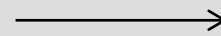




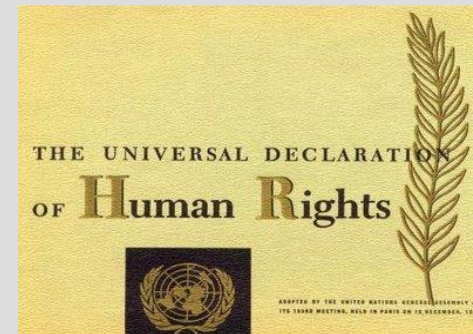
PACCHIANA PARRAVICINI E ASSOCIATI
STUDIO LEGALE

LA GENESI NORMATIVA SULLA PRIVACY

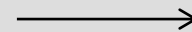
Il diritto alla privacy **nasce negli Stati Uniti alla fine del XIX secolo** (nel dicembre del 1890 due avvocati bostoniani pubblicano infatti un primo articolo su una rivista giuridica affermando “il diritto delle persone di essere lasciate in pace e ad essere protette nella loro sfera più intima)



• Il primo strumento giuridico internazionale in cui compare il tema della privacy – inteso come tutela della sfera privata dell'individuo contro le ingerenze altrui – è la **Dichiarazione Universale dei diritti dell'uomo** proclamata dall'Assemblea delle Nazioni Unite il **10 dicembre 1948**



• Il concetto di privacy con riferimento alla vita privata, al domicilio ed alla corrispondenza fa capolino nel continente europeo con la **Convenzione dei diritti dell'uomo (CEDU) del 1950**. Tuttavia l'art. 8 CEDU non fa ancora riferimento espresso alla tutela dei dati personali



• Per trovare un concetto di privacy più simile a quello dei giorni nostri occorre attendere la **Convenzione di Strasburgo** adottata dal Consiglio d'Europa il **28 gennaio 1981** in cui si parla di “protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale” →

• Tale Convenzione viene ratificata in Italia con estremo ritardo ossia solo **nel 1989 con la L. 98 del 21 febbraio**

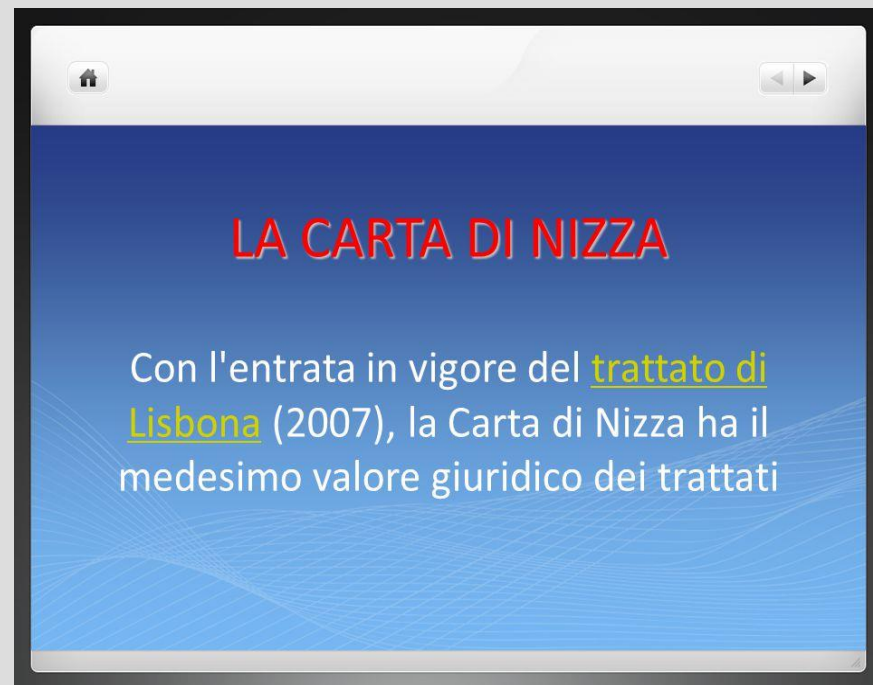
• Nel 2001 viene adottato un **Protocollo addizionale** alla Convenzione attraverso il quale vengono introdotte delle **disposizioni in materia di flussi di dati verso i paesi terzi** e viene istituita, per la prima volta, una **Autorità di controllo a livello nazionale** per la protezione dei dati →



.Con l'entrata in vigore del Trattato di Lisbona la Carta dei diritti fondamentali dell'UE (**Carta di Nizza**) assume il medesimo valore giuridico dei Trattati e quindi diviene pienamente vincolante per le istituzioni europee e gli Stati membri



.L'**art. 8** della Carta recita:” *ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate ed in base al consenso della persona interessata ...ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica*”



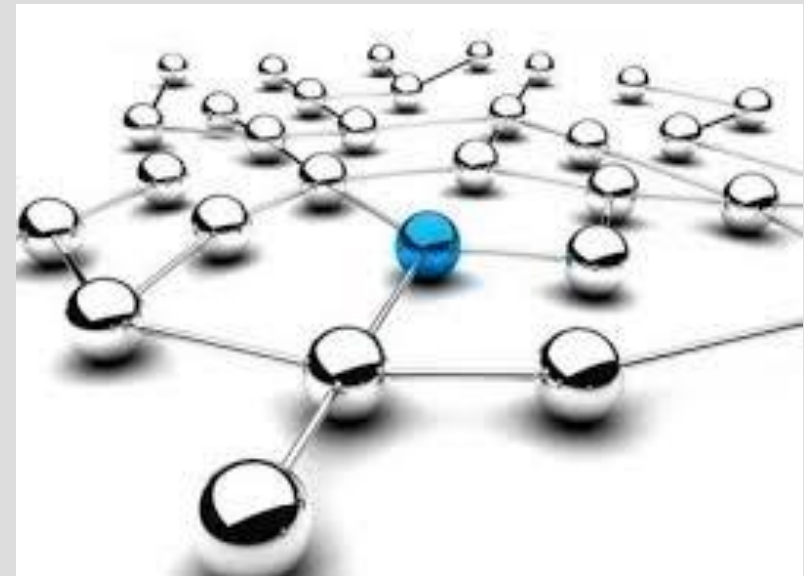
•Passando alle fonti secondarie dell'Unione:

