Protezione dei Dati, Privacy e Sicurezza Informatica

MILANO, 17 OTTOBRE 2018

AVV. ELENA GIUFFRÈ

Pacchetto protezione dati:

- Regolamento UE 2016/679 del 27/04/2016 (**GDPR**): relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (direttamente applicabile a decorrere dal 25 maggio 2018)

- Direttiva UE 2016 del 27/04/2016: relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione id tali dati (gli Stati devono recepirla antro 2 anni). Implementato dal D.Lgs. 18 maggio 2018, n. 51 (entrato in vigore lo scorso 8 giugno)

APPLICAZIONE DEL GDPR

- Il Entrata in vigore : **25 maggio 2016**:
- Direttamente applicabile in tutti gli stati Membri dell'UE
- Abroga la direttiva **95/46/CE**
- Il Codice della Privacy (D.Lgs. 196/2003, come modificato dal D.Lgs. N. 101 del 30 giugno 2018), che integra, e non sostituisce, il GDPR.

Rimangono in vigore:

- Linee guida del 23/12/2016 (emendate il 5/05/2017) emanate dal **Gruppo di Lavoro ex articolo 29** (il «Gruppo di Lavoro per la tutela delle persone con riguardo ai dati personali», istituito a norma dell'art. 29 della direttiva 95/46. E' un organo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designato da ciascuno Stato membro, dal Garante europeo per la protezione dei dati (GEPD), nonché dal rappresentante delle Commissione Europea. Sarà sostituito dal nuovo «Comitato europeo per la protezione dei dati», ai sensi dell'art. 68 del GDPR.)

FINALITA'

- Garantire una **disciplina sulla protezione dei dati personali uniforme ed omogenea** in tutta la UE, al fine di assicurare un livello coerente ed elevato di protezione
- Garantire la trasparenza agli operatori economici.
- Definire obblighi dei Titolari/Responsabili trattamento dei dati.
- Stabilire **sanzioni uguali in tutti i Paesi Ue.**
- Favorire **cooperazione tra autorità di controllo.**

QUANDO SI APPLICA

Il **Regolamento** si applica:

- al trattamento «interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali che siano contenuti in un archivio»
- **solo** al trattamento dei dati personali delle **persone fisiche.** Sono esclusi i dati relativi alle persone giuridiche

Non si applica ai trattamenti:

- a carattere esclusivamente **personale** o **domestico**
- effettuati dalle **autorità competenti** ai fini della prevenzione, indagine, esecuzione penale
- effettuati da **autorità di pubblica sicurezza**

TRATTAMENTO – PROFILAZIONE

- **"trattamento":** qualsiasi operazione o insieme di operazioni, compiute con o senza ausilio di processi automatizzati e applicate a dati personali o insieme 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.

- **"profilazione"**: forma di trattamento automatizzato attraverso cui è possibile valutare gli aspetti personali relativi ad una persona fisica ,in particolare per analizzare aspetti personali relativi alla persona (rendimento professionale, situazione economica, salute, preferenze personali, interessi)

AMBITO DI APPLICAZIONE TERRITORIALE

Dal punto di vista territoriale il Regolamento si applica:

- al trattamento di dati personali effettuato da un Titolare o Responsabile **stabilito nella UE**, indipendentemente dal fatto che il trattamento sia effettuato o meno nella UE (per esempio server fuori dall'Unione);
- al trattamento di dati personali effettuato da Titolari o Responsabili **non stabiliti nell'**UE, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione, se il trattamento ha ad oggetto dati personali di **interessati che si trovano nella UE** e riguarda (i) l'offerta di beni o servizi (anche non a pagamento) ai suddetti interessati
- al trattamento effettuato da un Titolare stabilito **in uno Stato extra UE** soggetto al diritto di uno Stato UE in virtù del diritto internazionale pubblico.

