MILANO
MONZA BRIANZA

F.I.M.A.A.

SCHEMA NOVITA' PRIVACY
Legge sulla Tutela dei Dati Personali

Il nuovo Regolamento UE n. 2016 / 679

Il Regolamento Ue n. 2016 / 679 si pone l'obiettivo di stabilire un complesso normativo volto alla protezione del trattamento dei dati personali delle persone fisiche, nonché di disciplinare le regole sulla libera circolazione dei dati personali. Il regolamento dell'Unione Europea produce effetti vincolanti all'interno dell'ordinamento giuridico nazionale e le norme in esso contenute vanno così a prevalere su quelle già esistenti nei singoli Stati membri dell'UE (per quanto ci riguarda nel decreto legislativo 30 giugno 2003, n. 196).

Il Regolamento Comunitario 2016 / 679 rivisita la disciplina in tema di trattamento dei dati personali richiamando in buona parte i principi già ad oggi vigenti nei vari ordinamenti giuridici degli Stati comunitari, integrandoli con alcune significative novità.
Definisce *"dato personale"* qualsiasi informazione riguardante una persona fisica identificata o identificabile *("interessato")* e *"trattamento del dato"* qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati ed applicate a dati personali o ad insiemi di dati personali.

Qui di seguito si illustrano le norme più rilevanti, man mano verranno forniti maggiori dettagli ed approfondimenti degli aspetti più particolari.

Liceità del trattamento (art. 6)
Il Regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all' art. 6 del Regolamento.
Per la precisione il trattamento è lecito quando:

- ✓ l'interessato ha espresso il proprio consenso (un consenso informato) al trattamento dei propri dati per una o più specifiche finalità;
- ✓ il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte;
- ✓ il trattamento è necessario per adempiere un obbligo legale a cui è soggetto il titolare del trattamento;
- ✓ lo stesso è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica ovvero quando è necessario per l'esecuzione di un compito di interesse pubblico o per il perseguimento del legittimo interesse del titolare del trattamento.

Trattamento di categorie particolari di dati personali (art. 9)

L'art. 9 del Regolamento, afferma il principio per cui *"è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".*

Il Regolamento prevede una deroga a tale divieto allorquando:

- ✓ l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche**,** salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui sopra*;*
- ✓ il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- ✓ il trattamento è necessario per la tutela di un interesse vitale dell'interessato o di un'altra persona fisica se l'interessato si trovi nell'incapacità di prestare il proprio consenso;
- ✓ il trattamento riguarda dati personali resi manifestamente pubblici dall' interessato;
- ✓ il trattamento è necessario per accertare, esercitare, o difendere un diritto in sede giudiziaria od ogni qualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- ✓ il trattamento è necessario per motivi di interesse pubblico.

L' informativa (artt. 13-14)

Il Regolamento definisce *"informativa"* quel nucleo di informazioni che il titolare del trattamento è tenuto a fornire ai soggetti di cui si appresta a trattare i dati. Tale definizione va interpretata secondo il principio di trasparenza. In particolare l'art. 13 del nuovo Regolamento enumera le informazioni che il titolare deve fornire all'interessato, qualora i dati personali siano raccolti presso di lui; mentre con il successivo art. 14 elenca quelle da rendersi ove i dati siano invece raccolti presso un soggetto diverso dall'interessato. Per l'appunto, nel caso in cui i dati vengano raccolti presso il titolare del trattamento, questi dovrà fornire all'interessato un'informativa che contenga:

a) l'identità e i dati di contatto del titolare e, ove applicabile del suo rappresentante;
b) i dati di contatto del Responsabile della Protezione dei Dati;
c) le finalità del trattamento;
d) i legittimi interessi del titolare di terzi;
e) i destinatari dei dati;
f) l'intenzione del titolare di trasferimento dei dati ad un paese terzo;
g) il periodo di conservazione dei dati o, se non è possibile, i criteri utilizzati per determinare tale periodo;
h) il diritto di accesso ai dati da parte dell'interessato, il diritto di rettifica e di cancellazione, la limitazione del trattamento o l'opposizione allo stesso e il diritto alla portabilità;
i) il diritto di revoca del consenso;
j) il diritto di reclamo all' autorità di controllo;
k) l'obbligatorietà o la non obbligatorietà di comunicare dati, nonché le possibili conseguenze di un eventuale rifiuto;
l) l'esistenza di un processo automatizzato come la profilazione e l'indicazione delle logiche utilizzate, dell'importanza e delle conseguenze del trattamento.

Nel caso in cui i dati raccolti vengano utilizzati per una finalità diversa da quella per cui gli stessi sono stati ottenuti, prima dell'ulteriore trattamento, il titolare ha l'obbligo di fornire all'interessato tutte le informazioni in merito alla finalità diversa per cui i dati verranno utilizzati, nonché tutte le necessarie ed ulteriori informazioni pertinenti.

Nella diversa ipotesi in cui, invece, i dati vengano raccolti presso soggetti diversi dall'interessato, l'art. 14 del Regolamento prevede che il responsabile del trattamento fornisca all'interessato un'informativa:

a) entro un termine ragionevole dall'ottenimento dei dati, al più tardi entro un mese in considerazione delle specifiche circostanze in cui i dati sono trattati;
b) in caso di prevista comunicazione con altro destinatario al più tardi al momento della prima divulgazione dei dati;
c) nel caso in cui i dati siano destinati alla comunicazione con l'interessato al più tardi al momento della prima comunicazione all'interessato.

In tutti questi casi, ad ogni modo, l'informativa deve contenere:

a) tutto quanto sopra indicato per l'ipotesi in cui i dati siano raccolti presso l'interessato (art. 13 Reg. n. 2016/679);
b) le categorie dei dati in questione;
c) i legittimi interessi perseguiti dal titolare del trattamento o da terzi qualora il trattamento sia basato su un legittimo interesse;
d) la fonte di provenienza dei dati e se questa ha carattere pubblico.

Anche in questo caso il titolare del trattamento, prima di procedere con qualsivoglia ulteriore trattamento non previsto inizialmente, deve fornire all'interessato le informazioni in merito alla diversa finalità dell'utilizzo dei suoi dati personali.

Gli unici casi in cui può essere omessa l'informativa sono i seguenti:

1) se si dispone già delle informazioni o sono informazioni note;
2) se comunicare tali informazioni comporta uno sforzo sproporzionato o è impossibile (valutazione che spetta al titolare del trattamento);
3) se l'ottenimento dei dati o la loro comunicazione sono previsti dal diritto dell'Unione;
4) se i dati devono restare riservati per un obbligo di segreto professionale.

Il diritto di accesso dell' interessato (art. 15)

Il diritto all'accesso prevede **in qualsiasi caso** il diritto di **ricevere una copia** dei dati personali oggetto di trattamento. Il titolare deve indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi. I titolari inoltre possono consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

Il diritto all'oblio (art. 17)

Il diritto *"all'oblio"* si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno reso pubblici i dati personali dell'interessato, ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi *"qualsiasi link, copia o riproduzione."* Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del nostro Codice Privacy (D.lgs. 196/2003), poiché 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 al trattamento (art. 18)

Si tratta di un diritto **diverso e più esteso rispetto al "blocco" del trattamento** di cui all' art. 7, comma 3, lettera a), del nostro Codice: in particolare è esercitabile **non solo in caso di violazione** dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche **se l'interessato chiede la rettifica dei dati** (in attesa di tale rettifica da

parte del titolare) o **si oppone al loro trattamento** ai sensi dell'art. 21 del Regolamento (in attesa della valutazione da parte del titolare). Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato, a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Diritto alla portabilità dei dati (art. 20)

Si tratta di uno dei nuovi diritti previsti dal Regolamento. **Non si applica ai trattamenti non automatizzati** (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio) e solo i dati che siano stati **"forniti" dall'interessato** al titolare. Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili ad un altro titolare indicato dall'interessato, se tecnicamente possibile.

