



# REGOLAMENTO N. 679/2016

## REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Ore 15,45 - dott. Michele Gallo - Associato e CEO GCERTI ITALY - dott. Sandro Sanna - Privacy Specialist

- Categorie particolari di dati (sensibili e giudiziari);
- Informativa e consenso;
- Titolare del trattamento/obblighi e responsabilità;
- Responsabile del trattamento / Incaricato al trattamento;
- Documentazione obbligatoria, tipologia e modalità compilazione;
- Data Protection Officer.



## Soggetti: **TITOLARE, RESPONSABILE, RDP**

**Titolare:** è la persona fisica o giuridica, la pubblica amministrazione o qualsiasi altro Ente, associazione od organismo cui competono le scelte di fondo sulle finalità e sulle modalità del trattamento dei dati, anche per ciò che riguarda la sicurezza.

Il titolare del trattamento non è, quindi, chi gestisce i dati, ma **chi decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa.**



# Soggetti: TITOLARE, RESPONSABILE, RPD

## TITOLARE DEL TRATTAMENTO - LE RESPONSABILITÀ

**Il titolare risponde in caso di violazione delle disposizioni del GDPR.**

Se più titolari o responsabili sono coinvolti nello stesso trattamento e sono responsabili del danno causato, ne rispondono in solido per l'intero danno, al fine di garantire l'intero risarcimento.

Ovviamente chi paga l'intera somma avrà diritto di regresso nei confronti degli altri responsabili per la quota.

Il titolare e il responsabile saranno esonerati da responsabilità se dimostrano che l'evento dannoso non è imputabile alla loro condotta, o se dimostrano di aver adottato tutte le misure idonee per evitare il danno stesso



# Soggetti: TITOLARE, RESPONSABILE, RDP

## Responsabile Trattamento dei Dati:

Nominato con un vero e proprio contratto/incarico è la persona fisica, giuridica, pubblica amministrazione o ente **che elabora i dati personali per conto del titolare del trattamento**

Il responsabile del trattamento dovrà avere innanzitutto una **competenza qualificata** (ad esempio, frequentazione di corsi di aggiornamento -in tal senso si può fare riferimento alle norme UNI 11697:2017), dovendo garantire una conoscenza specialistica della materia, e l'attuazione delle misure tecniche e organizzative in grado di soddisfare i requisiti stabiliti dal regolamento europeo. Inoltre dovrà garantire una particolare affidabilità, un requisito fondato su aspetti etici e deontologici (ad esempio, l'assenza di condanne penali).



# Soggetti: TITOLARE, RESPONSABILE, RDP

## Responsabile Trattamento dei Dati **QUALI SONO I COMPITI?**

- a) tratta i dati personali soltanto su istruzione documentata del titolare del trattamento;
- b) garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- c) adotta tutte le misure richieste ai sensi dell'articolo 32 ( sicurezza dei dati personali );
- d) tenendo conto della natura del trattamento, assiste il titolare del trattamento con misure tecniche e organizzative adeguate, alla tipologia di trattamento richiesto;
- e) assiste il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36;
- f) su scelta del titolare del trattamento, cancella o gli restituisce tutti i dati personali dopo che è terminata la prestazione.



## Soggetti: **TITOLARE, RESPONSABILE, RDP**

Non esiste un chiaro indirizzo se il responsabile del trattamento deve essere interno o esterno,  
è importante sottolineare  
la **competenza qualificata** per il ruolo che ricopre.



## Soggetti: TITOLARE, RESPONSABILE, RDP

### **SUB - Responsabile Trattamento dei Dati:**

E' consentita la nomina di **sub-responsabili del trattamento da parte di un responsabile**, per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile"



## Soggetti: **TITOLARE, RESPONSABILE, RDP**

**DPO ( Data Protection Officer ) / RDP ( Resp. Protezione Dati )**

Responsabile per la protezione dei dati: In base al RGPD, non solo i titolari, ma anche i responsabili del trattamento sono tenuti a nominare un Data Protection Officer.

La **designazione del DPO è obbligatoria** per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche, ovvero trattino su larga scala categorie particolari di dati personali.