(Vd. Sentenze Google Spain del 14/05/2014 causa C-131/12 e Weltimmo del 1^/10/2015 causa C-230/14 e parere n. 8/2010 del Gruppo di Lavoro ex art. 29 del 16/12/2010)

DEFINIZIONE DI DATO PERSONALE

- Recependo il parere 4/2017 del Gruppo di lavoro ex art. 29, si amplia il concetto di "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. Rimangono al di fuori del campo di applicazione della normativa sulla protezione dei dati personali il trattamento dei dati **"non personali"** come ad esempio i **dati anonimi** o il trattamento di dati effettuato da persone fisiche **per fini esclusivamente personali**.» (art. 4)

DEFINIZIONE DI DATO PERSONALE

… ancora

- «le persone fisiche possono essere associate ad identificativi on line …quali indirizzi IP, marcatori temporali (cookies) o identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare, se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzati per creare profili delle persone e identificarle (Considerando 30)

  (sentenza della Corte di Giustizia Ptarik Breyer del 19/10/2016 causa C-582/14, che ha identificato gli indirizzi IP come dati personali).

CATEGORIE PARTICOLARI DI DATI

- Eliminata la definizione di dati **sensibili** e di dati **giudiziar**i.

Ora si parla di "**Categorie particolari di dati personali**": dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i **dati genetici, i dati biometrici** intesi a identificare in modo univoco una persona fisica, i **dati relativi alla salute** o alla vita sessuale o all'orientamento sessuale della persona (art. 9)

(dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.)

DATI BIOMETRICI, GENETICI, RELATIVI ALLA SALUTE

Dati biometrici:

- Le fotografie che permettono l'identificazione univoca o l'autenticazione dell'interessato
- informazioni matematiche elaborate a partire dal volto di una persona, impronte digitali(es. impronta digitale per accesso al computer) dalle caratteristiche dell'iride, da elementi misurabili dal modo di camminare o di gesticolare.

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Con **Autorizzazione n. 8/2016 del Garante** tali dati possono essere utilizzati ad esempio per scopi di ricerca scientifica o statistica finalizzati alla tutela dell'interessato, di terzi della collettività in campo medico, biomedico ed epidemologico

Dati relativi alla salute:

- dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative allo stato di salute. Sono considerati dati sanitari anche i **dati genetici**, e le fotografie scattate a fini di interventi chirurgici

PRINCIPI DI LICEITÀ DEL TRATTAMENTO

Come il Codice Privacy, anche il regolamento generale europeo (GDPR) stabilisce che un trattamento di dati personali deve trovare fondamento in una **idonea base giuridica**.

I **fondamenti di liceità del trattamento** sono indicati dall'**art. 6 del Regolamento** e coincidono in linea di massima con quelli previsti dall'art. 2 ter e ss. del Codice Privacy:

- **consenso**, oppure
- adempimento obblighi contrattuali,
- interessi vitali della persona interessata o di terzi,
- obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri (esplicitato dall'art. 2 sexies del Codice Privacy e dalla parte II - artt. 50 e ss.);
- interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati (accesso ai documenti amministrativi e accesso civico vd. 2 sexies del Codice Privacy).

N.B. il consenso del minore di anni 14 (16 anni previsto dal GDPR) è espresso dagli esercenti la potestà genitoriale.

PRINCIPI DI LICEITÀ DEL TRATTAMENTO (CATEGORIE PARTICOLARI DI DATI)

E' vietato trattare le **categorie particolari di dati** (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), **salvo i seguenti casi**:

- **Consenso esplicito** per una o più finalità (il consenso di regola può essere anche implicito purchè inequivocabile). Non ha valore il silenzio o l'inattività;
- adempimento obblighi in materia di diritto del lavoro o della sicurezza sociale e protezione sociale;
- interessi vitali della persona interessata o di terzi;
- finalità di accertamento diritto in sede giudiziaria;

PRINCIPI DI LICEITÀ DEL TRATTAMENTO (CATEGORIE PARTICOLARI DI DATI)

- finalità di medicina preventiva e medicina del lavoro;
- motivi interesse pubblico nel settore della sanità pubblica, quali protezione da gravi minacce per la salute a carattere transfrontaliero;
- trattamento da parte di fondazioni, associazioni o altro organismo **no-profit** che perseguano finalità politiche, filosofiche, religiose o sindacali, nell'ambito delle loro legittime attività e con adeguate garanzie, a condizione che:

i. il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che
ii. i dati personali non siano comunicati all'esterno senza il consenso dell'interessato.

