l'officina dei numeri

circolare informativa 9/2017 del 27.11.2017
Studio Associato Picchio e Gorretta Via Fausto Coppi 3 – 15121 – Alessandria
tel. e fax 0131 443273 – 0131 267858 e-mail: infi@picgor.it
sito web: www.picgor.it

GDPR: NUOVO REGOLAMENTO UE SULLA PRIVACY A PARTIRE DAL 25 MAGGIO 2018

Premessa

Lo scorso 24 maggio 2016 è entrato in vigore il cd. **General Data Protection Regulation** (GDPR), cioè il nuovo "***Regolamento UE n. 2016/679*** *del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*", il quale verrà applicato in ogni Paese membro a partire dal **25 maggio 2018**.

Entro tale data ogni azienda dovrà adeguare la propria organizzazione interna e le proprie *policies* alle novità introdotte in materia di *privacy*. Il regolamento è direttamente applicabile e obbligatorio in tutti gli Stati membri e non occorrerà alcuna norma di recepimento; in Italia andrà a sostituire il D.Lgs. 30 giugno 2003, n. 196 – attuale Codice della Privacy – che non verrà abrogato ma dovrà essere disapplicato in favore della nuova disciplina nel caso di contrasto tra le due normative. Di converso, ove le previsioni del D.Lgs. 196/2003 fossero più severe, precise e vincolanti di quelle del GPDR, le stesse continueranno ad essere applicate, anche se dovranno essere interpretate alla luce dei principi generali del GPDR.

Il regolamento mira a rendere uniforme la tutela della privacy (divenuta ormai un diritto soggettivo di primaria importanza) in tutti i paesi delle UE.

Definizioni

Si riportano alcune definizioni rilevanti contenute nell'art. 4 del GDPR:

*"**Dato personale**": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*

*"**Trattamento**": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;*

Informativa e consenso (esplicito) al trattamento dei dati

L'informativa sulla tutela della riservatezza dei dati personali e il consenso al loro trattamento sono due adempimenti fondamentali che qualunque soggetto deve attuare nel caso in cui tratti dati personali - soprattutto se sensibili - di terze persone (ad es. clienti, fornitori, dipendenti, collaboratori, ecc.)

All'art. 12 vengono disciplinate le modalità con cui deve essere effettuata l'informativa che deve essere "***concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro***" mentre le informazioni devono essere fornite "***per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici***".

L'art. 13 ("*Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato*") prevede un elenco **tassativo** di informazioni da fornire all'interessato, con una disciplina più rigorosa rispetto a quella prevista dall'art. 13 del D.Lgs. 196/2003. Si afferma che nel momento in cui i dati sono ottenuti, il titolare del trattamento deve fornire all'interessato le seguenti informazioni, elencate al paragrafo 1:

*"a) **l'identità e i dati di contatto del titolare del trattamento** e, ove applicabile, del suo rappresentante;*

*b)**i dati di contatto del responsabile della protezione dei dati,** ove applicabile;*

*c)**le finalità del trattamento** cui sono destinati i dati personali nonché la base giuridica del trattamento;*

*d)qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), **i legittimi interessi** perseguiti dal titolare del trattamento o da terzi;*

*e)**gli eventuali destinatari** o le eventuali categorie di destinatari dei dati personali;*

*f) ove applicabile, **l'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…. il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.*

Il paragrafo 2 prevede ulteriori informazioni che il titolare del trattamento deve fornire al più tardi nel momento in cui i dati sono ottenuti:

*a) il **periodo di conservazione dei dati personali** oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;*

*e) **se la comunicazione di dati personali è un obbligo legale o contrattuale** oppure un **requisito necessario per la conclusione di un contratto**, e se l'interessato ha l'obbligo di fornire i dati personali nonché le **possibili conseguenze della mancata comunicazione di tali dati***

*f) **l'esistenza di un processo decisionale automatizzato**, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.*

In più dovranno essere indicati i **diritti dell'interessato** (si veda paragrafo successivo).

