

# REGOLAMENTO UE 679/2016

---

REGOLAMENTO PRIVACY

GDPR

(GENERAL DATA PROTECTION REGULATION)

---

LA NUOVA NORMATIVA PRIVACY TROVA DIRETTA APPLICAZIONE IN ITALIA DAL  
25/05/2018

ED ABROGA DIRETTAMENTE LA VECCHIA NORMATIVA (D.lgs.196/2003)

# OBIETTIVI DEL REGOLAMENTO 676/2016

---



## TUTELA I DATI PERSONALI

QUINDI:

LIMITA LA DIFFUSIONE DEI DATI SENZA CONSENSO

Furto/perdita dati GOOGLE/FACEBOOK

Vendita/trasferimento dati Es. mail tra compagnie dello stesso gruppo a fini pubblicitari

Uso improprio delle informazioni acquisite (es. richiesta preventivo ad hotel e conseguenti continue offerte commerciali)

# CHI E OBBLIGATO?

---

IL REGOLAMENTO PRIVACY SI APPLICA A TUTTE LE AZIENDE E PROFESSIONISTI CHE HANNO ALMENO UNA SEDE NELLA UE E CHE TRATTANO DATI PERSONALI

# COSA DOBBIAMO FARE?

---

DOBBIAMO GESTIRE IL DATO ATTRAVERSO UN'ATTENTA REGOLAMENTAZIONE INTERNA, CHE FA CAPO TITOLARE DEL TRATTAMENTO E/O AL RESPONSABILE DEL TRATTAMENTO (ACCOUNTABILITY)

(ART. 24-26 DEL REGOLAMENTO)

- LA GESTIONE DEL DATO DEVE AVVENIRE TENENDO CONTO DEI PROFILI DI RISCHIO E QUINDI ADOTTANDO LE MISURE TECNICHE E ORGANIZZATIVE ADEGUATE IN MODO DA ATTUARE EFFICACEMENTE I PRINCIPI DI PROTEZIONE DEI DATI E GARANTIRE NEL TRATTAMENTO I REQUISITI DEL REGOLAMENTO E LA TUTELA DEGLI INTERESSATI *cd. privacy by design*
- IL TITOLARE ATTUA LE MISURE ADEGUATE PER GARANTIRE CHE SIANO TRATTATI SOLO I DATI PERSONALI NECESSARI PER CIASCUNA FINALITÀ DEL TRATTAMENTO. OBBLIGO CHE VALE PER LA QUANTITÀ DEI DATI RACCOLTI, LA PORTATA DEL TRATTAMENTO, IL PERIODO DI CONSERVAZIONE E L'ACCESSIBILITÀ DEI DATI STESSI *cd. privacy by default*

(ART. 35-36 DEL REGOLAMENTO)

- VALUTAZIONE D IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI (**DPIA**) ULTERIORE VALUTAZIONE ALLA QUALE SONO OBBLIGATI I TITOLARI CHE DEBBANO INIZIARE UN TRATTAMENTO MOLTO RISCHIOSO PER I DIRITTI E LE LIBERTA DELLE PERSONE FISICHE , PER LA CARATTERISTICHE DEL TRATTAMENTO O DEGLI STRUMENTI ADOTTATI PER ESSO.

# TUTTO CIO IN COSA CONSISTE?

---

- **NOMINA DEL TITOLARE DEL TRATTAMENTO**  
=> NELLE PICCOLE REALTA COINCIDE CON IL TITOLARE D IMPRESA/DI STUDIO
- **NOMINA DEL RESPONSABILE DEL TRATTAMENTO**  
=> DEVE AVVENIRE CON CONTRATTO O ALTRO ATTO GIURIDICO  
=> NELLE PICCOLE REALTA SI CONSIGLIA DI FARLO COINCIDERE CON IL TITOLARE DEL TRATTAMENTO
- **NOMINA DI EVENTUALI INCARICATI AL TRATTAMENTO**  
=> DEVE AVVENIRE CON CONTRATTO (INCARICO) O ALTRO ATTO GIURIDICO  
=> REDIGERE APPOSITO MANSIONARIO

- L'ART 37 PREVEDE ANCHE LA NOMINA DI UNA NUOVA FIGURA:



## IL RESPONSABILE DELLA PROTEZIONE DEI DATI

*RDP/DPO Data Protection Officer*

Dovrà essere obbligatoriamente presente in tutte le aziende dove il trattamento presenti dei rischi specifici (ad esempio aziende che trattino dati sensibili, genetici )

Il RPD/DPO potrà essere un dipendente o un soggetto esterno

REQUISITI: dovrà possedere una conoscenza specialistica della normativa e della prassi in materia di protezione dei dati ed avere la capacità di assolvere ai compiti previsti dall'art.39 del regolamento

## COMPITI:

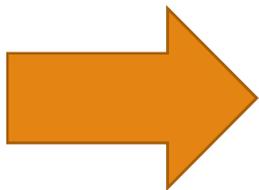
- a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati
- b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- d) cooperare con l'autorità di controllo; e
- e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. ,

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

## IL TITOLARE DEL TRATTAMENTO E IL RESPONSABILE DEL TRATTAMENTO DEVONO

### ISTITUIRE IL REGISTRO DEI TRATTAMENTI (ART 30)

- Si tratta di uno strumento fondamentale al fine del monitoraggio degli adempimenti e della garanzia dei diritti
- non è obbligatorio per il titolare del trattamento che occupi meno di 250 dipendenti
- a meno che:
  - i dati oggetto del trattamento possano presentare un rischio per i diritti e le libertà degli interessati;
  - Il trattamento non sia occasionale o includa dati sensibili, genetici, biometrici giudiziari (art 9 e 10)