•nel 1995, al fine di garantire una omogenea protezione dei dati delle persone, il legislatore europeo emana la **direttiva 95/46/CE**

•Lo scopo che emerge dai Considerando della direttiva è quello di **ARMONIZZARE** le normative nazionali in materia già esistenti in molti Stati europei ad eccezione dell'Italia

•In sostanza l'esigenza era quella di trovare un equilibrio tra il rispetto del diritto alla vita privata e la libera circolazione dei dati a livello europeo

•Quadro Giuridico Comune



La Direttiva 95/46/CE la pietra miliare della storia della protezione dei dati è stata la base normativa di riferimento sulla Privacy fino al 25 maggio u.s. data in cui è divenuto applicabile in tutti gli Stati membri il nuovo **REGOLAMENTO EUROPEO 2016/679**

La Direttiva 95/46/CE è stata recepita in Italia con la L. n. 675 del 1996 (in vigore dal maggio 1997) prima legge italiana di riferimento in materia di protezione dei dati personali

In 7 anni si sono poi succeduti 9 decreti legislativi e 2 DPR nonché numerose disposizioni regolamentari che hanno potenziato ulteriormente il numero delle norme in materia



.Il 1° gennaio 2004 veniva poi approvato il **D. Lgs. n. 196 del 30 giugno 2003 c.d. Codice in materia di protezione dei dati personali** composto da 186 articoli che raccoglieva le indicazioni e le direttive europee intervenute nel lasso di tempo intercorso dal 1996 al 2003

.Il Codice attualmente in vigore si compone di 3 parti che contengono, rispettivamente:

- .1) le disposizioni generali riguardanti le regole applicabili a tutti i trattamenti;
- .2) disposizioni particolari per specifici trattamenti;
- .3) le disposizioni relative alle azioni di tutela dell'interessato e al sistema sanzionatorio



.Il 25 gennaio 2012 la Commissione Europea ha presentato ufficialmente il c.d. “**pacchetto protezione dati**” con lo scopo di garantire un quadro giuridico coerente ed un sistema complessivamente armonizzato in materia di protezione dati nell'UE

.Il 4 maggio 2016 è stato pubblicato sulla G.U. dell'Unione europea il testo del regolamento europeo in materia di protezione dei dati personali

.Il **24 maggio 2016** è entrato ufficialmente in vigore il Regolamento che diventerà definitivamente applicabile in via diretta in tutti gli Stati membri a partire dal 25 maggio 2018

.Viene quindi concesso un tempo sufficientemente lungo per consentire alle imprese ed al settore pubblico di attrezzarsi per allineare i trattamenti ai nuovi standard



Il 21 marzo 2018 il Consiglio dei Ministri ha approvato in esame preliminare la **bozza del decreto legislativo** che introduce le disposizioni per **l'adeguamento della normativa nazionale al Regolamento europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**, nonché alla libera circolazione di tali dati.

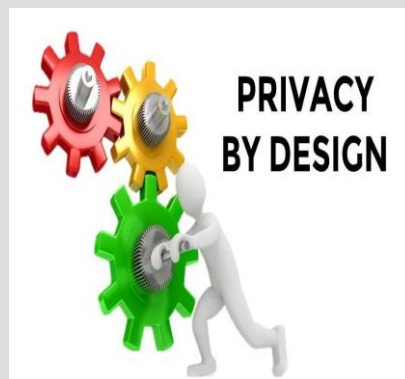
Dal 25 maggio 2018, data in cui le disposizioni di diritto europeo acquisteranno efficacia, **il vigente Codice in materia di protezione dei dati personali**, di cui al decreto legislativo 30 giugno 2003, n. 196, **sarà abrogato e la nuova disciplina in materia sarà rappresentata principalmente dalle disposizioni del suddetto Regolamento immediatamente applicabili** e da quelle recate dallo schema di decreto volte ad **armonizzare l'ordinamento interno al nuovo quadro normativo dell'Unione Europea in tema di tutela della privacy**.

La parte generale del Codice risulta sostituita in modo naturale dalle disposizioni del Regolamento, che su queste prevalgono e quasi nulla resta della parte generale del Codice.

La parte speciale del Codice è stata invece trasferita, con i necessari adeguamenti imposti dal Regolamento europeo, **nello schema di decreto**.

I principi del GDPR

CON IL REGOLAMENTO
COMUNITARIO VIENE DATA
PARTICOLARE RILEVANZA A QUESTI
4 PRINCIPI



IL PRINCIPIO DELLA TRASPARENZA

con la legge comunitaria vengono posti in capo al titolare obblighi di TRASPARENZA più stringenti rispetto alla precedente normativa

L'INFORMATIVA



Art. 12 GDPR

Linguaggio chiaro preciso e comprensibile soprattutto se il trattamento concerne i minori

Periodo di conservazione o criteri Utilizzati per determinarli

Diritti dell'interessato:
- accesso, rettifica, cancellazione, opposizione, limitazione, portabilità

Diritto di proporre reclamo
Autorità di controllo

Esistenza di un processo Decisionale automatizzato
profilazione

I punti di contatto (ad es. D.P.O.)

