# Privacy e protezione dei dati personali

---

**Seminario del corso**
**"Laboratorio di amministrazione di sistemi"**
**Scuola di Ingegneria, Università di Bologna**

10/05/17

**Claudia Cevenini**

# Norme di riferimento

**Codice in materia di protezione dei dati personali**
(D. Lgs. 30 giugno 2003, n. 196), c.d. **Codice privacy**

**Attenzione!!**
Nel 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione europea il **Regolamento Generale sulla protezione dei dati** (**Reg. UE 2016/679**), che modificherà le regole attuali.
Il Regolamento e le sue disposizioni saranno **direttamente applicabili** in tutti gli Stati membri – inclusa l'Italia - a partire **dal 25 maggio 2018**.

# Chi ha diritto alla protezione dei dati personali?

Diritto alla **protezione** dei **dati personali** deve essere garantito a **chiunque**.

Il Codice si applica ai trattamenti di dati personali delle **persone fisiche** (=individui) e NON delle persone giuridiche (= società, enti e associazioni).



# A quali trattamenti si applica il Decreto?

Ai trattamenti **elettronici**, **cartacei** o manuali.
A tutti i **trattamenti** di dati personali:
- effettuati da **soggetti stabiliti** nello **Stato**, o in un **luogo** soggetto alla sovranità dello **Stato**, anche se i **dati** sono **detenuti** all'**estero**,
- o da soggetti **extra europei** che impiegano **strumenti** localizzati **nello Stato** (eccezione: semplice transito dei dati nell'Unione Europea). Se si applica il Codice, il titolare del trattamento deve designare un rappresentante stabilito nel territorio dello Stato, al fine dell'applicazione della disciplina sul trattamento dei dati personali.

# Esclusioni dall'ambito di applicazione del Codice privacy

Sono esclusi dall'ambito di applicazione del Codice (= **non si applica il Codice**) i **trattamenti** effettuati da **persone fisiche** per **fini esclusivamente personali** che **non** prevedano la **diffusione** di dati o la loro **comunicazione sistematica**.

**ATTENZIONE!!!** Nonostante l'esclusione, a questi trattamenti si applicano le **norme** sulla **responsabilità** e sulla **sicurezza** dei **dati** previste negli **artt**. **15** e **31** del Codice.



# Alcuni concetti importanti 1/3

**Dato personale** = qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
I dati personali si distinguono in **comuni** e **sensibili**.

**Trattamento** = qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

# Alcuni concetti importanti 2/3

**Comunicazione** = dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

**Diffusione** = dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.



# Alcuni concetti importanti 3/3

**Titolare** = persona fisica, persona giuridica, pubblica amministrazione, ente, associazione od organismo cui competono le decisioni relative alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

**Responsabile** = persona fisica, persona giuridica, pubblica amministrazione, ente, associazione od organismo preposto dal titolare al trattamento di dati personali.

**Incaricato** = persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.

**Interessato** = persona fisica cui si riferiscono i dati personali.

# La designazione a responsabile

Il **responsabile** (persona fisica o giuridica) è designato facoltativamente dal titolare. **Tratta dati per conto del titolare**.
Il titolare può designare più responsabili.
La **designazione** deve essere in **forma scritta**, accompagnata da **istruzioni**.
I **compiti** affidati al responsabile devono essere **analiticamente specificati** per iscritto dal titolare.
Il responsabile deve rispettare la legge, attenersi alle istruzioni impartite e il titolare deve vigilare sulla puntuale osservanza della normativa e delle proprie istruzioni.
*Es. consulente del lavoro che tratta dati dei dipendenti delle società per cui fa le buste paga, call center che telefona ai clienti dei propri committenti.*



# La designazione a incaricato

Il trattamento può essere effettuato solo da **incaricati** (persone fisiche) che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle **istruzioni** impartite.

La **designazione** deve essere effettuata **per iscritto** e individuare puntualmente l'**ambito del trattamento consentito**.

Si considera tale anche la **documentata preposizione** della persona fisica a una **unità** per la quale è **individuato**, **per iscritto**, l'**ambito del trattamento consentito** agli addetti dell'unità medesima (es. ufficio commerciale/amministrativo).

# Principio di necessità

**Sistemi informativi** e **programmi informatici** devono essere **configurati** in modo da **ridurre al minimo** l'impiego di **dati personali**.
Il **trattamento** deve essere **escluso se** le stesse **finalità** possono essere perseguite con **dati anonimi** o con modalità che consentano l'identificazione solo in caso di necessità.



# Modalità del trattamento

I dati devono essere trattati in modo **lecito** e secondo **correttezza**.

**Liceità** = occorre fare riferimento a tutto l'ordinamento giuridico e non solo alle norme del Codice.

**Correttezza** = rispetto di tutte le regole, anche non codificate.

# Principio di finalità

I dati devono essere **raccolti** e **registrati** per **scopi**
-**determinati**
- **espliciti**
- **legittimi**

I dati devono essere **utilizzati** in **altre operazioni** del **trattamento** in **termini non incompatibili** con tali **scopi**.



# Requisiti dei dati

I dati devono essere:
- **esatti**,
- **aggiornati** (se necessario),
- **pertinenti**,
- **completi**,
- **non eccedenti** rispetto alle **finalità**.

# Durata di conservazione dei dati

I dati devono essere conservati in una forma che consenta l'**identificazione** dell'interessato per un **tempo non superiore** a quello **necessario** al raggiungimento degli **scopi** per cui i dati sono stati raccolti e trattati.

Se lo **scopo** è stato **raggiunto** i **dati** devono essere resi **anonimi o cancellati**.



# Riepilogo

I dati personali devono essere :
a) trattati in modo **lecito** e **corretto**;
b) raccolti e registrati per **scopi determinati**, **espliciti** e **legittimi**;
c) **esatti** e (se necessario) **aggiornati**;
d) **pertinenti**, **completi** e **non eccedenti** gli **scopi**;
e) conservati in modo da permettere l'**identificazione** dell'**interessato** per un **tempo non superiore** al **necessario**.

