CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

# SESSIONE FORMATIVA ON LINE

## CORSO DI FORMAZIONE GDPR BASE

Autore Dott.ssa Gloriamaria Paci

# Gloriamaria Paci

Nata a Rimini nel gennaio del 1969, dopo alcuni anni dedicati all'attività di giornalista pubblicista, nel 1998 decide di scommettere ed investire in un settore allora poco conosciuto: la normativa sulla tutela dei dati personali. Costituita la ditta individuale **Studio Consulenza Privacy Dott.ssa Gloriamaria Paci**, tutt'ora esistente, fornisce consulenza in materia di privacy e sicurezza dei dati personali.

L'esperienza di giornalista pubblicista, affiancata a quella di consulente privacy nel settore pubblico e privato, sia sul territorio italiano che in paesi Extra UE (RSM), verrà impiegata per pubblicare numerosi articoli e testi di settore.

Dall'ottobre 2017 è legale rappresentante dello **Studio Paci & C. Srl**, società specializzata nell'erogazione di servizi svolti nel settore specifico della privacy e della data protection, della sicurezza informatica, qualità, audit, formazione professionale.

Dal 2018 ricopre il ruolo di **Responsabile per la protezione dei dati personali** (Data protection Officer)

Dal 2019 è **Presidente dell'Associazione protezione diritti e libertà privacy APS**, una realtà che porta avanti progetti ed iniziative finalizzate all'aggregazione di quanti sono interessati alla salvaguardia dei diritti e delle libertà personali nell'ambito della protezione dei dati.

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE
PACI
PRIVACY

**Studio Paci & C. Srl**
**Studio Consulenza Privacy Dott.ssa Gloriamaria Paci**
**Via Edelweiss Rodriguez Senior, 13**
**47924 Rimini (Rn)**

**Telefono: 0541 – 1795431**
**Telefax: 0541 - 1794118**
**Cellulare:  347-5244264**
**Mail: info@consulenzepaci.it**
**Sito web: www.consulenzepaci.it**

Seguici sui social!
https://linktr.ee/studiopaci

# PREMESSA

## *Il valore della protezione dei dati personali*

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

*La protezione dei dati quale riconoscimento di un diritto costituzionalmente garantito*

Privacy non significa soltanto diritto di essere lasciati in pace o di proteggere la propria sfera privata

Diritto di controllare l'utilizzo e la circolazione dei propri dati personali che costituiscono il bene primario dell'attuale società dell'informazione

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Associazione Protezione Diritti e Libertà Privacy APS

La protezione dei dati personali è un diritto fondamentale perché tutela la dignità, la libertà, l'identità personale, l'eguaglianza, la non discriminazione, la riservatezza degli individui nei confronti dei soggetti pubblici e privati

# Il diritto alla protezione dei dati personali non è solo un diritto ma garanzia di libertà e democrazia

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Associazione Protezione Diritti e Libertà Privacy APS

Si rende ancora più necessaria l'adozione di politiche sulla sicurezza per tutelare i dati di chi si avvale della rete e dei servizi offerti da enti pubblici e privati

Vanno garantiti i canali di trasmissione e la connessione fra le banche dati.

Per raggiungere la compliance al GDPR è fondamentale la collaborazione fra professionisti e la creazione di modelli integrati

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

*La protezione dei dati personali è contemplata dall'articolo 8 della Carta dei diritti dell'Unione Europea*

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

*Carta dei diritti dell'Unione Europea*

## Art. 8 - Protezione dei dati di carattere personale

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

## *Considerando 4 Regolamento Europeo 2016/679*

(4) Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.

Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

# La normativa

# *Un po' di storia....*

**1995 Direttiva 95/46/CE**
**31/12/1996 Legge n. 675**
**30/6/2003 D. Lgs n. 196/03 – Integrato dal D.Lgs n. 101/2018**

**24 maggio 2016 – Regolamento Europeo 2016/679 (Entrata in vigore)**

**25 maggio 2018 - Regolamento europeo 2016/679 (Data di applicazione)**

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

GUIDA ALL'APPLICAZIONE DEL

# REGOLAMENTO EUROPEO

# IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

EDIZIONE AGGIORNATA **FEBBRAIO 2018**

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679 sostituisce la Direttiva 95/46/CE

Il 24 maggio 2016 è ufficialmente entrato in vigore il Regolamento europeo in materia di protezione dei dati personali (UE) 2016/679

Il testo, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.

A partire dal 25 maggio 2018, in tutti i Paesi della UE, deve essere garantito il perfetto allineamento fra la normativa nazionale in materia di protezione dei dati personali e la disposizione del Regolamento.

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679 sostituirà la Direttiva 95/46/CE

Insieme al GDPR, è stata emanata la Direttiva (UE) n. 2016/680 che si occupa del trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

Per recepire le norme della Direttiva è stato adottato il D. Lgs. n. 51/2018, che individua il Garante quale autorità di controllo anche per i trattamenti sopra richiamati.

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679 sostituirà la Direttiva 95/46/CE

Il Regolamento 2016/679 si applica solo ai trattamenti dei dati personali di ***persone fisiche***

Non disciplina il trattamento dei dati relativi a persone giuridiche

**173** - Considerando che indicano la motivazione degli articoli dell'atto

**99** - Articoli suddivisi in 11 capitoli

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

**Art. 3 - Il Regolamento si applica ai trattamenti dati:**

**Realizzati da titolari e responsabili stabiliti nell'UE**

**Realizzati da titolari e responsabili non stabiliti nell'UE e:**

1. ***Offrono beni o servizi, anche gratuiti, ai cittadini UE***
2. ***Monitorano il comportamento dei cittadini UE***

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# PRINCIPI E DEFINIZIONI

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 5 – Principi applicabili

**I dati devono essere trattati:**

**-In modo lecito, corretto e trasparente**
**-Raccolti per finalità determinate, esplicite e legittime**
**-Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità**
**- Esatti e, se necessario, aggiornati**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 5 – Principi applicabili

-Conservati in forma che consenta l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità

-Trattati in modo garantire una adeguata sicurezza, compresa la protezione mediante misure tecniche ed organizzative adeguate

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 6 – Liceità del trattamento

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

**-L'interessato ha espresso il consenso per una o più specifiche finalità**

**-Il trattamento è necessario all'esecuzione di un contratto**

**-Il trattamento è necessario per adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento**

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

**Art. 6 – Liceità del trattamento**

**-Il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica (*Es. Ente che si occupa di protezione civile*)**

**-Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento**

**- Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o le libertà fondamentali dell'interessato**

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

**Art. 4 - Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»).**

**Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online *o a uno o più elementi* caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## A titolo esemplificativo si considerano dati personali:

**Il nome ed il cognome, il numero di telefono o di cellulare ovvero l'indirizzo e – mail, i dati della carta di credito, i dati relativi ad un pagamento, la rilevazione della temperatura, il codice fiscale, l'immagine fotografica di una persona, le riprese video, una registrazione vocale, una targa automobilistica, un indirizzo IP, la cronologia della navigazione web, impronta digitale, la scansione della retina, le coordinate GPS, le analisi cliniche (pressione sanguigna, il livello di diabete ecc)**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 9 - Categorie particolari di dati personali:

**Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona**

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 10 - Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza è consentito solo sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Si tratta dei dati c.d. *"giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Articolo 4 - Trattamento:

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Per affrontare il nuovo Regolamento europeo sulla tutela dei dati personali occorre un metodo organizzativo privacy

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# LE FIGURE PREVISTE DALLA NORMATIVA

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## L'interessato

È la persona fisica, identificata o identificabile, alla quale si riferiscono i dati

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## *Art. 4, punto 7 - Il Titolare del trattamento*

- È il soggetto, persona fisica, giuridica, autorità pubblica, il servizio o altro organismo, che determina le finalità e i mezzi del trattamento

