'adeguatezza di tali misure deve derivare dai risultati della Valutazione d'impatto (DPIA), dall'evoluzione tecnica e dai costi di attuazione. Tale politica di sicurezza deve includere:

1. la capacità di assicurare che sia convalidata l'integrità dei dati personali;
2. la capacità di assicurare riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano dati personali;
3. la capacità di ripristinare la disponibilità e l'accesso ai dati in modo tempestivo, in caso di incidente fisico o tecnico che abbia un impatto sulla disponibilità, sull'integrità e sulla riservatezza dei sistemi e dei servizi di informazione;
4. in caso di trattamento di dati personali particolari (ex sensibili), misure di sicurezza aggiuntive per garantire la consapevolezza dei rischi e la capacità di adottare in tempo reale azioni di prevenzione, correzione e attenuazione, contro le vulnerabilità riscontrate o gli incidenti verificatisi, che potrebbero costituire un rischio per i dati;

5. un processo per provare, verificare e valutare regolarmente l'efficacia delle politiche, delle procedure e dei piani di sicurezza attuati per assicurare la continua efficacia.

Le misure appena citate devono come minimo:

1. garantire che ai dati personali possa accedere soltanto il personale autorizzato agli scopi autorizzati dalla legge;
2. proteggere i dati personali conservati o trasmessi dalla distruzione accidentale o illecita, dalla perdita o dalla modifica accidentale e dalla conservazione, trattamento, accesso o comunicazione non autorizzati o illeciti;
3. assicurare l'attuazione di una politica di sicurezza in relazione al trattamento dei dati personali.

È assai probabile che l'adesione a codici di condotta (approvati ai sensi dell'articolo 38 del Regolamento UE) o un meccanismo di certificazione (approvato ai sensi dell'articolo 39 del Regolamento UE) possano essere utilizzati come elementi per dimostrare la conformità ai requisiti di sicurezza sopra elencati. È il Comitato europeo per la protezione dei dati (in inglese "European Data Protection Board" o "EDPB") l'ente deputato a fornire interpretazioni, orientamenti, raccomandazioni e migliori prassi, per le misure tecniche e organizzative, compresa la determinazione di ciò che costituisce l'evoluzione tecnica - per settori specifici e in specifiche situazioni di trattamento dei dati -, in particolare tenuto conto degli sviluppi tecnologici e delle soluzioni di default. Inoltre, se necessario, la Commissione UE può adottare atti di esecuzione per precisare i requisiti delle misure sopra elencate, segnatamente per:

1. impedire l'accesso non autorizzato ai dati personali a soggetti terzi;
2. impedire qualunque forma non autorizzata di divulgazione, lettura, copia, modifica, cancellazione o rimozione dei dati personali;
3. garantire la verifica della liceità del trattamento.

4.7. Privacy by design e privacy by default

Si tratta dell'esplicitazione del principio dell'incorporazione della privacy fin dalla progettazione (by design) del processo aziendale e degli applicativi informatici di supporto, ovvero la messa in atto di meccanismi per garantire che siano trattati (by default) solo i dati personali necessari per ciascuna finalità specifica del trattamento (si tratta della ri-attualizzazione in chiave moderna del principio di necessità sancito dal Codice Privacy). Il Titolare del trattamento deve, pertanto, prevedere meccanismi di protezione dei dati fin dalla progettazione delle attività e per l'intera gestione del ciclo di vita dei dati - dalla raccolta alla cancellazione - incentrandosi sistematicamente sulle garanzie procedurali in merito all'esattezza, alla riservatezza, all'integrità, alla sicurezza fisica ed alla cancellazione dei dati.

Tali meccanismi vanno identificati sia by design, cioè nel momento in cui si definiscono le finalità e i mezzi del trattamento, che by default, cioè all'atto del trattamento stesso, tenuto conto dell'evoluzione tecnica e dei costi di attuazione, delle migliori prassi (best practices) internazionali e dei rischi del trattamento. A livello operativo vuol dire sia fare in modo che la quantità dei dati raccolti e la durata della conservazione (o eventuale diffusione) non vada oltre quanto necessario per le finalità perseguite, sia predisporre meccanismi che garantiscano che, di default, non siano resi accessibili dati ad un numero indefinito di persone e che gli interessati siano in grado di controllarne il flusso. Questo ha un forte impatto nello sviluppo di software destinati al trattamento di dati (es. CRM, ERP, gestionali aziendali) e sul rinnovamento del parco informatico delle amministrazioni, delle imprese e degli studi professionali.