IL DIRITTO ALL'OBLIO

• Il **diritto all'oblio** viene inserito per la prima volta in una norma e diviene un principio fondamentale (in passato era già stato introdotto da alcune pronunce della Corte di Giustizia e della Corte di Cassazione)



• l'interessato potrà chiedere al titolare di cancellare i propri dati personali anche on-line qualora ricorrano le seguenti condizioni

- 1) se i dati sono trattati solo sulla base del consenso
- 2) se i dati non sono più necessari per le iniziali finalità
- 3) se i dati sono trattati illecitamente
- 4) se vi è opposizione al trattamento

IL PRINCIPIO DELL'ACCOUNTABILITY

•Tra le prescrizioni introdotte dal Regolamento spicca sicuramente il principio dell'accountability che potrebbe essere tradotto con "responsabilizzazione"



•il Titolare del trattamento in base a tale principio dovrà provare di aver adottato tutte le politiche privacy e le misure adeguate conformi al regolamento (art. 5 comma II e 24 I comma)

Articoli del GDPR in cui si ritrova il Principio dell'accountability:

- art. 30 registro dei trattamenti;
- art. 40 codici di condotta;
- art. 42 certificazioni



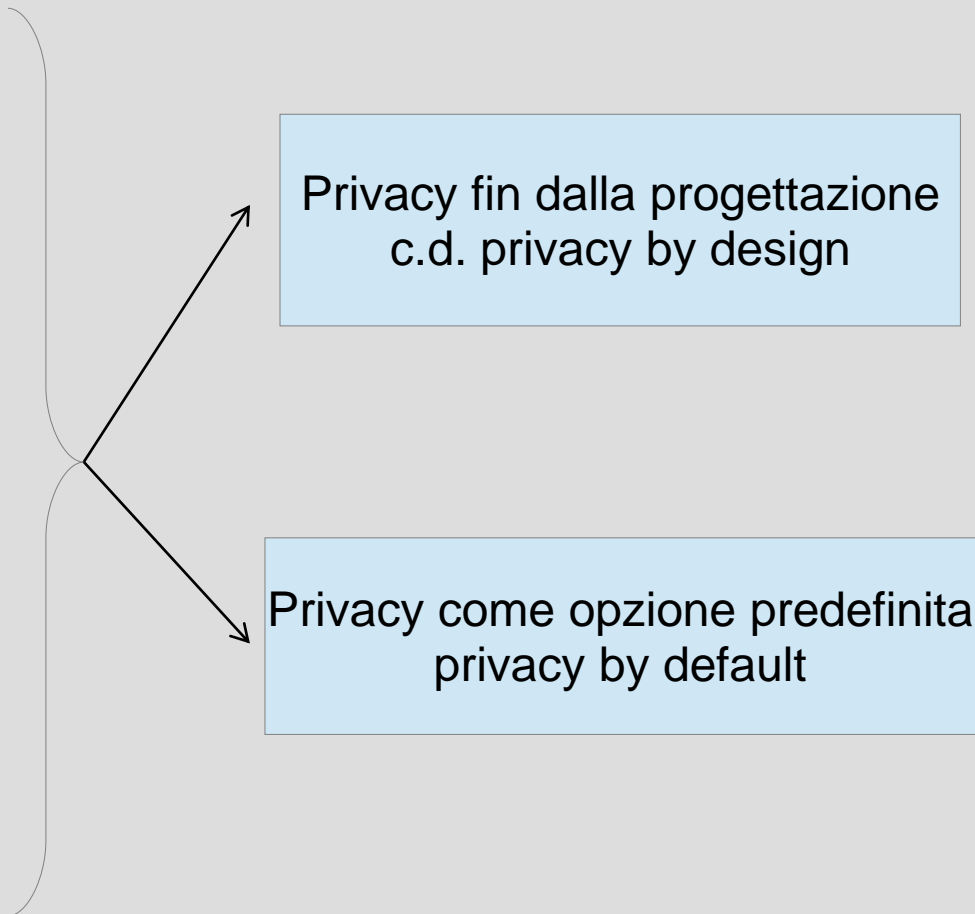
Utili per dimostrare il rispetto della normativa

PRIVACY BY DESIGN

L'articolo 25 del Regolamento introduce il principio di privacy by design e privacy by default, un approccio concettuale innovativo che impone alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti a tutela dei dati personali.

Le nuove tecnologie non vengono più viste come ostacolo alla materia della protezione dei dati personali ma in un'ottica di collaborazione rispetto a tale normativa

tutte le volte che in azienda si vorrà introdurre un nuovo servizio contraddistinto da una forte componente tecnologica si dovranno analizzare sin dalla fase della progettazione i possibili impatti sulla privacy



Privacy fin dalla progettazione
c.d. privacy by design

Privacy come opzione predefinita
privacy by default

LE NOVITA' DEL GDPR

12 step del General Data Protection (GDPR)

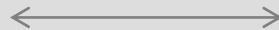


MAGGIORI DIRITTI DEL CITTADINO/INTERESSATO

Il Cittadino potrà intervenire nei confronti del Titolare del trattamento in modalità diverse al fine di garantire i propri diritti

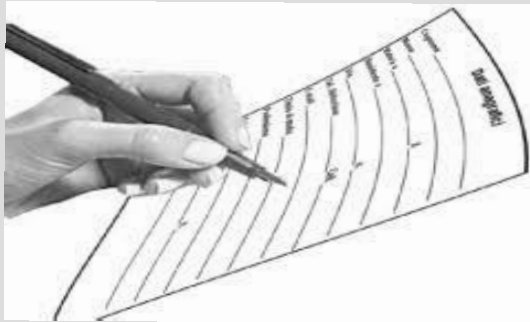


Il riconoscimento del potere di controllo e di conseguente intervento sui dati personali richiede che l'interessato



sia informato sulle finalità e sui presupposti di legittimità del trattamento in corso, sull'identità e sui dati di contatto del titolare e del responsabile della protezione dei dati, sugli eventuali destinatari dei dati personali e della possibilità che i dati siano trasferiti ad un Paese non appartenente alla UE (in quest'ultimo caso l'interessato dovrà anche essere informato dell'esistenza di garanzie adeguate)
L'interessato dovrà anche essere informato sui tempi di conservazione o sui criteri utilizzati per determinare tale periodo

DIRITTI DELL'INTERESSATO



L'interessato dovrà essere informato dei suoi diritti e sulle relative modalità di esercizio e precisamente sull'esistenza del diritto di chiedere al titolare

l'accesso ai dati personali

La rettifica e la cancellazione degli stessi

La limitazione del trattamento

Il diritto di opporsi al trattamento

Il diritto di portabilità dei dati

Possibilità di proporre reclamo all'Autorità di controllo

II CONSENSO COME CONDIZIONE DI LICEITA'



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 e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. 196/2003**

- consenso
- 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
- interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati

IL CONSENSO

Il CONSENSO dovrà essere **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), presenti all'interno di modulistica.

