Allegato 1 - INTRODUZIONE AL REGOLAMENTO 679/2016/UE

Contestualizzazione nuovo regolamento

Il nuovo Regolamento Europeo - Regolamento (UE) 2016/679 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 GUUE del 04 maggio 2016.

Il testo è disponibile alla risorsa:

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 direttamente applicabile e vincolante in tutti gli Stati membri 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. 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 al diritto.

Il Regolamento UE è stato approvato il 27 aprile 2016, entrato in vigore il 25 maggio dello stesso anno con piena attuazione dal 25 Maggio 2018, data a partire dalla quale ha abrogato 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 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 nuovo regolamento europeo sulla privacy e che è entrato in vigore il 19 settembre 2018.

Campo di applicazione del regolamento

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. 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, come espressamente affermato anche nei relativi considerando al testo, si applica anche al trattamento di 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 a 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. 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. Nella trattazione che segue viene fornita una sintesi, per punti distinti, delle principali e fondamentali novità derivanti dal nuovo Regolamento Europeo.

Cosa cambia con il nuovo regolamento

Il Regolamento UE cambia profondamente la prospettiva in cui si colloca la protezione dei dati personali sebbene a una prima lettura possa rispecchiare una impostazione simile a quella della Direttiva Madre rispetto al costrutto portante (informativa, finalità, consenso), ai ruoli, ai diritti degli interessati e ai doveri dei titolari e dei responsabili.

Il GDPR consacra il diritto alla protezione dei dati personali come diritto fondamentale e costituzionale configurandolo come diritto alla 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.

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" in "sostanziale e pro-attivo", il trattamento e la protezione dei dati personali evolvono nell'acquisire una propria e autonoma rilevanza all'interno dei processi organizzativi e gestionali di una 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 del quale introduce un vera e propria definizione dell'istituto del consenso esplicito, e della trasparenza rispetto alla quale perfeziona il catalogo delle informazioni da esporre nell'informativa; introducendone di nuovi (diritto alla portabilità, all'oblio, all'opposizione verso il trattamento di profilazione);
- accresce le responsabilità del titolare e del responsabile 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 motivando, in tal senso, il titolare e il responsabile a comportamenti e prassi virtuose;
- centralizza la governance e il controllo sul rispetto e la conformità dei trattamenti alla normativa, tramite la cooperazione e la valorizzazione delle Autorità di Controllo nazionali verso il Comitato; incoraggiando meccanismi di certificazione; ampliando il sistema vigilanza; rafforzando quello sanzionatorio sia nelle specifiche comuni che nelle misure applicative.

Dovere di documentazione e di informazione

E' divenuto necessario elaborare un sistema documentale di gestione della privacy contenente tutti gli atti, regolarmente aggiornati, elaborati per soddisfare i requisiti di conformità al Regolamento. È l'applicazione operativa del principio di rendicontazione (o 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 (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). Ancora più rilevante diviene l'obbligo di resa dell'informativa privacy e della acquisizione "granulare" dei consensi (specifici per ogni tipologia di trattamento), quando dovuti. Il Regolamento amplia il contenuto da inserire nell'Informativa rispetto al dettato dall'art. 13 del D.Lgs. 196/2003.

Accresciuta responsabilità dei titolari e dei responsabili del trattamento.

La responsabilità dei titolari (art. 24 e 25) e del responsabile (art. 28) si configura come una sostanziale assunzione di rischio, atteso che il titolare deve mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, la conformità del trattamento al regolamento 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 liberà delle persone fisiche.

A titolari e responsabili di trattamento si affianca una nuova figura obbligatoria per le pubbliche amministrazioni: il responsabile della protezione dei dati personali (c.d. "data protection officer").

Prioritariamente rientrano tra le responsabilità del Titolare e dei Responsabili: l'attuazione delle prassi di privacy by design/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, la valutazione prudenziale sulla violazione dei dati personali, del coefficiente di gravità e delle relative ricadute sul soggetto interessato.

Valutazione d'impatto sulla protezione dei dati

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

Stando a quanto disposto dal Considerando n° 70 del Regolamento, 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) 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.

L'Autorità di controllo redige e pubblica l'elenco di 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 previste misure organizzative e tecniche (comprese quelle di sicurezza) e ogni meccanismo ritenuto utile per la tutela dei diritti dei soggetti interessati.