Diritto di opposizione (art. 21)

Il cosiddetto *"diritto di opposizione*", per definizione consente all'interessato di opporsi *"in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano".* In virtù dell'esercizio di tale diritto il titolare potrà continuare a trattare i dati in suo possesso solo ove 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"*.

Inoltre, per i trattamenti che comportano attività di profilazione o di marketing diretto, il regolamento prevede che *"qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non potranno più essere oggetto di trattamento per tali finalità*".

Responsabilità del titolare (art. 24)

Il titolare del trattamento oltre a mettere in atto misure tecniche ed organizzative adeguate per garantire che il trattamento compiuto sia conforme al Regolamento, deve anche dimostrare che tali misure siano effettive, ossia vigenti. L'inadempimento è costituito dall'incapacità del titolare di dimostrare di aver adottato idonee misure di sicurezza per garantire un trattamento legittimo.

L'adesione ai codici di condotta o ricorrendo al rilascio di certificazioni da parte di appositi organismi riconosciuti con provvedimenti dell'Autorità Garante può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25)

Il titolare, prima di compiere una qualsiasi operazione di trattamento, deve verificare se le misure tecniche ed organizzative che intende attuare siano adeguate avendo riguardo al tipo di dati trattati, al contesto in cui avviene il trattamento e alla finalità dello stesso, alla probabilità e gravità di eventuali attentati ai diritti e libertà degli interessati. Ogni operazione che ha ad oggetto dati personali deve essere preceduta da un'attenta progettazione delle singole fasi di trattamento nelle quali il titolare predispone i presidi e le procedure per minimizzare i rischi di perdita, alterazione o accesso non autorizzato ai dati personali apprestando le necessarie garanzie a protezione dei dati al fine di soddisfare i requisiti del Regolamento.

Le impostazioni predefinite rappresentano l'ambito, gli strumenti e le modalità del trattamento predisposte dal titolare affinché siano utilizzati solo i dati personali necessari per ogni specifica

finalità del trattamento. Esse devono essere contenute nei limiti del trattamento minimo per il perseguimento del fine per cui i dati sono raccolti.

Notifica di una violazione dei dati personali all'autorità di controllo (art. 33)
Nel caso di violazione dei dati personali il titolare, senza ritardo, deve darne comunicazione all'Autorità Garante a meno che non sia in grado di dimostrare che la violazione non costituisca un rischio per i diritti e le libertà delle persone fisiche.
La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.

Comunicazione di una violazione dei dati all'interessato (art. 34)
Se il titolare ritiene che il rischio per i diritti e le libertà degli interessati sia elevato, allora deve informare anche l'interessato *"senza ingiustificato ritardo".*
Non è richiesta la comunicazione all'interessato quando:

- ✓ il titolare del trattamento ha messo in atto le misure tecniche ed organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- ✓ il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- ✓ la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Valutazione di impatto sulla protezione dei dati (art. 35)
Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il Regolamento obbliga i titolari a svolgere una valutazione di impatto in via preliminare quando sono in uso nuove tecnologie o quando si possono presentare rischi dei trattamenti. I titolari sono infatti tenuti non soltanto a garantire l'osservanza delle disposizioni del Regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza, la valutazione di impatto ne è un esempio.