**ATTENZIONE!!!** Se i dati sono trattati **in violazione** della legge **NON** possono essere **utilizzati**.

# Obblighi di sicurezza

I **dati personali** oggetto di trattamento devono essere **custoditi** e **controllati**, anche in relazione alle conoscenze acquisite in base al **progresso tecnico**, alla **natura dei dati** e alle specifiche **caratteristiche del trattamento**, in modo da **ridurre al minimo**, mediante l'adozione di **idonee** e **preventive misure di sicurezza**, i **rischi** di **distruzione** o **perdita**, anche accidentale, dei dati stessi, di **accesso non autorizzato** o di **trattamento non consentito** o **non conforme** alle **finalità** della raccolta.

(Misure di sicurezza 'idonee', v. art. 31 Codice Privacy)



# Art. 15 Codice privacy

**Danni cagionati per effetto del trattamento**
Chiunque cagiona **danno ad altri** per effetto del **trattamento di dati personali** è tenuto al **risarcimento** ai sensi dell'**articolo 2050 del codice civile**.

# Art. 2050 c.c.

**Responsabilità per l'esercizio di attività pericolose**

Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al **risarcimento**, **se non prova** di avere **adottato tutte** le **misure idonee** a **evitare il danno**.



# Misure minime di sicurezza

Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i **titolari** del trattamento sono **comunque tenuti** ad adottare le **misure minime**, volte ad assicurare un livello minimo di protezione dei dati personali.

"Il complesso delle misure **tecniche**, **informatiche**, **organizzative**, **logistiche** e **procedurali** di sicurezza che configurano il **livello minimo di protezione**."

Sono **OBBLIGATORIE**!!

**Sono elencate nell'Allegato B al Codice privacy**

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1557184

# Misure minime di sicurezza
# Trattamento con strumenti elettronici

## Sistema di autenticazione informatica

Ciascun incaricato deve avere proprie credenziali di autenticazione individuali (es. nome utente e password, dispositivo, caratteristica biometrica).
Devono essere impartite istruzioni agli incaricati sulla custodia delle credenziali.
Parola chiave: almeno 8 caratteri, senza riferimenti agevolmente riconducibili all'incaricato, modificata al primo utilizzo e successivamente almeno ogni 6 mesi (3 mesi in caso di dati sensibili).
Il codice utilizzato non può essere assegnato ad altri incaricati, neppure in tempi diversi



## Sistema di autenticazione informatica (segue)

Credenziali devono essere disattivate se inutilizzate da almeno 6 mesi o in caso di perdita della qualità che consente all'incaricato l'accesso ai dati.
Accesso con password: vanno impartite disposizioni scritte per definire le modalità con cui assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.
Le copie delle credenziali vanno custodite garantendone la segretezza e individuando per iscritto i soggetti incaricati della custodia, che devono informare tempestivamente l'incaricato dell'intervento effettuato.

# Misure minime di sicurezza

**Sistema di autorizzazione**

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

Prima del trattamento occorre individuare e configurare profili di autorizzazione per limitare l'accesso ai soli dati necessari per le operazioni di trattamento.

Periodicamente (almeno annualmente) occorre verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

E' possibile predisporre la lista degli incaricati per classi omogenee di incarico e per profili di autorizzazione.



# Misure minime di sicurezza

**Altre misure di sicurezza**

I dati devono essere **protetti** dal **rischio di intrusione** e dall'azione di **programmi informatici** diretti a **danneggiare** o **interrompere** un sistema informatico o telematico, attivando idonei strumenti elettronici da **aggiornare** almeno ogni **6 mesi**.

I **programmi per elaboratore** devono essere **aggiornati** almeno **annualmente** (ogni **6 mesi** in caso di **dati sensibili**) per prevenire vulnerabilità e correggerne difetti.

Devono essere impartite istruzioni organizzative e tecniche che prevedono il **salvataggio** dei **dati** con frequenza almeno **settimanale**.

# Misure minime di sicurezza

**Ulteriori misure in caso di dati sensibili o giudiziari**

I **dati** devono essere **protetti** contro l'**accesso abusivo**.

Vanno impartite istruzioni organizzative e tecniche per la custodia e l'uso dei **supporti rimovibili** per evitare accessi non autorizzati e trattamenti non consentiti.

I supporti rimovibili se non utilizzati sono distrutti o resi inutilizzabili, o possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Sono adottate idonee misure per garantire il **ripristino** dell'**accesso ai dati** in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a 7 giorni.



# Misure minime di sicurezza

**Intervento di soggetti esterni per 'messa a norma' misure di sicurezza**

Se il titolare adotta le misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione deve ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del disciplinare tecnico (Allegato B al Codice privacy).

# Misure minime di sicurezza
# Trattamento senza strumenti elettronici

Devono essere impartite **istruzioni scritte** per controllo e custodia di atti e documenti contenenti dati personali.
**Aggiornamento periodico dell'ambito di trattamento** degli incaricati o delle unità organizzative.
Liste di incaricati possono essere redatte anche per classi omogenee e profili di autorizzazione.



# Misure minime di sicurezza
# Trattamento senza strumenti elettronici

**Dati sensibili e giudiziari**
**Atti** e **documenti** sono **controllati** e **custoditi** fino alla restituzione in maniera che ad essi **non accedano persone prive di autorizzazione** e sono restituiti al termine delle operazioni affidate.
L'**accesso** agli **archivi** è **controllato**. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

# Informativa 1/2

Interessato deve essere **preventivamente informato**, per iscritto o oralmente, su:
a) **finalità** e **modalità** del trattamento;
b) natura **obbligatoria** o **facoltativa** del conferimento dei dati;
c) **conseguenze** del **rifiuto** di fornire i dati;
d) **soggetti** (o categorie di soggetti) a cui i dati possono essere **comunicati** o che possono venirne **a conoscenza**; eventuale **ambito** di **diffusione**;
e) **diritti** che può esercitare;
f) **estremi identificativi** del **titolare** (evtl. del responsabile).
Informativa può contenere dati ulteriori, o non contenere dati già noti alla persona che fornisce i dati o che potrebbero ostacolare funzioni ispettive o di controllo di soggetti pubblici (es. difesa dello Stato, prevenzione dei reati).