La responsabilità della valutazione d'impatto attiene prioritariamente il Titolare supportato dal Responsabile protezione dai dati.

Introduzione dei registri delle attività di trattamento – considerando 82, art. 30.

Il titolare e il responsabile di trattamento devono tenere i rispettivi registri delle attività.

Il registro del titolare deve contenere: riferimenti di contatto del titolare/i, del rappresentante del titolare del trattamento nell'Unione (in caso di non stabilimento nell'Unione) e del responsabile della protezione dei dati; le finalità; descrizione degli interessati e dei destinatari; la categoria dei dati personali trattati; la presenza di trasferimenti di dati verso un Paese Terzo un'organizzazione internazionale unitamente alla documentazione sulle appropriate garanzie; la tempistica della cancellazione dei dati; la descrizione della misure di sicurezza e organizzative adottate.

Il registro del responsabile deve contenere oltre alle due ultime voci previste ed elencate per il registro del titolare: i riferimenti di contatto dei responsabili, dei titolari per conto dei quali operano, dei rappresentanti e del responsabile della protezione dei dati; le categorie dei trattamenti effettuati per conto del titolare.

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).

Attuazione dei requisiti di sicurezza dei dati

L'attuale testo del Regolamento richiede la messa in atto di misure tecniche e organizzative adeguate per 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 di 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 i 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 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 illegale, dalla perdita o dalla modifica accidentale e dalla conservazione, trattamento, accesso o comunicazione non autorizzati o illegali;
3. assicurare l'attuazione di una politica di sicurezza in relazione con il trattamento dei dati personali.

È assai probabile che l'adesione a codici di condotta (approvati ai sensi dell'articolo 38 del Regolamento) o un meccanismo di certificazione (approvato ai sensi dell'articolo 39 del Regolamento) possano essere utilizzati come elementi per dimostrare la conformità ai requisiti di sicurezza sopra elencati. E' il Comitato europeo per la protezione dei dati l'ente deputato ad emettere 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 per la protezione fin dalla progettazione e per la protezione di default. Inoltre, se necessario, la Commissione UE può adottare atti di esecuzione per precisare i requisiti delle misure sopra elencate, in particolare per:

1. impedire l'accesso non autorizzato ai dati personali;
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.

Privacy by design e protezione di default

Si tratta dell'esplicitazione del principio dell'incorporazione della privacy fin dalla progettazione del processo aziendale e degli applicativi informatici di supporto, ovvero la messa in atto di meccanismi per garantire che siano trattati - di 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). I Titolari del trattamento devono, 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 nel momento in cui si definiscono le finalità e i mezzi del trattamento sia allatto del trattamento stesso, tenuto conto dell'evoluzione tecnica (e dei costi di attuazione) delle migliori prassi (best pratices) 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 il minimo 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.

Sicurezza e valutazione dei rischi - considerando 83, 84, art. 32

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

Titolare e responsabile sono tenuti tanto alla valutazione dei rischi quanto all'adozione delle misure che comprendono: la pseudonimizzazione, la cifratura; misure implementative della riservatezza, dell'integrità, 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. Alcuni indicatori di rischio (soprattutto connessi ai trattamenti informatizzati) sono declinati nella definizione di violazione di dato personale.

Obblighi di segnalazione in caso di violazioni sui dati

Con la nozione di violazione dei dati personali (c.d. "personal data breaches"), 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. I Titolari del trattamento, in caso di una violazione come sopra descritta, dovranno mettere in atto due differenti azioni: la notificazione della violazione all'Autorità di controllo e la segnalazione al diretto interessato.

Nel primo caso, accertata la violazione, la relativa notificazione 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; 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, dopo aver provveduto alla notificazione, deve comunicare la violazione al diretto interessato senza ritardo. In mancanza l'Autorità di Controllo, considerate le presumibili ripercussioni negative della violazione, può obbligare il Titolare a farlo. 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, i diritti esercitabili dall'interessato.

La comunicazione non è richiesta quando il Titolare 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.

Diritti dell'interessato

Consenso – considerando 39 e 42, art. 6, 7

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 necessariamente la forma scritta 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 il trattamento richieda il consenso, il titolare dovrà essere in grado di dimostrare inequivocabilmente di averlo ottenuto.