Per dati biometrici, genetici e relativi alla salute devono essere adottate misure di garanzia predisposte dal Garante (art. 2 septies Codice Privacy)

Trattamento di dati particolari

IL TRATTAMENTO – CONSENSO ESPLICITO

- Per tali dati personali vige il **divieto generale di trattamento**, **a meno che questo non sia consentito nei casi specifici** previsti dal GDPR, tra cui il **consenso esplicito** dell'interessato o in relazione a **esigenze specifiche**, in particolare se il trattamento è eseguito nel corso di **legittime attività** di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali.
- **Il consenso esplicito è una delle eccezioni al divieto generale**:
  - L'interessato deve essere il grado di comprendere i gravi rischi derivanti dal trattamento dei dati particolari;
  - Può consistere **anche in una dichiarazione orale registrata** oppure un processo integrato a più fasi in cui in un primo momento l'interessato potrà rispondere ad una e-mail dell'operatore autorizzando il trattamento dei propri dati personali e poi successivamente dovrà cliccare su di un link in una seconda e mail o sms inviato dal titolare per confermare nuovamente il consenso.
  - Se il consenso è stato ottenuto mediante strumenti elettronici, il titolare dovrebbe conservare tutte le informazioni pertinenti la specifica sessione in cui è stato acquisito il consenso.

Trattamento di dati particolari

IL TRATTAMENTO – LEGITTIME ATTIVITÀ DI ASSOCIAZIONI NON PROFIT

- **Il GDPR prevede che il consenso non sia necessario:**
- Quando il trattamento è svolto, con adeguate garanzie, da associazioni, enti o organismi senza scopo di lucro a carattere politico, filosofico religioso o sindacale per il perseguimento dei legittimi scopi statutari, e riguarda dati sensibili **di aderenti e soggetti che hanno contatti stabili con l'associazione**, **sempre che i dati non siano comunicati all'esterno o diffusi** (in tal caso è necessario il consenso dell'interessato).
  - Se quindi l'associazione o ente non profit raccoglie e tratta i dati personali comuni e sensibili dei propri soci per gli scopi statutari e non li comunica a terzi e non li diffonde, non ha l'obbligo di acquisire il loro consenso.
  - Si può ritenere che l'adesione all'associazione implichi un implicito consenso del socio a tutti quei trattamenti "fisiologici" dei dati degli associati che si svolgono in ambito associativo e che di prassi l'associazione svolge
    - es. conoscibilità di indirizzo e numero di telefono di un socio da parte degli altri soci, esposizione di foto dei soci nei locali dell'associazione o pubblicazione nel giornalino se inviato ai soli soci, ecc..

TRATTAMENTO RELATIVO A CONDANNE PENALI E REATI

- Il trattamento relativo a condanne penali e reati, da parte di soggetti diversi dalle autorità pubbliche (D.lgd. 51/2018), è consentito solo se autorizzato da norme di legge.

In ogni caso è consentito (art. 2 octies Codice Privacy e 10 GDPR):

- In materia di diritto del lavoro,
- Accertamento requisiti onorabilità;
- Sinistri /assicurazioni;
- Esercizio diritto di difesa;
- Accesso ai documenti amministrativi;
- Informative antimafia;
- Partecipazione a gare;
- Adempimenti antiriciclaggio;
- Ecc.