# Informativa 2/2

Se i **dati** sono **raccolti presso un terzo**, l'**interessato** deve ricevere l'**informativa** al momento della **registrazione** dei **dati o prima** della loro **comunicazione**, se prevista.

# Informativa - eccezioni

L’informativa non è dovuta se:
a) dati trattati in base a **obbligo** derivante da **legge**, **regolamento** o **normativa comunitaria**;
b) dati trattati per **investigazioni difensive**, o per **tutelare** un **diritto** in **giudizio**;
c) fornire l’informativa richiede un **impiego** di **mezzi manifestamente sproporzionato** rispetto al diritto tutelato, **o** è **impossibile**.



# Informativa – i curricula

L'informativa non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell’eventuale instaurazione di un rapporto di lavoro.
Al momento del primo contatto successivo all’invio del curriculum il Titolare è tenuto a fornire all'interessato, oralmente o per iscritto, un'informativa breve contenente almeno:
- le finalità e modalità del trattamento;
- i soggetti o le categorie di soggetti a cui i dati potranno essere comunicati o che potranno venirne a conoscenza;
- gli estremi identificativi del Titolare, del rappresentante se designato e dell'eventuale responsabile.

# Consenso

Il trattamento di dati personali effettuato da parte di **privati** ed **enti pubblici economici** è subordinato al **consenso espresso** dell'**interessato**.
I **soggetti pubblici non sono tenuti** a chiedere il consenso (sono previste eccezioni in campo sanitario).
C. può riguardare il trattamento nel suo **complesso** o solo **alcune operazioni**.
C. è **valido** se:
- **libero**,
- riferito a uno **specifico trattamento**,
- **documentato per iscritto**,
- **informato.**



# Casi in cui è possibile il trattamento senza consenso 1/2

- Trattamento necessario per adempiere a un **obbligo di legge**, **regolamento** o **normativa comunitaria**
- T. necessario per eseguire **obblighi di un contratto** di cui l'**interessato** è **parte** o per adempiere a sue specifiche richieste
- T. di dati reperiti in **pubblici registri**, **elenchi**, **atti** o **documenti conoscibili da chiunque**
- T. di dati relativi ad **attività economiche** (nel rispetto del segreto industriale)
- T. necessario per **salvaguardare** la **vita** o **l'incolumità fisica** di un **terzo**

# Casi in cui è possibile il trattamento senza consenso 2/2

- T. necessario per **investigazioni difensive** o per **tutelare** un **diritto in giudizio**; è esclusa la diffusione;
- T. necessario (nei casi individuati dal Garante e in base ai principi di legge) per tutelare un **interesse legittimo** del **titolare** o di un **terzo destinatario** dei dati (es. attività di gruppi bancari e società controllate e collegate); è esclusa la diffusione;
- T. effettuato da **enti *non profit*** di dati degli **aderenti**, per scopi statutari e con determinate modalità (escluse la comunicazione all'esterno e la diffusione);
- T. necessario per **scopi storici**, **scientifici** o **statistici**.



# Divieto di comunicazione o diffusione

La comunicazione e la diffusione sono **vietate**:

- per decisione del **Garante** o dell'**autorità giudiziaria**;
- se riguardano **dati** personali di cui è stata ordinata la **cancellazione** o **decorso il tempo** per il quale era **necessario** trattare dati **identificativi**;
- per **finalità diverse** da quelle indicate nella **notificazione** (se prevista).
-

**Eccezioni**: comunicazione e diffusione effettuate a forze di polizia, autorità giudiziaria, soggetti pubblici per difesa o sicurezza dello Stato o per prevenire, accertare o reprimere reati.

# Dati sensibili

Dati personali idonei a rivelare l'**origine razziale** ed **etnica**, le **convinzioni religiose**, **filosofiche** o di altro genere, le **opinioni politiche**, l'adesione a **partiti**, **sindacati**, **associazioni** od **organizzazioni** a carattere **religioso**, **filosofico**, **politico** o **sindacale**, nonché i dati personali idonei a rivelare lo stato di **salute** e la **vita sessuale**.



# Trattamento dei dati sensibili 1/3

Per il trattamento di dati sensibili sono necessari:
- **informativa** contenente l'indicazione che saranno trattati dati sensibili;
- **consenso** dell'**interessato manifestato in forma scritta**;
- **autorizzazione** del **Garante**.

**Eccezioni**: questi adempimenti non sono richiesti per i dati trattati da enti religiosi riguardo ai loro aderenti (non sono permesse comunicazione o diffusione); dati sull'adesione di organizzazioni sindacali e di categoria ad altre associazioni sindacali o di categoria.

# Trattamento dei dati sensibili 2/3

ATTENZIONE: quando è prevista un'autorizzazione del Garante il requisito è soddisfatto se sono state emanate dal Garante **autorizzazioni relative a determinate categorie di titolari o di trattamenti**, pubblicate nella Gazzetta Ufficiale della Repubblica italiana (c.d. **Autorizzazioni Generali**).

Esempi:

AG al trattamento dei dati sensibili nei rapporti di lavoro.

AG al trattamento dei dati sensibili da parte degli investigatori privati.

