

**PRIVACY: REGOLAMENTO N. 679/2016**

**NORMATIVA COMUNITARIA E  
NUOVI ADEMPIMENTI IN  
MATERIA DI PRIVACY**

Avv. Guido Palombi



**SALONIA  
ASSOCIATI  
STUDIO LEGALE**

# AMBITO DI APPLICAZIONE E NUOVO APPROCCIO PRATICO

Regolamento UE del Parlamento Europeo e del Consiglio n. 679 del 27 aprile 2016.

1. **Oggetto:** insieme di norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
2. **Ambito di applicazione:** tutti i trattamenti automatizzati e non, ad esclusione di:
  - Attività extra UE.
  - Politica estera e sicurezza comune.
  - Finalità personali o domestiche.
  - Prevenzione, indagine, accertamento reati, sicurezza pubblica.
3. **Ambito di applicazione territoriale:**
  - Stabilimento del Titolare, Titolare o Responsabile del trattamento nell'UE;
  - Titolare e Responsabile fuori UE, qualora gli Interessati siano in UE, in caso di:
    - a. offerta di beni e servizi;
    - b. monitoraggio comportamento degli Interessati.

## ENTRATA IN VIGORE - ABROGAZIONI

### Entrata in vigore:

Il Regolamento **entrerà in vigore** in tutti i Paesi facenti parte dell'UE con effetti a decorrere dal **25 maggio 2018**.

Da tale data, sarà pertanto **necessario adeguare la documentazione Privacy aziendale** al fine di renderla conforme al Regolamento.

### Abrogazioni:

A decorrere dall'entrata in vigore del Regolamento è **abrogata la Direttiva 95/46/CE** avente ad oggetto la tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione degli stessi.

**Resta in vigore la normativa nazionale**, in particolare il D.Lgs. 196/2003 (c.d. Codice in materia di protezione dei dati personali), nella misura in cui non sia in contrasto con le previsioni del Regolamento.

## PRIVACY BY DESIGN, PRIVACY BY DEFAULT

### **Privacy by design:**

Approccio secondo cui le imprese devono predisporre i necessari strumenti di tutela (ad es. pseudonomizzazione) e protezione dei dati personali prima di iniziare il trattamento, con il fine di prevenire, più che correggere in un momento successivo, una possibile violazione. E' necessaria una valutazione del rischio (*risk based approach*) prima di iniziare il trattamento.

### **Privacy by default:**

Le imprese dovrebbero trattare i dati personali nella misura necessaria e sufficiente per le finalità previste del trattamento e per il periodo strettamente necessario a tale scopo. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti.

La **gestione dei dati personali** non è più solo un adempimento ma **diventa un processo aziendale** che deve essere gestito modificando l'organizzazione delle imprese. Si va verso la predisposizione di un **Modello Organizzativo** nella gestione dei dati personali finalizzato a prevenire i rischi di utilizzo illecito dei dati.

## ACCOUNTABILITY

1. E' il principio della “responsabilizzazione” di Titolari e Responsabili nel trattamento dei dati, che si sostanzia nell'adozione di comportamenti volti a dimostrare l'attuazione delle misure e tutele previste dal Regolamento.
2. Il Regolamento intende spostare sui Titolari e Responsabili del trattamento la decisione circa le modalità, le garanzie e i limiti del trattamento.
3. In particolare, il Titolare del trattamento deve mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare il grado di conformità delle attività di trattamento con il Regolamento.
4. Il Titolare può dimostrare che il trattamento dei dati è conforme al Regolamento attraverso l'adozione di misure di sicurezza o l'adesione ai Codici di Condotta o meccanismi di certificazione (la cui predisposizione è fortemente incoraggiata dagli Stati membri, dalle Autorità di controllo e dalle Istituzioni Europee).

# REQUISITI DEL TRATTAMENTO ED INFORMATIVA DA FORNIRE AGLI INTERESSATI

## REQUISITI DI LEGITTIMITA' E CONDIZIONI DI LICEITA' DEL TRATTAMENTO

Il Regolamento individua i requisiti di legittimità del trattamento nella (i) Liceità, correttezza e trasparenza, (ii) Limitazione della finalità, (iii) Minimizzazione dei dati, (iv) Esattezza, (v) Limitazione della conservazione, (vi) Integrità e riservatezza.

