# CASSA ITALIANA DI PREVIDENZA ED ASSISTENZA GEOMETRI

# L'ADEGUAMENTO DELLA NORMATIVA NAZIONALE AL REGOLAMENTO UE N. 679/2016 - GDPR

***Roma, 13 giugno 2018***

***Avv. Giovanni Guerra***

**DA PIU' DI 20 ANNI** NELLA UE E' IN VIGORE UNA DIRETTIVA GENERALE SULLA PROTEZIONE DEI DATI PERSONALI (DIR. 95/46/CE), RECEPITA IN ITALIA NEL 1996 ED ATTUALMENTE DISCIPLINATA DAL CODICE SULLA PROTEZIONE DEI DATI PERSONALI (D.LGS. 196/2003)

DOPO 20 ANNI E' STATO APPROVATO **IL REGOLAMENTO (UE) 2016/679 – GENERAL DATA PROTECTION REGULATION (GDPR)**

È ENTRATO IN VIGORE IL 24 MAGGIO 2016 MA
E' DIVENTATO DIRETTAMENTE APPLICABILE IN ITALIA ED IN TUTTI GLI STATI MEMBRI DELLA UE A PARTIRE DAL **25 MAGGIO 2018**

DA TALE DATA E' ABROGATA LA DIR. 95/46/CE E SONO DISAPPLICABILI DIVERSE DISPOSIZIONI DELLA NORMATIVA ITALIANA SULLA PRIVACY

# OBIETTIVI PRINCIPALI DEL GDPR

- **SUPERARE IL DISOMOGENEO RECEPIMENTO DA PARTE DEGLI STATI MEMBRI DELLA DIRETTIVA E GARANTIRE UN LIVELLO UNIFORME DI PROTEZIONE DELLE PERSONE IN TUTTA LA UE E PREVENIRE DISPARITÀ CHE POSSONO OSTACOLARE LA LIBERA CIRCOLAZIONE DEI DATI NELLA UE**

- **GARANTIRE STESSE REGOLE DEL GIOCO PER LE IMPRESE OPERANTI NELLA UE , MA ANCHE PER LE IMPRESE EXTRA UE CHE OFFRONO SERVIZI A CITTADINI DELLA UE!**

- **RAFFORZARE GLI STRUMENTI DI TUTELA DEGLI INDIVIDUI A FRONTE DELLA DIGITALIZZAZIONE DEI SERVIZI CON FORTE APPESANTIMENTO DELLE SANZIONI PECUNIARIE (FINO A 10 O 20 MLN DI EURO, 2 O 4 % FATTURATO GLOBALE ANNUO!)**

# WORK ANCORA IN PROGRESS!

**IL GDPR LASCIA ALCUNI MARGINI DI INTERVENTO ED ATTUAZIONE ALLA COMMISSIONE UE, AI LEGISLATORI NAZIONALI, AUTORITÀ EUROPEE E NAZIONALI DI CONTROLLO (EDPB E GARANTE PRIVACY)**

**NECESSITÀ DI UN ADEGUAMENTO DELLA NORMATIVA ITALIANA ALLE NUOVE DISPOSIZIONI DEL GDPR: VEDI LA LEGGE 163/2017 DI DELEGAZIONE EUROPEA 2016/2017**

**RICOGNIZIONE DEI PROVVEDIMENTI DEL GARANTE PRIVACY**

## Definizioni: conferme e novità (art. 4)

- Nel GDPR vengono confermate molte definizioni della Dir. 95/46 e del Codice privacy:
- «**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*.
- sono indicate le definizioni di «**dati relativi alla salute», «dati genetici» e «dati biometrici»**, ma non ci sono più le definizioni di «dati sensibili» e «dati giudiziari», indicate rispettivamente come **categorie particolari di dati personali e dati personali relativi a condanne penali e a reati**


Avv. Giovanni Guerra

## Addio alle nozioni formali di «dati sensibili» e «dati giudiziari»:

- - «**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;
- - «**dati biometrici**»: i 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 relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

## Principali figure soggettive nel trattamento dei dati

**Titolare**

*Soggetto che determina finalità e mezzi del trattamento dei dati personali*

**Responsabile**

*Soggetto che tratta i dati per conto del titolare*

*(es.: un outsourcer o fornitore di servizi informatici)*

Non c'è una definizione formale di «**incaricati**», ma si fa comunque riferimento alle «**persone autorizzate**» al trattamento dei dati personali sotto l'autorità del titolare o del responsabile del trattamento