La formula utilizzata per chiedere il consenso dovrà essere **COMPENSIBILE, SEMPLICE, CHIARA** (art. 7.2).

I soggetti pubblici, così come accade oggi, non dovranno, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9, altre disposizioni del Codice: artt. 18, 20)

Per i dati "sensibili" (si veda art. 9 regolamento) il consenso **DEVE** essere "**esplicito**"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la PROFILAZIONE – art. 22)

NON deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) **DEVE** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Il **consenso dei minori** è valido **a partire dai 16 anni**; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci

DIRITTO DI ACCESSO



DIRITTO DI ACCESSO molto simile a quello che già conosciamo l'art. 15 del Regolamento riconosce all'interessato il diritto di ottenere dal titolare del trattamento la conferma o meno dell'esistenza di un trattamento di dati personali a lui riferiti e, nel caso, di ottenere l'accesso ai dati personali ed in particolare alle seguenti informazioni:

- le finalità del trattamento;
- le categorie dei dati trattati;
- i destinatari a cui i dati sono stati o saranno comunicati;
- il periodo di conservazione;

la possibilità di richiedere al titolare la rettifica o la cancellazione dei dati o la loro limitazione e la possibilità di opporsi al loro trattamento;

- il diritto di proporre reclamo;
- l'esistenza di un processo decisionale automatizzato compresa la profilazione e le logiche utilizzate per tale trattamento.

Pertanto rispetto alla disciplina codicistica il contenuto dell'accesso è più ampio riferendosi anche al periodo di conservazione e all'esistenza degli ulteriori diritti riconosciuti all'interessato.

Attraverso l'accesso l'interessato mantiene il controllo sui dati che lo riguardano e, in ragione delle informazioni fornitegli, è in grado di verificare la legittimità del trattamento decidendo nel caso di intervenire su di esso attraverso la richiesta di integrazione cancellazione e opposizione

DIRITTO DI RETTIFICA, INTEGRAZIONE E CANCELLAZIONE



Secondo l'art. 16 del Regolamento l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza giustificato ritardo. L'interessato ha, inoltre, il diritto di ottenere l'integrazione dei dati personali incompleti.

Per il diritto alla cancellazione valgono le considerazioni già svolte per il diritto all'oblio

DIRITTO DI LIMITAZIONE



Secondo l'art. 18 del Regolamento il diritto di limitazione opera solo nelle 4 ipotesi tassativamente indicate in tale articolo e consiste nel potere dell'interessato di imprimere sui dati a lui riferiti un vincolo di indisponibilità e di inutilizzabilità.

I dati pertanto, a seguito dell'esercizio del diritto di limitazione, non saranno cancellati ma il loro trattamento ad opera del titolare si ridurrà alla sola operazione di conservazione e sospensione temporanea di ogni ulteriore trattamento ---- analogie con la misura del blocco dei dati sancita dall'art. 12 lett. b) della Direttiva 95/46/CE

DIRITTO ALLA PORTABILITA' DEI DATI



Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Costituisce a ben vedere uno sviluppo del diritto d'accesso.

In prima approssimazione si può affermare che l'esercizio del diritto alla portabilità consente all'interessato di ottenere dal titolare del trattamento i dati personali in un formato strutturato d'uso comune e leggibile ovvero il trasferimento di detti dati dall'originario titolare del trattamento ad un altro. La portabilità facendo circolare dati personali direttamente tra i titolari del trattamento agevola lo sviluppo di un mercato concorrenziale dei servizi della società dell'informazione.

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 (*si veda il considerando 68 per maggiori dettagli*).

Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

DIRITTO DI OPPOSIZIONE



L'art. 21 del Regolamento riconosce il diritto dell'interessato di opporsi al trattamento dei dati personali in qualsiasi momento **per motivi connessi alla sua situazione particolare**. L'opposizione al trattamento dei dati personali costituisce una dichiarazione di volontà che produce l'effetto di interrompere in via definitiva il trattamento salvo che il titolare dimostri l'esistenza di motivi legittimi cogenti per proseguire con il trattamento che prevalgono sugli interessi, sui diritti e sulla libertà dell'interessato oppure per l'accertamento l'esercizio la difesa di un diritto in sede giudiziaria. L'articolo 21 prevede che ricevuta la richiesta di opposizione al trattamento il titolare deve astenersi dal trattare ulteriormente i dati personali; sebbene la norma non lo espliciti si ritiene di poter affermare che il titolare debba procedere alla cancellazione dei dati non potendosi ritenere sufficiente ai fini della corretta interpretazione della formula "si astiene ulteriormente dal trattare i dati personali" che il titolare si limiti alla loro conservazione, considerando che anche mera conservazione dei dati configura un trattamento.

Il diritto di opposizione consiste in un potere di inibizione esercitabile per motivi connessi alla sua situazione particolare a prescindere dal illegittimità del trattamento attraverso cui l'interessato controlla i propri dati personali.

Vi è poi una specifica previsione al paragrafo 2 e 3 dell'articolo 21 del regolamento nel caso in cui il diritto di opposizione concerna il trattamento effettuato per finalità di marketing diretto. In questo caso il diritto di opposizione potrà essere esercitato dall'interessato in qualsiasi momento e senza la necessità di motivare le ragioni dell'opposizione.

TRASFERIMENTO DEI DATI EXTRA UE



Come noto il GDPR prevede che tutti i fornitori di servizi che promuovono la propria attività anche in Stati europei devono rispettare, nelle operazioni di trattamento dei dati personali degli interessati europei, il GDPR.