### **Condizioni di liceità del trattamento:**

Il trattamento è lecito solo se ricorre almeno una delle seguenti condizioni:

1. Consenso dell'Interessato.
2. Obblighi contrattuali o precontrattuali.
3. Obblighi di legge cui è soggetto il Titolare del trattamento.
4. Interessi vitali dell'Interessato o di terzi (Residuale rispetto alle altre condizioni).
5. Interesse pubblico o esercizio di pubblici poteri.
6. Interesse legittimo prevalente del Titolare del trattamento o di terzi cui i dati vengono comunicati a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato.

## CONSENSO

- Non è richiesta la forma scritta, ma il Titolare deve essere in grado di dimostrare che l'Interessato ha prestato il consenso.
- Per i dati sensibili il consenso deve essere esplicito.
- Può essere revocato in qualsiasi momento.

La richiesta di consenso deve essere:

- Chiara.
- Distinguibile dalle altre materie.
- Forma comprensibile e facilmente accessibile.
- Linguaggio semplice.

Minori:

- Consenso valido se il minore ha compiuto i 16 anni.

## INFORMATIVA (1 / 3)

L'Informativa presentata agli interessati deve essere:

- » Concisa.
- » Facilmente accessibile.
- » Di facile comprensione.
- » Linguaggio semplice e chiaro.
- » Scritta, anche in formato elettronico.
- » Ok all'utilizzo di icone.

L'Informativa è fornita, in linea generale, **per iscritto e preferibilmente in formato elettronico.**

Possibile utilizzo di icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto.  
Se presentate elettronicamente, le icone devono essere visibili da dispositivo automatico.

## INFORMATIVA (2/3)

In caso di **raccolta dei dati presso l'Interessato**, l'Informativa dovrà indicare:

- » I dati del Titolare del trattamento.
- » Responsabile della protezione dei dati (RPD), se esistente.
- » Finalità e base giuridica del trattamento.
- » Interesse legittimo del Titolare o di terzi, se esistente.
- » Destinatari dei dati.
- » Intenzione di trasferire dati in un paese extra UE, se esistente.
- » Periodo di conservazione dei dati.
- » Diritti degli Interessati (accesso, rettifica, cancellazione, limitazione opposizione, portabilità).
- » Diritto di revocare il consenso, se esistente.
- » Diritto di proporre reclamo;
- » Conseguenze della mancata comunicazione dei dati, se esistente.
- » Esistenza di processi decisionali automatizzati (anche profilazione).

L'informativa non è necessaria se e nella misura in cui l'interessato già dispone delle informazioni.

## INFORMATIVA (3/3)

Nel caso in cui i dati **NON siano raccolti presso l'Interessato**, l'Informativa dovrà avere il medesimo contenuto di quella presentata in caso di raccolta di dati presso l'Interessato, ad eccezione delle eventuali conseguenze della mancata comunicazione dei dati, con l'aggiunta di: (i) l'indicazione delle categorie dei dati oggetto del trattamento; (ii) la fonte da cui hanno origine i dati personali.

### Tempi:

- » L'informativa deve essere comunicata **non oltre 1 mese dall'ottenimento dei dati**.

### Eccezioni:

- » L'informativa non deve essere comunicata se:
  1. L'Interessato già dispone delle informazioni.
  2. Comunicazione impossibile/sforzo sproporzionato per il Titolare.
  3. Ottenimento e comunicazione previsti da UE.
  4. Segreto professionale.

# DIRITTI DEGLI INTERESSATI

## DIRITTI DEGLI INTERESSATI

Nell'ambito del trattamento dei propri dati personali gli Interessati hanno i seguenti diritti:

- A. Diritto di accesso;
- B. Diritto alla rettifica;
- C. Diritto all'oblio (cancellazione);**
- D. Diritto alla limitazione del trattamento;
- E. Diritto alla portabilità dei dati;**
- F. Diritto di opposizione.

Il Titolare deve rispondere all'interessato entro 1 mese dall'esercizio di uno dei diritti sopra indicati.

Obbligo di notifica delle eventuali rettifiche, cancellazioni o limitazioni ai destinatari cui sono stati comunicati i dati.

Le informazioni fornite, e l'esercizio dei diritti, sono gratuite salvo il caso di richieste infondate, eccessive o ripetitive per cui può essere previsto un contributo economico.