# Soggetti: **TITOLARE, RESPONSABILE, RDP**

## **DPO / RDP QUALI SONO I REQUISITI?**

1. possedere un'adeguata conoscenza della normativa;
2. adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il RPD non può essere un soggetto che decide sulle finalità o sugli strumenti del trattamento di dati personali;
3. operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (RPD/DPO esterno).

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.



# Soggetti: TITOLARE, RESPONSABILE, RDP

## DPO / RDP IN QUALI CASI E' PREVISTO?

Dovranno designare obbligatoriamente un RPD:

- a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
- b) tutti i soggetti la cui attività principale **richiede il monitoraggio regolare e sistematico degli interessati su larga scala**;
- c) tutti i soggetti la cui attività principale **consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici**.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD, è comunque possibile una nomina su base volontaria.

Un gruppo di imprese o soggetti pubblici possono nominare un unico RPD.



# Soggetti: **TITOLARE, RESPONSABILE, RDP**

## **DPO / RDP QUALI SONO I COMPITI?**

- a) sorvegliare l'osservanza del regolamento;
- b) collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
- c) informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- d) cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
- e) supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento .



Soggetti: **TITOLARE, RESPONSABILE, RDP**

## **COSA SI INTENDE CON LARGA SCALA?**

1. Il territorio geografico – quanto ampio è il territorio all'interno del quale effettuo il trattamento;
2. Il volume e la tipologia dei dati trattati;
3. La percentuale di interessati sul totale di una popolazione di riferimento;
4. La durata del trattamento.

Qualora un titolare definisca che i propri trattamenti non sono da considerare su Larga Scala, è tenuto a motivare la propria scelta




Soggetti: **TITOLARE, RESPONSABILE, RDP**

**DOTT. SANDRO SANNA**  
Privacy Specialist



## Dato Personale


- **Dato personale:** si intende qualsiasi dato che consente di inquadrare una determinata persona fisica, identificata o identificabile, anche indirettamente, oppure qualsiasi informazione (es. codice fiscale, impronta digitale, traffico telefonico, immagine, voce) riguardanti una persona la cui identità può comunque essere accertata mediante informazioni supplementari
- **Interessato:** La persona a cui si riferiscono i dati soggetti al trattamento si definisce "interessato".



## Dato Personale > Categorie di dati

**Dati identificativi:** Sono quei dati che consentono l'identificazione diretta dell'interessato esempio:

nome e cognome / indirizzo di casa / indirizzo email / numero identificativo nazionale / numero di passaporto / indirizzo IP (quando collegato ad altri dati) / numero di targa del veicolo / numero di patente / volto, impronte digitali o calligrafia / numeri di carta di credito / identità digitale / data di nascita / luogo di nascita / informazioni genetiche / numero di telefono / account name o nickname.




# Dato Personale > Categorie di dati

## **Dati soggetti a trattamento speciale (dati sensibili):**

L'articolo 9 del GDPR sancisce un generale divieto di trattare alcuni tipi di dati, cioè quelli che rivelino:

- **Biometrici** (*intesi a identificare in modo univoco una persona fisica (ad esempio, un gruppo di fotografie caricate online, oppure negli aeroporti dove l'immagine dell'individuo viene scansionata per identificarlo)*);
- Relativi alla Salute, alla Vita Sessuale o all'orientamento sessuale
- Relativi ai dati Giudiziari (*rivelano l'esistenza di provvedimenti penali*)
- L'origine razziale o etnica / le opinioni politiche / le convinzioni religiose o filosofiche / l'appartenenza sindacale / genetici





# Dato Personale > Categorie di dati

Questo tipo di dati possono essere trattati solo nei casi espressamente indicati (alcuni esempi):

- a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali;
- b) il trattamento è necessario per assolvere gli obblighi in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato da norme giuridiche o contratti collettivi;
- c) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- d) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro;
- e) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica;

Inoltre, i dati personali di cui all'articolo 9 del GDPR possono essere trattati se il trattamento avviene ad opera o sotto la responsabilità di un professionista soggetto al segreto professionale



# GDPR: alcune delle principali novità

## REGISTRO DEI TRATTAMENTI [vedi esempio](#)

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30.

Ha lo scopo generare un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.



# GDPR: alcune delle principali novità

## REGISTRO DEI TRATTAMENTI \_ **RACCOMANDAZIONI**

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali.

Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta.