Per il trattamento di dati sensibili (il GDPR parla di categorie particolari di dati) è necessario il consenso (art.9 comma 2 lettera a)) a meno che il trattamento non sia necessario per la tutela di diritti di grado superiore dell'interessato stesso o pubblici o di terzi, oppure per obbligo di legge, qualora l'interessato non sia in grado di fornire il consenso (art. 9 comma 2 lettere c, f, g, i, j).

Informativa – considerando da 58 a 73, art. 12, 13, 14

Il titolare del trattamento è tenuto a fornire l'informativa all'interessato, indipendentemente dall'obbligo di acquisire il consenso, salvo il caso in cui l'interessato sia già in possesso delle informazioni (art. 13 co. 4) o in altri casi particolari descritti nel regolamento (art. 14 co. 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 rappresentante e del responsabile della protezione dei dati personali;

- 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 sia basato sull'art. 6, paragrafo 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 a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso di trasferimenti di cui all'articolo 46 e 47, o all'articolo 49, comma 2, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stai 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 a un obbligo legale o contrattuale oppure se si tratta di un requisito necessario per la conclusione di un contratto, nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative circa la logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

A 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 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 dei dati.
- La necessità di indicare eventuali processi automatici di profilazione e le conseguenze per l'interessato di tale trattamento dati.

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 ottenuti 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'articolo 89, paragrafo 1, 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 adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni.

<u>Caratteristiche dell'informativa</u>

Il regolamento 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 agevolare la comprensione, il regolamento 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.

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 servizi resi loro disponibili.

Diritti "tradizionali" – considerando da 58 a 73, art. 12 a 17

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

Tra le novità previste nel nuovo GDPR rispetto alla Direttiva 95/46/CE e al Codice Italiano si citano:

- il riscontro deve essere fornito senza ingiustificato ritardo e, comunque, al più tardi entro 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. Nel caso di diniego, il riscontro deve essere fornito al più tardi entro un mese dal ricevimento della richiesta
- la definizione da parte del titolare di eventuali oneri sull'interessato nei casi particolari previsti nell'art. 12 comma 5.

A differenza della normativa previgente, è posto meno 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 a utilizzare un linguaggio semplice e chiaro.

Nuovi Diritti: diritto di limitazione; diritto di opposizione alla profilazione; diritto alla cancellazione / all'oblio; diritto alla portabilità; – art. 18, 20, 21, 22

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

Il diritto alla limitazione rappresenta un diritto diverso e più esteso rispetto al "blocco" del trattamento già previsto dal codice, in particolare, 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, o dell'accertamento diritti in sede giudiziaria, di tutela diritti di altra persona fisica o giuridica, o in presenza di un interesse pubblico rilevante.

Il diritto di opposizione alla profilazione che 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 che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il diritto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata nel caso questi siano stati resi pubblici on-line. I titolari hanno l'obbligo di informare della richiesta di cancellazione ogni altro titolare che tratta i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione". Inoltre l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento.

Il diritto alla portabilità 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; fanno eccezione quindi i dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare.

Sintesi delle principali novità

Le principali novità sono sintetizzate per parole chiave nelle seguenti tabelle.

Consenso	Libero, specifico, informato, inequivocabile e concludente.
Informativa	Informazioni di contatto titolare, rappresentante e responsabile protezione dei dati; 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. Usabilità dell'esposizione.
Valutazione impatto	Ripensamento delle tecnologie a supporto dei trattamenti. Analisi e eventuale consultazione preventiva con l'Autorità Garante per le implicazioni sui diritti e le libertà delle persone. Obbligo del titolare, supportato dal responsabile protezione dati.
Sicurezza	Analisi dei rischi e di valutazione dell'adeguatezza delle misure tecniche e organizzative. Obbligo congiunto del titolare e del responsabile del trattamento dati.
Violazione dei dati	Equiparazione della fattispecie accidentale con quella dolosa.
Privacy by Design	Applicazione delle tutele di trattamento sin dalla sua progettazione e avvio.
Privacy by Default	Pseudonimizzazione e Minimizzazione (di dati e tempi) come garanzia e misura di PbD. Obbligo del titolare.
Responsabile PDP (detto anche DPO)	Si interfaccia con le Autorità Garanti. Supporta titolare e responsabile del trattamento. Obbligatorio nelle PA.
Registro Trattamenti	Registri di competenze in cui indicare le caratteristiche, le modalità e le finalità del trattamento. Lo redigono titolare e responsabile del trattamento.
Sanzioni	Sanzioni amministrative pecuniarie fino a 20 000 000 EUR. (per le imprese, fino al 4% del fatturato globale annuo dell'esercizio precedente).
Autorità	Comitato di controllo europeo: assicura la uniforme applicazione del Regolamento. 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 e trasmetterli ad altri.
Oblio	L'interessato ha diritto alla de-indicizzazione o alla cancellazione delle informazioni che lo riguardano.
Sportello Unico	Unicità dell'interlocutore territoriale. Semplificazione e uniformità di gestione nell'applicazione del nuovo regolamento.