4.8. Misure di sicurezza e valutazione dei rischi - Considerando 83, 84, art. 32 GDPR

Il Regolamento UE prevede misure di sicurezza idonee da adottare in relazione alla valutazione dei rischi.

Il Titolare del trattamento e il Responsabile esterno del trattamento sono tenuti tanto alla valutazione dei rischi quanto all'adozione delle misure che comprendono: la pseudonimizzazione e la cifratura; le misure implementative della riservatezza, dell'integrità e della disponibilità delle informazioni; la resilienza dei sistemi e delle applicazioni di trattamento, nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico.

Le misure vanno contemperate allo stato dell'arte, ai costi di attuazione, alla natura, al contesto e alla finalità di trattamento.

4.9. Obblighi di segnalazione in caso di violazioni dei dati (Data Breach) - artt. 33 e 34 GDPR

Con la nozione di violazione dei dati personali (c.d. "Data Breach"), si intende: la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati. Il Titolare del trattamento, in caso di una violazione come sopra descritta, a meno che non ricorrano condizioni particolari che comportano scelte diverse, dovrà mettere in atto due differenti azioni: la notifica della violazione all'Autorità di Controllo e la segnalazione al diretto interessato i cui dati personali sono stati violati.

Nel primo caso, accertata la violazione, la relativa notifica deve contenere una serie nutrita di informazioni: la natura della violazione medesima, le categorie e il numero di interessati coinvolti; l'identità e le coordinate di contatto del DPO; l'elenco delle misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione dei dati; la descrizione degli impatti derivanti dalla violazione; le misure proposte o adottate per porre rimedio alla violazione e attenuarne gli effetti. Inoltre, l'Autorità di Controllo conserva un registro pubblico delle tipologie di violazione notificate. Nel caso in cui, poi, la violazione rischi di pregiudicare i dati, attentare alla vita privata, ai diritti o agli interessi legittimi dell'interessato, il Titolare del trattamento, dopo aver valutato la portata dell'episodio, deve comunicare la violazione al diretto interessato senza ritardo. In mancanza di tale comunicazione, l'Autorità di Controllo, considerate le presumibili ripercussioni negative della violazione, può obbligare il Titolare del trattamento a comunicare l'evento lesivo all'interessato. La comunicazione all'interessato deve essere esaustiva e redatta in un linguaggio semplice e chiaro e descrivere la natura e le conseguenze della violazione, le misure raccomandate per attenuare i possibili effetti pregiudizievoli e i diritti esercitabili dall'interessato.

La comunicazione non è richiesta quando il Titolare del trattamento dimostra in modo convincente all'Autorità di Controllo di aver utilizzato le opportune misure tecnologiche di protezione (es. cifratura) e che tali misure sono state applicate, proprio, ai dati violati (es. furto tablet con dati sanitari cifrati). Queste misure tecnologiche di protezione devono rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

4.10. Diritti dell'interessato

4.10.a. Consenso – Considerando 39 e 42, artt. 6 e 7 GDPR

Il consenso in generale deve essere: libero, specifico, informato e inequivocabile; non è ammesso il consenso tacito o presunto. Deve essere reso e manifestato attraverso dichiarazione o azione positiva inequivocabile e concludente (come la selezione di un'apposita casella in un sito web, la scelta di specifiche impostazioni tecniche o qualsiasi altra dichiarazione o comportamento che indichi chiaramente la volontà dell'interessato di accettare il trattamento proposto). Non è richiesta la forma scritta ex lege, anche se questa risulta essere la modalità più idonea ad accertare che il consenso sia stato inequivocabilmente fornito e che sia esplicito. Si precisa che nel caso in cui il trattamento richieda il consenso, il Titolare del trattamento dovrà essere in grado di dimostrare inequivocabilmente di averlo ottenuto in conformità a quanto previsto dall'ordinamento. Per il trattamento di dati particolari (ex sensibili) è necessario il consenso (art. 9, par.2, lettera a) del GDPR) a meno che il trattamento di dati personali non si fondi su uno degli altri presupposti di liceità individuati al paragrafo 2 dell'art. 9 del GDPR. In altri termini, il consenso come base giuridica può essere utilizzato per trattare dati particolari (ex sensibili) in via residuale, cioè laddove non possano essere utilizzati gli altri presupposti ex art. 9, par. 2, del GDPR.