## RESPONSABILITÀ DEL TITOLARE DEL TRATTAMENTO *(art. 24 GDPR)*

Tenuto conto della **natura,** dell'**ambito di applicazione**, del **contesto** e delle **finalità** del trattamento, nonché dei **rischi aventi probabilità e gravità diverse** per i diritti e le libertà delle persone fisiche [**approccio basato sul rischio**]

-il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate** per **garantire**, ed **essere in grado di dimostrare**, che il trattamento è effettuato **conformemente** al GDPR

-tali misure sono **riesaminate e aggiornate qualora necessario**

Se ciò è proporzionato rispetto alle attività di trattamento, le predette misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

L'adesione ai codici di condotta e a meccanismi di certificazione può essere utilizzata come elemento per dimostrare il rispetto (compliance) degli obblighi del titolare del trattamento


Avv. Giovanni Guerra

## RESPONSABILE DEL TRATTAMENTO

Art. 4.8) – Definizione di **Responsabile**

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

Differenze con l'attuale normativa italiana: da rivedere la figura del **responsabile** «**interno**» del trattamento


Avv. Giovanni Guerra

## Outsourcing dei servizi: responsabile del trattamento (art. 28)

Il titolare del trattamento 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 GDPR e garantisca la tutela dei diritti dell'interessato.

**I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto** (o da altro atto giuridico a norma del diritto europeo o nazionale), 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.

## Contratto con il Responsabile (art. 28.3)

Il contratto 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;

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 di sicurezza richieste dal GDPR (art. 32);

d) rispetti le condizioni per ricorrere a un altro responsabile del trattamento;

# Contratto con il Responsabile (art. 28.3)

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;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 GDPR, 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 europeo o nazionale 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.

## GESTIONE DEGLI ULTERIORI RESPONSABILI (c.d. subfornitori)

**Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento** *(art. 28. 2)*

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.

## GESTIONE DEGLI ULTERIORI RESPONSABILI

Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, **su tale altro responsabile del trattamento sono imposti, mediante un contratto** (o un altro atto giuridico), **gli stessi obblighi in materia di protezione dei dati contenuti nel contratto** o in altro atto giuridico tra il titolare e il responsabile del trattamento, **prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR**.

**Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.** *(art. 28. 4).*

# Incaricati = persone autorizzate al trattamento

**Art. 29 - Trattamento sotto l'autorità del titolare e del responsabile del trattamento**

Il responsabile del trattamento, o **chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Il contratto tra il titolare ed il responsabile del trattamento deve garantire che **le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza (**Art. 28.2.b) GDPR)

***DIFFERENZE CON LE ATTUALI MODALITA' DI NOMINA DEGLI INCARICATI***

***LA FIGURA DELL'AMMINISTRATORE DI SISTEMA: POSSIBILI EVOLUZIONI***

## Conferma dei principi generali (art. 5 GDPR)

I dati personali sono:

a)trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);

b)raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; … («**limitazione della finalità**»);

c)adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);

d)esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);




Avv. Giovanni Guerra

# Principi generali (art. 5)

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; … («**limitazione della conservazione**»);

f) 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**»).

**2. Il titolare del trattamento** (ossia la banca) **è competente per il rispetto dei principi sopra indicati e in grado di comprovarlo («responsabilizzazione»** o **«accountability»).**

## Nuovo approccio nella gestione degli adempimenti privacy

**ACCOUNTABILITY:** Il titolare del trattamento è **COMPETENTE PER IL RISPETTO («COMPLIANCE»)** dei principi generali applicabili al trattamento dei dati personali **E IN GRADO DI COMPROVARLO!**

**RISK-BASED APPROACH**: adottare **adeguate misure organizzative e tecniche** tenendo conto della **natura e finalità del trattamento**, nonché dei **rischi aventi probabilità e gravità diverse** per i diritti e le libertà delle persone fisiche.

I rischi possono derivare da trattamenti di dati personali suscettibili di cagionare **un danno fisico, materiale o immateriale**, in particolare, se il trattamento può comportare **discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati** personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti o venga loro impedito l'esercizio del controllo sui dati personali; in caso di categorie particolari di dati, dati penali, minori, profilazione, larga scala


Avv. Giovanni Guerra

## PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE (*PRIVACY BY DESIGN)*

Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,

- **sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso**
- **il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione**, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.