Consenso dell'interessato

- Il consenso dell'interessato rappresenta la **principale precondizione di liceità** del trattamento.
- *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* (Art. 4 GDPR).
- Il consenso deve essere quindi:
  - **Informato**;
  - **Specifico**, riferito cioè ad una o più finalità del trattamento;
  - **Libero**, prestato cioè senza condizionamenti e senza dover subire pregiudizi (l'esecuzione di un contratto, compresa la prestazione di un servizio, non deve essere subordinata ad un consenso non necessario per tale esecuzione);
  - **Inequivocabile:** deve prevedere una **chiara azione positiva**, che non lasci alcun dubbio che col proprio comportamento l'interessato abbia voluto comunicare il proprio consenso (e.g. spuntare una casella o inserire la mail in un campo dove è specificata la finalità di utilizzo), che **non deve essere per forza esplicito**, ma **non può essere tacito** (l'inerzia non può costituire manifestazione di consenso, come anche i form precompilati e caselle già prespuntate).
- La **richiesta di consenso** deve essere **presentata in modo chiaramente distinguibile** dalle altre materie in forma comprensibile in un linguaggio semplice e chiaro**.**
- Il titolare DEVE essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.
  - b

Consenso dell'interessato

- **Da ricordare:**
  - Correlazione consenso-finalità dichiarate dal titolare;
  - Deve essere prestato in maniera specifica e intellegibile per ciascuna delle finalità indicate dal titolare;
  - Il titolare deve informare l'interessato della **sua facoltà di revocare il consenso in qualsiasi momento** con la stessa facilità con cui lo ha accordato e dimostrare che il consenso al trattamento dei dati personali sia stato prestato;
  - Il consenso acquisito precedentemente al 25 maggio 2018 "*resta valido*" se ha tutti i requisiti sopra indicati:
    - Deve essere nuovamente richiesto **se è stato prestato in modo tacito**, come nel caso di caselle preselezionate, o se i titolati non sono in grado di dimostrare che un valido consenso è stato ottenuto e di aver informato gli interessati sulle modalità di revoca dello stesso.
    - Non deve essere rinnovato, ad esempio, se sono disponibili meccanismi che consentano agli interessati di revocarlo facilmente e se è stato chiaramente espresso dall'interessato.

Informativa

- I principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue **finalità**… e di eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e i contesti specifici in cui i dati personali sono trattati (GDPR - considerando 62).
- **Principio di finalità**
  - Significa che **la raccolta dei dati e il loro successivo utilizzo devono avere precise e determinate finalità**, che vanno comunicate all'interessato e poi rispettate.
  - Per le **associazioni non profit** le finalità del trattamento dei dati generalmente coincidono o sono compresi negli scopi istituzionali indicati nello statuto.
    - Quindi, non si potrà, senza l'informazione specifica e/o l'autorizzazione ai soci/beneficiari usare tali dati per scopi diversi da quelli istituzionali: ad esempio non si potrà comunicare il nome e l'indirizzo o altre informazioni a terzi per pubblicità, iniziative commerciali o per propaganda elettorale o comunque per scopi che non riguardano l'ente.

Informativa

- L’informativa costituisce il principale obbligo in capo a chi svolge un trattamento di dati personali.
  - Serve per far conoscere all’interessato come il titolare gestisce e utilizza i dati che lo riguardano.
  - È presupposto essenziale per dare il consenso al trattamento, quando questo è richiesto dalla legge.
  - È disciplinata dall’articolo 13 GDPR
- Deve essere fornita all’ interessato
  - **prima di effettuare la raccolta dei dati**;
  - in **forma concisa, trasparente, intelligibile e facilmente accessibile**;
  - **con linguaggio semplice e chiaro**;
  - **per iscritto o con altri mezzi, anche elettronici**, o anche **oralmente**, purché sia richiesto dall’interessato e sia comprovata con altri mezzi l'identità dell'interessato;
  - anche in combinazione con **icone standardizzate** per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un **quadro d'insieme del trattamento previsto**. Se presentate elettronicamente, le icone devono essere leggibili da qualsiasi dispositivo.