4.10.b. Informativa – Considerando da 58 a 73, artt. 12, 13 e 14 GDPR

Il Titolare del trattamento è tenuto a fornire l'informativa all'interessato, indipendentemente dall'obbligo di acquisirne il consenso, salvo il caso in cui l'interessato sia già in possesso delle informazioni (art. 13, par. 4) o in altri casi particolari descritti nel Regolamento (art. 14, par. 5).

Contenuti dell'informativa

Il Titolare del trattamento è tenuto a informare il soggetto interessato in merito a:

- identità e dati di contatto del Titolare del trattamento, del suo legale rappresentante e del Data Protection Officer (DPO);
- le finalità del trattamento cui sono destinati i dati personali, nonché la base giuridica del trattamento ed i legittimi interessi perseguiti dal Titolare del trattamento o da terzi (qualora il trattamento sia basato sull'art. 6, par. 1, lettera f) del GDPR);
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e, nel caso in cui i dati personali non siano raccolti presso l'interessato, anche le categorie di dati trattati e le relative fonti di provenienza;
- l'eventuale intenzione del Titolare del trattamento di trasferire dati personali ad un Paese terzo o ad un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso di trasferimenti di cui agli articoli 46 e 47, o all'articolo 49, paragrafo 2, del GDPR, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- i diritti azionabili dall'interessato comprendenti: l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l'opposizione; oltre al diritto alla portabilità dei dati; la revoca del consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; il diritto di proporre reclamo a un'Autorità di Controllo;
- la necessità di comunicare i dati personali in base ad un obbligo legale o contrattuale oppure se si tratta di un requisito necessario per la conclusione di un contratto; la natura obbligatoria o facoltativa del conferimento; le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, le informazioni significative circa la logica utilizzata, nonché l'importanza di tale trattamento e le conseguenze previste per l'interessato.

Al riguardo, si segnalano alcuni punti di attenzione:

- deve essere chiarito l'eventuale trasferimento di dati in un Paese terzo (ad esempio nel caso di utilizzo di servizi cloud). Si ricorda che anche per tali servizi è responsabilità del Titolare del trattamento garantire la sicurezza dei dati e le modalità di accesso da parte dell'interessato;
- rispetto alla normativa previgente, occorrerà garantire – in specifici casi - la limitazione del trattamento dati e la portabilità degli stessi;
- la necessità di indicare eventuali processi automatici di profilazione e le conseguenze per l'interessato.

Inoltre, si precisa che:

- nel caso in cui i dati siano raccolti presso l'interessato, il Titolare del trattamento che intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, dovrà fornire all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente;

- nel caso in cui i dati non siano stati raccolti presso l'interessato, il Titolare del trattamento che intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, potrà non fornire l'informativa all'interessato qualora risulti impossibile o farlo implicherebbe uno sforzo sproporzionato (in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici e fatte salve le condizioni e le garanzie di cui all'art. 89, par. 1, del GDPR o nella misura in cui l'obbligo di rendere l'informativa rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In questo caso, il Titolare del trattamento deve comunque adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni).

Caratteristiche dell'informativa

Il Regolamento UE specifica in dettaglio le caratteristiche espositive dell'informativa, che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; veicolata da un linguaggio chiaro e semplice (soprattutto nel caso in cui gli interessanti siano minori).
Per agevolarne la comprensione, il Regolamento UE incoraggia l'utilizzo di icone in combinazione con la forma estesa per presentare i contenuti dell'informativa in forma sintetica, icone che dovranno essere identiche in tutta l'UE e dovranno essere definite dalla Commissione europea.
Una maggiore comprensione e chiarezza dell'informativa si potrebbe altresì ottenere mediante la redazione di più informative che si differenzino, ad esempio, in relazione alle diverse categorie di interessati e/o ai servizi resi loro disponibili.

4.10.c. Diritti "tradizionali" – Considerando da 58 a 73, artt. 12 a 17 GDPR

I diritti azionabili dall'interessato già previsti dalla Direttiva Madre e dal Codice Privacy, oltre a quello di ricevere idonea informativa, riguardano: il diritto di accesso, la rettifica, la cancellazione e l'opposizione al trattamento.

Rispetto alla Direttiva 95/46/CE ed al Codice Privacy, vengono di seguito elencate le novità previste dal GDPR:

- il riscontro all'interessato deve essere fornito senza ingiustificato ritardo e, comunque, non oltre un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste;
- la definizione da parte del Titolare del trattamento di eventuali oneri sull'interessato nei casi particolari previsti nell'art. 12 par. 5, del GDPR.