Avv. Giovanni Guerra

## PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA (*PRIVACY BY DEFAULT*)

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.

Tale obbligo vale per la **quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità**.

In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

L'adesione ad un **meccanismo di certificazione** può essere utilizzato come elemento per dimostrare la conformità ai requisiti di privacy by design e by default.

## Registri delle categorie di attività di trattamento (art. 30)

Ogni titolare del trattamento tiene un registro delle attività di trattamento dei dati personali effettuate sotto la propria responsabilità.

Ciascun responsabile del trattamento tiene un registro delle categorie di attività di trattamento dei dati personali svolte per conto di un titolare del trattamento.

I registri sono tenuti in forma scritta, anche in formato elettronico e, su richiesta, messi a disposizione dell'autorità di controllo.

Esclusione degli obblighi per imprese con meno di 250 dipendenti, a meno di trattamenti rischiosi o di dati particolari e penali.

## REGISTRO DEL TITOLARE DEL TRATTAMENTO

Nome e dati di contatto del titolare, del contitolare, del rappresentante del titolare e del DPO

Finalità del trattamento

Descrizione delle categorie di interessati e delle categorie di dati personali

Categorie di destinatari a cui i dati personali sono stati o saranno comunicati

Trasferimenti di dati verso un paese terzo o un'organizzazione internazionale

Termini ultimi, ove possibile, previsti per la cancellazione delle diverse categorie di dati

Descrizione generale delle misure tecniche e organizzative di sicurezza

# Designazione del DPO nei soggetti pubblici - *art 37*

1. Titolare e Responsabile designano **sistematicamente** un responsabile della protezione dei dati (DPO) ogniqualvolta:

a) il **trattamento è effettuato da un'autorità pubblica o da un organismo pubblico**, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

Non c'è obbligo per organismi privati incaricati di funzioni pubbliche o che esercitano poteri pubblici, ma consigliato come buona prassi da seguire …

Per definizione di «organismo pubblico» …


Avv. Giovanni Guerra

# Definizione di «organismo pubblico» (art. 2 direttiva 2003/98/CE sul riutilizzo dell'informazione nel settore pubblico)

1) "**ente pubblico**", le autorità statali, regionali o locali, gli organismi di diritto pubblico e le associazioni formate da una o più di tali autorità oppure da uno o più di tali organismi di diritto pubblico;

2) "**organismo di diritto pubblico**", qualsiasi organismo:

a) istituito per soddisfare specificatamente bisogni d'interesse generale aventi carattere non industriale o commerciale; e

b) dotato di personalità giuridica; e

c) la cui attività è finanziata in modo maggioritario dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico, oppure la cui gestione è soggetta al controllo di questi ultimi, oppure il cui organo d'amministrazione, di direzione o di vigilanza è costituito da membri più della metà dei quali è designata dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico;

# Definizione di «organismo pubblico» (Nuove Faq sul Responsabile della Protezione dei dati (RPD o DPO) in ambito pubblico pubblicate il 15.12.2017 sul sito del Garante per la Protezione dei Dati Personali)

«Allo stato, in ambito pubblico, devono ritenersi tenuti alla designazione di un DPO i soggetti che oggi ricadono nell'ambito di applicazione degli artt. 18 - 22 del Codice Privacy, che stabiliscono le regole generali per i trattamenti effettuati dai soggetti pubblici (ad esempio, le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc.).

Occorre, comunque, considerare che, nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), può risultare comunque fortemente raccomandato, ancorché non obbligatorio, procedere alla designazione di un DPO. In ogni caso, qualora si proceda alla designazione di un DPO su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i DPO designati in via obbligatoria».

# Designazione del DPO (art. 37 GDPR)

Il Titolare e il Responsabile designano **sistematicamente** un Responsabile della Protezione dei Dati RPD(Data Protection Officer - DPO) ogniqualvolta:

…

- **- 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**; oppure
- **- le attività principali** del titolare del trattamento o del responsabile del trattamento consistono **nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati**

# Requisiti del DPO (art. 37 GDPR)

RPD è designato in funzione delle **qualità professionali**, in particolare della **conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati**, e della **capacità di assolvere i compiti**

Vanno valutate le sue **competenze ed esperienze specifiche, e n**on sono richieste attestazioni formali sul possesso delle conoscenze o l'iscrizione ad appositi albi professionali **(***v. newsletter Gar. 15.09.2017***).**

RPD può essere:

- un **dipendente** del titolare del trattamento o del responsabile del trattamento oppure
- **assolvere i suoi compiti in base a un contratto di servizi**

Il titolare del trattamento o il responsabile del trattamento **pubblica i dati di contatto** del RPD e li comunica all'autorità di controllo.