- In caso di contitolarità più Titolari che determinano congiuntamente le finalità e i mezzi del trattamento) è necessario un accordo interno su ruoli, responsabilità e rapporti con gli interessati (Articolo 26)

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## *Il Titolare del trattamento – Obblighi generali*

- Istituisce un registro delle attività di trattamento

- Mette in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio (compresa una procedura di notifica delle violazioni di dati personali)

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## *Il Titolare del trattamento – Obblighi generali*

- Effettua una valutazione di impatto quando il trattamento presenta rischi elevati per i diritti e le libertà delle persona fisiche

- Designa il RPD (DPO), quando previsto

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## *Art. 28 - Il Responsabile del trattamento*

- È il soggetto, persona fisica, giuridica, autorità pubblica, il servizio o altro organismo, che tratta i dati per conto del Titolare
- Deve presentare garanzie sufficienti per attuare misure tecniche e organizzative adeguate
- Il rapporto tra Titolare e Responsabile è regolato da nomina obbligatoria e documentata con un contratto o altro atto giuridico

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## *Art. 28 - Il Responsabile del trattamento*

- A sua volta un Responsabile può designare un altro responsabile alla condizione che vi sia una autorizzazione scritta, specifica o generale, del Titolare del trattamento
- Il rapporto tra un Responsabile e un altro responsabile deve essere regolato da un atto contrattuale o con altro atto giuridico che specifici compiti e responsabilità
- Il Responsabile dovrà informare immediatamente il Titolare qualora, a suo parere, vi siano violazioni del Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati personali
- Di fronte al Titolare il primo Responsabile risponde anche degli inadempimenti del secondo Responsabile

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## *Art. 29 – Trattamento sotto l'autorità del Titolare o del Responsabile*

- Non è espressamente disciplinato
- Soggetti che agiscono sotto l'autorità del Titolare o del Responsabile e che trattano dati personali
- Obbligo di istruzione

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 2-quaterdecies – D. Lgs 196/03

Art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati)

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che *specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche*, espressamente designate, che operano sotto la loro autorità.

2. 2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

*Art. 29 – Trattamento sotto l'autorità del Titolare o del Responsabile*

- Persone autorizzate al trattamento (ex incaricati): esecutori materiali delle operazioni di trattamento
- Devono rispettare le istruzioni fornite dal titolare
- Devono conservare le credenziali di autenticazione in modo che altre persone (anche colleghi) non ne vengano a conoscenza
- Devono utilizzare i dati solo per l'attività lavorativa svolta
- Non devono fornire dati di cui agli artt. 9 e 10 al di fuori dei soggetti autorizzati a trattare tali dati
- Devono rispettare l'obbligo di riservatezza sui dati trattati afferenti la propria mansione


# Il Responsabile della protezione dei dati (RPD)

**La scheda presenta la figura del Responsabile della protezione dei dati (RPD) in base a quanto previsto dal Regolamento (UE) 2016/679, dalle Linee-guida dell'EDPB e dal Codice in materia di protezione dei dati personali (d.lgs. 196/2003)**

## QUALI SONO I REQUISITI?

Il Responsabile della protezione dei dati, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali,** anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.
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.

## IN QUALI CASI E' PREVISTO?

Dovranno designare obbligatoriamente un RPD:

a) amministrazioni, enti pubblici e autorità giudiziarie nell'esercizio delle loro funzioni;
b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono 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.

## QUALI SONO I COMPITI?

Il Responsabile della protezione dei dati dovrà, in particolare:

a) **sorvegliare l'osservanza del regolamento,** valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
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** .

**La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base alle evoluzioni normative. Per un quadro completo: www.garanteprivacy.it/rpd**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## *ARTT. 37, 38, 39 – Responsabile della protezione dei dati*

Dovranno *designare obbligatoriamente* un Responsabile della protezione dei dati personali:

a) Amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;

b) Tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il controllo *regolare e sistematico degli interessati*

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.

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## *RESPONSABILE PROTEZIONE DATI PUO' ESSERE UN SOGGETTO ESTERNO*

A grandi linee, se si opta per un RPD interno, possono sussistere situazioni di conflitto con riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento.

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## QUALI SONO I REQUISITI

- Il Responsabile della protezione dei dati personali, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. Possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali;
2. Adempiere alle sue funzioni in piena indipendenza ed in assenza di conflitti di interesse;
3. Svolgere la propria attività quale dipendente del titolare o del responsabile oppure sulla base di un contratto di servizio.

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## QUALI SONO I COMPITI

Il Responsabile della protezione dei dati personali dovrà:

a) Informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) Verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;

c) Fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## QUALI SONO I COMPITI

Il Responsabile della protezione dei dati personali dovrà:

d) Fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;

e) Fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

# NUOVI PRINCIPI

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Nuovo principio
## Art. 24 - ACCOUNTABILITY

I dati sono trattati sotto la responsabilità del Titolare del trattamento, che assicura e comprova, per ciascuna operazione, la conformità alle disposizioni del Regolamento

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE
PACI
PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Nuovo principio
## Art. 24 - ACCOUNTABILITY

La responsabilizzazione non si attua solo osservando i principi del Regolamento Europeo ma anche dimostrando che vengono rispettati

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Nuovo principio
## Art. 24 - ACCOUNTABILITY

E’ quindi necessario possedere un corpo normativo procedurale di regole interne ed un sistema di gestione che consenta a posteriori di dimostrare il coretto adempimento

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Nuovo principio
## Art. 24 - ACCOUNTABILITY

L'importanza della responsabilizzazione viene elevata mediante l'introduzione di un esplicito principio di responsabilità che obbliga il titolare del trattamento a dimostrare la piena conformità a tutti gli altri principi in materia di protezione dei dati

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

**Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 4 ottobre 2017**

# Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

## COSA È?

È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGDP)** che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.

## PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione *(accountability)* in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.** Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti**, e **non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

## IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

## CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** *(Chief Information Security Officer, CISO)* e **del responsabile IT.**

## QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

## QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

**La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/regolamentoue**

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Nuovo principio
## Art. 35 - PRIVACY IMPACT ASSESSMENT

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

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Nuovo principio
## Art. 35 - PRIVACY IMPACT ASSESSMENT

Attraverso la valutazione d'impatto il Titolare disporrà delle conoscenze necessarie sulle misure, sulle garanzie e sui meccanismi previsti per attenuare il rischio e assicurare la conformità del trattamento agli standard normativi.

Nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, il WP29 raccomanda di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati.

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Nuovo principio
## Art. 35 - PRIVACY IMPACT ASSESSMENT

Attraverso la valutazione d'impatto il Titolare disporrà delle conoscenze necessarie sulle misure, sulle garanzie e sui meccanismi previsti per attenuare il rischio e assicurare la conformità del trattamento agli standard normativi.

La valutazione d'impatto è richiesta in alcuni casi (a titolo esemplificativo se i dati personali sono trattati per effettuare profilazioni – utilizzo di dati biometrici – sorveglianza di zone accessibili al pubblico – trattamento di categorie particolari di dati personali o di dati relativi a condanne penali e reati).