Informativa

CONTENUTO DELL'INFORMATIVA

- Contenuti dell'informativa (art. 13 GDPR):
  - Identità e contatti del titolare;
  - Identità e contatti del responsabile della protezione dati (DPO), se nominato;
  - Finalità del trattamento;
  - La base giuridica del trattamento;
  - Le categorie di dati oggetto del trattamento (solo ove i dati non siano raccolti presso l'interessato);
  - Categorie di persone a cui i dati verranno comunicati;
  - Qualora il trattamento si basi sulla necessità di perseguire un legittimo interesse del titolare del trattamento o di terzi, la specificazione di quali siano i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
  - L'ambito del trasferimento all'estero (ovviamente extra UE) o a un'organizzazione internazionale dei dati personali;

Informativa

CONTENUTO DELL'INFORMATIVA (CONTINUA)

- Il **periodo di conservazione dei dati** personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- la **specifica esistenza del diritto alla portabilità dei dati**;
- l'esistenza del **diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca (ex nunc);
- la **eventuale esistenza di un processo decisionale automatizzato**, compresa la profilazione;
- il diritto di **proporre reclamo** al Garante per la protezione dei dati personali;
- nel caso di dati personali **non raccolti direttamente presso l'interessato** (art. 14 regolamento) l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese dalla raccolta** o nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato o con un terzo, al **più tardi al momento di tale comunicazione** e deve indicare:
  - Il diritto di **proporre reclamo** ad un'autorità di controllo;
  - La fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

Informativa

- **Per i trattamenti iniziati prima del 25 maggio è necessario informare nuovamente gli interessati fornendo tutte le informazioni di cui agli artt. 13 e 14 del GDPR**, ivi inclusi la base giuridica e il periodo di conservazione dei dati, non richiesti dal previgente art. 13 del Codice Privacy.
- **Non richiesta se**:
  - L'interessato dispone già delle informazioni;
  - Comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato;
  - Qualora il professionista effettui il trattamento dei dati personali sulla base di un contratto con un cliente;
  - I dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale.

I DIRITTI DELL'INTERESSATO

- Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura tecnica organizzativa a ciò idonea.
  - Le modalità per stabilire l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli **artt. 11 e 12 GDPR**.
  - **L'esercizio dei diritti è**, in linea di principio, **gratuito**, ma il titolare potrà stabilire un eventuale contributo per l'interessato se le richieste sono manifestamente infondate o eccessive (il titolare ha l'onere di dimostrarne il carattere manifestamente infondato).
  - I diritti sono esercitabili in qualsiasi momento. La **richiesta** potrà essere inoltrata mediante **strumenti elettronici.**
  - **Il termine per la risposta all'interessato è,** anche in caso di diniego, **per tutti i diritti (compreso il diritto di accesso), 1 mese**, estendibili fino a 3 mesi in casi di particolare complessità.
  - La risposta fornita all'interessato deve essere "intelligibile", concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.
  - Se il titolare non fornisce riscontro o risponde in maniera parziale o inadeguata, l'interessato può rivolgersi all'autorità giudiziaria oppure presentare un ricorso al Garante.

IL DIRITTO DI RETTIFICA ED INTEGRAZIONE

- L'interessato ha il diritto di ottenere dal titolare del trattamento la **rettifica dei dati personali inesatti** che lo riguardano.
- L'interessato ha il diritto di ottenere, elemento di novità del GDPR, **l'integrazione dei dati personali incompleti**, anche fornendo una dichiarazione integrativa con cui si cerca di preservare la qualità del dato personale e quindi l'identità personale senza modificare dati di tipo valutativo o relativi a giudizio apprezzamenti di tipo soggettivo. Ad esempio:
  - Selezione del personale: alla scadenza dei termini per la presentazione della domanda è riconosciuto il diritto di rettifica limitato ai dati relativi ai criteri di ammissibilità.
  - Procedure di valutazione: non possono essere rettificate le considerazioni soggettive del superiore contenute in un report.
  - In ambito sanitario: diritto di integrare i dati sanitari esistenti con un secondo parere medico.
  - Procedimenti amministrativi e disciplinari: facoltà di aggiungere commenti all'interno del fascicolo personale.
- Rettifiche e integrazioni devono essere rese note a ciascuno dei soggetti a cui i dati sono stati comunicato (salvo ciò **comporti uno sforzo sproporzionato)**