## DIRITTO DI ACCESSO, DIRITTO DI RETTIFICA, DIRITTO DI OPPOSIZIONE

DIRITTO DI ACCESSO	DIRITTO DI RETTIFICA	DIRITTO DI OPPOSIZIONE
<p>Diritto ad ottenere la conferma circa l'esistenza del trattamento nonché l'accesso a specifiche informazioni relative al trattamento dei dati.</p> <ul style="list-style-type: none"><li>▪ Diritto di richiedere una copia delle informazioni.</li><li>▪ E' incentivata la possibilità di consultare i dati direttamente da remoto.</li></ul>	<p>Diritto di ottenere la rettifica e l'integrazione dei propri dati personali.</p>	<p>Diritto di opporsi al trattamento per motivi derivanti dalla situazione particolare dell'interessato.</p> <p>Diritto di opporsi, in qualsiasi momento, al trattamento effettuato per finalità di telemarketing, compresa la profilazione.</p>

## DIRITTO ALL'OBLIO (CANCELLAZIONE)

- Diritto di ottenere la **cancellazione dei propri dati personali** e conseguente obbligo del Titolare del trattamento di procedere nelle seguenti ipotesi:
  - Dati non più necessari rispetto alle finalità del trattamenti.
  - Revoca del consenso su cui si basa il trattamento.
  - Opposizione al trattamento.
  - Dati trattati illecitamente.
  - Dati da cancellare per adempiere ad un obbligo di legge.
  - Dati raccolti per l'offerta di servizi per la società dell'informazione.
  
- Obbligo per il Titolare di informare gli altri Titolari della richiesta dell'Interessato di cancellarli.
  
- Diritto all'oblio **NON si applica** per:
  - L'esercizio del diritto alla libertà di espressione e di informazione.
  - Adempimento di un obbligo legale o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.
  - motivi di interesse pubblico nel settore della sanità pubblica.
  - fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.
  - accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

## DIRITTO DI LIMITAZIONE DEL TRATTAMENTO

- ✓ Diritto più esteso rispetto al blocco del trattamento ai sensi dell'art. 7 comma 3 lett. a) del D.Lgs. 196/2003.
- ✓ L'Interessato può ottenere la limitazione del trattamento se:
  - A. contesta l'esattezza dei dati, per il periodo necessario al Titolare del trattamento per effettuare la verifica;
  - B. trattamento illecito e richiesta di limitazione;
  - C. dati necessari per l'esercizio in sede giudiziaria;
  - D. opposizione dell'Interessato in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'Interessato.
- ✓ Il **dato personale** oggetto della limitazione **dovrà essere "contrassegnato"**, in attesa delle successive determinazioni, attraverso idonei strumenti (anche elettronici).

## DIRITTO ALLA PORTABILITÀ DEI DATI

Diritto dell'Interessato di **ricevere dal Titolare i propri dati, in formato leggibile da dispositivo automatico**, e di **trasferirli ad altro Titolare**, a condizione che:

- il trattamento si basi sul consenso o su un contratto;
- il trattamento sia eseguito con mezzi automatizzati (no cartaceo);
- il trattamento abbia ad oggetto dati "forniti" dall'Interessato.

Se richiesto dall'Interessato e tecnicamente possibile il Titolare deve essere in grado di garantire il trasferimento diretto dei dati al nuovo Titolare del trattamento.

E' opportuno che il Titolare utilizzi un **formato dei dati interoperabile**, così da poter garantire agevolmente l'eventuale trasferimento.

# TITOLARE, RESPONSABILE DEL TRATTAMENTO E RESPONSABILE DELLA PROTEZIONE DEI DATI

## TITOLARE DEL TRATTAMENTO

- 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 presente regolamento” (Accountability). L’adesione a Codici di Condotta o meccanismi di certificazione costituisce un elemento idoneo a rappresentare il rispetto del Regolamento.
- Possibile **contitolarità del trattamento**. In tale ipotesi i contitolari dovranno disciplinare per iscritto i rispettivi compiti e responsabilità, con particolare riguardo all’esercizio dei diritti degli Interessati.
- Il Titolare (o il Responsabile) che si trovi fuori UE dovrà nominare un Rappresentante all’interno dell’UE che costituirà l’interlocutore diretto per le Autorità di controllo e gli Interessati.

## RESPONSABILE DEL TRATTAMENTO

- Il Responsabile del trattamento deve essere nominato tra coloro che presentino **garanzie sufficienti** per mettere in atto misure tecniche e organizzative adeguate a quanto previsto nel Regolamento.
- Può nominare un altro Responsabile previa autorizzazione scritta del Titolare, ma resta responsabile di possibili inadempimenti del sub-Responsabile.
- Deve essere incaricato attraverso un **contratto** che preveda espressamente “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”;
- Il Regolamento individua inoltre ulteriori obblighi del Responsabile che devono essere indicati nel contratto.

## RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD) 1 / 3

- Il Regolamento introduce la figura del Responsabile della Protezione dei Dati (RPD) il quale ha il compito di svolgere attività che non si limitano al mero controllo formale circa il livello di protezione dei dati, ma si estendono al supporto strategico alle decisioni operative del Titolare. E' un vero e proprio **manager del trattamento dei dati** (o *privacy designer*).
- Il Titolare e il Responsabile del trattamento nominano il RPD nei seguenti casi:
  1. trattamento effettuato da un'Autorità pubblica o organismo pubblico;
  2. trattamenti che, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
  3. le attività principali del Titolare o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali (dati sensibili) o di dati relativi a condanne penali e a reati.
- Possibilità di nominare un unico RPD nell'ambito di un Gruppo di imprese.  
Il RPD è designato tra i dipendenti del Titolare o Responsabile del trattamento ovvero tra professionisti terzi, in funzione delle sue qualità professionali, con particolare riferimento alla conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati.

## RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD) 2/3

1. Il RPD deve essere **autonomo ed indipendente**.
2. E' tempestivamente e costantemente coinvolto dal Titolare e dal Responsabile in tutte le questioni relative al trattamento.
3. Il Titolare ed il Responsabile del trattamento forniscono al RPD le **risorse necessarie** per assolvere i compiti assegnatigli e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
4. Il RPD riferisce direttamente al vertice gerarchico del Titolare o del Responsabile del trattamento.
5. Gli Interessati possono contattare il RPD per tutte le questioni attinenti al trattamento.
6. Obbligo di segretezza e possibilità di svolgere attività diverse purché non vi sia conflitto di interessi.

## RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD) 3/3

Il RPD è incaricato di **eseguire ALMENO** i seguenti compiti:

1. informare e fornire consulenza al Titolare o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi di legge relativi alla protezione dei dati;
2. verificare il rispetto della normativa applicabile 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;
3. fornire, se richiesto, un parere in merito alla Valutazione d'Impatto e sorvegliarne lo svolgimento;
4. cooperare con l'Autorità di controllo;
5. fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento.

# MODALITÀ OPERATIVE E SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI

## REGISTRO DELLE ATTIVITÀ (1 / 2)

Il **Titolare ed il suo rappresentante** devono tenere un **Registro delle Attività** in cui sono elencati i trattamenti svolti ed indicate le seguenti informazioni:

- I. Dati di contatto del Titolare del trattamento.
- II. Finalità del trattamento.
- III. Descrizione delle categorie di Interessati e dei dati personali.
- IV. Eventuale trasferimento dei dati verso paesi extra UE.
- V. Termini ultimi per la cancellazione dei dati.
- VI. Descrizione delle misure di sicurezza tecniche e organizzative applicate al trattamento.

Il **Responsabile ed il suo rappresentante** devono tenere un **Registro di tutti i trattamenti svolti per conto di un Titolare** del trattamento, che riporti le seguenti informazioni:

- I. Dati di contatto del Responsabile e del Titolare del trattamento e suo rappresentante per conto del quale è effettuato il trattamento.
- II. Le categorie dei trattamenti effettuati per conto di ogni Titolare.
- III. Eventuale trasferimento di dati verso paesi extra UE.
- IV. Descrizione delle misure di sicurezza tecniche e organizzative.

## REGISTRO DELLE ATTIVITÀ (2/2)

I Registri sono tenuti in **forma scritta** (anche in formato elettronico).

L'obbligo della tenuta del Registro:

**SI**

**SI applica** alle imprese con un **numero di dipendenti uguale o maggiore di 250**;

**NO**

**NON si applica** alle imprese o organizzazioni con **meno di 250 dipendenti**, a meno che il trattamento che esse effettuano (i) possa presentare un **rischio per i diritti e le libertà dell'Interessato**, (ii) il trattamento **non sia occasionale** o includa il trattamento di **dati sensibili**, o i dati personali relativi a **condanne penali e a reati**.