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Nuovo principio
# Art. 35 - PRIVACY IMPACT ASSESSMENT

| | | |
|---|---|---|
| Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero). | - Dati sensibili o dati aventi carattere estremamente personale.<br>- Dati riguardanti soggetti interessati vulnerabili<br>- Trattamento di dati su larga scala. | **SI** |
| L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe | - Monitoraggio sistematico<br>- Uso innovativo o applicazione di soluzioni tecnologiche od organizzative. | SI |
| Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc. | - Monitoraggio sistematico<br>- Dati riguardanti soggetti interessati vulnerabili. | SI |
| La raccolta di dati pubblici dei media sociali per la generazione di profili. | - Valutazione o assegnazione di un punteggio.<br>- Trattamento di dati su larga scala.<br>- Creazione di corrispondenze o combinazione di insiemi di dati.<br>- Dati sensibili o dati aventi carattere estremamente personale. | SI |

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Nuovo principio
# Art. 35 - PRIVACY IMPACT ASSESSMENT

| | | |
|---|---|---|
| Istituzione che crea una banca dati antifrode e di gestione del rating del credito a livello nazionale. | Valutazione o assegnazione di un punteggio.<br>- Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente<br>- Impedisce agli interessati di esercitare un diritto<br>o utilizzare un servizio o un contratto<br>- Dati sensibili o dati aventi carattere estremamente personale. | **SI** |
| Conservazione per finalità di archiviazione di dati sensibili personali pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o sperimentazioni cliniche. | Dati sensibili<br>- Dati riguardanti soggetti interessati vulnerabili.<br>- Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o<br>un contratto. | SI |

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Nuovo principio
# Art. 35 - PRIVACY IMPACT ASSESSMENT

| Esempi di trattamento | Possibili criteri pertinenti | E' Richiesta |
|---|---|---|
| Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91). | - Dati sensibili o dati aventi carattere estremamente Personale<br>- Dati riguardanti soggetti interessati vulnerabili. | **NO** |
| Una rivista online che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati. | - Trattamento dati su larga scala | NO |
| Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web.<br>- Valutazione o assegnazione di un punteggio. | - Valutazione o assegnazione di un punteggio | **NO** |

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Nuovo principio
## Art. 25 - PRIVACY BY DESIGN

*Privacy by design* significa protezione dei dati fin dalla progettazione.

Il Titolare dovrà ridurre al minimo il trattamento dei dati personali, mediante l'utilizzo di misure (tecniche ed organizzative) quali a titolo esemplificativo, la pseudonimizzazione dei dati personali.

Tali misure devono essere adottate in fase di sviluppo, progettazione, selezione ed utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni devono tenere conto del diritto alla protezione dei dati, in modo da assicurarsi che i titolari ed i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati personali.

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Nuovo principio
## Art. 25 - PRIVACY BY DESIGN E BY DEFAULT

*Privacy by default* significa che la tutela della protezione del dato deve diventare l'impostazione predefinita.

Il Titolare del trattamento deve adottare misure tecniche ed 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.

Tale principio punta a prevenire piuttosto che a correggere nonché ad utilizzare il minor numero possibile di dati personali….

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Nuovo principio
## Art. 25 - PRIVACY BY DESIGN PRIVACY BY DEFAULT

- *Lucchetti e serrature*
- *Firewall*
- *Antivirus/antimalware*
- *Allarmi anti-intrusione*
- *Sistemi di sorveglianza*
- *Backup, Recovery*
- *Disaster Recovery*
- *Business Continuity*
- *Governance, Risk & Compliance*

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# NUOVI OBBLIGHI GENERALI

Associazione
Protezione Diritti e Libertà
Privacy

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 30 – I REGISTRI DELLE ATTIVITA' DI TRATTAMENTO

Il Titolare del trattamento ed il Responsabile del trattamento devono tenere i registri delle attività di trattamento effettuati.

Tale adempimento formale va a sostituire la notificazione di cui all'art. 37 del D.Lgs n. 196/03 e prevede i contenuti previsti dal Dpss.

Tali documenti sono di due tipi:

- Il Registro del Titolare del trattamento
- Il Registro del Responsabile del trattamento

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 30 – IL REGISTRO DEL TITOLARE DEVE CONTENERE

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;
– le finalità del trattamento;
– una descrizione delle categorie di interessati e delle categorie di dati personali;
– le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
– 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;
– 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 di cui all'articolo 32 paragrafo 1.

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 30 – IL REGISTRO DEL RESPONSABILE DEVE CONTENERE

– il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
– le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
– 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;
– ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

# Violazioni di dati personali *(data breach)*

## *Gli adempimenti previsti*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

**Il Garante per la protezione dei dati personali ha adottato una serie di provvedimenti che fissano per amministrazioni pubbliche e aziende l'obbligo di comunicazione nei casi in cui - a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o comunque trattati. La scheda, che ha mere finalità divulgative, riassume i casi finora esaminati.**

### SOCIETA' TELEFONICHE E INTERNET PROVIDER

**Art. 32-*bis* del Codice in materia di protezione dei dati personali (d. lgs. 196/2003), Regolamento UE 611/13, Provvedimento del Garante n. 161 del 4 aprile 2013 [doc. web n. 2388260]**

- **L'obbligo di comunicazione al Garante** *(mediante un apposito modello di comunicazione)* riguarda i fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli *internet point*, le reti aziendali).
- In caso di violazione dei dati personali, società di tlc e Isp **devono**:
  a. **entro 24 ore** dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione
  b. **entro 3 giorni dalla scoperta,** informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 161 del 4 aprile 2013.
- La comunicazione agli utenti **non è dovuta** se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati.
- Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un **inventario** costantemente aggiornato delle violazioni subite.
- **SANZIONI AMMINISTRATIVE PREVISTE (art. 162-*ter* del Codice in materia di protezione dei dati personali)**
  - per mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro;
  - per omessa o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata;
  - per mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.

### BIOMETRIA

**Provvedimento n. 513 del 12 novembre 2014 [doc. web n. 3556992]**

- **Entro 24 ore** dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

### DOSSIER SANITARIO ELETTRONICO

**Provvedimento n. 331 del 4 giugno 2015 [doc. web n. 4084632]**

- **Entro 48 ore** dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

### AMMINISTRAZIONI PUBBLICHE

**Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029]**

- **Entro 48 ore** dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

**Per approfondimenti, consultare i provvedimenti pubblicati sul sito: www.garanteprivacy.it**

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Artt. 33, 34 – Data Breach

Il titolare del trattamento dovrà comunicare entro 72 ore, dal momento dell'individuazione, **eventuali violazioni dei dati personali (data breach) all'Autorità nazionale di protezione dei dati (Autorità di controllo)**.

Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato ***anche tutti gli interessati*** e offrire indicazioni su come intende limitare le possibili conseguenze negative.

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Artt. 33, 34 – Data Breach

Se il numero delle persone coinvolte è elevato, è comunque richiesta una comunicazione pubblica o adatta a raggiungere quanti più interessati possibile (ad esempio, tramite un'inserzione su un quotidiano o una comunicazione sul sito web del titolare).

L'Autorità di protezione dei dati potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Considerando 85

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio:

- Perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti;
- Discriminazione;
- Furto o usurpazione d'identità;
- Perdite finanziarie;
- Decifratura non autorizzata della pseudonimizzazione;
- Pregiudizio alla reputazione;
- Perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 32 – SICUREZZA DEL TRATTAMENTO

La valutazione dei rischi, a differenza della valutazione di impatto che è un'attività riservata ai rischi elevati e presuppone il coinvolgimento, nelle ipotesi più delicate l'Autorità Garante, è sempre necessaria, poiché è sempre necessaria la sicurezza dei trattamenti

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 32 – SICUREZZA DEL TRATTAMENTO

Qualche esempio di misure tecniche

-Pseudononimizzazione
-Cifratura
-Minimizzazione dei dati e trattamenti
-Definizione del periodo di conservazione ed accessibilità dei dati

Qualche esempio di misura organizzativa

-Designazioni e suddivisioni delle responsabilità
- Predisposizione di policy, disciplinari, linee guida interne
- Formazione per incaricati
- Adesioni a codici di condotta o conseguimento di certificazioni

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 32 – SICUREZZA DEL TRATTAMENTO

Se le misure non vengono adottate correttamente, possono insorgere rischi per i diritti e le libertà delle persone fisiche.