Tuttavia gli Stati non facenti parte dell'Unione non sono soggetti al rispetto delle disposizioni previste dal Regolamento e, di conseguenza, il livello di sicurezza, di garanzia e di tutela dei *personal data* può non corrispondere e non equivalere a quello europeo.

L'espansione del commercio e della cooperazione internazionale, la globalizzazione e la diffusione di piattaforme on-line rendono però sempre più comuni e frequenti flussi di dati verso paesi extra UE. Il legislatore europeo, per garantire comunque un livello di sicurezza adeguato, impone con gli artt. 44 e seguenti del GDPR determinate condizioni affinché un trasferimento dati verso paesi terzi possa essere effettuato.

IL TRASFERIMENTO E' AMMESSO IN TRE SITUAZIONI PARTICOLARI

1. Trasferimento sulla base di una **DECISIONE SULL'ADEGUATEZZA sul livello di protezione** presa dalla Commissione europea. La valutazione di adeguatezza deve tener conto di precisi elementi espressamente previsti dall'art. 45 comma 2 del Regolamento. Deve essere poi svolto un riesame periodico di tale decisione almeno ogni quattro anni, al fine di mantenere sotto controllo l'effettiva esistenza di un livello di protezione adeguato e in linea con quanto previsto dal GDPR. Tali decisioni della Commissione devono essere pubblicate nella Gazzetta Ufficiale dell'UE e pubblicate sul sito della Commissione europea stessa. Una volta riconosciuto adeguato un determinato paese, tutti i trasferimenti verso quello Stato non devono più ottenere autorizzazioni specifiche di alcun tipo.

3. **NORME VINCOLANTI TRA GRUPPI DI IMPRESA** (BCR – Binding Corporate Rules). Strumento volto a consentire il trasferimento verso paesi extra UE tra società facenti parte dello stesso gruppo d'impresa. Consistono in una serie di clausole contrattuali che dettano principi (in linea con il Regolamento 679/2016 e che assicurano un livello di protezione adeguato) vincolanti per tutte le società facenti parte del gruppo. Le BCR devono essere esaminate e approvate dall'autorità di controllo nazionale o europea che deve verificare la sussistenza dei contenuti minimi espressamente previsti dall'art. 47 del GDPR.

A queste tre situazioni esistono deroghe eccezionali previste tassativamente dal legislatore europeo. In particolare il trasferimento è comunque ammesso solo se:

a) l'interessato ha espressamente ed esplicitamente consentito al trasferimento, dopo essere stato informato dei possibili rischi (e del fatto che il trasferimento stesso non rientra in nessuna delle tre situazioni tipo di cui sopra), o quando tale trasferimento è necessario per l'esecuzione di un contratto a favore dell'interessato o per importanti motivi di ordine pubblico, interessi vitali o, infine, per accertare, esercitare o difendere un diritto in sede giudiziaria.

Da ultimo il trasferimento verso paesi extra UE è ammesso solo se non è ripetitivo, riguarda un numero limitato di interessati ed è necessario per il perseguimento di interessi legittimi cogenti del titolare del trattamento, su cui non prevalgono gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. In tali occasioni il titolare informa comunque l'autorità di controllo e, oltre alla solita informativa "standard", mette a conoscenza l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti.

Al di fuori di tali situazioni ordinarie ed eccezionali, il trasferimento dei dati personali verso Paesi terzi non è mai consentito.

VIOLAZIONE INFORMATICA (DATA BREACH)



[L'art. 33 del Regolamento Europeo 679/2016](#) introduce una grossa novità nello scenario della sicurezza dei dati: in particolare il titolare del trattamento nel caso di violazione **dei propri sistemi informatici (c.d. data breach) dovrà notificare detta violazione senza giustificato ritardo e comunque ove possibile entro 72 ore** da cui si viene a conoscenza della violazione

.CASI REALI DI DATA BREACH CONSISTENTI

- **JP Morgan**, banca internazionale, con la sottrazione di quasi 79 milioni di record
- **E-bay**, piattaforma di e-commerce, che si è vista sottrarre 145 milioni di record
- **Gruppo Benetton**, multinazionale di abbigliamento che ha visto trafugati le bozze di una collezione
- **Sony**, trafugati più di 30 milioni di record con il fermo dei sistemi per 3 giorni

Questi sono solo alcuni dei casi, i più noti perché portati all'onore delle cronache, che **hanno visto le aziende essere protagoniste di attacchi informatici**. In realtà migliaia e migliaia sono le imprese, anche piccole o piccolissime, che sono state oggetto di attacchi informatici che hanno compromesso la sicurezza dei loro sistemi.

QUALI SONO GLI ADEMPIMENTI DOPO AVER SUBITO UN DATA BREACH?

1 – Descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

Questo punto presuppone la presenza in azienda di **personale informatico adeguatamente preparato** oppure un servizio esterno con qualche bravo sistemista (meglio se con un contratto che citi espressamente questo punto).

Inoltre è **necessaria la presenza di policy aziendali** che permettano all'azienda di avere sempre contezza del numero degli interessati di cui si tratta i dati e delle relative registrazioni di dati.

2 – Comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

Il [Data Protection Officer](#) o altro incaricato preventivamente nominato diventa il punto di contatto con il Garante.

3 – Descrivere le probabili conseguenze della violazione dei dati personali;

Indipendentemente da un obbligo di legge, sarebbe opportuno **verificare preventivamente quali siano i rischi nel trattare i dati**. Avere chiari i pericoli ed i rischi è importante anche nel trattare i dati.

4 – Descrivere le 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, se del caso, per attenuarne i possibili effetti negativi

Anche in questo caso, **andare ad identificare che misure adottare in piena crisi**, a seguito di un evento dannoso, in un momento in cui si è nel mirino del Garante ed avendo poco tempo (72 ore –3 giorni- dalla scoperta dell'evento) **risulta molto difficile ed impegnativo**. Molto meglio analizzare la questione preventivamente ed **individuare una serie di miglioramenti alle proprie misure di sicurezza** che potrebbero essere implementati nel tempo e che **possono evitare data breach**.