A differenza della normativa previgente, è posto in maniera meno rilevante l'accento sul riscontro da fornire all'interessato per quanto attiene le modalità del trattamento: viceversa, è posto l'accento su altri elementi come, ad esempio, il periodo di conservazione e le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi. Si precisa inoltre che la risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre alla circostanza per cui deve essere utilizzato un linguaggio semplice e chiaro.

4.10.d. Nuovi diritti: diritto alla cancellazione/oblio, diritto di limitazione, diritto alla portabilità, diritto di opposizione alla profilazione – artt. 17, 18, 20, 21 e 22 GDPR

Questi nuovi diritti estendono o rafforzano analoghi diritti presenti nella Direttiva Madre e attuati dal Codice Privacy.

Il diritto "all'oblio" (art. 17 GDPR) si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata nel caso in cui questi siano stati resi pubblici on-line. In base al Considerando 66 del GDPR, che ha inteso potenziare il diritto all'oblio nell'ambiente online, il "Titolare del trattamento che ha pubblicato dati personali è obbligato a informare i Titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali". Inoltre, l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo la revoca del consenso al trattamento.

Il diritto di limitazione del trattamento (art. 18 GDPR) rappresenta un diritto diverso e più esteso rispetto al "blocco" del trattamento già previsto dal Codice Privacy. In particolare, tale diritto è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati stessi, bensì anche nelle more che sia riscontrata da parte del Titolare una richiesta di rettifica dei dati o di opposizione al trattamento. In condizioni di limitazione e con la sola eccezione della conservazione, ogni altro trattamento del dato è consentito solo in presenza del consenso dell'interessato, dell'accertamento dei diritti in sede giudiziaria, di tutela dei diritti di altra persona fisica o giuridica o in presenza di un interesse pubblico rilevante.

Il diritto alla portabilità dei dati (art. 20 GDPR) si applica ai dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato e solo per i dati che siano stati "forniti" dall'interessato al Titolare del trattamento; fanno eccezione quindi i dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del Titolare del trattamento.

Il diritto di opposizione alla profilazione (artt. 21 e 22 GDPR) riconosce all'interessato il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare (legata ad esempio al proprio rendimento professionale o alla propria situazione economica, di salute, ecc.), al trattamento dei dati personali che lo riguardano, compresa la profilazione. 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 tali da prevalere sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

4.10.e. Nuovi diritti: diritto alla cancellazione/oblio, diritti. Sintesi delle principali novità del GDPR

Le principali novità sono di seguito sintetizzate tramite parole chiave.

Consenso: libero, specifico, informato, inequivocabile e concludente.

Informativa: informazioni di contatto del Titolare, del Rappresentante e del Data Protection Officer (DPO); indicazione della finalità di trattamento; destinatari e categorie di dati trattati; trasferimento dati personali in Paesi terzi; diritti azionabili e implicazioni; ricorrenza di altre basi giuridiche diverse dal consenso.

Valutazione d'impatto (DPIA): analisi ed eventuale consultazione preventiva con l'Autorità Garante per le implicazioni sui diritti e sulle libertà delle persone. Obbligo del Titolare del trattamento, supportato dal Data Protection Officer (DPO).

Sicurezza: analisi dei rischi e di valutazione dell'adeguatezza delle misure tecniche e organizzative.

Obbligo congiunto del Titolare e del Responsabile esterno del trattamento dei dati.

Violazione dei dati (Data Breach): equiparazione della fattispecie accidentale con quella dolosa.

Privacy by Design: applicazione delle tutele di trattamento sin dalla sua progettazione e dal suo avvio.

Privacy by Default: pseudonimizzazione e minimizzazione (di dati e tempi) come garanzia e misura di Privacy by Default. Obbligo del Titolare del trattamento.

Data Protection Officer (DPO): si interfaccia con le Autorità Garanti. Supporta il Titolare e il Responsabile esterno del trattamento. Obbligatorio nelle PA.

Registro dei trattamenti: Registro di competenze in cui indicare le caratteristiche, le modalità e le finalità del trattamento. Lo redigono in via separata il Titolare del trattamento e il Responsabile esterno del trattamento ex art. 28 GDPR.

Sanzioni: sanzioni amministrative pecuniarie fino a 20 milioni di euro (per le imprese, fino al 4% del fatturato globale annuo dell'esercizio precedente).

Autorità: Comitato di controllo europeo: assicura l'uniforme applicazione del Regolamento UE.

Autorità di Controllo: autorità pubblica indipendente di uno Stato membro.