I danni che ne conseguono all'interessato si suddividono:

- Danni immateriali: perdita del controllo sui dati personali, la limitazione dei diritti dell'interessato, la discriminazione, il pregiudizio alla reputazione, la perdita di riservatezza dei dati personali protetti da segreto professionale, il furto o l'usurpazione d'identità;

- Danni materiali: violazioni delle misure di sicurezza – come la decifratura non autorizzata della pseudononimizzazione o la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati – ma anche le perdite finanziarie e gli altri rischi economici.

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# NUOVI DIRITTI

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

Scheda di sintesi a mero scopo divulgativo. Per un quadro completo della materia, si rimanda alla legislazione in tema di protezione dei dati personali e ai provvedimenti dell'Autorità.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Conosci i principali diritti previsti dal Regolamento (UE) 2016/679?

Il Regolamento (articoli 15-22) riconosce importanti diritti in materia di protezione dei dati personali, che possono essere esercitati rivolgendosi al titolare del trattamento (soggetto pubblico, impresa, associazione, partito, persona fisica, ecc.).

## Accesso ai propri dati personali

Hai il diritto di sapere se è in corso un trattamento di dati personali che ti riguardano e - se confermato - di ottenere una copia di tali dati ed essere informato su: l'origine dei dati; le categorie di dati personali trattate; i destinatari dei dati; le finalità del trattamento; l'esistenza di un processo decisionale automatizzato, compresa la profilazione; il periodo di conservazione dei dati; i diritti previsti dal Regolamento.

## Rettifica, cancellazione, limitazione del trattamento, portabilità dei dati personali

Puoi chiedere - nei casi previsti dal Regolamento - che i dati personali a te riferiti siano rettificati o cancellati, o che ne venga limitato il trattamento. Puoi inoltre chiedere che i dati che tu hai fornito al titolare siano trasferiti ad un altro titolare («diritto alla portabilità»), nel caso in cui il trattamento si basi sul tuo consenso o su un contratto con te stipulato e venga effettuato con mezzi automatizzati .

## Opposizione al trattamento

Puoi opporti al trattamento dei tuoi dati personali per motivi connessi alla tua situazione particolare, da specificare nella richiesta; oppure senza necessità di motivare l'opposizione, quando i tuoi dati sono trattati per finalità di marketing diretto.

## Come si esercitano questi diritti?

Puoi presentare, gratuitamente e senza particolari formalità (per esempio, tramite posta elettronica, posta raccomandata, ecc.), una richiesta di esercizio dei diritti al titolare del trattamento (sul sito www.garanteprivacy.it è disponibile un modulo facsimile) . Il titolare del trattamento è tenuto entro 1 mese a rispondere alla richiesta, o a comunicare un eventuale ritardo nella risposta in caso di richieste numerose e/o complesse (la proroga non può comunque superare i 2 mesi). Se la risposta non perviene nei tempi indicati o non la ritieni soddisfacente, puoi rivolgerti al Garante per la protezione dei dati personali, mediante un reclamo ai sensi dell'art. 77 del Regolamento, oppure all'autorità giudiziaria.

**Scopri di più su: www.garanteprivacy.it/home/diritti**

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Il Regolamento comporterà

Maggiore tutela delle informazioni dei residenti europei riguardo alla navigazione Internet e presenti nei cloud computing con l'introduzione di nuovi diritti:

-Portabilità dei dati

-Diritto all'oblio

-Diritto di essere informati in caso di violazioni (Data Breaches)

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

ù

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI


# Il diritto alla portabilità dei dati (art. 20 RGPD)

**La scheda presenta gli elementi generali del diritto alla «portabilità dei dati» introdotto dal Regolamento (UE) 2016/679, entrato ufficialmente in vigore il 24 maggio 2016 e che sarà direttamente applicato in tutti gli Stati membri a partire dal 25 maggio 2018**

## COSA È?

È un diritto innovativo previsto dall'**articolo 20** del Regolamento che e consente all'interessato di **ricevere** i dati personali forniti a un titolare, in **un formato strutturato, di uso comune e leggibile da dispositivo automatico**, e di **trasmetterli** ad un **altro titolare del trattamento senza impedimenti**.

## QUALI VANTAGGI PUO' OFFRIRE?

- facilitare il **passaggio da un fornitore di servizi all'altro** fungendo, quindi, da fattore di promozione della concorrenza fra i singoli fornitori;
- consentire la **creazione di nuovi servizi** nel quadro della strategia per il mercato unico digitale;
- offrire la possibilità di **«riequilibrare» il rapporto fra interessati e titolari del trattamento** tramite l'affermazione dei diritti e del controllo spettanti agli interessati in rapporto ai dati personali che li riguardano.

## COSA PERMETTE DI FARE?

- **ricevere dati personali** trattati da un titolare e **conservarli** su un supporto personale in vista di un utilizzo ulteriore per scopi personali, senza trasmetterli a un altro titolare *(ad es. recuperare l'elenco dei brani musicali preferiti detenuto da un servizio di musica in streaming, per scoprire quante volte si sono ascoltati determinati brani);*
- **trasmettere dati personali da un titolare del trattamento a un altro titolare del trattamento** *(ad es, un diverso fornitore di servizi).*

L'esercizio del diritto alla portabilità dei dati **non pregiudica** nessuno degli altri diritti dell'interessato che può, ad esempio,

- continuare a fruire del servizio offerto dal titolare anche dopo un'operazione di portabilità;
- esercitare il diritto di cancellazione.

## QUANDO TROVA APPLICAZIONE?

Occorre siano soddisfatte **tre condizioni:**

1. i dati personali devono essere **trattati attraverso strumenti automatizzati** (quindi sono esclusi gli archivi cartacei), sulla base del **consenso preventivo dell'interessato** o per l'**esecuzione di un contratto** di cui è parte l'interessato;
2. i dati personali di cui si chiede la portabilità devono **riguardare l'interessato** ed essere quelli **forniti dall'interessato consapevolmente e in modo attivo** *(ad es.: i dati di registrazione - indirizzo postale, nome utente, età, ecc.- inseriti compilando un modulo online*). Sono compresi anche i dati **generati e raccolti** attraverso le **attività dell'utente** che fruisce di un servizio o utilizza un dispositivo.
   Il diritto alla portabilità **non** si applica invece ai dati personali che sono **derivati o dedotti** dalle informazioni **fornite dall'interessato** *(ad es.: il profilo-utente creato analizzando i dati grezzi di un contatore intelligente*), poiché non si tratta di dati forniti dall'interessato bensì creati dal titolare del trattamento.
3. l'esercizio del diritto alla portabilità **non deve ledere i diritti e le libertà altrui**. Ad es., se l'insieme dei dati trasferiti su richiesta dell'interessato contiene dati personali che riguardano altre persone fisiche, il nuovo titolare dovrebbe trattarli solo in presenza di un'idonea base giuridica.

**La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento.**
**Per un quadro completo si invita a consultare la pagina [www.garanteprivacy.it/portabilita](www.garanteprivacy.it/portabilita)**

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

***CODICI DI CONDOTTA E CERTIFICAZIONI***

***AUTORITA' DI CONTROLLO***

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# INFORMATIVA E CONSENSO

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 13 – Informazioni da fornire all'interessato

- L'informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti.
- Per facilitare la comprensione dei contenuti, nell'informativa si potrà fare ricorso anche a icone, identiche in tutta l'Unione europea.
- Gli interessati dovranno sapere se i loro dati sono trasmessi al di fuori dell'Ue e con quali garanzie; cosi come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti, come quelli a fini di marketing diretto.