Se si confrontano l'attuale Codice della privacy italiano e il GDPR si può agevolmente notare come quest'ultimo preveda un'informativa molto più specifica, volta a garantire un trattamento al massimo della correttezza e della trasparenza.

L'art. 4,, paragrafo 1, n. 11) definisce il **consenso**:

qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Il consenso deve essere **esplicito**, anche se non necessariamente fornito per iscritto – pur essendo opportuno, anche ai fini probatori – e deve essere richiesto in forma **comprensibile** con un **linguaggio semplice e chiaro**.

In seguito a tali modifiche il **Garante per la protezione dei dati personali**, nella "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali", raccomanda i titolari di trattamento di verificare **la rispondenza** tra le **informative** attualmente utilizzate da ognuno e le **novità** introdotte dal Regolamento UE sull'informativa e il consenso, in modo da aggiornare e apportare le integrazioni eventualmente necessarie entro il 25 maggio 2018.

Diritti degli interessati al trattamento

La disciplina relativa ai diritti degli interessati ha subito un cambiamento non marginale rispetto all'attuale Codice della Privacy che all'art. 7 elencava, in modo generico, i diritti dell'interessato.

Il GDPR prevede sia un **disciplina più generica** all'art. 13 comma 2 – dalla lettera b) alla lettera d) – dove si ha un mero elenco dei diritti degli interessati, sia una **disciplina più dettagliata** prevista dagli artt. 15-22, dove ad ogni articolo corrisponde l'approfondimento di un singolo diritto tra quelli elencati all'art. 13.

Il cambiamento opera sia come approfondimento della disciplina già esistente che come aggiunta di nuovi diritti esercitabili dall'interessato. Occorre ricordare che **nell'informativa fornita all'interessato devono esser anche elencati tutti i diritti che quest'ultimo può esercitare**.

In particolare, l'interessato può far valere il:

- **diritto di accesso (art.15)** che consiste nel "*diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano*" e di ottenere l'accesso ai dati personali e alle informazioni elencate all'art. 13;

- **diritto di rettifica (art. 16)** che consiste nel "*diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo*";

- **diritto all'oblio o alla cancellazione (art. 17)** con il quale si intende sia il "*diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo*" (con la previsione di alcune ipotesi in cui sorge in capo al titolare del trattamento l'**obbligo** di cancellare i dati personali dell'interessato), sia il **diritto all'oblio informatico – novità** del GDPR **–** dove si prevede che "i*l titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali";*

- **diritto di limitazione di trattamento (art. 18)** che consiste nel "*diritto di ottenere dal titolare del trattamento la limitazione del trattamento*";

- **obbligo di notifica (art. 19)** per il quale si prevede che "*il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate*";

- **diritto alla portabilità dei dati (art. 20)** che è il diritto dell'interessato "*di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano"* in modo tale da poterli trasmettere agevolmente all'occorrenza ad un altro fornitore di servizi o a un altro titolare del trattamento;

- **diritto di opposizione (art. 21)** è il "*diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano*";

- **processo decisionale automatizzato (art. 22)** per il quale "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato*".

Soggetti

Restano le figure del **titolare del trattamento** e del **responsabile del trattamento**, di cui si da la definizione rispettivamente ai nn. 7) e 8) dell'art. 4:

*7) **"titolare del trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;*

*8) "**responsabile del trattamento**": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;*

L'art. 28 delinea la figura del **responsabile del trattamento** e il contenuto del **contratto** o altro atto giuridico di nomina che deve essere tassativamente stipulato tra titolare e responsabile:

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico …. che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32 [NDR: misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio]*;*

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. … omissis ...

Sparisce, almeno testualmente, l'incaricato al trattamento di cui non si fa più menzione nel GDPR, ma allo stesso tempo si ha una definizione di "*terzo*" al n. 10) dell'art. 4, nella quale si includono le "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile"*, descrizione che sembrerebbe nella sostanza assimilabile a quella del "vecchio" incaricato al trattamento, come affermato dal Garante della privacy.