NUOVI DIRITTI

Profilazione: l'interessato ha il diritto di non subire trattamenti automatizzati (profilazione) inconsapevoli.

Portabilità dei dati: l'interessato ha il diritto ottenere la restituzione dei propri dati personali trasmessi e trattatati da un Titolare del trattamento e trasmetterli ad altri.

Oblio: l'interessato ha diritto alla de-indicizzazione o alla cancellazione delle informazioni che lo riguardano.

6. I soggetti del trattamento

Il GDPR individua i soggetti coinvolti nel trattamento sulla base:

1) delle finalità per le quali sono raccolti i dati personali:

- il Titolare del trattamento è la persona giuridica o la persona fisica che raccoglie i dati personali per proprie finalità e decide in autonomia i mezzi del trattamento di tali dati;
- il Contitolare è la persona giuridica o la persona fisica che condivide le finalità con un altro Contitolare (o con altri Contitolari) e stabilisce insieme a questo (o questi) le modalità di trattamento dei dati;
- il Responsabile esterno del trattamento è la persona giuridica o la persona fisica che esegue dei trattamenti di dati per conto del Titolare sulla base di un contratto o di altro atto giuridico;
- il Destinatario è la persona giuridica o la persona fisica che riceve i dati dal Titolare del trattamento per eseguire i trattamenti secondo le istruzioni ricevute o che esegue trattamenti per proprie finalità (nel qual caso diventa a sua volta Titolare per i trattamenti dei dati ricevuti);
- il soggetto autorizzato/incaricato del trattamento è la persona fisica che ha ricevuto dal Titolare del trattamento precise istruzioni per l'esecuzione dei trattamenti di dati di sua competenza;
- l'interessato è la persona fisica che fornisce i propri dati personali a un Titolare del trattamento per le finalità specificate nell'informativa, o comunque, in generale, quel soggetto a cui fanno riferimento i dati trattati dal Titolare;

2) delle caratteristiche del Titolare/Responsabile esterno del trattamento e delle tipologie e quantità di dati trattati:

- il Data Protection Officer (DPO) è la persona giuridica o la persona fisica che segue tutti i vari aspetti relativi all'applicazione del GDPR per conto del Titolare/Responsabile esterno del trattamento e che deve obbligatoriamente essere presente nelle Pubbliche Amministrazioni;

3) dell'ambito territoriale:

- il Rappresentante nell'Unione del Titolare/Responsabile esterno del trattamento che ha la propria sede in uno Stato terzo è la persona giuridica o la persona fisica che su mandato del
- Titolare/Responsabile esterno del trattamento funge da interlocutore per gli interessati e per le Autorità di Controllo dell'Unione (ferma restando la responsabilità generale del Titolare del trattamento o del Responsabile esterno del trattamento);
- l'Autorità di Controllo è la persona giuridica pubblica istituita da ogni Stato membro per sovrintendere all'applicazione ed al rispetto del GDPR nell'ambito del proprio territorio;
- il Comitato europeo per la protezione dei dati è la persona giuridica che a livello europeo ha il compito di coordinare il lavoro delle varie Autorità di Controllo e di supportare la Commissione europea.

6.1. Titolare del trattamento (art. 4, par. 1, punto 7) GDPR)

Il Titolare del trattamento è definito all'art. 4, par. 1, punto 7) del GDPR 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". Pertanto, il Titolare del trattamento non viene designato o nominato da qualcuno, ma diventa tale nel momento in cui raccoglie dati personali con l'intento di trattarli per finalità lecite (come previsto agli artt. 6 e 9 del GDPR), decidendone anche le modalità di trattamento.

6.2. Contitolare (art. 26 GDPR)

Il soggetto terzo che condivide le decisioni sulle finalità per le quali trattare i dati e che contribuisce a definire le modalità di trattamento. Il contenuto essenziale dell'accordo stipulato ai sensi dell'art. 26 del GDPR fra i Contitolari deve essere messo a disposizione dell'interessato. Questi può esercitare i propri diritti nei confronti di ogni Contitolare a prescindere dalla ripartizione di responsabilità interne eventualmente stabilite tra i Contitolari.

6.3. Responsabile esterno del trattamento dati (artt. 4, par. 1, punto 8) e 28 GDPR)

Il GDPR definisce all'art. 4 il Responsabile esterno del trattamento quale "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento" e ne descrive le funzioni all'art. 28. Differisce dalla figura di Responsabile prevista dal Codice Privacy soprattutto per quanto concerne la responsabilità solidale con il Titolare rispetto a eventuali inadempienze.