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art. 13 – Informazioni da fornire all'interessato

### *Requisiti informativa*

- Eventuale trasferimento verso Paesi extra-UE e relativo strumento di liceità
- Periodo di conservazione o criteri per determinarlo
- Diritti dell'interessato, compreso quello di proporre reclamo all'Autorità di controllo
- L'identità e dati di contatto del Titolare e ove applicabile del Rappresentante – Responsabile per la protezione dei dati
- La base giuridica per ogni finalità del trattamento
- Se si persegue un obiettivo di interesse pubblico indicare quale sia e se è proporzionato all'obiettivo legittimamente perseguito
- Gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# IMPIANTO SANZIONATORIO

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Art 83 - TIPOLOGIA

**Sanzioni amministrative – Disciplinate dal Regolamento**

**Sanzioni penali (anche pecuniarie) – Rimesse agli stati membri**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Responsabilità civile - Art. 82, - 1

**Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile del trattamento**

**Un Titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il Regolamento**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Responsabilità civile

**Un Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del Regolamento specificatamente diretti ai Responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare**

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Responsabilità civile

**Il Titolare del trattamento o il Responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Responsabilità civile

**Qualora più Titolari o Responsabili del trattamento siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni Titolare o Responsabile, è responsabile in solido per l'intero ammontare del danno con diritto di rivalsa**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## Responsabilità civile

**Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## CARATTERISTICHE

Il Regolamento Europeo precisa che le sanzioni amministrative pecuniarie devono essere in concreto *effettive*, *proporzionate* e *dissuasive*

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

## OMOGENEITA' NELL'APPLICAZIONE

Il Comitato Europeo elabora per i Garanti le «Linee guida sulla fissazione delle sanzioni amministrative»

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Nel fissare l'ammontare di una sanzione amministrativa si terrà *conto della natura*, della *gravità* e della *durata della violazione*, del *carattere doloso o colposo* e del *grado di cooperazione* con l'Autorità di controllo

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

La violazione delle disposizioni seguenti è soggetta a sanzioni amministrative fino a 10.000.000 €, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

Consenso minori;
Trattamento che non richiede identificazione;
Protezione dei dati by design e by default;
Obblighi dei contitolari;
Stabilimento in ambito UE;
Doveri del Responsabile del trattamento;
Trattamenti consentiti;
La registrazione dei trattamenti;
La cooperazione con le autorità di supervisione;
Sicurezza del trattamento;
Notificazione del Data breach e sua comunicazione all'interessato;
Data Protection Impact Assessment;
Consultazione preventiva;
Designazione, Posizione, Attribuzioni del DPO;
Certificazioni e organismi di certificazione;
Monitoraggio dei codici di condotta

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

La violazione delle disposizioni seguenti è soggetta a sanzioni amministrative fino a 20.000.000 €, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

Principi sul trattamento dei dati;
Legalità del trattamento;
Consenso;
Trattamento di speciali categorie di dati;
Diritti dell'interessato;
Trasferimento dei dati in ambito extra UE;
Trattamento in ambito giornalistico e del diritto di espressione;
Rispetto delle disposizioni delle autorità;
Accesso ai dati da fonti pubbliche;
Trattamento dei numeri identificativi;
Trattamento dei dati del personale;
Trattamenti archivistici di interesse pubblico riguardo dati scientifici, storici, di ricerca, o statistici;
Obbligo di segretezza;
Opinioni religiose

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# CONSIGLI DI CARATTERE GENERALE

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati

- Se, e quando è possibile, tenere la scrivania e l'apparecchio telefonico lontano dalla porta d'ingresso o da sportelli informativi riducendo il tono della voce

- Il monitor dell'elaboratore deve essere rivolto verso l'incaricato e non visibile dai soggetti esterni

- Quando si procede alla registrazione dei dati, verificare se sono stati trascritti con esattezza

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati

- In linea generale, non fornire telefonicamente dati e informazioni di carattere sensibile (soprattutto sanitari e giudiziari) se non si è certi dell'identità del destinatario

- Nel trasmettere via fax o mail certificati medici, referti, esami clinici o documenti similari contenenti comunque dati particolari potrebbe essere opportuno chiamare il destinatario per accertare la sua presenza per la ricezione ovvero si potrebbe comunicare un codice identificativo del soggetto interessato e quindi inviare la copia della documentazione in forma cifrata limitando la possibilità di conoscenza dei dati identificativi dell'interessato nei soli casi indispensabili

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati

- Attenzione ad avere certezza sull'identità dell'interlocutore che deve essere autorizzato a trattare i dati in questione

- Attenzione all'uso di telefoni cellulari per finalità di servizio. Nel comunicare informazioni di terzi, parlare sottovoce per evitare che soggetti non autorizzati possano venire impropriamente a conoscenza di dati

- In caso di assenza dell'incaricato per malattia, non comunicare tale informazione a terzi. Limitarsi a riferire il giorno in cui l'incaricato sarà nuovamente al lavoro

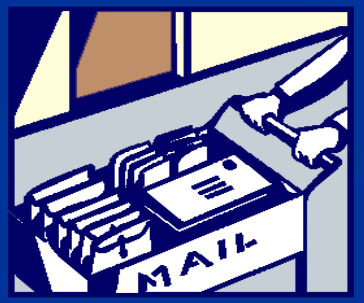
Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati

- Evitare di lasciare incustoditi su scrivanie, tavoli, sale d'aspetto, centralino, e singoli uffici aperti al pubblico, cartelle cliniche, tabulati, moduli, cartelle, atti, fascicoli e ogni tipo di documenti che contengano dati personali

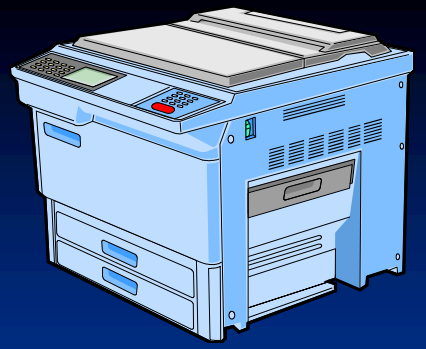
- Particolare attenzione deve essere prestata al trasporto del materiale da e per l'archivio.
  Lo smistamento dei materiali terminali l'elaborazione (stampe, tabelle, tabulati, registri ecc), ai fini della sicurezza riveste un'importanza straordinaria. Per evitare che informazioni raccolte e da trasmettere finiscano al personale non autorizzato. Può essere d'aiuto **creare un registro di invio** e di consegna dei vari documenti da inviare ai destinatari




Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati



- Ridurre o limitare il numero delle fotocopie effettuate.
  In presenza di più soggetti autorizzati al trattamento è possibile assegnare codici identificativi personali in modo da avere una traccia del numero delle fotocopie effettuate dai singoli incaricati

- Non lasciare le fotocopie non riuscite vicino alla fotocopiatrice ma procedere alla loro distruzione

- Con una scansione viene copiata l'immagine del documento, memorizzata su hard disk e conservata all'interno della macchina.
  Immagine che potrà anche essere stampata conservandone il file. La fotocopiatrice diventa uno strumento elettronico a tutti gli effetti

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati

- Se l'invio di documenti originali o fotocopie deve avvenire per posta ordinaria, è preferibile utilizzare una raccomandata che consente di tracciare il movimento del documento ed offre maggiori garanzie dell'avvenuta consegna al destinatario

- Qualunque sia il tipo di spedizione adottato, verificare sempre che il destinatario abbia ricevuto tutti i documenti privi di alterazioni o manomissioni effettuate in fase di trasporto

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati

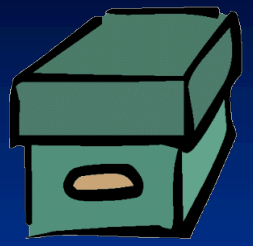
- Utilizzare, se è possibile, l'apparecchio distruggi-documenti.
  Si dovrebbe sempre provvedere a distruggere adeguatamente
  i documenti cartacei prima di gettarli, preferendo lo strappo sistematico
  invece dell'accartocciamento dei fogli.
  Questo vale per ricevute, post-it con
  appunti (soprattutto quelli annotati
  durante le telefonate) e in genere tutto
  il materiale destinato ad essere cestinato