LA NUOVA FIGURA DEL DPO



Il nuovo Regolamento Europeo riconosce nel D.P.O. uno degli elementi chiave all'interno del nuovo sistema di governance dei dati fondato sul principio dell'accountability e prevede una serie di condizioni in rapporto alla nomina, allo stato e ai compiti specifici di questa nuova figura.

I responsabili della protezione dei dati (D.P.O.) sono al centro di questo nuovo quadro giuridico in molti ambiti e sono chiamati a facilitare l'osservanza delle disposizioni del regolamento:

- oltre a favorirne l'osservanza attraverso strumenti di accountability (supportando la valutazione di impatto e conducendo o supportando audit in materia di protezione dei dati)
- i DPO fungono da interfaccia tra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno dell'azienda o di un ente.

Al titolare o al responsabile del trattamento spetta il compito fondamentale di **consentire lo svolgimento efficace dei compiti cui il DPO** è preposto: la nomina di un DPO è solo il primo passo perché lo stesso dovrà disporre anche di **autonomia risorse** sufficienti a svolgere in modo efficace i compiti cui è chiamato.

LE LINEE GUIDA DEL GARANTE

LE LINEE GUIDA SUL DPO

Il **13 dicembre 2016** il Gruppo dei Garanti europei ha emanato le prime linee guida sul responsabile della protezione dei dati che specificano i requisiti soggettivi e oggettivi di questa figura.

Nel documento vengono specificate le condizioni in cui scatta **l'obbligo di nomina** del DPO (anche attraverso esempi concreti) le **competenze professionali** e le **garanzie di indipendenza e inamovibilità** di cui il DPO deve godere nello svolgimento delle proprie attività di indirizzo e controllo all'interno dell'organizzazione del titolare.

NOMINA OBBLIGATORIA DEL DPO

CASI IN CUI E' OBBLIGATORIA LA NOMINA DEL DPO

In base all'articolo 37 primo paragrafo del Regolamento Europeo la nomina del DPO è obbligatoria in **tre casi** particolari:

- 1) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
- 2) se le **attività principali** del titolare o del responsabile consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico di interessati su larga scala**;
- 3) se le attività principale del titolare o del responsabile consistono nel **trattamento su larga scala** di dati personali che rivelano l'origine razziale o etnica le opinioni politiche le convinzioni religiose o filosofiche l'appartenenza sindacale nonché di dati genetici dati biometrici dati relativi alla salute e alla vita sessuale o all'orientamento sessuale della persona o di dati personali relativi a condanne penali e reati (art. 9 "categorie particolari di dati).

COSA FARE SE SI DECIDE DI NON NOMINARE IL DPO

Tranne quando sia evidente che un soggetto non è tenuto a nominare il dpo i titolari e responsabili devono **documentare le valutazioni compiute all'interno dell'azienda** per stabilire se si applichi o meno l'obbligo di nomina di un DPO così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti.

Tale analisi fa parte della documentazione da produrre in base al principio di responsabilizzazione (e in base a l'obbligo di dotarsi delle politiche del trattamento dei dati ai sensi dell'articolo 24 GDPR).

Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario per esempio se il titolare o il responsabile intraprendono nuove attività o forniscono nuovi servizi ad alto contenuto tecnologico che potrebbero ricadere nel novero dei casi elencati all'articolo 37 paragrafo 1 GDPR sulla nomina obbligatoria del DPO

QUALI SONO I PRESUPPOSTI DI OBBLIGATORIETA'

Art. 37 comma 1 lettera B): il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogni qualvolta **le attività principali del titolare del trattamento e del responsabile del trattamento** consistano in trattamenti che per loro natura ambito di applicazione e/o finalità richiedano il **monitoraggio regolare e sistematico degli interessati su larga scala**.

Nel considerando 97 si afferma che le attività principali di un titolare del trattamento: “riguardano le sue **attività primarie** ed esulano dal trattamento dei dati personali le attività accessorie”.

Con attività principali si possono intendere le **operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento**.

D'altro canto tutti gli organismi pubblici e privati svolgono determinate attività quali ad esempio il pagamento delle retribuzioni al personale che pur essendo necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo devono essere considerate solitamente accessorie e non vengono annoverate fra le attività principali

MONITORAGGIO SU LARGA SCALA

Sulla base delle linee guida possiamo ritenere che si possa parlare di trattamento su larga scala nei seguenti casi:

- a) numero di soggetti interessati cui i dati si riferiscono (in termini o di preciso numero o di percentuale rispetto a una rilevante porzione della popolazione)
- b) ammontare/grandezza dei database e del volume delle informazioni trattate;
- c) durata o indefinitività delle attività di trattamento dei dati
- d) estensione geografica delle attività di trattamento

PRESUPPOSTI DI OBBLIGATORIETA'

Alcuni esempi di soggetti che svolgono trattamenti su larga scala:

- 1) trattamento di dati di pazienti da parte di un ospedale
- 2) trattamento di dati di viaggiatori che utilizzano un sistema di trasporto pubblico
- 3) trattamento in tempo reale di dati di geolocalizzazione di clienti di una catena di fast food per fini statistici
- 4) trattamento di dati della clientela da parte di una banca ad una compagnia di assicurazioni nel normale svolgimento delle relazioni contrattuali e commerciali con dei clienti
- 5) trattamento di dati di utenti di un motore di ricerca ai fini di analisi comportamentale a scopi di marketing
- 6) trattamento di dati di traffico di ubicazione e dei contenuti della clientela da parte degli internet Service providers

COSA SI INTENDE PER MONITORAGGIO “REGOLARE O SISTEMATICO”

Per **monitoraggio regolare** i garanti dell'Unione Europea forniscono tale interpretazione

- 1) Continuo o ad intervalli determinati per particolari periodi di tempo
- 2) ricorrente a scadenze di tempo fisso
- 3) Comunque costante e avente luogo periodicamente