AG al trattamento dei dati sensibili da parte dei liberi professionisti



# Trattamento dei dati sensibili 3/3

In alcuni casi è necessaria l'**autorizzazione** del **Garante** ma **non** occorre il **consenso**:

- t. di dati degli aderenti effettuato da **enti *no profit*** a carattere politico, filosofico, religioso, sindacale per scopi statutari legittimi (no comunicazione o diffusione);
- t. necessario per salvaguardare **vita** o **incolumità fisica** di un **terzo**;
- t. necessario per **investigazioni difensive** o per **tutelare** un **diritto** in **giudizio**;
- t. necessario per adempimenti di legge, regolamento o norme comunitarie per la **gestione** di un **rapporto** di **lavoro**.

Dati relativi allo **stato di salute non** possono essere **diffusi** da parte dei soggetti pubblici.

# Notificazione al Garante 1/2

In casi specifici (art. 37) il titolare deve **notificare al Garante** il che intende effettuare il trattamento di dati particolari, ad esempio dati:

- **genetici**,
- **biometrici** o
- che indicano la **posizione geografica** di **persone** od **oggetti** mediante **reti** di comunicazione elettronica;
- dati trattati con **strumenti elettronici** per definire il **profilo** o la **personalità** dell'interessato o analizzare **abitudini** o **scelte** di **consumo** o **monitorare** l'**utilizzo** di **servizi** di **comunicazione elettronica**;



# Notificazione al Garante 2/2

- **dati sensibili** in banche di dati per **selezione** del **personale** per conto terzi, **dati sensibili** utilizzati per **sondaggi di opinione**, **ricerche di mercato** e altre ricerche campionarie;
- **dati** registrati in apposite banche di dati gestite con strumenti elettronici e relative al **rischio** sulla **solvibilità** economica, alla **situazione patrimoniale**, al corretto adempimento di obbligazioni, a **comportamenti illeciti** o **fraudolenti**.

# Trasferimento di dati extra UE 1/2

Il trasferimento di dati, anche temporaneo, è possibile se:

- **consenso espresso** dell'interessato, o
- **autorizzazione** del **Garante** sulla base di adeguate garanzie, o in casi particolari, es.
- t. necessario per eseguire **obblighi di un contratto** di cui è **parte** l'interessato, o adempiere a **richieste** dell'interessato, per concludere o eseguire un **contratto a favore** dell'interessato; o
- t. necessario per salvaguardia di un **interesse pubblico** individuato per legge o regolamento; o
- t. necessario per salvaguardia della **vita** o **incolumità fisica** di un **terzo**;



# Trasferimento di dati extra UE 2/2

- t. necessario per **investigazioni difensive** o per **tutelare** un diritto in **giudizio**;
- t. effettuato in seguito a richiesta di **accesso** a **documenti amministrativi** o di estrazione di dati da **pubblichi elenchi**, registri, ecc. conoscibili da chiunque;
- t. necessario per scopi **storici**, **statistici** o **scientifici**;
- t. riguarda dati di **persone giuridiche**, **enti** o **associazioni**.

# Trasferimenti extra UE vietati

**Tranne nei casi** espressamente **consentiti** dal Codice, il **trasferimento anche temporaneo** fuori dal territorio dello Stato, con qualsiasi mezzo e in qualsiasi forma, di **dati personali** verso un **Paese extra UE** è **vietato** quando l'**ordinamento del Paese di destinazione o di transito dei dati non assicura un adeguato livello di tutela delle persone**.

Sono valutate anche le modalità di trasferimento e dei trattamenti previsti, le finalità, la natura dei dati e le misure di sicurezza adottate.



# Registro pubblico delle opposizioni

Chi è titolare di una **numerazione** riportata negli **elenchi telefonici iscrivendosi al registro** può **opporsi** a **telefonate** per fini di:

- **invio** di **materiale pubblicitario** o
- **vendita diretta**, o
- **ricerche di mercato** o
- **comunicazione commerciale**.

In caso di violazione sono previste sanzioni che prevedono il pagamento di una somma da diecimila euro a centoventimila euro.

# Attenzione però...

Anche se un abbonato è iscritto nel registro è **consentito** l'**utilizzo** del suo **numero telefonico** per finalità pubblicitarie o di comunicazione commerciale da parte di **singoli soggetti** che abbiano **raccolto o raccolgano tali dati da fonti diverse dagli elenchi telefonici**, purché ciò sia avvenuto o avvenga nel rispetto del Codice.

Gli utenti possono in qualsiasi momento negare il consenso "commerciale". Dopo, non potranno più essere contattati.



# Cessazione del trattamento

Quando cessa un trattamento i dati sono:

- **distrutti**; o
- **ceduti** ad altro titolare per un trattamento compatibile con gli **scopi originari**; o
- **conservati** per **scopi personali** (non comunicati sistematicamente o diffusi); o
- **conservati** o **ceduti** per **scopi storici**, **statistici** o di **ricerca scientifica**.

Se i dati sono **ceduti** in modo **contrario** alla **normativa** vigente, la **cessione** è **priva di effetti**.

# Diritti dell'interessato 1/3

L'interessato ha diritto di avere:
1) **conferma** dell'**esistenza** di **dati** che lo riguardano e la loro **comunicazione**;
2) **indicazione** di:
- **origine** dei **dati**,
- **finalità** e **modalità** del **trattamento**;
- **logica** impiegata nel trattamento con **strumenti elettronici**;
- **estremi identificativi** di **titolare**, **responsabili**, **incaricati**, **rappresentante**;
- **soggetti** o **categorie di soggetti** a cui i dati possono essere comunicati o che possono venirne a conoscenza.



# Diritti dell'interessato 2/3

3a) **Aggiornamento**, **rettificazione**, **integrazione** dei **dati.**
3b) **Cancellazione**, **trasformazione** in **forma anonima** o **blocco** dei **dati trattati** in **violazione** di **legge** (inclusi i dati di cui non è necessaria la conservazione per gli scopi del trattamento).
3c) **Attestazione** che **attività 3a)** e **3b)** sono state portate a conoscenza dei soggetti a cui i dati sono stati **comunicati** o **diffusi** (eccezione: se tale attestazione è impossibile o se richiede un impiego di mezzi sproporzionato).