# GDPR: alcune delle principali novità

## Valutazione di impatto del trattamento ( D.P.I.A )

E' un **onere posto direttamente a carico del titolare del trattamento**, col quale si assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali, imponendo al titolare l'onere di una valutazione preventiva delle conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati. Il responsabile del trattamento deve assistere il titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

La valutazione del rischio, da realizzare per ogni singolo trattamento, dovrà portare il titolare a decidere in autonomia se sussistono rischi elevati inerenti il trattamento, in assenza dei quali potrà procedere oltre. Se invece ritenesse sussistenti detti rischi, dovrà individuare le misure specifiche richieste per attenuare o eliminare il rischio (che non sono indicate dal regolamento).



## GDPR: alcune delle principali novità

### **D.P.I.A – CONTENUTI MINIMI**

La valutazione di impatto deve contenere almeno:

- la descrizione sistematica dei trattamenti previsti, la finalità del trattamento, compreso l'interesse legittimo perseguito dal titolare;
- la valutazione dei rischi;
- le misure previste per affrontare i rischi, incluse le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al regolamento.



## GDPR: alcune delle principali novità

### **DPIA - PIA tool**

Il CNIL (autorità di controllo francese) ha messo a disposizione un software open source per la valutazione di impatto sia nella versione standalone (da scaricare sul computer) che in quella online. Anche il Garante italiano segnala questo software come tool per realizzare la valutazione.



GDPR: alcune delle principali novità

## **DIRITTO ALL'OBLIO - Articolo 17**

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:



## GDPR: alcune delle principali novità

### **DIRITTO ALL'OBLIO - Articolo 17**

- a) I dati personali non sono più necessari;
- b) Revoca del consenso e/o Opposizione al trattamento;
- d) I dati personali sono stati trattati illecitamente;
- e) I dati personali devono essere cancellati per adempiere un obbligo legale;

Il titolare del trattamento, se ha reso pubblici dati personali è obbligato, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione





# GDPR: alcune delle principali novità

## **DATA BREACH**

Per violazione dei dati personali (data breach) si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati da aziende o pubbliche amministrazioni.

Un data breach, quindi, non è solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un notebook di un dipendente). Il nuovo regolamento generale europeo prescrive specifici adempimenti nel caso di una violazione di dati personali.



# GDPR: alcune delle principali novità

## DATA BREACH – CASI DI NOTIFICA

Spetta al responsabile del trattamento avvertire il titolare dell'avvenuta violazione dei dati. Il titolare dovrà, a quel punto, notificare l'evento all'autorità di controllo.

La normativa (articolo 33 GDPR) prevede l'obbligo di comunicare alle autorità di controllo la violazione dei dati, ma solo se il titolare ritiene probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati. Tutti i titolari del trattamento sono soggetti alla norma. La notifica dovrà avvenire entro 72 ore e comunque "senza ingiustificato ritardo".



## GDPR: alcune delle principali novità

### **DATA BREACH – NOTIFICA CHI E' OBBLIGATO**

I fornitori di servizi di comunicazione elettronica sono oggi tenuti a comunicare al Garante le violazioni dei dati personali (Data breach) che detengono nell'ambito delle proprie strutture.

*In caso di mancato rispetto delle procedure di notifica della violazione si applica la sanzione amministrativa fino ad un importo di 10 milioni di euro oppure il 2% del fatturato dell'intera società*



# GDPR: alcune delle principali novità

## **PRIVACY BY DESIGN E BY DEFAULT**

- La privacy by design richiede che il TITOLARE adotti e attui misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati;
- La privacy by default presuppone, invece, nella modalità operativa del trattamento, misure e tecniche che, per impostazione predefinita, garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento



# GDPR: alcune delle principali novità

## **SANZIONI**

le sanzioni previste nel regolamento siano di importi molti elevati fino al 20 milioni di euro o il 4% del fattura mondiale annuale.

Non è stato comunicato da parte dell'Autorità il rinvio all'applicazione delle sanzioni



# GDPR: alcune delle principali novità

## Q & A

### Grazie per l'attenzione

Relatore:

Michele Gallo | [direzione@gcerti.it](mailto:direzione@gcerti.it) – 3312914314

-----  
Sandro Sanna | privacy specialist