IL DIRITTO ALL'OBLIO

- Diritto dell'interessato ad ottenere, senza giustificato ritardo, la **cancellazione dei propri dati personali che non siano più necessari** per le finalità per le quali sono stati raccolti o altrimenti trattati, o quando l'interessato **abbia revocato il proprio consenso**, o si sia **opposto al trattamento** dei dati personali che lo riguardano, o quando il **trattamento dei suoi dati personali non sia altrimenti conforme** al GDPR.
  - Il titolare che ha pubblicato on line dati personali deve informare gli altri titolari del trattamento che trattano tali dati personali di **cancellare qualsiasi link verso tali dati personali** o copia o riproduzione di detti dati.
  - **Possibilità di opporsi** solo in casi di: esercizio del diritto alla libertà di espressione e di informazione; adempimento di un obbligo legale o un compito di interesse pubblico; motivi di interesse pubblico nel settore della sanità pubblica; a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; per accertare, esercitare o difendere un diritto in sede giudiziaria.
- **Diritto all'oblio su internet** inteso come:
  - Diritto alla cancellazione dell'indicizzazione dei dati;
  - Diritto a rientrare nell'anonimato tutelando l'interesse a non subire alterazioni del proprio patrimonio morale e sociale acquisito in ragione della dimenticata vicenda che lo ha riguardato.

OBBLIGO NOTIFICA IN CASO DI RETTIFICA O CANCELLAZIONE DEI DATI PERSONALI O LIMITAZIONE DEL TRATTAMENTO

- 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, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.
  - Il Considerando 31 precisa che "Le **autorità pubbliche** a cui i dati personali sono comunicati conformemente a un obbligo legale ai fini dell'esercizio della loro missione istituzionale, quali autorità fiscali e doganali, unità di indagine finanziaria, autorità amministrative indipendenti o autorità dei mercati finanziari, responsabili della regolamentazione e della vigilanza dei mercati dei valori mobiliari, **non dovrebbero essere considerate destinatari qualora ricevano dati personali che sono necessari per svolgere una specifica indagine nell'interesse generale**, conformemente al diritto dell'Unione o degli Stati membri."

Diritto alla portabilità

- Diritto dell'interessato di **trasmettere o ottenere la trasmissione di propri dati personali** da un titolare a cui li aveva forniti in precedenza ad un altro titolare, senza impedimenti.
  - Tale diritto è esercitabile quando: il trattamento è effettuato con mezzi automatizzati; e il trattamento si basa sul consenso precedentemente rilasciato dall'interessato; o il trattamento si basa su un contratto o su trattative precontrattuali in corso con l'interessato.
  - L'interessato ha il diritto di **ottenere in formato strutturato**, di uso comune e leggibile da dispositivo automatico, i propri dati personali al fine di trasmetterli a un altro Titolare, ma anche il diritto di ottenere che il primo Titolare a cui ha fornito i dati, li **trasmetta direttamente** a un diverso Titolare, se tecnicamente fattibile.

Diritto di opposizione

- L'interessato può opporsi, in qualsiasi momento, al trattamento **per motivi connessi alla sua situazione particolare senza indicarne le ragioni**.
- Il titolare, per impedire l'interruzione del trattamento, deve provare la prevalenza delle finalità del trattamento sulle esigenze dell'interessato.