- Attenzione a riciclare la carta, per prendere appunti, poichè potrebbe
  contenere importanti documenti

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati



- Per un corretto smaltimento, i documenti devono essere inseriti in contenitori chiusi (buste, scatoloni, contenitori plastici) senza specificarne il contenuto

- Per la raccolta differenziata della carta, assicurarsi che i contenitori consegnati agli operatori vengano smaltiti secondo procedura

- Prima di procedere allo smaltimento, evitare di lasciare incustoditi scatoloni fuori o dentro i locali. Verificare la posizione dei contenitori per il smaltimento della carta

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati

- All'accensione del Pc o del terminale, digitare la parola chiave possibilmente senza farsi vedere da occhi indiscreti

- Nel caso si utilizzino strumenti elettronici, quando si fanno pause e, comunque ogni volta che si abbandona la propria postazione di lavoro per un periodo prolungato, i personal computer vanno posti in posizione di attesa, utilizzando lo screensaver (eventualmente con password)

- Assicurarsi che sia presente un controllo antivirus sui file utilizzati

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati


- Scegliere una password originale.
  Da evitare nomi propri, comuni, di familiari o animali da salotto.
  Non trascriverla o annotarla su fogli lasciati incustoditi
  e visibili ad estranei.

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati


- **Sono la prima e spesso l'unica tutela che abbiamo**

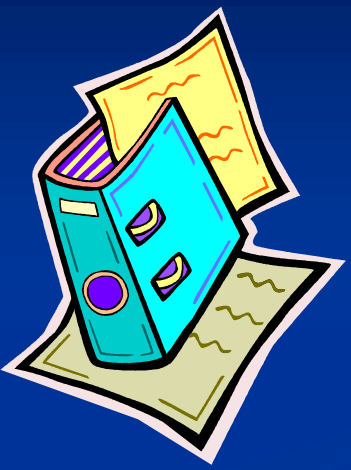
  Ricordarsi che la maggioranza degli attacchi avviene perchè l'attaccante viene a conoscenza della password della vittima:
  - scoprendola (password lasciata in evidenza e/o in chiaro)
  - indovinandola (password legata ad informazioni note dell'utente)
  - ricostruendola (password troppo corta e troppo semplice)
  - trafugandola (password utilizzata su un altro servizio compromesso)

- **Regole di comportamento da adottare:**
  - mai usare la stessa password per piu servizi e/o account diversi
  - evitare di usare riferimenti personali e/o parole di senso compiuto
  - sceglierle piuttosto lunghe (almeno otto caratteri)
  - aggiungere cifre e caratteri speciali (meglio se non all'inizio o alla fine)
  - cambiarle periodicamente…valgono i 3 mesi dell'Allegato B)

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE
PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati



- Adottare un sistema che limiti il numero di accessi falliti in fase di autenticazione dell'utente

- Predisporre un registro delle violazioni o dei tentativi di violazione per prevenire o accertare possibili accessi non autorizzati

- Effettuare controlli periodici sulle operazioni svolte dagli incaricati alla manutenzione software ed hardware per accertarsi che nello svolgimento delle loro mansioni non accedano, neppure accidentalmente, ai dati personali che non rientrano nel loro profilo di autorizzazione

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati

- Eseguire obbligatoriamente il controllo antivirus di ogni file allegato ricevuto via e-mail (anche nel caso in cui si conosca il mittente)

- Nel caso si presentino questi sintomi (messaggi strani, impossibilità di accedere al disco, mancanza di spazio su disco, perdita di file o aumento del volume dei file, ecc), è possibile, anzi, quasi sicuramente si è in presenza di un virus

- Se già si è verificato un incidente informatico, poiché le probabilità che se ne verifichino di nuovi sono maggiori, le aree di rischio dovranno essere esaminate con maggiore attenzione (dalla singola stazione di lavoro, alle stampanti, ai supporti di memorizzazione, ecc.)

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati

- Fare aggiornamenti automatici a programmi da possibili vulnerabilità o difetti (Patch)

- Al termine della giornata lavorativa, spegnere sempre il Pc o il terminale della propria postazione di lavoro

- Rivolgersi all'Amministratore di sistema in caso di anomalie

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Privacy in pillole
# Accorgimenti per il trattamento dati

## Supporti removibili

- Fare una verifica presso gli uffici ed accertarsi che non vi siano supporti removibili (chiavette usb, hard disk esterni ecc) non più utilizzati. Previa verifica del contenuto procedere alla distruzione degli stessi

- Per evitare malfunzionamenti dei supporti, non esporli a temperature troppo alte o troppo basse

- Dopo aver proceduto alla formattazione completa per un eventuale riutilizzo, ove questo sia tecnicamente possibile, se dovessero danneggiarsi è necessario distruggerli per evitare che soggetti non autorizzati procedano al recupero dei dati

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# IL PHISHING: Attenzione ai «pescatori» di dati personali

Il phishing è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda - username e password, codici di accesso (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito – con l'intento di compiere operazioni fraudolente.

La truffa avviene di solito via e-mail, ma possono essere utilizzati anche sms, chat e social media. Il «ladro di identità» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali, per gestire la pratica per un rimborso fiscale o una cartella esattoriale, ecc..

In genere, i messaggi di phishing invitano a fornire direttamente i propri dati personali, oppure a cliccare un link che rimanda ad una pagina web dove è presente un *form* da compilare. I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

## ALCUNI CONSIGLI PER DIFENDERSI

### 1. IL BUON SENSO PRIMA DI TUTTO

Dati, codici di accesso e password personali non dovrebbero mai essere comunicati a sconosciuti. E' bene ricordare che, in generale, banche, enti pubblici, aziende e grandi catene di vendita non richiedono informazioni personali attraverso e-mail, sms, social media o chat: quindi, meglio evitare di fornire dati personali, soprattutto di tipo bancario, attraverso tali canali. Se si ricevono messaggi sospetti, è bene non cliccare sui link in essi contenuti e non aprire eventuali allegati, che potrebbero contenere virus o programmi *trojan horse* capaci di prendere il controllo di pc e smartphone. Spesso dietro i nomi di siti apparentemente sicuri o le URL abbreviate che si trovano sui social media si nascondono link a contenuti non sicuri. Una piccola accortezza consigliata è quella di posizionare sempre il puntatore del mouse sui link prima di cliccare: in molti casi si potrà così leggere in basso a sinistra nel browser il vero nome del sito cui si verrà indirizzati.

### 2. OCCHIO AGLI INDIZI

I messaggi di phishing sono progettati per ingannare e spesso utilizzano imitazioni realistiche dei loghi o addirittura delle pagine web ufficiali di banche, aziende ed enti. Tuttavia, capita spesso che contengano anche grossolani errori grammaticali, di formattazione o di traduzione da altre lingue. E' utile anche prestare attenzione al mittente (che potrebbe avere un nome vistosamente strano o eccentrico) o al suo indirizzo di posta elettronica (che spesso appare un'evidente imitazione di quelli reali). Meglio diffidare dei messaggi con toni intimidatori, che ad esempio contengono minacce di chiusura del conto bancario o di sanzioni se non si risponde immediatamente: possono essere subdole strategie per spingere il destinatario a fornire informazioni personali.