Una novità rilevante è la regolamentazione della **contitolarità del trattamento** (art. 26) che si ha quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento. Essi individuano in modo trasparente, con un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14, salva che sia diversamente disposto. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

DPO: Data Protection Officer

L'innovazione più rilevante apportata dal GDPR è la previsione (artt. 37-39) di una nuova figura che in alcune ipotesi sarà obbligatoriamente da inserire nel contesto aziendale: il **Data Protection Officer** (**DPO)** ossia il **responsabile della protezione dei dati**. Si

tratta di un professionista esperto in materia di normativa e prassi sulla gestione dei dati personali, che può essere dipendente del titolare o del responsabile del trattamento o un collaboratore esterno con il quale si stipula un contratto d'opera o di servizi. Il DPO riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

L'obbligo di nomina (art. 37) sussiste quando il trattamento è effettuato da un'autorità pubblica o un organismo pubblico (tranne che per le autorità giurisdizionali); inoltre l'obbligo sussiste anche per qualunque soggetto che tratti su larga scala dati sensibili (relativi cioè alla salute, vita sessuale, genetici, giudiziari , biometrici) e nel caso in cui il trattamento richieda il controllo regolare e sistematico e su larga scala degli interessati.

Il titolare o il responsabile del trattamento pubblica i **dati di contatto** del responsabile della protezione dei dati e li comunica all'autorità di controllo. Gli interessati potranno contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

I compiti del DPO sono definiti dall'art. 39:

*a) i**nformare e fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento i**n merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni** dell'Unione o degli Stati membri relative alla protezione dei dati;*

*b) **sorvegliare l'osservanza del presente regolamento, di altre disposizioni** dell'Unione o degli Stati membri **relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento** in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;*

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

*d) **cooperare con l'autorità di controllo**; e*

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Affinché il DPO possa svolgere questi compiti, il titolare e il responsabile del trattamento:

a) si assicurano che egli sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;

b) sia adeguatamente sostenuto anche con la messa a disposizione delle risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;

c) mantenga la sua autonomia e terzietà, assicurandosi che non riceva alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati, né subisca penalizzazioni o ritorsioni di sorta a causa dell'adempimento dei propri compiti.

Il DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti; può svolgere altri compiti e funzioni purché non diano adito ad un conflitto di interessi.

Registro dell'attività di trattamento

L'obbligo della tenuta del cd. r**egistro delle attività di trattamento,** previsto all'art. 30, è un'altra delle **novità** introdotte dal GDPR. L'obbligo sorge in capo a due soggetti, ossia il titolare del trattamento e il responsabile del trattamento. Secondo alcuni il registro sarebbe "l'erede" dell'abrogato Documento Programmatico sulla Sicurezza – DPS – poiché sostanzialmente sono entrambi volti all'ottenimento dello stesso obiettivo, cioè quello di essere un documento che definisca nel dettaglio le caratteristiche principali dei trattamenti svolti e le misure di sicurezza applicate per la tutela dei dati trattati.

L'art. 30 elenca una serie di **informazioni** che il **registro, redatto in forma scritta** (anche in formato elettronico) **deve tassativamente contenere**. Al paragrafo 1 si fa riferimento al registro del titolare del trattamento, che deve precisare:

*- il **nome** e i **dati di contatto** del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;*

*- le **finalità del trattamento**;*

*- una descrizione delle **categorie di interessati** e delle **categorie di dati personali**;*

*- le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;*

*- ove applicabile, i **trasferimenti di dati personali verso un paese terzo** o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;*

*- ove possibile, i **termini** ultimi previsti per la **cancellazione delle diverse categorie di dati**;*

*- ove possibile, una **descrizione generale delle misure di sicurezza tecniche e organizzative** di cui all'articolo 32, paragrafo 1.*

Per quanto riguarda il responsabile del trattamento fondamentalmente gli elementi del registro, elencati al paragrafo 2, sono gli stessi di quello del titolare, con alcune differenze:

- i nomi e i dati di contatto da indicare sono gli stessi tranne che quelli del/dei **responsabile/i del trattamento**, e quelli di ogni **titolare del trattamento per conto del quale agisce il responsabile del trattamento;**

- devono essere indicate le **categorie dei trattamenti effettuati per conto di ogni titolare del trattamento**.