# Posizione del DPO (Art. 38 GDPR)

deve essere **tempestivamente e adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali.

deve essere **sostenuto nell'esecuzione dei suoi compiti** e gli devono essere fornite le **risorse necessarie** per adempiere ai propri compiti nonché l'accesso ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica

**non deve ricevere alcuna istruzione** per quanto riguarda l'esecuzione dei propri compiti (indipendenza e autonomia)

**non può essere rimosso o penalizzato** per l'adempimento dei propri compiti (ma non per altre motivazioni!)

**riferisce direttamente al vertice gerarchico** del titolare del trattamento o del responsabile del trattamento

è **tenuto al segreto o alla riservatezza** in merito all'adempimento dei propri compiti, in conformità del diritto europeo o nazionale

può svolgere altri compiti e funzioni che **non diano adito a un conflitto di interessi**.

## Compiti del DPO (Art. 39)

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

b) **sorvegliare l'osservanza del GDPR**, 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;

## Compiti del DPO (Art. 39)

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

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

Gli interessati possono contattare il RPD per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.

# SICUREZZA DEL TRATTAMENTO *(art. 32)*

Secondo un approccio basato sul rischio (inclusa una valutazione dello stato dell'arte e dei costi di attuazione), il titolare e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

**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**.


Avv. Giovanni Guerra

# SUPERAMENTO DELLE MISURE MINIME DI SICUREZZA

Il Garante, nella recente *Guida all'applicazione del Regolamento*, ha indicato che **l'art. 32 contiene una «*lista aperta e non esaustiva*» di misure di sicurezza** e che, **dopo il 25 maggio 2018, *non potranno sussistere obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del Regolamento.***

***Rapporto con altre misure indicate dal Garante come quelle relative al tracciamento degli accessi e delle operazioni***




Avv. Giovanni Guerra

# NOTIFICA DELLE VIOLAZIONI DI DATI (*DATA BREACH*)

- In caso di violazione dei dati personali, **il titolare** del trattamento **notifica** la violazione all'autorità di controllo competente **senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza**, **a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche**. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. (art. 33) – *v. linee guida WP 250*

- Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.




Avv. Giovanni Guerra

# COMUNICAZIONE DEL DATA BREACH ALL'INTERESSATO (*art. 34)*

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, **il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo**.

**NON È RICHIESTA LA COMUNICAZIONE ALL'INTERESSATO** se:

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




Avv. Giovanni Guerra

## Valutazione d’impatto per i trattamenti di dati ad elevato rischio (art. 35)

Quando un tipo di trattamento, allorché prevede in particolare **l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali** (*Data Protection Impact Assessment - DPIA*).

E’ richiesta in particolare nei seguenti casi :

- una valutazione sistematica e globale di aspetti personali, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.




Avv. Giovanni Guerra

# Valutazione d’impatto sulla protezione dei dati

- L'autorità di controllo redige e rende pubblico un **elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto** sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al Comitato Europeo Protezione Dati (*European Data Protection Board - EDPB*).

- L'autorità di controllo può inoltre redigere e rendere pubblico un **elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto** sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

- Procedura fondamentale per **garantire e dimostrare la *compliance*** al GDPR per i trattamenti di dati ad alto rischio - V. *linee guida WP 248*

In caso di mancata determinazione di misure sufficienti per la riduzione di rischi elevati, c’è l’obbligo di **consultazione preventiva dell’Autorità di controllo** (art. 36 GDPR)




Avv. Giovanni Guerra

# I presupposti di liceità del trattamento dei dati

Art. 6 – liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

- a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- c) il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;
- d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- e) il trattamento è necessario per **l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento;
- f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. [*non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti*]

# Base giuridica per l'esecuzione di un compito di pubblico interesse o connesso all'esercizio di pubblici poteri

**Articolo 6 - Liceità del trattamento**

3. La base su cui si fonda il trattamento dei dati di cui al par. 1, lettere c) ed e), **deve essere stabilita: a) dal diritto dell'Unione; o b) dal diritto dello Stato membro cui è** soggetto il titolare del trattamento.