Per **monitoraggio sistematico** essi forniscono tale interpretazione

- 1) basato su un sistema metodico organizzato e preconfigurato
- 2) avente luogo come parte di un piano generale di raccolta dei dati personali
- 3) effettuato come parte di una qualsiasi strategia

ESEMPI DI MONITORAGGIO REGOLARE E SISTEMATICO

- Gestione operativa di una rete di telecomunicazioni
- fornitore di servizi di telecomunicazione
- profilazione e scoring ai fini di Risk Assessment (ad esempio per scopi di credit scoring, fissazione di premi assicurativi, prevenzione di frodi, prevenzione di antiriciclaggio)
- Tracciatura della posizione geografica attraverso app sul cellulare
- programmi di fidelizzazione
- pubblicità comportamentale
- monitoraggio del benessere della Salute
- monitoraggio dello stato della forma fisica e dello stato sanitario attraverso dispositivi indossabili o portatili
- televisioni a circuito chiuso
- sistemi di home authentication
- veicoli Smart

OBBLIGO DI NOMINA DEL DPO RAPPORTI TRA TITOLARE E RESPONSABILE DEL TRATTAMENTO

Per quanto riguarda la nomina del DPO l'articolo 37 **non distingue tra titolare o responsabile del trattamento**. Potrà essere il solo titolare ovvero il solo responsabile, oppure sia l'uno sia l'altro, a dover nominare un DPO.

Questi ultimi saranno poi tenuti alla reciproca collaborazione

Una piccola azienda a conduzione familiare operante nel settore della distribuzione di elettrodomestici in una città si serve di un responsabile del trattamento la cui attività principale consiste nel fornire servizi di tracciamento degli utenti del sito web oppure all'assistenza per attività di pubblicità e marketing mirati. Le attività svolte dall'azienda e dai clienti non generano trattamenti di dati su larga scala in considerazione del ridotto numero di clienti della gamma relativamente limitata di attività. Tuttavia, il responsabile del trattamento, che conta numerosi clienti come questa piccola azienda familiare svolge nel suo complesso trattamenti su larga scala.

Ne deriva che il responsabile deve nominare un DPO ai sensi dell'articolo 37 primo paragrafo lettera B al contempo l'azienda in quanto tale non è soggetta all'obbligo di nomina del DPO

CARATTERISTICHE DEL DPO

Il Data Protection officer **non deve ricevere** dal titolare o dal responsabile del trattamento **delle istruzioni** per quanto riguarda l'esecuzione dei compiti affidatigli (e figura del tutto autonoma) **ne è soggetto al potere disciplinare** sanzionatorio per l'adempimento dei propri compiti (ad esempio in ciò, tra l'altro, risiedono i caratteri distintivi tra data Protection officer e responsabile del trattamento che al contrario deve ricevere istruzioni scritte del soggetto al controllo e all'autorità del titolare del trattamento lvi compresi i profili sanzionatori).

Va **tempestivamente e adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali, deve avere le **risorse necessarie ed il potere di spesa** per assolvere ai compiti assegnati, accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica (ad esempio **spese per il suo aggiornamento professionale**).

L'articolo 39 del regolamento individua il nucleo minimo (che comunque può essere anche esteso) dei compiti assegnati al responsabile della protezione dei dati

COMPITI E FUNZIONI DEL DPO

Il DPO è incaricato almeno dei seguenti compiti

- 1) informare e **fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi di legge sulla protezione dei dati
- 2) **sorvegliare l'osservanza del regolamento** e delle altre leggi (sia UE che nazionali) sulla protezione dei dati nonché delle politiche del titolare del trattamento e 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
- 3) fornire se richiesto un **parere in merito alla valutazione d'impatto** sulla protezione dei dati e sorvegliare lo svolgimento
- 4) **cooperare con il garante fungendo altresì da punto di contatto** sulle questioni connesse al trattamento tra cui la consultazione preventiva ed effettuare se del caso consultazioni relativamente a qualunque altra questione

IL DPO RIFERISCE DIRETTAMENTE AL VERTICE ANZIENDALE

Il DPO deve avere un **rapporto continuo e diretto con i vertici aziendali**

Per vertice gerarchico si intende il vertice amministrativo-gestionale cioè ad esempio il consiglio di amministrazione.

Il DPO non solo deve riferire cioè mettere a conoscenza il consiglio di amministrazione delle indicazioni e delle raccomandazioni da lui fornite nel quadro delle sue funzioni di informazione consulenza a favore del titolare o del responsabile del trattamento ma deve altresì redigere una **relazione annuale** delle attività svolte da sottoporre al CDA

Non solo, il rapporto e le interlocuzioni tra il DPO e il vertice gerarchico possono esplicitarsi anche come segue: se il titolare o il responsabile assumono decisioni incompatibili con il Regolamento Europeo e che disattendono le indicazioni/consulenze/richieste fornite dal DPO quest'ultimo deve avere la possibilità di **manifestare il proprio dissenso** al più alto livello del management ad esempio facendo verbalizzare in CDA il suo dissenso e facendo pervenire una relazione al più alto livello del management

COME VA COINVOLTO IL DPO

L'azienda deve assicurare il tempestivo e immediato coinvolgimento del DPO tramite la sua informazione/consultazione fin dalle fasi iniziali di qualsiasi progetto;

il DPO deve essere annoverato tra gli interlocutori da consultare all'interno dell'azienda da parte di tutti i reparti aziendali;

il DPO deve partecipare ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento. Ciò significa che occorrerà garantire per esempio:

- che il DPO sia invitato a partecipare su base regolare alle riunioni del Management di alto e medio livello;
- la presenza del DPO ogniqualvolta devono essere assunte decisioni che impattano sulla protezione dei dati.
- Il DPO deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
- che il parere del DPO riceva sempre la dovuta considerazione.