# Diritti dell'interessato 3/3

4) L'interessato ha diritto di **opporsi** al **trattamento** di **dati** che lo riguardano:
a) per **motivi legittimi**, anche se i dati sono pertinenti agli scopi;
b) per l'**invio** di **materiale pubblicitario**, o di **vendita diretta**, o per **ricerche** di **mercato** o **comunicazione commerciale**.



# Sanzioni amministrative

**Omessa o inidonea informativa** (*6.000-36.000 €*) ;
**Cessione illecita di dati** (*10.000-60.000 €*) ;
**Omessa o incompleta notificazione** al Garante (20.000-120.000 *€*);
**Omessa informazione o esibizione di documenti** al Garante (*10.000-60.000 €*).

Casi di maggiore gravità: sanzione raddoppiata.

Se inefficaci in relazione a condizioni economiche del contravventore: sanzioni quadruplicate.

# Trattamento illecito di dati

Salvo che il fatto costituisca più grave reato, chiunque, al **fine** di trarne per sè o per altri **profitto o** di recare ad altri un **danno**, **tratta dati personali in violazione** degli **artt. 18, 19, 23, 123, 126 e 130,** o in applicazione dell'articolo **129**, è **punito**, **se dal fatto deriva nocumento**, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.
Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri **profitto o** di recare ad altri un **danno**, tratta dati personali in violazione degli **articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45**, è **punito**, **se dal fatto deriva nocumento**, con la reclusione da uno a tre anni.



# Omesse misure minime

Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a 2 anni.
All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una **prescrizione** fissando un **termine per la regolarizzazione** non eccedente il periodo di **tempo tecnicamente necessario**, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque **non superiore a 6 mesi**. Nei **60 giorni successivi** allo scadere del termine, se risulta l'**adempimento** alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una **somma** pari al **quarto del massimo della sanzione amministrativa**. L'adempimento e il pagamento estinguono il reato.

# Amministratori di sistema

Provvedimento del Garante del 27 novembre 2008 - "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di "**amministratore di sistema**"

AS = figura professionale in ambito informatico che si occupa della gestione e manutenzione di un impianto di elaborazione o sue componenti.

Equiparati ad AS = amministratori di basi di dati, amministratori di reti, di apparati di sicurezza, di sistemi software complessi.

Non considerati AS i soggetti che solo occasionalmente intervengono sui sistemi di elaborazione e software (es. per manutenzione o riparazione guasti o malfunzionamenti).



# AS: misure e accorgimenti prescritti al titolare 1/2

Occorre valutare **esperienza**, **capacità** e **affidabilità** del soggetto designato.

Occorrono:

- **designazione individuale**,
- **elenco analitico** degli **ambiti** di **operatività consentiti** in base al **profilo** di **autorizzazione** assegnato.

# AS: misure e accorgimenti prescritti al titolare 2/2

Almeno ogni anno il **titolare verifica l'operato** degli AS.
Adozione di **sistemi di registrazione degli accessi logici (client e server) alle macchine e agli archivi elettronici**. **Log di accesso** devono essere **completi**, **inalterabili** e consentire la **verifica di integrità**.
Registrazioni devono includere **riferimenti temporali** e **descrizione** dell'**evento** e vanno **conservate per almeno 6 mesi**. Non sono registrate le attività eseguite.



# Controllo a distanza dei lavoratori

**Statuto dei lavoratori** (L. 300/70) pone limiti e divieti, ribaditi dal Codice privacy.
**Art. 4 'Impianti audiovisivi e altri sistemi di controllo'**
Gli **impianti audiovisivi** e gli altri strumenti da cui derivi anche la possibilità di **controllo a distanza** dell'attività dei **lavoratori** possono essere impiegati esclusivamente per **esigenze organizzative e produttive**, per la **sicurezza del lavoro** e per la **tutela del patrimonio aziendale** e possono essere installati previo **accordo collettivo** stipulato dalla **rappresentanza sindacale unitaria o** dalle **rappresentanze sindacali aziendali**.
*Articolo recentemente modificato con i decreti attuativi del c.d. 'Jobs Act'. Nuove regole in vigore dal 24 settembre 2015.*

# Se manca accordo

In mancanza di accordo gli **impianti e gli strumenti** che consentono il **controllo a distanza** possono essere installati previa **autorizzazione** della **Direzione territoriale del lavoro** o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del **Ministero del lavoro e delle politiche sociali**.

# Attenzione! Eccezione

Le **procedure e regole** viste finora (accordo con i sindacati, autorizzazione della Direzione territoriale del lavoro o del Ministero del lavoro e delle politiche sociali) **non si applicano** agli **strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa** e agli **strumenti di registrazione degli accessi e delle presenze**.

# Uso dei dati

Cosa può fare il datore di lavoro con i dati raccolti?

Le informazioni raccolte sono **utilizzabili** a **tutti i fini connessi al rapporto di lavoro** a condizione che sia data **al lavoratore adeguata informazione:**

- **delle modalità d'uso degli strumenti** e
- **di effettuazione dei controlli** e
- nel **rispetto** di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196 (**Codice privacy**).