Il Responsabile esterno del trattamento dati è un soggetto esterno (cioè distinto dal Titolare) che esegue, in base ad un contratto/convenzione o ad un altro atto giuridico, dei trattamenti di dati personali per conto del Titolare e ne risponde in solido in caso di inadempienze nei confronti degli interessati. In determinate circostanze (Valutazione d' impatto, Registro dei trattamenti, eventuale nomina del Data Protection Officer, ecc.), al Responsabile esterno del trattamento sono attribuiti i medesimi compiti che l'ordinamento giuridico attribuisce al Titolare del trattamento con riferimento alla propria organizzazione. Il Responsabile esterno del trattamento non può a sua volta nominare un altro Responsabile (cd. Sub-Responsabile) se non a fronte di un'autorizzazione scritta del Titolare: la catena delle responsabilità, suddivisa anche su più livelli, deve essere nota al Titolare. Nel contratto - a valle - con il Sub-Responsabile devono essere riportati gli stessi obblighi in materia di protezione dei dati personali previsti - a monte - nel contratto tra il Responsabile esterno ex art. 28 GDPR e il Titolare del trattamento.

Nell'informativa rivolta agli interessati devono essere indicati i destinatari o le categorie di destinatari, anche interni, ai quali sono comunicati i dati per il loro trattamento. Nel caso di trasferimento di dati in un Paese terzo è obbligatorio informare di ciò l'interessato e il Titolare deve verificare che il Responsabile esterno assicuri un'adeguata protezione ai dati oggetto di trasferimento extra-europeo.

6.4. Soggetti autorizzati/incaricati del trattamento (artt. 29 GDPR e 2-quaterdecies Codice Privacy)

Come precisato dall'Autorità Garante per la protezione dei dati personali nella "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali - edizione aggiornata febbraio 2018", "le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento": ne consegue che quanto disposto all'art. 29 del GDPR possa concretizzarsi con l'individuazione dei soggetti autorizzati al trattamento dei dati (prima denominati "incaricati") all'interno dell'Organizzazione. È sottolineata, inoltre, l'importanza di "istruire" i soggetti, rendendosi dunque necessario prevedere percorsi formativi adeguati per coloro che saranno coinvolti nel trattamento dei dati.

Nell'informativa devono essere indicati i destinatari o le categorie di destinatari ai quali sono comunicati i dati per il loro trattamento.

Analogamente a quanto si è verificato fino all'entrata in vigore effettiva del GDPR (25 maggio 2018), è possibile ancora oggi individuare i soggetti che sono autorizzati al trattamento dei dati mediante una nomina individuale da parte del Titolare o del Responsabile esterno del trattamento dei dati oppure individuando i trattamenti che competono all'Unità Organizzativa di afferenza del soggetto, che risulta pertanto incaricato per "documentata preposizione ad unità organizzativa". La necessità di prevedere la designazione per iscritto del singolo incaricato o la documentata preposizione non emerge in maniera esplicita dall'art. 29 del GDPR. Il termine "istruzione" del soggetto da parte del Titolare del trattamento indica che è necessaria una formazione specifica alla persona per ritenerla "autorizzata" ai trattamenti di dati personali di sua competenza. Del resto, già nella disposizione "data protection by default and by design", è previsto che in fase di progettazione di un'attività che comporti trattamento di dati personali debbano essere individuate le misure di sicurezza idonee alla protezione dei dati, e di conseguenza anche le opportune istruzioni per gli incaricati.

L'individuazione dei soggetti autorizzati al trattamento dati è una misura di sicurezza a livello organizzativo che comunque il Titolare del trattamento è tenuto ad adottare.

Salvo ulteriori precisazioni da parte del Garante, gli amministratori di sistema (categoria di soggetti disciplinata, tra le altre, anche dal Provvedimento n. 300 del 2008 dell'Autorità Garante per la protezione dei dati personali, cui si rimanda) risultano essere incaricati con particolari compiti, pertanto per questa tipologia è opportuno mantenere la nomina individuale.