I soggetti del trattamento

Il GDPR individua i soggetti coinvolti nel trattamento sulla base:

1) delle finalità per le quali sono raccolti:

- il Titolare è la persona giuridica o la persona fisica che raccoglie i dati personali per proprie finalità e decide i mezzi per il trattamento;
- il Contitolare è la persona giuridica o la persona fisica che condivide le finalità con altro Contitolare e stabilisce insieme a questi le modalità di trattamento,
- il Responsabile 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 altro atto giuridico,
- il Destinatario è la persona giuridica o la persona fisica che riceve i dati dal Titolare 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 è la persona fisica che ha ricevuto dal titolare precise istruzioni per l'esecuzione dei trattamenti dati di sua competenza;
- l'interessato è la persona fisica che fornisce i propri dati personali a un Titolare per le finalità specificate nell'informativa;

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

- il Responsabile della Protezione dei Dati è la persona giuridica o la persona fisica che segue tutti i vari aspetti relativi all'applicazione del GDPR per conto del Titolare/Responsabile, deve obbligatoriamente essere presente nelle pubbliche amministrazioni;

3) dell'ambito territoriale:

- il Rappresentante nell'Unione del Titolare/Responsabile che ha la propria sede in uno stato terzo è la persona giuridica o la persona fisica che su mandato del Titolare/Responsabile 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 del trattamento);
- l'Autorità di Controllo è la persona giuridica pubblica istituita da ogni Stato membro per sovrintendere all'applicazione e 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.

Titolare del trattamento

Il titolare è definito all'art. 4 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 non viene designato o nominato ma diventa tale al momento che raccoglie dati personali con l'intento di trattarli per finalità lecite, come previsto all'art. 6, e decide le modalità di trattamento.

Contitolare

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 fra i contitolari deve essere reso noto all'interessato. Questi può esercitare i propri diritti nei confronti di ogni contitolare.

Responsabile del trattamento dati

Il GDPR definisce all'art. 4 il Responsabile 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 dall'attuale Codice, soprattutto per quanto concerne il rispondere in solido con il Titolare di eventuali inadempienze.

Il responsabile del trattamento dati è un soggetto esterno che esegue, in base a un contratto/convenzione o altro atto giuridico, dei trattamenti di dati personali per conto del titolare e ne risponde in solido in caso di inadempienze. Al Responsabile spettano tutti i compiti del Titolare all'interno del proprio organismo (valutazione impatto, registro dei trattamenti, eventuale nomina del Responsabile della Protezione Dati, ecc.) Il Responsabile così individuato non può a sua volta nominare un altro Responsabile se non dietro autorizzazione scritta del Titolare: la catena delle responsabilità deve essere nota al Titolare. Nei contratti con sub-responsabili devono essere riportati gli stessi obblighi in materia di protezione dei dati personali previsti dal contratto tra responsabile e titolare.

Nell'informativa 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 assicuri un'adeguata protezione dei dati.

Soggetti autorizzati

Nelle linee guida del Garante si afferma che "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 dati all'interno dell'Organizzazione, prima denominati "incaricati". È sottolineata l'importanza di "istruire" i soggetti, sarà quindi opportuno prevedere percorsi formativi adeguati per coloro che saranno coinvolti nel trattamento dati.

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

Analogamente a quanto è stato fatto fino ad oggi, è possibile individuare i soggetti che sono autorizzati al trattamento dei dati, mediante una nomina individuale da parte del Titolare o Responsabile del trattamento 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 così come concepita dall'attuale normativa, non emerge in maniera esplicita dall'art. 29 del GDPR. Il termine" istruzione" del soggetto da parte del titolare indica che è necessaria una formazione/informazione 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 trattamenti 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 è tenuto ad adottare.