La **finalità del trattamento è determinata in tale base giuridica** o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito




Avv. Giovanni Guerra

# Presupposti di liceità del trattamento (art. 6)

**Articolo 6 - Liceità del trattamento**

2. **Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.**

# Disposizioni relative a specifiche situazioni di trattamento (capo IX)

- Libertà d'espressione e d'informazione
- Accesso del pubblico a documenti ufficiali
- Numero di identificazione nazionale
- Rapporti di lavoro
- Archiviazione nel pubblico interesse, ricerca scientifica, storica e a fini statistici
- Obblighi segretezza
- Chiese e associazioni religiose




Avv. Giovanni Guerra

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

Principio di base:

È vietato trattare dati personali:

- che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale
- 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

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

Eccezioni:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche

   i. salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che 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 i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;



Avv. Giovanni Guerra

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

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

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

e) il trattamento è necessario per **finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

- Se i dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

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

i) il trattamento è necessario **per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici**, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

**Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute**

## Trattamento dei dati personali relativi a condanne penali e reati (art. 10)

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati

Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

## INFORMAZIONI, COMUNICAZIONI E MODALITÀ TRASPARENTI PER ESERCIZIO DIRITTI DELL'INTERESSATO (art. 12)

Il titolare del trattamento **adotta misure appropriate** per fornire all'interessato l'**informativa** per dati raccolti presso l'interessato e non (artt. 13 e 14) **in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro,** in particolare nel caso di informazioni destinate specificamente ai minori

Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici - se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato

Le informazioni da fornire agli interessati (informativa) possono essere fornite 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 sono leggibili da dispositivo automatico.

Le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate saranno definite con atti delegati della Commissione UE


Avv. Giovanni Guerra

## AGGIORNAMENTO DELLE INFORMATIVE PRIVACY (art. 13)

Oltre ai nuovi riferimenti normativi, vi sono alcuni, nuovi elementi da aggiungere rispetto a quelli attuali che restano confermati**:**

- **dati di contatto del responsabile** protezione dati, ove applicabile;
- **base giuridica** del trattamento e **legittimi interessi** perseguiti dal titolare o da terzi;
- **trasferimento dati personali extra UE** e garanzie appropriate
- **periodo di conservazione dei dati** (o criteri per determinare tale periodo);
- **diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- **diritto di proporre reclamo** a un'autorità di controllo;
- 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;
- l'esistenza di un **processo decisionale automatizzato, compresa la profilazione**.




Avv. Giovanni Guerra

# RAFFORZAMENTO DEI DIRITTI DEGLI INTERESSATI (artt. 15 – 22)

- Diritto di **accesso** ai dati;
- Diritto di rettifica ed integrazione dei dati inesatti ed incompleti
- Diritto di **cancellazione o** diritto all'**oblio***;*
- Diritto di **limitazione di trattamento** contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- Obbligo notifica rettifica, cancellazione o limitazione del trattamento;
- Diritto alla **portabilità** dei dati
- Diritto di opposizione per motivi legittimi e al marketing
- **Processo decisionale automatizzato e profilazione**

**Riscontro entro 1 mese o, in base a complessità delle richieste, altri 2 mesi**

Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti , oppure rifiutare di soddisfare la richiesta


Avv. Giovanni Guerra

## DIRITTO ALLA CANCELLAZIONE («DIRITTO ALL'OBLIO» - (*art. 17*)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, se i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati, se i dati personali sono stati trattati illecitamente, ecc.

Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato 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.

Comunque non si applica se i dati sono trattati per l'adempimento di un obbligo legale, per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, ecc.


Avv. Giovanni Guerra

## DIRITTO DI LIMITAZIONE DEL TRATTAMENTO (*art. 18*)

«**Limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro (art. 4.3) GDPR)

L'interessato ha il diritto di ottenere dal titolare del trattamento la **limitazione del trattamento** quando ricorre una delle seguenti ipotesi:

l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

l'interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

## DIRITTO ALLA PORTABILITÀ DEI DATI (*art. 20*)

L'interessato ha il **diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti** a un titolare del trattamento e ha **il diritto di trasmettere tali dati a un altro titolare** del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti **qualora il trattamento si basi sul consenso, o su un contratto, e il trattamento sia effettuato con mezzi automatizzati**.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il **diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro**, se tecnicamente fattibile.

l diritto alla portabilità dei dati non deve ledere i diritti e le libertà altrui.