Ai sensi de paragrafo 5 dell'art. 30: la **tenuta del registro è obbligatoria** soltanto per le **imprese o organizzazioni con almeno 250 dipendenti**, salvo che il trattamento:

- presenti un rischio per i diritti e le libertà dell'interessato;

- il trattamento sia occasionale;

- includa l'elaborazione di categorie particolari di dati o dati relativi a condanne penali o specifici reati indicati nell'articolo.

Misure di sicurezza

Sia per il registro del titolare che per quello del responsabile si fa richiamo alle **misure di sicurezza tecniche e organizzative**, la cui disciplina è mutata rispetto a quanto previsto nel D.Lgs. 196/2003, in particolare per quanto riguarda la loro modalità di adozione. Infatti, mentre all'articolo 33 del Codice della Privacy si parla di adozione di misure di sicurezza **minime,** l'articolo 32 del Regolamento UE invece prevede un differente sistema di adozione rispetto a quello fino ad ora adottato, facendo sorgere in capo al titolare e al responsabile del trattamento l'incombenza di mettere in atto non più misure minime, ma

***misure** tecniche e organizzative **adeguate** per garantire un livello di sicurezza adeguato al rischio*

indicandone alcuni esempi, come:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Non esiste più quindi, come in precedenza, un elenco determinato di misure da adottare, ma sarà ogni volta impiegata la misura più adatta al caso concreto, ossia quella (o quelle, poiché è ragionevole pensare che si debbano adottare più misure che combinate insieme garantiscano un adeguato livello di protezione dei dati) che si sarà individuata più adatta al caso di specie dopo aver effettuato la **valutazione del rischio**.

Per la valutazione del rischio bisogna tener conto

dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Il titolare del trattamento e il responsabile del trattamento dovranno assicurarsi che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non sia stato preventivamente istruito in tal senso dal titolare del trattamento

Principi

Il Regolamento UE ha introdotto tre nuovi principi in tema di privacy, quali:

- il **principio dell'accountability (art. 24)** ossia di **responsabilizzazione**, per il quale si incarica il titolare del trattamento di porre in essere **autonomamente** misure giuridiche, tecniche e organizzative adeguate per la protezione dei dati personali che vengono trattati, tenendo quindi conto del contesto e delle specifiche circostanze in cui il trattamento si realizza.

- il principio di **privacy by design (art. 25, par. 1)** ossia **protezione dei dati fin dalla progettazione**, attraverso la riduzione al minimo del trattamento dei dati personali mediante misure tecniche e organizzative quali per esempio la pseudonimizzazione dei dati;

- il principio di **privacy by default (art. 25, par. 2)** in forza del quale la tutela della protezione del dato deve divenire l'**impostazione predefinita:** *" il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento".*

Data Breach

Quando si parla di **data breach** si intende la **violazione dei dati personali** e quindi degli standard di sicurezza che sono stati adottati; in tale situazione il titolare del trattamento, come disciplinato all'art. 33, deve notificare la violazione all'autorità di controllo competente senza indugio e se possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che appaia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Nel caso in cui si sia superato il termine delle 72 ore se ne dovrà spiegare il motivo; la notifica deve contenere la descrizione di quanto accaduto, le probabili conseguenze derivanti dalla violazione e la descrizione delle misure attuate per porvi rimedio.

Sanzioni

Come ultimo occorre fare un cenno alle sanzioni previste dal nuovo Regolamento UE.

Generalmente, il responsabile del risarcimento dei danni derivanti da un trattamento che violi il regolamento è il titolare del trattamento; il responsabile del trattamento risarcisce il danno soltanto nel caso in cui non abbia adempiuto agli obblighi che sorgevano a suo carico.

Ogni paese membro può inoltre stabilire e adottare norme nazionali per sanzionare penalmente eventuali violazioni del regolamento UE. Per quanto riguarda l'entità delle sanzioni amministrative applicabili, si può arrivare al massimo di 20 milioni di euro, oppure al 4% del fatturato annuo globale, nel caso di violazioni del GDPR, come stabilito dall'articolo 83