IL REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI PERSONALI

# IL REGOLAMENTO (UE) 2016/679

- PUBBLICATO NELLA GUCE L119 DEL 4 MAGGIO 2016
- ENTRATO IN VIGORE IL 24 MAGGIO 2016
- SI APPLICA A DECORRERE DAL **25 MAGGIO 2018**
- ABROGA LA DIRETTIVA 95/46/CE DALLA STESSA DATA
- **DIRETTAMENTE APPLICABILE** IN TUTTI GLI STATI MEMBRI
- **MARGINE DI AUTONOMIA** AGLI STATI MEMBRI SU SPECIFICI AMBITI
- RILEVANTI **OBBLIGHI E RESPONSABILITÀ** A CARICO DI TITOLARI E RESPONSABILI
- NUOVI **ADEMPIMENTI** (VALUTAZIONE D'IMPATTO, REGISTRI TRATTAMENTO, ECC.)
- RAFFORZAMENTO DEI DIRITTI DELL'INTERESSATO

# AMBITO DI APPLICAZIONE TERRITORIALE

- IL REGOLAMENTO **SI APPLICA** AL TRATTAMENTO DI DATI PERSONALI:
- EFFETTUATO DA **TITOLARE** O **RESPONSABILE STABILITO** NELL'**UE**, **INDIPENDENTEMENTE DAL LUOGO DI TRATTAMENTO DEI DATI**
- EFFETTUATO DA **TITOLARE** O **RESPONSABILE NON STABILITO** NELL'**UE**, SE RIGUARDA DATI DI **INTERESSATI** CHE **SI TROVANO NELL'UE**:
  - PER L'OFFERTA DI **BENI** O LA PRESTAZIONE DI **SERVIZI** O
  - PER **MONITORARE** IL LORO **COMPORTAMENTO** ALL'INTERNO DELL'UE.

# AMBITO DI APPLICAZIONE MATERIALE

- IL REGOLAMENTO **SI APPLICA** AL TRATTAMENTO DI DATI PERSONALI:
- INTERAMENTE O PARZIALMENTE **AUTOMATIZZATO** E AL TRATTAMENTO **NON AUTOMATIZZATO** DI DATI PERSONALI CONTENUTI IN UN ARCHIVIO O DESTINATI A FIGURARVI
- IL REGOLAMENTO **NON SI APPLICA** AL TRATTAMENTO DI DATI PERSONALI:
- EFFETTUATO DA PERSONE FISICHE PER L'ESERCIZIO DI **ATTIVITÀ ESCLUSIVAMENTE PERSONALI O DOMESTICHE**
- EFFETTUATO DALLE **AUTORITÀ COMPETENTI** A FINI DI **PREVENZIONE, INDAGINE, ACCERTAMENTO O PERSEGUIMENTO DI REATI O ESECUZIONE DI SANZIONI PENALI, SALVAGUARDIA** CONTRO **MINACCE ALLA SICUREZZA PUBBLICA E** LA **PREVENZIONE DELLE STESSE**

# INFORMATIVA

IDENTITÀ E CONTATTI DI TITOLARE E RESPONSABILE, FINALITÀ DEL TRATTAMENTO, DESTINATARI O CATEGORIE DI DESTINATARI DEI DATI, DIRITTI DELL'INTERESSATO, NATURA OBBLIGATORIA O FACOLTATIVA DEL CONFERIMENTO DEI DATI, ECC.
OVE APPLICABILE, L'**INTENZIONE** DEL TITOLARE DI **TRASFERIRE DATI** PERSONALI A UN **PAESE TERZO** E L'ESISTENZA O L'ASSENZA DI UNA **DECISIONE DI ADEGUATEZZA** DELLA COMMISSIONE O, SE DEL CASO, IL RIFERIMENTO ALLE **GARANZIE APPROPRIATE** O **OPPORTUNE** E I **MEZZI** PER OTTENERE UNA **COPIA** DI TALI **DATI** O IL **LUOGO** DOVE SONO STATI RESI DISPONIBILI
**PERIODO DI CONSERVAZIONE DEI DATI** OPPURE, SE NON È POSSIBILE, I **CRITERI** UTILIZZATI **PER DETERMINARE TALE PERIODO**
ESISTENZA DI UN **PROCESSO DECISIONALE AUTOMATIZZATO**, COMPRESA LA **PROFILAZIONE, ALMENO IN TALI CASI, INFORMAZIONI SIGNIFICATIVE SULLA LOGICA UTILIZZATA, IMPORTANZA E PREVISTE CONSEGUENZE** DI TALE TRATTAMENTO

# CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

IL **TITOLARE** DEVE ESSERE IN GRADO DI **DIMOSTRARE** CHE L'INTERESSATO HA PRESTATO IL PROPRIO **CONSENSO**

SE IL CONSENSO È PRESTATO NEL CONTESTO DI UNA **DICHIARAZIONE SCRITTA CHE RIGUARDA ANCHE ALTRE QUESTIONI**, LA **RICHIESTA DI CONSENSO** È:

- PRESENTATA IN MODO **CHIARAMENTE DISTINGUIBILE** DALLE ALTRE MATERIE,
- IN **FORMA COMPRENSIBILE** E **FACILMENTE ACCESSIBILE**,
- CON UN **LINGUAGGIO SEMPLICE** E **CHIARO**.

NESSUNA PARTE DI UNA TALE DICHIARAZIONE CHE VIOLI IL REGOLAMENTO È VINCOLANTE.

NEL **VALUTARE** SE IL **CONSENSO** SIA STATO **LIBERAMENTE PRESTATO**, SI TIENE NELLA MASSIMA CONSIDERAZIONE L'EVENTUALITÀ, TRA LE ALTRE, CHE L'**ESECUZIONE** DI UN CONTRATTO SIA **CONDIZIONATA AL CONSENSO NON NECESSARIO** ALL'ESECUZIONE DEL CONTRATTO STESSO.