V. *Linee guida WP 242 - impatti tecnologici*




Avv. Giovanni Guerra

# Profilazione e processi decisionali automatizzati nel GDPR (art. 22)

L'interessato ha il **diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona**.

Tale diritto non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

c) si basi sul consenso esplicito dell'interessato.

Il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione – V. *linee guida WP 251*

## Condizioni e garanzie per i trasferimenti di dati all'estero *(extra UE)*

**Il trasferimento di dati è ammesso solo** :

-verso **Paesi Terzi che garantiscono un livello di protezione adeguato in base alle decisioni della Commissione europea**: elenco pubblicato *on line* (es.: Svizzera, Canada, Israele, recente accordo con USA-UE su c.d. Scudo Privacy)

-se esistono garanzie adeguate come **clausole contrattuali standard, norme vincolanti d'impresa (BCR), adesione a codici di condotta o certificazioni privacy** (con impegno ad applicare nel proprio Paese)

***Le passate decisioni della Commissione ed autorizzazioni del Garante restano comunque in vigore finché non modificate, sostituite o abrogate***

-se, in assenza delle precedenti, ricorrano **ulteriori condizioni, come il consenso dell'interessato, l'esecuzione di obblighi contrattuali**, ecc.

***Attenzione nei servizi in cloud a verificare l'ubicazione dei data center o server (se in Paesi dentro o fuori la UE)***


Avv. Giovanni Guerra

## CODICI DI CONDOTTA (art. 40)

Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente Regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del GDPR

*Da condizioni di liceità del trattamento a **best practices** per dimostrare la compliance al GDPR!*

**Monitoraggio dei codici di condotta approvati (art. 41).**

Fatti salvi i compiti e i poteri dell'autorità di controllo competente, il controllo della conformità con un codice di condotta può essere effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente.


Avv. Giovanni Guerra

# Certificazioni privacy (art. 42 GDPR)

**Viene prevista dal GDPR l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al GDPR** dei trattamenti effettuati dai titolari e dai responsabili del trattamento.

La certificazione è volontaria e accessibile tramite una procedura trasparente ed è rilasciata al titolare o al responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti

La certificazione non riduce la responsabilità del titolare o del responsabile del trattamento riguardo alla conformità al GDPR e lascia impregiudicati i compiti e i poteri delle autorità di controllo

## Modalità di rilascio delle certificazioni privacy

I soggetti legittimati al rilascio della certificazione sono l'Autorità di controllo competente (per l'Italia, il Garante per la protezione dei dati personali) oppure gli organismi di certificazione.

Tali organismi, in base al GDPR, possono essere accreditati dall'Autorità di controllo competente o dall'Organismo nazionale di accreditamento (per l'Italia, ACCREDIA), o da entrambi (cfr. art. 43, paragrafo 1, del regolamento), secondo i requisiti previsti dalla norma UNI CEI EN ISO/IEC 17065:2012 (che stabilisce i requisiti per gli organismi di certificazione di prodotti, processi e servizi) integrata da "requisiti aggiuntivi" che devono essere stabiliti dall'Autorità di controllo competente.

*Il Garante Privacy e ACCREDIA hanno richiamano l'attenzione sulla necessità di attendere la definizione di criteri e requisiti comuni per la conformità delle certificazioni in materia di protezione dati al Regolamento UE 2016/679 (v. comunicato stampa 18.07.17 del Garante ed Accredia)*

# Autorità di controllo (art. 55-59)

Ogni autorità di controllo (come il ns. Garante) è competente **nel territorio del rispettivo Stato membro ad eseguire i relativi compiti di sorveglianza, consulenza, trattazione reclami, ecc. e ad esercitare poteri di indagine, correttivi (inclusi quelli sanzionatori), autorizzativi e consultivi**

L'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare /responsabile del trattamento è competente ad agire in qualità di **autorità di controllo capofila** per i trattamenti transfrontalieri effettuati dal suddetto titolare o responsabile del trattamento, secondo la **procedura di cooperazione** tra autorità (art. 60 – *v. Linee guida WP244*)

Le autorità si prestano assistenza reciproca (art. 61) e se del caso conducono operazioni congiunte (art. 62)


Avv. Giovanni Guerra

## Coerenza del GDPR e Comitato europeo protezione dati

Al fine di contribuire all'applicazione coerente del GDPR in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il **meccanismo di coerenza** (art. 63)

In questo senso sono previsti inoltre:

-Parere del Comitato europeo per la protezione dei dati (art. 64)