## SICUREZZA DEL TRATTAMENTO

- ✓ Il Titolare e il Responsabile del trattamento mettono in atto **misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato** ed in particolare, *inter alia*:
  - la pseudonimizzazione e la cifratura dei dati personali;
  - la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
  
- ✓ Nel valutare il livello di sicurezza si tiene conto di dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

## VIOLAZIONE DEI DATI PERSONALI

- Il Titolare, anche informato dal Responsabile del trattamento, notifica la violazione all'**Autorità di controllo** entro 72 ore da quando ne è venuto a conoscenza, salvo che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
- Il Titolare del trattamento notifica la violazione all'**Interessato** qualora essa sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
- In ogni caso non è richiesta la notifica all'Interessato qualora:
  - Il Titolare ha adottato misure di protezione dei dati adeguate.
  - Il Titolare ha messo in atto, successivamente, misure adeguate a protezione da possibili rischi elevati.
  - La comunicazione richiederebbe sforzi sproporzionati.

## VALUTAZIONE DI IMPATTO (1 / 2)

Se il trattamento presenta un rischio elevato per i diritti e le libertà delle persone, il Titolare, consultandosi con il Responsabile del trattamento, deve preliminarmente effettuare una **Valutazione di Impatto** dei trattamenti sulla protezione dei dati.

La Valutazione di Impatto è sempre richiesta nei seguenti casi:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, 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 anche relativi a condanne penali e a reati;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

## VALUTAZIONE DI IMPATTO (2/2)

La Valutazione di impatto deve contenere:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

Qualora la Valutazione d'Impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio, quest'ultimo, prima di procedere al trattamento, deve consultare l'Autorità di controllo.

# TRASFERIMENTO DEI DATI VERSO PAESI EXTRA UE O ORGANISMI INTERNAZIONALI

## TRAFERIMENTO DI DATI VERSO PAESI EXTRA UE O ORGANISMI INTERNAZIONALI

- ⇒ Il trasferimento può essere effettuato se lo Stato terzo (extra UE) o l'Organizzazione ha superato la **decisione di adeguatezza** della Commissione Europea.
- ⇒ In mancanza di una decisione di adeguatezza, il Titolare o il Responsabile può trasferire i dati solo se ha fornito **garanzie adeguate** e a condizione che gli **Interessati dispongano di diritti azionabili e mezzi di ricorso effettivi**.
- ⇒ E' incoraggiata l'adozione, da parte delle Autorità di controllo, di **norme vincolanti di impresa** da utilizzare per lo scambio di dati all'interno di gruppi di imprese con sedi anche in paesi extra UE.
- ⇒ Divieto di trasferire dati in un paese extra UE sulla base di decisioni giudiziarie o amministrative, salvo che esista un accordo bilaterale.
- ⇒ Possibilità di trasferire i dati verso paesi extra UE ed organismi internazionali anche in assenza di una decisione di adeguatezza o garanzie adeguate, in base a delle ipotesi specifiche indicate nel Regolamento.

# **STRUMENTI DI TUTELA E REGIME SANZIONATORIO**

## RECLAMO ALL'AUTORITÀ DI CONTROLLO E RICORSO GIURISDIZIONALE

Ogni Interessato ha diritto di proporre:

- 1) **reclamo all'Autorità di controllo** competente nello Stato membro in cui ha la residenza ovvero nel luogo in cui si è verificata la violazione, qualora il trattamento che lo riguarda violi il Regolamento;
- 2) **ricorso giurisdizionale**, dinanzi alla competente Autorità Giudiziaria, **nei confronti del Titolare o Responsabile del trattamento**, qualora ritenga che i diritti di cui gode a norma del Regolamento siano stati violati a seguito di un trattamento;
- 3) **ricorso giurisdizionale** (azionabile da qualsiasi persona fisica o giuridica), dinanzi alla competente Autorità Giudiziaria, **avverso una decisione giuridicamente vincolante dell'Autorità di controllo** che la riguarda nonché in caso l'autorità di controllo non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto.