Responsabile della protezione dei dati (art. 37)
Il responsabile della protezione dei dati deve sempre essere tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. È chiamato ad assumere un ruolo decisivo sia nell'ambito dei trattamenti compiuti dai titolari che per quelli compiuti dai responsabili del trattamento. Al responsabile della protezione dei dati sono fornite le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Codici di condotta (art. 40)
I codici di condotta possono essere redatti dalle Associazioni e dalle Organizzazioni che rappresentano categorie di titolari del trattamento o di responsabili del trattamento e devono tenere conto delle caratteristiche specifiche dei settori di riferimento e delle diverse esigenze connesse alle dimensioni aziendali.
In particolare, secondo l'art. 40 del Regolamento, potrebbero concernere:

- ✓ il trattamento corretto e trasparente dei dati;
- ✓ i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;

- ✓ la raccolta dei dati personali;
- ✓ la pseudonimizzazione dei dati personali;
- ✓ l'informazione fornita al pubblico e agli interessati;
- ✓ l'esercizio dei diritti degli interessati;
- ✓ la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
- ✓ le misure di sicurezza;
- ✓ la notifica dei data breach e la relativa comunicazione agli interessati;
- ✓ il trasferimento di dati personali verso paesi terzi;
- ✓ le procedure stragiudiziali di composizione delle controversie.

Il progetto di codice dovrà essere sottoposto all'Autorità Garante nazionale che esprimerà un parere a riguardo. Se il parere è positivo e l'applicazione del Codice riguarda solamente lo Stato membro in cui è presentato, l'Autorità registrerà e pubblicherà il Codice realizzato**.** Nel caso in cui, invece, il progetto di codice di condotta si riferisca a trattamenti realizzati in vari Stati membri, prima che vi sia approvazione definitiva, occorre un secondo esame a livello europeo, con il coinvolgimento del Comitato europeo per la protezione dei dati. Qualora, anche a seguito di tale controllo, il progetto ottenga un parere favorevole, sarà registrato e pubblicato.
Ai sensi del Regolamento, inoltre, la Commissione ha il potere di decidere che il codice di condotta abbia validità generale all'interno dell'Unione: in tal modo il codice è reso applicabile a tutto il settore di riferimento, in tutto il territorio dell'Unione Europea.
Il comitato raccoglie in un apposito registro tutti i Codici di condotta e la Commissione è tenuta a dare pubblicità a quelli che hanno acquisito validità generale.

Diritto di proporre reclamo all'autorità di controllo (art. 77)
L'interessato che ritenga che il trattamento che lo riguarda violi il Regolamento ha il diritto di proporre reclamo ad un'autorità di controllo nello Stato membro in cui risiede abitualmente e/o lavora oppure nel luogo ove si è verificata la presunta violazione.
L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale.

Diritto al risarcimento e responsabilità (art. 82)
L' articolo 82 prevede il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento per chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento.
Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento.

Sanzioni amministrative pecuniarie (art. 83)
Sono stati previsti **inasprimenti** delle sanzioni in caso di violazioni del Regolamento.
Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

- ✓ la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione, nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- ✓ il carattere doloso o colposo della violazione;
- ✓ le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- ✓ il grado di responsabilità del titolare del trattamento o del responsabile del trattamento

tenendo conto delle misure tecniche e organizzative da essi messe in atto;
- ✓ eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- ✓ il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- ✓ le categorie di dati personali interessate dalla violazione;
- ✓ la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- ✓ qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- ✓ l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;
- ✓ eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Gli Stati membri, in conformità a quanto sopraindicato, devono prevedere sanzioni amministrative fino a **10 milioni di euro** oppure, nel caso in cui il trasgressore sia un'impresa, fino al **2% del fatturato mondiale annuo conseguito nell'esercizio precedente** (alla data in cui è stata rilevata la violazione)
Tali importi raddoppiano (**20 milioni** o il **4% del fatturato mondiale**) quando:
- ✓ si violano le condizioni per il rilascio del consenso informato;
- ✓ trattamento di dati giudiziari o sensibili;
- ✓ mancato riscontro al legittimo esercizio dei diritti dell'interessato;
- ✓ trasferimento dei dati verso Paesi che non garantiscono livelli adeguati di tutela;
- ✓ violazione di un ordine dell' Autorità Garante.

Inoltre sono stati rafforzati i poteri delle Autorità Garanti nazionali.