6.5. Data Protection Officer – DPO (artt. 37, 38 e 39 GDPR)

Con l'avvento del Regolamento UE è stata introdotta la nuova figura del "Responsabile per la Protezione dei Dati" (o, appunto, in inglese "Data Protection Officer"), con una funzione di potenziale ausilio al Garante nell'ambito delle strutture di impresa. È divenuto obbligatorio nominare tale figura nei seguenti casi:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- le attività principali del Titolare del trattamento o del Responsabile esterno del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività principali del Titolare del trattamento o del Responsabile esterno del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 (dati particolari/sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Il DPO deve essere designato per un dato periodo ed in funzione delle qualità professionali e della conoscenza specialistica della normativa. Il Titolare del trattamento deve assicurarsi che ogni altra eventuale funzione professionale della persona che riveste il ruolo di DPO sia compatibile con i compiti e le funzioni dello stesso e non dia adito a conflitto di interessi (deve quindi essere autonomo, indipendente e non ricevere alcuna istruzione per l'esercizio delle sue attività). Il DPO, il cui mandato può essere rinnovabile, può essere assunto oppure adempiere ai suoi compiti in base ad un contratto di servizi. Il Titolare del trattamento, che a seconda della forma contrattuale, può essere datore di lavoro o committente, deve fornire al DPO tutti i mezzi, inclusi il personale, i locali, le attrezzature e ogni altra risorsa necessaria per adempiere alle sue funzioni e per mantenere la propria conoscenza professionale. I principali compiti del DPO, il cui nominativo deve essere comunicato all'Autorità di Controllo e al pubblico, sono quelli di:

- sensibilizzare e consigliare il Titolare del trattamento in merito agli obblighi (misure e procedure tecniche e organizzative) derivanti dal Regolamento UE;
- sorvegliare l'applicazione delle politiche, compresa l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e l'effettuazione degli audit connessi all'attività svolta;
- sorvegliare l'applicazione del Regolamento UE, con particolare riguardo alla protezione dei dati fin dalla progettazione, alla protezione di default, alla sicurezza dei dati, alle informazioni degli interessati ed alle richieste degli stessi per esercitare i diritti riconosciuti dall'ordinamento;
- controllare che il Titolare del trattamento effettui la Valutazione d'impatto sulla protezione dei dati (DPIA) e richieda all'Autorità di Controllo l'autorizzazione preventiva o la consultazione preventiva nei casi previsti dalla legge;
- fungere da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento e consultarla, se del caso, di propria iniziativa;
- informare i rappresentanti del personale (es. rappresentanti sindacali) sui trattamenti che riguardano i dipendenti.

Si può quindi affermare che ci si è incamminati verso la creazione di una nuova categoria professionale che deve disporre di precise e specifiche competenze sia giuridiche che informatiche nell'ambito della protezione dei dati personali.

6.6. Destinatario (art. 4, par. 1, punto 9) GDPR)

Il GDPR definisce all'art. 4, par. 1, punto 9) il "destinatario" come quella "persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi". Pertanto, debbono essere considerati destinatari tutti i soggetti che ricevono dati personali da un Titolare del trattamento, sia che siano interni che esterni, sia che li ricevano per eseguire trattamenti per conto del Titolare del trattamento o che li ricevano per conseguire proprie finalità. I destinatari o le categorie di destinatari ai quali verranno comunicati i dati devono essere definiti in fase di raccolta dei dati per inserirli nell'informativa all'interessato. Nel caso in cui il destinatario sia un soggetto che risiede in un Paese non membro dell'Unione, è richiesto che il Titolare verifichi che le garanzie per la protezione dei dati offerte da tale destinatario siano adeguate a quanto richiesto dall'ordinamento giuridico.

Nell'informativa da fornire all'interessato non solo devono essere indicati i destinatari o le categorie di destinatari ai quali saranno comunicati i dati, ma devono essere elencate anche le strutture interne o le categorie di personale che verranno a conoscenza dei dati personali nello svolgimento della loro attività lavorativa.

Nel caso in cui il destinatario sia un soggetto "terzo" che riceve i dati per perseguire proprie finalità, diventerà a sua volta Titolare del trattamento. Il destinatario che riceve i dati da altro Titolare del trattamento per perseguire finalità proprie è tenuto a fornire l'informativa all'interessato nel più breve tempo possibile, sempre che ciò non sia impossibile o richieda uno sforzo sproporzionato o se l'interessato dispone già dell'informazione o nel caso in cui la comunicazione sia necessaria per adempiere ad un obbligo di legge.