DATA BREACH

- La sicurezza rappresenta uno dei principi fondamentali del GDPR in base al nuovo Articolo 5, secondo cui i dati devono essere trattati in maniera da garantire un'**adeguata sicurezza** dei dati personali, **compresa la protezione**, mediante misure tecniche e organizzative adeguate, **da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali** ("integrità e riservatezza").
  - Le misure di sicurezza devono garantire un livello di sicurezza adeguato al rischio del trattamento.
  - Dal 25 maggio 2018 non sono più previsti obblighi di adozione di misure "minime" di sicurezza poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del GDPR. Conformemente, l'articolo 33 del Codice della Privacy è stato abrogato.
  - L'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni. Si tiene conto di:
    - Costi attuazione.
    - Contesto e finalità del trattamento.
    - Rischio e probabilità per diritti e le libertà dei soggetti persone fisiche.

DATA BREACH

- I data breach sono **violazioni** relative alla sicurezza **che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi**.
- **Obbligo** per il titolare del trattamento **di notifica al Garante entro 72 ore** e comunque senza ingiustificato ritardo di un'avvenuta violazione dei dati personali.
- Nei casi di violazioni particolarmente gravi, tale obbligo sussiste anche nei confronti degli interessati, sempre "senza ingiustificato ritardo".
- L'obbligo riguarda tutti i titolari del trattamento indipendentemente dal fatto di essere fornitori di servizi di comunicazione elettronica.

La notifica deve contenere:

- Natura della violazione dei dati personali, comprese le categorie dei dati ed il numero degli interessati questione;
- Nome e dati di contatto del responsabile;
- Descrizione delle probabili conseguenze della violazione;
- Misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche per attenuarne eventuali effetti negativi;
- Se la notifica non viene effettuata entro 72 ore, la notifica è corredata da una giustificazione motivata.

Le **figure soggettive**:

- L'interessato
- Titolare del trattamento
- Responsabile del trattamento
- Il sub- responsabile del trattamento
- Rappresentante designato dal titolare
- La nuova figura del responsabile della protezione dati (DPO)

IL TITOLARE DEL TRATTAMENTO

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.**

Obblighi del titolare:

- **Fornire** agli interessati l'informativa di cui all'**art. 13 del Regolamento**
- **Acquisire** il consenso degli interessati che dovrà essere prestato per trattamenti determinati e distinti, in modo chiaro e libero e comunque essere sempre revocabile
- Se necessario, nominare il *Data Protection Officer* (DPO)
- **Predisporre** un procedimento, fruibile ed effettivo, che consenta agli interessati di esercitare i diritti riconosciuti dalla legge
- **Effettuare** la valutazione di impatto privacy (c.d. PIA)
- **Redigere** un registro dei trattamenti
- **Nominare** i responsabili del trattamento
- **Adottare** le misure di sicurezza che, nel rispetto del principio di *accountability*, vengono lasciate alla valutazione del titolare
- **Predisporre** una procedura da utilizzare in caso di *data breach*

RESPONSABILE

E' responsabile, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

L'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli il responsabile al titolare.

Il **responsabile** è tenuto a :

- Istituire il registro delle categorie di attività di trattamento svolte per conto del titolare
- Designare il **DPO**
- Nominare un rappresentate qualora non sia stabilito in territorio europeo
- Notificare al titolare senza giustificato ritardo la violazione dei dati personali

- Responsabilità per non aver adempiuto agli obblighi del regolamento
- Esclusione responsabilità solidale con il titolare
- Il Responsabile del trattamento può a sua volta designare dei responsabili del trattamento previa autorizzazione scritta specifica o generale del titolare del trattamento.