## SANZIONI AMMINISTRATIVE

- Le sanzioni amministrative irrogate dalle Autorità di controllo devono essere, in ogni singolo caso, effettive, proporzionate e dissuasive.
- Il Regolamento individua gli elementi da prendere in considerazione per l'applicazione della sanzione amministrativa.
- Le sanzioni applicabili, individuate nel Regolamento, sono pari a:
  - ⇒ I. fino ad **Euro 10.000.000,00**, o per le imprese, **fino al 2 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, per le violazioni degli obblighi relativi a: minori, obblighi del Titolare e Responsabile, obblighi dell'organismo di certificazione, obblighi dell'organismo di controllo;
  - ⇒ II. fino ad **Euro 20.000.000,00**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, per le violazioni degli obblighi relativi a: principi di base del trattamento, comprese le condizioni relative al consenso, diritti degli interessati, trasferimento dati a paese extra UE, obblighi imposti dagli stati membri per specifiche categorie – anche in ambito lavorativo – 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.
  - ⇒ III. Le sanzioni amministrative pecuniarie sono inflitte in aggiunta alle, o in luogo delle, sanzioni di cui all'art. 58 par. 2 lett. da a) a h) e j) del Regolamento (ad es. avvertimenti, ammonimenti, ingiunzioni, limitazioni ai trattamenti, ordine di cancellazione, rettifica o limitazione del trattamento, revoca della certificazione o ingiunzione all'Organismo certificatore di ritirare o non emettere la certificazione, ordine di sospensione dei flussi di dati verso un destinatario).

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
<p>Fino a <b>10.000.000 EUR</b> o, per le imprese, fino al <b>2%</b> del fatturato mondiale totale annuo dell'esercizio precedente, se superiore</p>	Art. 8	<p>Verifica che il consenso del trattamento sia prestato o autorizzato dal titolare della responsabilità genitoriale nel caso di offerta diretta di servizi della società dell'informazione a minori di età inferiore ai 16 anni.</p>
	Art. 11	<p>Obbligo di non conservazione, acquisizione o trattamento di informazioni per identificare l'Interessato se le finalità del trattamento non richiedono o non richiedono più l'identificazione dell'Interessato.</p>
	Art. 25	<p>Adozione di misure tecniche e organizzative atte ad attuare i principi di protezione dei dati, la tutela dei diritti degli Interessati e la garanzia che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità di trattamento (c.d. <i>privacy by design e by default</i>).</p>
	Art. 28	<p>Designazione del Responsabile del trattamento e rispetto degli obblighi e compiti posti a carico del Responsabile.</p>

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
<p>Fino a <b>10.000.000 EUR</b> o, per le imprese, fino al <b>2%</b> del fatturato mondiale totale annuo dell'esercizio precedente, se superiore</p>	Art. 30	Tenuta dei Registri delle attività di trattamento.
	Art. 32	Adozione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio
	Art. 33 - 34	Notifica delle violazioni all'Autorità di controllo e all'Interessato.
	Art. 35 e 36	Obbligo di procedere alla valutazione di impatto ed alla successiva consultazione, ove richiesto dal Regolamento.
	Art. 37 - 39	Prescrizioni in tema di designazione del Responsabile della protezione dei dati ( <i>Data Protection Officer</i> ).

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
<p>Fino a <b>20.000.000 EUR</b> o, per le imprese, fino al <b>4%</b> del fatturato mondiale totale annuo dell'esercizio precedente, se superiore</p>	Art. 5	Rispetto dei principi applicabili al trattamento liceità, correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
	Art. 6	Rispetto delle condizioni di liceità del trattamento.
	Art. 7	<ul style="list-style-type: none"> <li>• Dimostrazione della prestazione del consenso e del rispetto delle condizioni per il consenso.</li> <li>• Tutela del diritto dell'Interessato di revoca del consenso.</li> </ul>
	Art. 9	Rispetto delle condizioni di liceità del trattamento di categorie particolari di dati personali.

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
<p>Fino a <b>20.000.000 EUR</b> o, per le imprese, fino al <b>4%</b> del fatturato mondiale totale annuo dell'esercizio precedente, se superiore</p>	<p>Art. da 12 a 22</p>	<ul style="list-style-type: none"> <li>• Obblighi informativi nei confronti dell'Interessato.</li> <li>• Tutela dei diritti dell'Interessato (diritto d'accesso; di rettifica; all'oblio; di limitazione del trattamento; di notifica in caso di rettifica o cancellazione dei dati o limitazione del trattamento; alla portabilità dei dati; di opposizione; alla profilazione consenziente).</li> </ul>
	<p>Art. da 44 a 49</p>	<p>Obblighi connessi al trasferimento dei dati personali verso Paesi terzi o organizzazioni internazionali.</p>
	<p>Cap IX</p>	<p>Qualsiasi obbligo previsto dalle legislazioni degli Stati membri per specifiche situazioni di trattamento a norma del Capo IX del Regolamento.</p>
	<p>Art. 58</p>	<p>Rispetto di un ordine, di una limitazione di trattamento o di un ordine di sospensione di flussi di dati dell'Autorità di controllo o di un negato accesso ai sensi dell'Art, 58, par. I.</p>