In caso di disaccordi vanno documentate le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal DPO

- che il DPO sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente

LE SAZIONI PREVISTE DAL GDPR

Tra le caratteristiche salienti del nuovo Regolamento europeo sulla privacy (GDPR General Data Protection Regulation), la parte sanzionatoria occupa, per l'Interesse dei Titolari, un posto sicuramente di rilievo.

Il Costo di una mancata compliance normativa è infatti destinato a salire notevolmente



nei casi più gravi fino a 20 milioni di euro, o se superiore, fino al 4% del fatturato annuo mondiale (ex art. 83 del GDPR)

CRITERI PER L'APPLICAZIONE DELLE SANZIONI

Mentre **le sanzioni penali rimangono di competenza di ogni singolo Stato**, le nuove sanzioni amministrative sono disciplinate dagli artt. 83 ed 84 del Regolamento.

Ai sensi dell'art. 83 paragrafo 1 ogni autorità di vigilanza (in Italia il Garante della privacy) dovrà garantire, in ogni singolo caso, che **la sanzione sia effettiva, proporzionata e dissuasiva**.

Al fine di determinare l'ammontare della sanzione occorrerà tener conto:

- della **natura**, della **gravità** e della **durata** della violazione, anche in considerazione del **numero degli interessati** e dei **danni** da questi subiti;
- del carattere **intenzionale o colposo** dell'infrazione;
- delle **azioni intraprese** dal Titolare o dal Responsabile **per mitigare i danni** subiti dagli interessati;
- del **grado di responsabilità** del Titolare o del Responsabile, anche sotto il **profilo tecnico, e le misure organizzative** attuate per prevenire le violazioni;
- delle eventuali rilevanti **violazioni precedenti** da parte del Titolare o del Responsabile;
- del livello di **cooperazione con l'autorità di vigilanza**, al fine di porre rimedio alla violazione e mitigarne i possibili effetti negativi;
- delle **categorie di dati personali oggetto della violazione**;
- dell'**adesione a codici di condotta** o a meccanismi di **certificazione** riconosciuti;
- di ogni altro **fattore aggravante o attenuante** applicabile alle circostanze del caso;
- dei **benefici finanziari ottenuti**, o le perdite evitate, direttamente o indirettamente, per effetto della violazione commessa.

CUMULO FORMALE

Se il Titolare o il Responsabile hanno commesso, intenzionalmente o per negligenza, più violazioni alle disposizioni del Regolamento connesse a una stessa operazione di trattamento di dati personali, l'importo totale della **sanzione non dovrà superare l'importo indicato per la violazione più grave**

ART. 83 paragrafo 4

Sono soggette a **sanzioni amministrative fino a 10 milioni di euro, o in caso di un'impresa, fino al 2% del fatturato totale annuo mondiale dell'esercizio precedente**, se superiore, le violazioni delle disposizioni relative agli obblighi del Titolare o del Responsabile di cui agli articoli

- 8 (consenso dei minori),
- 11 (trattamenti che non richiedono l'identificazione degli interessati),
- 25 (privacy by design e privacy by default),
- 26 (cotitolarità del trattamento),
- 27 (nomina rappresentante del Titolare non stabilito nell'Unione Europea),
- 28 (Responsabili del trattamento),
- 29 (istruzioni e autorità del Titolare),
- 30 (documentazione relativa a ciascun trattamento di dati personali),
- 31 (cooperazione con l'autorità di vigilanza),
- 32 (sicurezza del trattamento),
- 33 (notificazione dei data breach all'autorità),
- 34 (comunicazione dei data breach agli interessati),
- 35 (DPIA – Data Protection Impact Assessment),
- 36 (consultazione preventiva dell'autorità di vigilanza),
- 37, 38 e 39 (designazione, posizione e compiti del DPO – Data Protection Officer),
- 41, 42 e 43 (codici di condotta e processi di certificazione).

ART 83 Paragrafo 5

Sanzioni amministrative fino a **20 milioni di euro, o in caso di un'impresa, fino al 4% del fatturato totale annuo mondiale dell'esercizio precedente**, se superiore, sono invece previste per le violazioni in materia di principi base del trattamento, condizioni per il consenso, diritti degli interessati, trasferimento di dati personali all'estero, mancata ottemperanza a un ordine o a una limitazione temporanea o definitiva del trattamento disposti dall'autorità di vigilanza.

POTERI CORRETTIVI DEL GARANTE AI SENSI DELL'ART. 58 paragrafo 2

A tali sanzioni l'Autorità Garante potrà affiancare i seguenti poteri correttivi:

- rivolgere avvertimenti al titolare ed al responsabile sulla conformità dei trattamenti
- rivolgere ammonimenti al titolare o al responsabile del trattamento nel caso in cui abbiano violato le disposizioni del presente regolamento;
- ingiungere al titolare o al responsabile del trattamento di conformarsi alle richieste dell'interessato;
- ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
- imporre una limitazione provvisoria o definitiva del trattamento;
- ordinare la rettifica la cancellazione di dati personali o la limitazione del trattamento
- revocare la certificazione

CONSIDERANDO 148 DEL GDPR

Dalla lettura del considerando 148 si ricava che:

«in caso di violazione minore o se la sanzione che dovrebbe essere irrogata costituisse un onere sproporzionato per la persona fisica, potrebbe essere rivolto un **AMMONIMENTO** anziché imposta una sanzione pecuniaria.

Si dovrebbe prestare tuttavia attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti, alla maniera in cui l'autorità di controllo ha preso conoscenza della violazione, al rispetto dei provvedimenti disposti nei confronti del titolare del trattamento o del responsabile del trattamento, all'adesione a un codice di condotta e eventuali altri fattori aggravanti o attenuanti»

GRAZIE A TUTTI PER L'ATTENZIONE



**PACCHIANA PARRAVICINI E ASSOCIATI
STUDIO LEGALE**

AVV. CRISTIANO MICHELA

**Corso Siccardi 11bis - 10122 Torino
tel. 011 5629063 - fax. 011 5176811
c.michela@avvocatipacchiana.com**