OBBLIGHI ORGANIZZATIVI TITOLARE E RESPONSABILE DEL TRATTAMENTO

Il Regolamento introduce poi **obblighi organizzativi** nuovi con riferimento ai ruoli e alle funzioni sia del titolare che del responsabile del trattamento **che rivelano l'applicazione del *principio di accountability*** ad esempio :

- il Titolare deve attuare **misure tecniche ed organizzative adeguate** per garantire e dimostrare che il trattamento è effettuato conformemente al Regolamento. Le misure devono essere riesaminate periodicamente e aggiornate, ove necessario.
- **Adesione a Codici di condotta o a meccanismi di certificazione:** può essere utilizzata come elemento per dimostrare il rispetto degli obblighi imposti al Titolare del trattamento come ad esempio (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 notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato; il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali)

La **pseudonimizzazione**:

Particolare trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

SUB-RESPONSABILI DEL TRATTAMENTO

Può essere nominato da un responsabile sulla base di eventuali istruzioni impartite dal titolare del trattamento *(art. 28, paragrafo 4)*, per specifiche attività di trattamento. Il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

RAPPRESENTANTE

- figura di contatto e di garanzia che agisce per conto ed in luogo del soggetto rappresentato assolvendo agli obblighi posti dal regolamento in capo al titolare e al responsabile che rappresenta ogniqualvolta il trattamento presenti un elevato rischio per i diritti e le libertà degli interessati.
- Resta ferma la responsabilità in solido **ex art 1218 e 1710 cc** del titolare e responsabile del trattamento che in caso di inadempienza del rappresentante impongono a quest'ultimo coattivamente l'osservanza dei propri obblighi.

DATA PROTECTION OFFICER

"Responsabile della protezione dei dati" (Data Protection Officer) introdotto dall'**art. 37 del Regolamento**.

Si tratta di un supervisore indipendente che supporta il titolare e il responsabile nel garantire che l'organizzazione sia conforme al GDPR.

- non deve ricevere dal Titolare o dal Responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati **né è soggetto a potere disciplinare o sanzionatorio** per l'adempimento dei propri compiti.
- Non ingerenza nell'esercizio delle sue funzioni da parte del responsabile o incaricato
- Monocratico
- Indipendenza ed autonomia
- Ha risorse finanziarie necessarie per adempiere i propri compiti (autonomia finanziaria).
- E' una figura apicale

LA NUOVA FIGURA DI DPO

Tra i principali compiti:

- **Informare** e fornire consulenza al titolare o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione europea o degli Stati membri relativi alla protezione dei dati personali.
- **Sorvegliare** l'osservanza delle norme sulla protezione dei dati nonché delle politiche del titolare 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.
- **Fornire**, se richiesto, un parere sulla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35.
- **Cooperare** con il Garante e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento di dati personali.

DPO

E’ obbligatorio quando:

- il trattamento è effettuato da un’autorità pubblica (o organismo di diritto pubblico)
- 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
- le attività principali del titolare o del responsabile si esplicano nel trattamento **su larga scala** di categorie particolari di dati personali di cui all’art. 9 o 10 del Regolamento (dati che rivelino l’origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, biometrici, dati relativi alla salute o alla vita sessuale o orientamento sessuale, o dati relativi a condanne penali e a reati)

Le Linee Guida hanno fornito alcuni esempi di trattamento su «larga scala» :

- Ospedali;
- Servizio di trasporto pubblico
- Trattamenti di geolocalizzazione reali per finalità statistiche;
- Compagnie assicuratrici;
- Motori di ricerca;
- Fornitori di servizi telefonici

NON rientrano:

- Trattamento del singolo medico
- Trattamento di clienti da parte dell'avvocato per condanne penali

DPO

Tale soggetto riflette l'approccio responsabilizzante che è proprio del Regolamento.
Il ruolo può essere affidato a una figura: **interna** (rapporto di lavoro subordinato – "dipendente") o **esterna** (contratto di servizi).

- Il DPO va designato in funzione delle **elevate qualità professionali e conoscenza specialistica della normativa** e della prassi in materia di protezione dei dati.
- Un gruppo imprenditoriale può nominare un DPO.
- I dati di contatto del DPO devono essere comunicati al Garante della protezione personali per questioni concernenti il trattamento.

Seminario Data Protection_18 luglio 2018

ashurst