IN OGNI CASO E OPPORTUNO REDIGERE IL REGISTRO DEI TRATTAMENTI PER ESSERE IN GRADO DI DIMOSTRARE (A FRONTE DI UN CONTROLLO O DI UNA CONTESTAZIONE) LA TIPOLOGIA DI DATI TRATTATI, LE PROCEDURE E LE GARANZIE MESSE IN ATTO PER IL TITOLARE DEI DATI

## COSA DEVE CONTENERE IL REGISTRO DEI TRATTAMENTI?

### ART. 30

- a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

# I titolari del trattamento dovranno anche:

ART.12-14

---



## **REDIGERE L INFORMATIVA**

ASSOLVE IL PRINCIPIO DI TRASPARENZA EFFETTIVA

FORNISCE ALL'INTERESSATO TUTTE LE INFORMAZIONI E COMUNICAZIONI RELATIVE AL TRATTAMENTO IN FORMA CONCISA TRASPARENTE E FACILMENTE ACCESSIBILE

FORNISCE LE INFORMAZIONI IN MERITO AL TITOLARE DEL TRATTAMENTO

PUO' ESSERE ANCHE ORALE, MA DOVRA' ESSERE PROVATA L'IDENTITA' DELL'INTERESSATO CHE LA RICEVE

COMPRENDE INFORMAZIONI RELATIVE AL PERIODO DI CONSERVAZIONE DEI DATI E MODALITA' TECNICHE ATTRAVERSO CUI QUESTA AVVIENE

DEVE RENDERE EDOTTO L'INTERESSATO IN MERITO A TUTTI I DIRITTI CHE GLI SONO STATI RICONOSCIUTI DAL REGOLAMENTO (ARTT. 15-21) ED ALLE MODALITA' CON CUI RICHIEDERNE L'APPLICAZIONE



## I DIRITTI DELL'INTERESSATO

1. DIRITTO DI ACCESSO AI DATI (ART 15)
2. DIRITTO DI RETTIFICA (ART.16)
3. DIRITTO ALLA CANCELLAZIONE (*CD. DIRITTO ALL OBLIO* ART.17)
4. DIRITTO ALLA PORTABILITA DEI DATI (ART.20)
5. DIRITTO DI OPPOSIZIONE (ART. 21)

# I titolari del trattamento dovranno anche:

ART.7

---



## ACQUISIRE IL CONSENSO

IL CONSENSO è IL FONDAMENTO DELLA LICEITA' DEL TRATTAMENTO

DEVE ESSERE PRESTATO IN MANIERA CHIARA E SEMPLICE, IN FORMA COMPRENSIBILE E ACCESSIBILE

NON è OBBLIGATORIA LA FORMA SCRITTA MA IL TITOLARE è ONERATO DI DIMOSTRARE CHE *L'INTERESSATO HA PRESTATO IL PROPRIO CONSENSO AL TRATTAMENTO DEI DATI PERSONALI*

RESTA VALIDO IL CONSENSO ACQUISITO PRIMA DEL 25/05/2018 SE HA TUTTI I REQUISITI INDICATI DAL REGOLAMENTO, DIVERSAMENTE IL TITOLARE DOVRA ACQUISIRE UN NUOVO CONSENSO CON DATA ANTECEDENTE 25/05/2018.

# Il consenso può essere:

---

## FACOLTATIVO

È considerato lecito quando è necessario :

- nell'ambito di un contratto o ai fini della sua conclusione e/o esecuzione;

Per adempiere ad un obbligo legale

Per la salvaguardia di interessi vitali

Per l'esecuzione di un compito di interesse pubblico

## OBBLIGATORIO

Per tutte quelle situazioni dove non sia facoltativo.

Deve:

rendere chiaro che l'interessato ha acconsentito al trattamento nella piena consapevolezza della misura e delle modalità con le quali in trattamento stesso avviene

Contenere l'indicazione dell'identità del titolare del trattamento dei dati;

Contenere la finalità del trattamento cui sono destinati i dati personali;

Contenere la specifica indicazione del diritto alla revoca del consenso;

Contenere la separazione tra i consensi prestati rispetto ai dati ed alle finalità di trattamento, laddove distinti.



## DATA BREACH (art. 35)

---

I titolari del trattamento devono notificare all'autorità di controllo le violazioni di dati personali senza ingiustificato ritardo e, dove possibile, entro 72 ore dal momento in cui ne sono venuti a conoscenza, a meno che sia improbabile che la violazione 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, dovrà essere corredata dei motivi del ritardo (art.33).



Quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica, con un linguaggio semplice e chiaro, la violazione all'interessato senza ingiustificato ritardo (art.34).

# SANZIONI (Art.83)

---

Individua i criteri che le autorità di controllo devono utilizzare per valutare l'opportunità di irrogare una sanzione amministrativa e l'importo della stessa.

Devono essere in ogni caso:

Effettive

proporzionate

Dissuasive

Il regolamento non fissa un importo specifico per ogni singola violazione, ma solo un massimale.

La violazione delle citate disposizioni è soggetta, a seconda delle diverse tipologie, a sanzioni amministrative pecuniarie fino a 10 o 20 milioni di euro o, per le imprese, fino al 2% o 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.