### 3. PROTEGGERSI MEGLIO

E' utile installare e tenere aggiornato sul pc o sullo smartphone un programma antivirus che protegga anche dal phishing. Programmi e gestori di posta elettronica hanno spesso sistemi di protezione che indirizzano automaticamente nello spam la maggior parte dei messaggi di phishing: è bene controllare che siano attivati e verificarne le impostazioni. Meglio non memorizzare dati personali e codici di accesso nei browser utilizzati per navigare online. In ogni caso, è buona prassi impostare password alfanumeriche complesse, cambiandole spesso e scegliendo credenziali diverse per ogni servizio utilizzato: banca online, e-mail, social network, ecc. *[vedi anche la scheda del Garante con i consigli per gestire le password in sicurezza ]*, a meno di disporre di sistemi di autenticazione forte (*strong authentication*).

### 4. ACQUISTI ONLINE IN SICUREZZA

Se si fanno acquisti online, è più prudente usare carte di credito prepagate o altri sistemi di pagamento che permettono di evitare la condivisione di dati del conto bancario o della carta di credito.

### 5. LA PRUDENZA NON E' MAI TROPPA

Per proteggere conti bancari e carte di credito è bene controllare spesso le movimentazioni e attivare sistemi di *alert* automatico che avvisano l'utente di ogni operazione effettuata. Nel caso si abbia il dubbio di essere stati vittime di phishing è consigliabile contattare direttamente la banca o il gestore della carta di credito attraverso i canali di comunicazione conosciuti e affidabili.


Per segnalazioni e richieste di ulteriori informazioni: urp@gpdp.it

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# MISURE DI SICUREZZA

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Art. 32 – SICUREZZA DEL TRATTAMENTO

La valutazione dei rischi, a differenza della valutazione di impatto che è un'attività riservata ai rischi elevati e presuppone il coinvolgimento, nelle ipotesi più delicate l'Autorità Garante, *è sempre necessaria, poiché è sempre necessaria la sicurezza dei trattamenti*

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Art. 32 – SICUREZZA DEL TRATTAMENTO

Mantenere e garantire la sicurezza delle informazioni è un requisito fondamentale per evitare che siano effettuati trattamenti dati in violazione del Regolamento Europeo

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

**ERRORI DA EVITARE….**

Non bisogna confondere la gestione dei rischi con il tema delle misure di sicurezza

Il rischio non si riferisce al titolare ma al soggetto interessato

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

**Regolamento UE 2016/679**

**Valutazione dei rischi inerenti il trattamento dei dati personali**

**distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale**

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

**Capire se i processi di sicurezza informatica sono adeguati per proteggere le informazioni aziendali**

**Analizzare i processi ed identificare i rischi di sicurezza per definire le protezioni con il miglior rapporto costo/efficacia**

**Orientare l'Organizzazione a gestire la sicurezza informatica in modo proattivo**

**Giustificare gli investimenti nel settore della sicurezza informatica**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

## Punto di partenza analisi dei rischi

☐ Analisi del contesto e individuazione dei beni da proteggere;
☐ Identificare le minacce;
☐ Identificare le vulnerabilità;
☐ Rapportare le minacce alle vulnerabilità;
☐ Definire l'impatto su ciascun bene delle minacce – vulnerabilità in relazione al mancato rispetto dei requisiti; ☐ Valutare il rischio per ciascun bene

Il rischio non si riferisce al titolare ma al soggetto interessato

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

## Attenzione al fattore umano….

**Inutile investire risorse economiche elevate in apparati tecnologici ultra-sofisticati per difendersi dalle intrusioni informatiche, se si sottovaluta il fattore umano**

**La sicurezza non è un problema di tecnologia, bensì di *persone e gestione***

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

**Attenzione al fattore umano….**

- Scarsa consapevolezza e cultura da parte dell'utente finale
- Errata percezione dei rischi delle azioni nel ciberspazio
- Assunzione fondamentale e che tutti siano in buona fede

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

**Infatti, l'uomo tende naturalmente a:**

- **Collaborare**
- **Avere fiducia negli altri e a mettersi a disposizione (richiesta ragionevole)**
- **Fornire (in buona fede) ad hacker travestiti da colleghi, superiori, consulenti, tecnici informazioni preziosissime, che li metteranno in grado di violare la rete informatica aziendale**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali
# Chi si attacca principalmente

**Addetti alle portinerie, centralinisti, segretarie, custodi:**

- Detengono molte informazioni delle quali ignorano l'importanza
- Scarsa cultura informatica
- Spesso pronti ad eseguire gli ordini impartiti come gentili richieste da un ipotetico superiore

**Addetti ai centri di assistenza clienti (help-desk)**

- Hanno accesso a tantissime informazioni
- Per attitudine professionale sono abituati a fornire informazioni.

**Amministratori di sistema, gli operatori al computer e gli addetti ai sistemi telefonici**

- Detentori delle informazioni più critiche per la sicurezza del
- sistema

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

**Attenzione …..non solo competenze tecniche**

Per gli hacker è assai più facile farsi dare informazioni critiche con tecniche di ingegneria sociale

⇩

Fine Stereotipo Hacker (timido, introverso ecc.)

⇩

L'hacker spesso abbina le capacità informatiche con quelle psicologiche di persuasione e raggiro, al fine di ottenere le informazioni più sensibili

# Analisi dei rischi
# Obiettivi principali

**Da cosa ci si deve difendere**

- **Minacce esterne:**
  - terzi estranei, curiosi od ostili
  - concorrenti sleali
  - organizzazioni criminali
  - hacker, cyberterroristi, tecnovandali, attivisti, ...

- **Minacce interne:**
  - errore, incuria, disattenzione, approssimazione, …
  - dipendenti infedeli, insoddisfatti, vendicativi, ...
  - dipendenti curiosi, smanettoni, "furbi", …
  - personale esterno (consulenti, clienti, fornitori, …)

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

## Fattori di vulnerabilità….

- Bug presenti nei processi e nelle policy aziendali
- Numero elevato di dipendenti distribuiti territorialmente in diverse sedi e stabilimenti
- Presenza di siti web troppo ricchi di informazioni
- Carenze di formazione sulla sicurezza
- Mancata classificazione dei dati
- Assenza di un piano di segnalazione degli incidenti

# Analisi dei rischi
# Obiettivi principali

## Vittime preferite .....

- **Persone che non hanno niente da perdere nel fornire una informazione sensibile**
- **Persone che tendono a sottostimare il pieno valore delle informazioni**
- **Persone che ritengono inutili le procedure (perdita di tempo)**
- **Persone che non valutano appieno le conseguenze delle loro azioni**
- **Persone che sanno di non subire sanzioni disciplinari rivelando informazioni sensibili**

# Analisi dei rischi
# Obiettivi principali

## Cosa si attacca …strumenti fisici

- Telefoni (fisso, cellulare, pubblico)
- Fax
- PC, notebook
- Scanner
- Stampanti
- Server di posta

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

**COME PROTEGGERSI ……..**

**Addestramento ed educazione del personale:**

- ✓ **consapevolezza dei rischi, dell'importanza delle informazioni, delle procedure di sicurezza e dei metodi comunemente adottati dagli hacker**
- ✓ **distruggere il materiale cartaceo**
- ✓ **chiudere uffici e cassettiere**
- ✓ **tenere in ordine le scrivanie**
- ✓ **non inviare password ed account via e-mail**
- ✓ **non essere prevedibili**

**40% del budget sicurezza aziendale**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

**Classificazione delle informazioni:**

**Identificare i documenti protetti.**

**Le informazioni dovrebbero essere quindi suddivise in:**

- ✓ **confidenziali**
- ✓ **personali**
- ✓ **interne**
- ✓ **pubbliche (le sole a poter essere diffuse)**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

## Procedure di identificazione degli esterni:

- ✓ l'identificazione di chiamata
- ✓ in caso di identità sconosciuta interpellare un responsabile
- ✓ far esibire ai dipendenti dei badge (foto)
- ✓ politica che proibisca di dare i numeri interni di dipendenti