# DIRITTI DELL'INTERESSATO - 1

- **DIRITTO DI ACCESSO**
- TITOLARE FORNISCE UNA **COPIA DEI DATI** OGGETTO DI TRATTAMENTO
- **DIRITTO DI RETTIFICA E CANCELLAZIONE** (C.D. **DIRITTO ALL'OBLIO**)
- TITOLARE HA OBBLIGO DI CANCELLARE I DATI SENZA INGIUSTIFICATO RITARDO SE:
  - DATI NON PIÙ NECESSARI RISPETTO ALLE FINALITÀ
  - INTERESSATO REVOCA IL CONSENSO
  - INTERESSATO SI OPPONE AL TRATTAMENTO
  - DATI TRATTATI ILLECITAMENTE
  - DATI DEVONO ESSERE CANCELLATI PER ADEMPIERE UN OBBLIGO LEGALE

**DIR. DI CANCELLAZIONE NON SI APPLICA** SE IL **TRATTAMENTO** È **NECESSARIO** PER:

- **ADEMPIMENTO DI UN OBBLIGO LEGALE CUI È SOGGETTO IL TITOLARE**
- ESECUZIONE DI UN **COMPITO** SVOLTO NEL **PUBBLICO INTERESSE** O NELL'**ESERCIZIO DI PUBBLICI POTERI** DI CUI È INVESTITO IL **TITOLARE** DEL TRATTAMENTO
- **L'ACCERTAMENTO, L'ESERCIZIO O LA DIFESA DI UN DIRITTO IN SEDE GIUDIZIARIA**

# DIRITTI DELL'INTERESSATO - 2

- **DIRITTO DI LIMITAZIONE DEL TRATTAMENTO**
- **DIRITTO ALLA PORTABILITÀ DEI DATI**
  - **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
  - **TRASMETTERE** TALI **DATI** A UN **ALTRO TITOLARE SENZA IMPEDIMENTI** DA PARTE DEL **TITOLARE CUI LI HA FORNITI**
  - **OTTENERE** LA **TRASMISSIONE DIRETTA DEI DATI DA UN TITOLARE ALL'ALTRO, SE TECNICAMENTE FATTIBILE**
- **DIRITTO DI OPPOSIZIONE** PER MOTIVI CONNESSI ALLA SUA SITUAZIONE PARTICOLARE
- **DIRITTO DI OPPOSIZIONE** PER **MARKETING DIRETTO** O **PROFILAZIONE**

# RESPONSABILE DEL TRATTAMENTO

- EFFETTUA TRATTAMENTI DEI DATI **PER CONTO DEL TITOLARE** DEL TRATTAMENTO
- CON L'**AUTORIZZAZIONE SCRITTA** DEL **TITOLARE** (SPECIFICA O GENERALE) PUÒ **RICORRERE AD ALTRO RESPONSABILE**
- **TRATTAMENTI** DEL **RESPONSABILE** SONO **DISCIPLINATI** DA UN **CONTRATTO** O DA **ALTRO ATTO GIURIDICO**, CHE **VINCOLI** IL **RESPONSABILE AL TITOLARE** E CHE DISCIPLINI: **DURATA** DEL TRATTAMENTO, **NATURA E FINALITÀ** DEL TRATTAMENTO, **TIPO DI DATI, CATEGORIE DI INTERESSATI, OBBLIGHI E DIRITTI** DEL **TITOLARE**
- **ISTRUZIONE DOCUMENTATA** DEL TITOLARE
- **COMMISSIONE** EUROPEA PUÒ STABILIRE **CLAUSOLE** CONTRATTUALI **TIPO**
- CONTRATTO È STIPULATO IN **FORMA SCRITTA**, **ANCHE** IN FORMATO **ELETTRONICO**.

# REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO - 1

- OGNI **TITOLARE** E **RESPONSABILE** DEL TRATTAMENTO TIENE UN **REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO** SVOLTE SOTTO LA PROPRIA RESPONSABILITÀ
- NOME E DATI DI CONTATTO DEL TITOLARE E DEL RESPONSABILE; FINALITÀ DEL TRATTAMENTO; DESCRIZIONE DELLE CATEGORIE DI INTERESSATI E DELLE CATEGORIE DI DATI PERSONALI; CATEGORIE DI DESTINATARI; OVE APPLICABILE, I TRASFERIMENTI DI DATI VERSO UN PAESE TERZO, IDENTIFICAZIONE DEL PAESE TERZO, DOCUMENTAZIONE DELLE GARANZIE ADEGUATE; OVE POSSIBILE, I TERMINI ULTIMI PREVISTI PER LA CANCELLAZIONE DELLE DIVERSE CATEGORIE DI DATI; OVE POSSIBILE, UNA DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE
- I REGISTRI SONO TENUTI IN **FORMA SCRITTA**, ANCHE IN FORMATO ELETTRONICO

# REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO - 2

**NON DEVONO TENERE IL REGISTRO** LE **IMPRESE** ED **ORGANIZZAZIONI** CON **MENO DI 250 DIPENDENTI, A MENO CHE** IL **TRATTAMENTO** CHE ESSE EFFETTUANO POSSA PRESENTARE UN **RISCHIO** PER I DIRITTI E LE LIBERTÀ DELL'**INTERESSATO**, IL TRATTAMENTO **NON** SIA **OCCASIONALE** O **INCLUDA** IL TRATTAMENTO DI **CATEGORIE PARTICOLARI** DI DATI C.D. "**SENSIBILI**" O I **DATI** PERSONALI RELATIVI A **CONDANNE** PENALI E A **REATI**.

# NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ DI CONTROLLO

IN CASO DI **VIOLAZIONE** DEI **DATI PERSONALI** (C.D. “DATA BREACH”), IL **TITOLARE NOTIFICA** LA **VIOLAZIONE** ALL'**AUTORITÀ DI CONTROLLO 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

IL **TITOLARE** DEL TRATTAMENTO **DOCUMENTA** QUALSIASI **VIOLAZIONE** DEI DATI PERSONALI, COMPRESE LE **CIRCOSTANZE** A ESSA RELATIVE, LE SUE **CONSEGUENZE** E I **PROVVEDIMENTI** ADOTTATI PER PORVI RIMEDIO. TALE DOCUMENTAZIONE CONSENTE ALL'AUTORITÀ DI CONTROLLO DI VERIFICARE IL RISPETTO DI QUESTA DISPOSIZIONE

# COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO

- QUANDO LA VIOLAZIONE DEI DATI PERSONALI PUÒ PRESENTARE UN RISCHIO ELEVATO PER I DIRITTI E LE LIBERTÀ DELLE PERSONE, IL TITOLARE COMUNICA LA VIOLAZIONE ALL'INTERESSATO SENZA INGIUSTIFICATO RITARDO.
- NON È RICHIESTA LA COMUNICAZIONE SE:
  - TITOLARE HA ATTUATO MISURE TECNICHE E ORGANIZZATIVE DI PROTEZIONE (ES. CIFRATURA)
  - TITOLARE HA SUCCESSIVAMENTE ADOTTATO MISURE ATTE A SCONGIURARE UN RISCHIO ELEVATO
  - COMUNICAZIONE RICHIEDEREBBE SFORZI SPROPORZIONATI.

# VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

- QUANDO UN TIPO DI **TRATTAMENTO**, IN PARTICOLARE SE PREVEDE L'USO DI **NUOVE TECNOLOGIE**, CONSIDERATI LA NATURA, L'OGGETTO, IL CONTESTO E LE FINALITÀ DEL TRATTAMENTO, PUÒ PRESENTARE UN **RISCHIO ELEVATO**, IL **TITOLARE** EFFETTUA, **PRIMA** DEL **TRATTAMENTO**, UNA **VALUTAZIONE DELL'IMPATTO** DEI TRATTAMENTI PREVISTI SULLA PROTEZIONE DEI DATI PERSONALI. UNA SINGOLA VALUTAZIONE PUÒ ESAMINARE UN INSIEME DI TRATTAMENTI SIMILI CHE PRESENTANO RISCHI ELEVATI ANALOGHI.
- IN PARTICOLARE È RICHIESTA IN CASO DI:
  - **VALUTAZIONE SISTEMATICA E GLOBALE DI ASPETTI PERSONALI,** BASATA SU **TRATTAMENTO AUTOMATIZZATO, PROFILAZIONE,** SU CUI SI FONDANO **DECISIONI CHE HANNO EFFETTI GIURIDICI O INCIDONO SIGNIFICATIVAMENTE**
  - **TRATTAMENTO**, SU **LARGA SCALA**, DI **DATI SENSIBILI** O DI **DATI** RELATIVI A **CONDANNE PENALI**
  - **SORVEGLIANZA SISTEMATICA SU LARGA SCALA** DI UNA **ZONA ACCESSIBILE AL PUBBLICO**

# CONSULTAZIONE PREVENTIVA

IL **TITOLARE**, PRIMA DI PROCEDERE AL TRATTAMENTO, **CONSULTA L'AUTORITÀ DI CONTROLLO** 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.

# RESPONSABILE DELLA PROTEZIONE DEI DATI - 1

IL TITOLARE E IL RESPONSABILE DEL TRATTAMENTO DESIGNANO SISTEMATICAMENTE UN **RESPONSABILE DELLA PROTEZIONE DEI DATI** QUANDO:

- **TRATTAMENTO** EFFETTUATO DA UN'**AUTORITÀ PUBBLICA** O DA UN **ORGANISMO PUBBLICO, ECCETTUATE LE AUTORITÀ GIURISDIZIONALI**
- ATTIVITÀ PRINCIPALI DEL TITOLARE E DEL RESPONSABILE DEL T. = TRATTAMENTI CHE RICHIEDONO IL **MONITORAGGIO REGOLARE E SISTEMATICO** DEGLI INTERESSATI SU **LARGA SCALA**
- ATTIVITÀ PRINCIPALI DEL TITOLARE O DEL RESPONSABILE DEL TRATTAMENTO CONSISTONO NEL **TRATTAMENTO, SU LARGA SCALA, DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI)**

# RESPONSABILE DELLA PROTEZIONE DEI DATI - 2

IL RESPONSABILE DELLA PROTEZIONE DEI DATI 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 DI CUI ALL'ARTICOLO 39.
IL RESPONSABILE DELLA PROTEZIONE DEI DATI 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**.

# PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE

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.

# PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA

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.

# SANZIONI

OGNI **AUTORITÀ DI CONTROLLO** HA IL **POTERE** DI INFLIGGERE UNA **SANZIONE AMMINISTRATIVA PECUNIARIA**, IN FUNZIONE DELLE CIRCOSTANZE DI OGNI SINGOLO CASO

LA VIOLAZIONE DI ALCUNE DISPOSIZIONI (ART. 83, C. 4) È SOGGETTA A 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** (ES. OBBLIGHI DEL TITOLARE DEL TRATTAMENTO E DEL RESPONSABILE DEL TRATTAMENTO EX ART. 8, 11, 25-39, 42 E 43, OBBLIGHI ORGANISMI DI CERTIFICAZIONE E DI CONTROLLO).

LA VIOLAZIONE DI ALTRE DISPOSIZIONI (ART. 83, C. 5) È SOGGETTA A 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** (ES. VIOLAZIONE PRINCIPI DI BASE, CONSENSO, DIRITTI DEGLI INTERESSATI, TRASFERIMENTI A PAESI TERZI, ECC.).

# SANZIONI - LIVELLO NAZIONALE

GLI **STATI MEMBRI** STABILISCONO LE **NORME** RELATIVE ALLE **ALTRE SANZIONI** PER LE **VIOLAZIONI** DEL PRESENTE REGOLAMENTO IN PARTICOLARE PER LE VIOLAZIONI NON SOGGETTE A SANZIONI AMMINISTRATIVE PECUNIARIE EX ART. 83, E

ADOTTANO TUTTI I **PROVVEDIMENTI** NECESSARI PER ASSICURARNE L'**APPLICAZIONE**. TALI SANZIONI DEVONO ESSERE **EFFETTIVE**, **PROPORZIONATE** E **DISSUASIVE**.

OGNI STATO MEMBRO NOTIFICA ALLA COMMISSIONE LE DISPOSIZIONI DI LEGGE ADOTTATE AL PIÙ TARDI ENTRO IL 25 MAGGIO 2018, E COMUNICA SENZA RITARDO OGNI SUCCESSIVA MODIFICA.