-Composizione delle controversie da parte del Comitato (art. 65)

-Procedura d'urgenza (art. 66)

-Scambio di informazioni (art. 67)

Il nuovo **Comitato europeo per la protezione dei dati** (EDPB): organismo della UE dotato di personalità giuridica, composto dai presidenti/ rappresentanti di ogni autorità di controllo e del **Garante europeo protezione dati** (EDPS). Ha compiti di sorveglianza e consultivi e adotta linee guida, raccomandazioni e best practices in diversi ambiti (art. 68-76)

## Reclamo all'autorità di controllo (art. 77)

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il GDPR ha il **diritto di proporre reclamo a un'autorità di controllo**, segnatamente

- **nello Stato membro in cui risiede abitualmente**,
- **Lavora**
- oppure del luogo **ove si è verificata la presunta violazione.**

L'autorità di controllo a cui è stato proposto il reclamo **informa il reclamante dello stato o dell'esito del reclamo**, compresa la possibilità di un ricorso giurisdizionale.

*Un piccolo cambiamento rispetto alle attuali 3 forme di tutela amministrativa dell'interessato previste dal Codice privacy (reclami, segnalazioni e ricorsi al Garante)!*

## Ricorsi giurisdizionali vs. autorità di controllo oppure titolare/ responsabile

Fatto salvo ogni altro ricorso amministrativo o extragiudiziale,

- ogni persona fisica o giuridica ha il **diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda**, dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita **(art. 78)**
- ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del GDPR siano stati violati a seguito di un trattamento: le azioni nei confronti del titolare o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente **(art. 79)**

**In linea con le attuali previsioni del Codice privacy!**

**Possibile previsione di class action (art. 80)!**

## Diritto al risarcimento e responsabilità (art. 82)

**Chiunque subisca un danno materiale o immateriale** causato da una violazione del presente regolamento **ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento**.

Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il GDPR. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del GDPR specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Ogni titolare o responsabile coinvolti nel trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

***Confermata la possibilità per il cliente di chiedere anche il risarcimento dei danni non patrimoniali!***

## Sanzioni amministrative pecuniarie (art. 83)

**Sanzioni amministrative pecuniarie fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per la violazione, tra le altre, delle seguenti disposizioni:**

**8** - Consenso dei minori in relazione ai servizi della società dell'informazione

**25** - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

**28** - Responsabile del trattamento

**29** - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

**30** - Registri delle attività di trattamento

**32** - Sicurezza del trattamento

**33** - Notifica di una violazione dei dati personali all'autorità di controllo

**34** - Comunicazione di una violazione dei dati personali all'interessato

**35** - Valutazione d'impatto sulla protezione dei dati

**36** - Consultazione preventiva

**37** – Designazione, posizione e compiti del responsabile della protezione dei dati (DPO)

**42** - Certificazione

## sanzioni amministrative pecuniarie (art. 83)

Sanzioni amministrative pecuniarie **fino a 20.000.000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore, per violazione delle seguenti disposizioni:

- i **principi di base del trattamento**, comprese le condizioni relative al consenso;
- **i diritti degli interessati**;
- i **trasferimenti di dati personali** a un destinatario in un paese terzo;
- l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo

*V. WP 253 - Necessità di un allineamento della normativa nazionale!*

## Criteri di applicazione delle sanzioni pecuniarie

Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la **natura**, la **gravità** e la **durata** della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere **doloso o colposo** della violazione;

c) le **misure adottate** dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il **grado di responsabilità** del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali **precedenti violazioni** pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

## Criteri di applicazione delle sanzioni pecuniarie

f) il **grado di cooperazione con l'autorità di controllo** al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le **categorie di dati personali interessate** dalla violazione;
h) la **maniera in cui l'autorità di controllo ha preso conoscenza della violazione**, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i) **qualora siano stati precedentemente disposti provvedimenti** nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il **rispetto di tali provvedimenti**;
j) **l'adesione ai codici di condotta o ai meccanismi di certificazione** approvati;
k) eventuali **altri fattori aggravanti o attenuanti** applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

## Sanzioni penali (art. 84)

**Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del GDPR**, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente Regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente Regolamento. **Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del *ne bis in idem* quale interpretato dalla Corte di giustizia (considerando 149)**

Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del GDPR in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

*adeguamento della normativa nazionale (disposizioni da notificare alla Commissione europea)*

# DOMANDE?

## Grazie per la Vostra attenzione!