6.7. Interessato

L'interessato è la persona fisica alla quale si riferiscono i dati trattati: questo è necessariamente una persona fisica, in quanto il GDPR tutela esclusivamente i dati delle persone fisiche, non prendendo invece in considerazione i dati delle persone giuridiche. L'interessato è dunque il soggetto "proprietario" dei dati personali e conserva su questi dei diritti nei confronti del Titolare del trattamento e di tutti coloro che li trattano per suo conto. Il GDPR, al Capo III, elenca nel dettaglio tali diritti. Alcuni di questi, a seconda della finalità per la quale i dati sono stati raccolti, potrebbero non essere esercitabili dagli interessati nel caso concreto, quindi, dovrà essere realizzata una valutazione caso per caso. Tuttavia, la risposta alle richieste dell'interessato deve comunque essere tempestiva e, anche nel caso in cui non sia possibile soddisfarla, occorre specificare la motivazione del rifiuto. La risposta

deve essere fornita entro un mese dalla richiesta; tale periodo può essere prorogato per altri due mesi qualora la richiesta sia particolarmente impegnativa per il Titolare del trattamento, pur dovendo questo avvisare l'interessato della proroga entro un mese dalla richiesta. Il Titolare del trattamento ha inoltre il compito di facilitare all'interessato l'accesso ai suoi dati predisponendo dei canali di comunicazione dedicati (ad esempio, pubblicando i recapiti o i dati di contatto del DPO).

Per la descrizione dei trattamenti si usa raggruppare gli interessati in categorie omogenee a seconda del tipo di rapporto che questi hanno con il Titolare del trattamento.

6.8. Autorità di Controllo e Comitato europeo per la protezione dei dati personali

Le Autorità di Controllo sono incaricate di "sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione" (art. 51, par. 1, del GDPR).

Ogni Stato membro istituisce una o più autorità pubbliche indipendenti. Nel caso in cui siano molteplici, allora dovrà essere designata quella che avrà il ruolo di rappresentarla nel Comitato europeo per la protezione dei dati e che avrà funzioni di coordinamento delle varie Autorità di controllo, per rendere coerenti e in linea con il GDPR le varie decisioni che a queste competono. Il Comitato ha inoltre funzioni di supporto per la Commissione europea.

All'Autorità di Controllo nazionale devono essere comunicati eventuali Data Breach.

Le Autorità di Controllo sono competenti ad accogliere e decidere su eventuali reclami presentati dagli interessati.

7. Conclusioni sul Regolamento europeo 679/2016 (GDPR)

La rilevanza generale del Regolamento UE, come appare chiaro, ha una notevole portata sia in termini giuridici che fattuali. Non si tratta di una semplice revisione avente ad oggetto la protezione dei dati personali, bensì di un intervento normativo a fronte dell'esperienza maturata negli ultimi anni su settori sino ad oggi solo sfiorati, che avrà effetti anche sulla concezione stessa della "privacy", facendola calare sempre all'interno dei processi e dell'organizzazione aziendale non più come elemento/adempimento successivo, ma piuttosto come presupposto ancillare e propedeutico già nelle fasi di progettazione dei processi. Il fine primario del nuovo quadro giuridico è, poi, quello di apportare migliorie per le persone fisiche e per i Titolari del trattamento (aziende, imprese, enti pubblici), di dimostrarsi valido anche per i prossimi anni ed in grado di reggere gli impatti posti, in particolare, dall'avvento delle nuove tecnologie (pensiamo, ad esempio, alle sfide, in ottica privacy, derivanti dal Cloud Computing o dall'Internet of Things - IoT). Si può quindi affermare che si sta assistendo ad un passaggio da un sistema di tipo formalistico, come quello antecedente, e per certi aspetti ancora attuale, ad uno di alta responsabilizzazione sostanziale in cui è richiesto un ruolo proattivo ai Titolari del trattamento e a tutti coloro che, in generale, trattano dati personali.

In conclusione, una risposta efficace ed efficiente agli obblighi sopra descritti non può non passare dalla predisposizione e formalizzazione di un preciso organigramma privacy interno che "regoli il traffico" e vada a definire il "chi fa cosa", coerentemente alle mansioni aziendali. Si ritiene di rilevante importanza sottolineare due ulteriori aspetti: da una parte, la predisposizione, a livello contrattuale in caso di trattamenti esternalizzati, di precise clausole che prevedano la sottoscrizione di Service Level Agreement (SLA) o Privacy Level Agreement (PLA), mentre dall'altra la predisposizione di un "Sistema 231" (responsabilità amministrativa delle persone giuridiche), che si sostanzi sempre più in pratiche di controllo interno aziendale - anche secondo lo schema PDCA: Plan, Do, Check, Act - per la protezione dell'organizzazione dalla commissione dei reati presupposto quali i reati informatici ed i trattamenti illeciti di dati (di cui, in particolare, all'art. 24 del D.Lgs. 231/2001).