Salvo ulteriori precisazioni da parte del Garante, gli amministratori di sistema risultano essere incaricati con particolari compiti, pertanto per questa tipologia è opportuno mantenere la nomina individuale.

Data Protection Officer – DPO (o Privacy Officer)

Già nel 2006, il Presidente del Garante Privacy Francesco Pizzetti, affermava "Vedo con molto favore l'istituzione della figura del Data Protection Officer (DPO) specialmente per le aziende e le corporation medie e grandi. La diffusione di questa figura non potrebbe che aiutare l'azione del Garante e la diffusione stessa della privacy nell'ambito delle strutture di impresa". Con l'avvento del nuovo Regolamento Ha trovato previsione la nuova figura del "Responsabile per la protezione dei dati". E' divenuto obbligatorio nominare il DPO 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 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
- 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 (dati particolari / sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Il DPO va designato per un dato periodo ed in funzione delle qualità professionali, della conoscenza specialistica della normativa. I Titolari del trattamento devono 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 in qualità di DPO 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 a 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 va comunicato all'Autorità di Controllo e al pubblico, sono quelli di:

- sensibilizzare e consigliare il Titolare in merito agli obblighi (misure e procedure tecniche e organizzative) derivanti Regolamento;
- sorvegliare l'applicazione delle politiche compresa l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e l'effettuazione degli audit connessi;

- sorvegliare l'applicazione del Regolamento, con particolare riguardo alla protezione fin dalla progettazione, alla protezione di default, alla sicurezza dei dati, alle informazioni dell'interessato ed alle richieste degli stessi per esercitare i diritti riconosciuti;
- controllare che il Titolare effettui la Valutazione d'impatto sulla protezione dei dati (c.d. DPIA) e richieda all'Autorità di Controllo l'autorizzazione preventiva o la consultazione preventiva nei casi previsti;
- 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. Allo stato attuale lo schema di certificazione più attendibile realizzato per attestare le competenze dei professionisti chiamati a svolgere il ruolo di DPO in outsourcing è quello realizzata dall'ente di certificazione TUV Italia (Schema di certificazione CDP) il cui registro pubblico degli abilitati è rinvenibile al seguente indirizzo: http://www.tuv.it/it-it/area-clienti/ricerca-figure-professionali-certificate.

Destinatario

Il GPDR all'art. 4 definisce destinatario "la 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, sia che siano interni o esterni, sia che li ricevono per eseguire trattamenti per conto del titolare sia che li ricevono 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 che il destinatario sia un soggetto che risiede in un paese non membro dell'Unione, è richiesto che il Titolare verifichi che le garanzie offerte da questi per la protezione dei dati siano adeguate.

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

Nel caso il destinatario sia un soggetto "terzo" che riceve i dati per perseguire proprie finalità, diventerà a sua volta titolare. Il destinatario che riceve i dati da altro titolare per perseguire finalità proprie è tenuto a dare 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 a un obbligo di legge.

Interessato

L'interessato (data subject) è la persona fisica alla quale si riferiscono i dati trattati. È sempre una persona fisica. L'interessato è quindi il soggetto "proprietario" dei dati personali e su questi conserva dei diritti nei confronti del titolare del trattamento. 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. La risposta alle richieste dell'interessato deve comunque essere tempestiva e, anche nel caso non sia possibile soddisfarla, occorre specificare la motivazione del rifiuto. Il titolare ha il compito di facilitare l'accesso all'interessato ai suoi dati, predisponendo dei canali di comunicazione dedicati, quali ad esempio i recapiti del Responsabile della Protezione dei Dati.

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.

Autorità di controllo e comitato europeo

Le autorità di controllo sono incaricate di "sorvegliare l'applicazione del presente regolamento (GDPR) 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" (punto 1) art. 51 del GDPR).

Ogni stato membro istituisce una o più autorità pubbliche indipendenti. Nel caso siano più di una deve essere designata quella che le rappresenterà nel Comitato europeo per la protezione dei dati, che ha 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.

Conclusioni sul nuovo regolamento europeo

La rilevanza generale del regolamento, come appare chiaro, ha una notevole portata. Non si tratta di una semplice revisione, 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 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 per 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 attuale, ad uno di alta responsabilizzazione sostanziale in cui è richiesto un ruolo proattivo ai Titolari del trattamento.

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. Di non meno importanza è anche, 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), 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 le 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).