Il regolamento europeo sulla privacy n° 679/2016 , approvato il 14 aprile del 2016 dal Parlamento europeo, sarà direttamente applicabile negli stati membri a partire dal **25 MAGGIO 2018**, termine che non verrà prorogato. Il regolamento si applica a tutte le realtà imprenditoriali, professionali e nell'ambito pubblico e sanitario. Il regolamento integra il "codice privacy" italiano che fa capo al decreto legislativo n° 196 del 2003. Il nuovo regolamento europeo rende uniforme tutte le leggi nazionali degli stati membri in tema di privacy, quindi le regole sono uniche per tutti gli stati. Il principio fondamentale del nuovo regolamento è la protezione dei dati personali e la protezione dei diritti e delle libertà fondamentali delle persone fisiche. Quindi chiunque tratti dati personali di persone fisiche è tenuto a mettere in atto delle misure idonee a garanzia di un corretto trattamento. Le sanzioni in caso di mancanza dell'applicazione delle norme privacy sono molto alte sia dal punto di vista civile che penale.

Il regolamento europeo è obbligatorio per venire incontro all'esigenza di "proteggere" i dati personali da un utilizzo improprio senza che l'interessato sia coinvolto in una eventuale diffusione non autorizzata (consenso). Se da una parte vi è l'esigenza del titolare (azienda/impresa) di perseguire i suoi legittimi interessi nell'utilizzo dei dati, anche nei casi di consenso esplicito dell'interessato, non viene meno comunque il principio che i dati personali sono sempre di "proprietà" dell'interessato, quale persona fisica identificata o identificabile. Per tale ragione il regolamento impone una serie di misure ritenute adeguate, per limitare l'utilizzo dei dati (minimizzazione) e per un corretto utilizzo di tali dati, attraverso la creazione di procedure che tutti gli incaricati aziendali dovranno utilizzare per come previsto dalle norme. La creazione di un modello di gestione della privacy passa attraverso una necessaria ricognizione aziendale, con lo scopo di identificare i processi (trattamenti), l'elenco delle strutture informatiche, la suddivisione dei ruoli, i livelli di accesso consentiti agli incaricati. Tale modello, con il nuovo regolamento europeo assume un carattere "dinamico" che a differenza di quanto precedentemente veniva effettuato a norma del codice privacy 196/03, prevede un controllo periodico attraverso la cosiddetta attività di "audit". L'Audit Privacy è una valutazione dei processi aziendali sul grado di rispetto della normativa vigente. Si può paragonare a un check up va effettuato da un esperto, l'auditor, che potremmo paragonare al medico. L'audit dal punto di vista pratico consiste in una intervista al titolare del trattamento dati in azienda, che si svolge periodicamente. Le domande sono dirette a conoscere in che modo i dati vengono raccolti e trattati. Nel caso venga riscontrato qualcosa che va perfezionato in azienda sul fronte della raccolta e trattamento dati, chi svolge l'audit (che deve essere un esperto di data protection sia a livello giuridico che informatico) prescrive le "cure" del caso.

In ultimo, ma non per importanza, il nuovo regolamento impone una costante e documentata formazione del personale incaricato, che deve essere effettuata ogni qualvolta vi sono novità dal punto di vista normativo, quando ricorrono casi (adeguamento tecnologico, nuovo trattamento) che prevedono uno specifico impatto in materia di privacy, quando vi sono cambi di ruoli e/o mansioni all'interno dell'azienda, immissione di nuovo personale, ecc.

In conclusione va sottolineato come l'apparato sanzionatorio del regolamento europeo rafforza il concetto di "protezione" che si aggiunge a quello ancora in vigore previsto dal Dlgs 196/03 (codice privacy).

EFINIZIONI PRINCIPALI

1) **Dato Personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) **Interessato** : la persona fisica che conferisce i propri dati personali;
3) **Trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
4) **Titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

5) **Responsabile del Trattamento** : a persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
6) **Informativa** : Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni relative al trattamento dei suoi dati;
7) **Consenso**: Una dichiarazione scritta e inequivocabile rilasciata dall'interessato prima dell'inizio del trattamento dei suoi dati.

Con il Nuovo Regolamento il Titolare ha un ruolo più proattivo e obblighi più pregnanti, finalizzati non soltanto al formalistico rispetto delle regole, ma anche all'adozione di tutti gli accorgimenti tecnici e organizzativi necessari a garantire la sicurezza effettiva nei trattamenti, anche sotto il profilo della sicurezza.

Privacy by design (*) e by default (**) (art. 25)

- La privacy by design richiede che Il Titolare adotti e attui misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati.

- La privacy by default presuppone invece, nella modalità operativa del trattamento, misure e tecniche che, per impostazione predefinita, garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento.