# Analisi dei rischi
# Obiettivi principali

## Penetration test:

- simulare attacchi di ingegneria sociale
- verificare se i dipendenti adottano e rispettano le misure di sicurezza
- verificare se i dipendenti riportano i tentativi o i casi di intromissione

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

**Social Network ed ingegneria sociale ….**

- **Nel mondo globalizzato, ogni persona condivide una buona parte di sé direttamente sui social network (Facebook, Twitter , Istantgram ecc…) senza sapere o preoccuparsi che fine facciano le informazioni che pubblica**
- **Le informazioni possono essere assorbite dalla rete e riutilizzate per i fini più vari, spesso criminali (oblio della rete)**
- **I social network rappresentano il luogo ideale - per un ingegnere sociale - dove acquisire numerose informazioni (personali, fotografiche, geografiche, geografiche)**
- **Favoriscono una fase di reperimento (social footprinting) molto più rapida e semplificata**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Analisi dei rischi
# Obiettivi principali

**Come evitare ciò?**

- **Pubblicare il meno possibile (informazioni personali)**
- **Limitare al minimo il numero di foto**
- **Preservare la propria e l'altrui privacy, evitando di offrire informazioni private**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# VIDEOSORVEGLIANZA

Associazione
Protezione Diritti e Libertà
Privacy APS

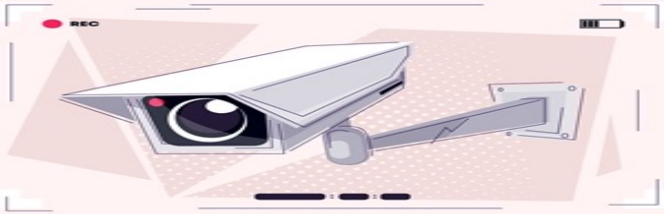
CONSULENZE PACI PRIVACY

www.gpdp.it/videosorveglianza gennaio 2022

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# Sistemi di VIDEOSORVEGLIANZA installati da PERSONE FISICHE

## Le REGOLE da seguire




**Le persone fisiche possono, nell'ambito di attività di carattere personale o domestico, attivare sistemi di videosorveglianza a tutela della sicurezza di persone o beni senza alcuna autorizzazione e formalità, purché:**

- ✓ le telecamere siano idonee a riprendere SOLO aree di PROPRIA ESCLUSIVA PERTINENZA;
- ✓ vengano attivate MISURE TECNICHE PER OSCURARE PORZIONI DI IMMAGINI in tutti i casi in cui, per tutelare adeguatamente la sicurezza propria o dei propri beni, sia inevitabile riprendere parzialmente anche AREE di TERZI;
- ✓ nei casi in cui sulle aree riprese insista una SERVITÙ DI PASSAGGIO in capo a terzi, sia acquisito formalmente (una tantum) il CONSENSO del soggetto titolare di tale diritto;
- ✗ NON siano oggetto di ripresa AREE CONDOMINIALI COMUNI o di TERZI;
- ✗ NON siano oggetto di ripresa AREE APERTE AL PUBBLICO (strade pubbliche o aree di pubblico passaggio);
- ✗ NON siano oggetto di COMUNICAZIONE A TERZI o di DIFFUSIONE le immagini riprese.

**La scheda ha finalità meramente divulgative Per una piena e corretta comprensione degli adempimenti, si raccomanda la consultazione della normativa in materia e dei provvedimenti del Garante**

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Videosorveglianza: le FAQ del Garante

## Le risposte alle domande più frequenti (FAQ) in tema di videosorveglianza e protezione dei dati personali

*(a cura del Garante per la protezione dei dati personali)*

1) Quali sono le regole da rispettare per installare sistemi di videosorveglianza?
2) Occorre avere una autorizzazione da parte del Garante per installare le telecamere?
3) Le persone che transitano nelle aree videosorvegliate devono essere informate della presenza delle telecamere?
4) In che modo si fornisce l'informativa agli interessati?
5) Quali sono i tempi dell'eventuale conservazione delle immagini registrate?
6) È possibile prolungare i tempi di conservazione delle immagini?
7) Quali sistemi di videosorveglianza necessitano di valutazione d'impatto preventiva?
8) Si possono installare telecamere all'interno degli istituti scolastici?
9) Il datore di lavoro pubblico o privato può installare un sistema di videosorveglianza nelle sedi di lavoro?

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# Videosorveglianza: le FAQ del Garante

## Le risposte alle domande più frequenti (FAQ) in tema di videosorveglianza e protezione dei dati personali

*(a cura del Garante per la protezione dei dati personali)*

**10) L'installazione di sistemi di videosorveglianza può essere effettuata da persone fisiche per fini esclusivamente personali, atti a monitorare la proprietà privata?**

**11) Quali sono le regole per installare un sistema di videosorveglianza condominiale?**

**12) Si possono utilizzare telecamere di sorveglianza casalinghe c.d. smart cam?**

**13) I Comuni possono utilizzare telecamere per controllare discariche di sostanze pericolose ed "eco piazzole" per monitorare le modalità del loro uso, la tipologia dei rifiuti scaricati e l'orario di deposito?**

**14) Si può utilizzare un sistema di videosorveglianza per trattare categorie particolari di dati?**

**15) I sistemi elettronici di rilevamento delle infrazioni inerenti violazioni del codice della strada vanno segnalate da cartello/informativa?**

**16) Ci sono casi di videosorveglianza in cui non si applica la normativa in materia di protezione dati?**

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# European Data Protection Board

**Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - Versione 2.0 Adottate il 29 gennaio 2020**

**Le Linee Guida Dell'EDPB prevedono:**

**1) Adozione di misure tecniche e organizzative**

**2) La descrizione generale del sistema di videosorveglianza;**

**3) L'applicazione dei principi di «privacy by design e by default;**

**4) La predisposizione della Data Protection Impact Analisys (DPIA) ove necessario.**

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# JOBS ACT ed il DLgs 151/2015

Dlgs 151/2015:"Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunita', in attuazione della legge 10 dicembre 2014, n. 183"

**Titolo II: Disposizioni in materia di rapporto di lavoro e pari opportunita'**

Capo I: Disposizioni in materia di rapporto di lavoro

**Art. 23 Modifiche all'articolo 4 della legge 20 maggio 1970, n. 300 e all'articolo 171 del decreto legislativo 30 giugno 2003, n. 196**

introduce la nuova disciplina in materia di **impianti audiovisivi e altri strumenti di controllo a distanza dei** lavoratori, sostituendo l'articolo 4 della legge n.300/1970 (Statuto dei lavoratori) che a partire dal 1970 disciplinava la materia

La disposizione attua il criterio di delega di cui all'articolo 1, comma 7, lettera f), della legge delega n.183/2014: *"revisione della disciplina dei controlli a distanza, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore"*

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

# Il nuovo art 4 L.300/70 rispetto al previgente testo

| Previgente testo dell'Art. 4 L.300/70 | Vigente testo dell'Art 4 L.300/70, ai sensi dell'art 23 D.Lgs 151/2015 |
|---|---|
| *"Art. 4. Impianti audiovisivi.*<br>*1. È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.*<br><br>*2. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.*<br><br>*3. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.*<br><br>*4. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale."* | *«Art. 4 (Impianti audiovisivi e altri strumenti di controllo). -*<br>*1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilita' di controllo a distanza dell'attivita' 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. In alternativa, nel caso di imprese con unita' produttive ubicate in diverse province della stessa regione ovvero in piu' regioni, tale accordo puo' essere stipulato dalle associazioni sindacali comparativamente piu' rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unita' produttive dislocate negli ambiti di competenza di piu' Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.*<br><br>*2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*<br><br>*3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalita' d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.».* |

Associazione Protezione Diritti e Libertà Privacy APS

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

CONSULENZE PACI PRIVACY

# *GRAZIE PER L'ATTENZIONE*