(*) costruire le regole prima dell'inizio del trattamento - (**) regole standard per garantire le misure di sicurezza minime/idonee

Accresciuti obblighi di trasparenza (artt. 5 e 12)

Il Legislatore europeo dedica una sezione del Nuovo Regolamento alla "Trasparenza" e, con riferimento alle modalità di trattamento dei dati, richiede che le informazioni all'interessato:

- Siano rese con un linguaggio semplice e chiaro, soprattutto nel caso di minori;

- Abbiano sempre forma scritta , l'informativa in forma orale essendo ammessa solo quando ciò è richiesto dall'interessato e l'identità di questi possa essere provata con altri mezzi;

- Prevedano:

(1) il periodo di conservazione dei dati personali,

(2) il diritto di proporre reclamo ad un'autorità di controllo,

(3) l'intenzione del titolare di trasferire dati personali a un paese terzo.

Data breach – Violazione dei dati (artt. 33 e 34)

Il Nuovo Regolamento estende tale obbligo di comunicazione a tutti i Titolari e Responsabili, quali che siano i trattamenti posti in essere. Hanno l'obbligo di comunicare l'avvenuta violazione di dati personali:

- al Garante per la protezione dei dati personali;

- in determinati casi, anche al contraente/cliente.

Nello specifico, il Responsabile deve informare il Titolare senza ingiustificato ritardo della violazione e quest'ultimo deve notificare la violazione, a sua volta senza ingiustificato ritardo, all'autorità di controllo (i.e., al Garante) e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Valutazione d'impatto sulla protezione dei dati (art. 35)

Quando un determinato trattamento - tenuto conto dell'uso di nuove tecnologie e della sua natura, del contesto e delle finalità - può presentare un rischio elevato per i diritti e libertà delle persone fisiche, il Titolare deve effettuare una valutazione d'impatto dello stesso sulla protezione dei dati ("Valutazione d'Impatto"). È previsto che il Titolare riveda costantemente la Valutazione d'Impatto.

Registri delle attività di trattamento (art. 30)

Il Responsabile e il Titolare devono tenere un registro delle attività di trattamento in forma scritta, anche in formato elettronico, contenente gli elementi di cui all'art. 30 del Nuovo Regolamento.

Diritti dell'interessato

Diritto all'oblio (art. 17)

Il diritto dell'individuo ad essere "dimenticato" dalle banche dati, dai mezzi di informazione, o dai motori di ricerca. Il Nuovo Regolamento attua il riconoscimento su base legislativa del diritto all'oblio. In particolare, l'interessato ha diritto di chiedere che siano cancellati e non più sottoposti a trattamento i suoi dati personali:

(1) che non siano più necessari per le finalità per le quali sono stati raccolti;
(2) quando abbia ritirato il consenso o si sia opposto al trattamento o il trattamento dei dati personali non sia altrimenti conforme al Nuovo Regolamento.

Portabilità dei dati (art. 20)

L'interessato ha il diritto di:

(1) ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati che lo riguardano forniti al Titolare;
(2) trasmettere i propri dati (ad esempio, quelli relativi al proprio "profilo utente") da un Titolare (ad esempio un social network) ad un altro Titolare, senza impedimenti da parte di colui al quale sono stati forniti in precedenza.

Nuove figure soggettive

Il Nuovo Regolamento individua, come destinatari delle sue disposizioni, ulteriori figure rispetto al Codice Privacy.

- **Responsabile della protezione dati ("RDP") (art. 37)**

Il Titolare o il Responsabile devono designare un RDP qualora:

(1) il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico;
(2) le attività principali del Titolare o del Responsabile consistano in trattamenti che, per loro natura, campo di applicazione e/o finalità richiedano il controllo regolare e sistematico degli interessati su larga scala;
(3) il Titolare o il Responsabile trattino dati sensibili o giudiziari.

L'RDP deve essere designato in base alla sua professionalità e, in particolare, alla sua conoscenza della legislazione di protezione dei dati ed è tenuto, a:

- informare e consigliare il Titolare o il Responsabile in merito agli obblighi derivanti dal Nuovo Regolamento e da altre disposizioni dell'UE;
- sorvegliare che il Nuovo Regolamento sia osservato;
- fornire, se richiesto, un parere in merito alla Valutazione d'Impatto;
- cooperare con l'autorità di controllo.

Sanzioni

Il trattamento sanzionatorio viene uniformato e inasprito in tutti gli Stati membri UE.

Sanzioni amministrative (art. 83)

Il Nuovo Regolamento prevede che l'autorità di controllo abbia il potere di imporre sanzioni amministrative per un importo pecuniario massimo predeterminato, tenendo conto, di determinati indici ad esempio:

(1) la natura, la gravità e la durata della violazione,

(2) il carattere doloso o colposo della stessa,

(3) le misure adottate dal Titolare.

Le sanzioni variano a seconda del trasgressore, se si tratta di persona fisica o impresa.

Altre sanzioni (art. 84)

Il Nuovo Regolamento prevede che saranno gli Stati membri a stabilire le norme relative alle altre sanzioni assicurandone la proporzionalità e l'efficacia dissuasiva. Con riferimento all'Italia, non è da escludere il **mantenimento dell'attuale quadro sanzionatorio per illeciti penali** delineato dal Codice Privacy, con le necessarie modifiche in funzione de nuovo quadro di obblighi e requisiti previsti dal Nuovo Regolamento.