Associazione
Protezione Diritti e Libertà
Privacy

SESSIONE FORMATIVA ON LINE

CONSULENZE PACI PRIVACY

Il REGOLAMENTO EUROPEO 2016/679

Gloriamaria Paci

Nata a Rimini nel gennaio del 1969, dopo alcuni anni dedicati alla carta stampata, nel 1998 la Dott.ssa Gloriamaria Paci decide di scommettere ed investire in un settore allora poco conosciuto: la normativa sulla tutela 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.

Relatrice a convegni, seminari e corsi di formazione, con l'introduzione del Regolamento Europeo 2016/679, oggi ricopre il ruolo di Responsabile per la protezione di dati personali per privati ed enti pubblici.

Presidente dell'Associazione protezione diritti e libertà privacy, 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

CONSULENZE PACI PRIVACY

Il Regolamento europeo in materia di protezione dei dati personali 2016/679 sostituirà 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, quando dovrà 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

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

PRINCIPI E DEFINIZIONI

Associazione Protezione Diritti e Libertà Privacy

Autore Dott.ssa Gloriamaria Paci

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

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

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

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

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)

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.

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

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

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

LE FIGURE PREVISTE DALLA NORMATIVA

Associazione Protezione Diritti e Libertà Privacy

Autore Dott.ssa Gloriamaria Paci

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

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

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

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

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

Associazione Protezione Diritti e Libertà Privacy

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

L'Incaricato del trattamento

- 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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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) 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

Associazione Protezione Diritti e Libertà Privacy

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

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.

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.

Associazione Protezione Diritti e Libertà Privacy

Autore Dott.ssa Gloriamaria Paci

CONSULENZE PACI PRIVACY

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

NUOVI PRINCIPI

Associazione Protezione Diritti e Libertà Privacy

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

Nuovo principio

Art. 24 - ACCOUNTABILITY

Nel GDPR 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

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

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

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. - Dati riguardanti soggetti interessati vulnerabili - 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 - 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 - 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. - Trattamento di dati su larga scala. - Creazione di corrispondenze o combinazione di insiemi di dati. - Dati sensibili o dati aventi carattere estremamente personale.	SI

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

Nuovo principio
Art. 35 - PRIVACY IMPACT ASSESSMENT

Esempi di trattamento	Possibili criteri pertinenti	E' Richiesta
Istituzione che crea una banca dati antifrode e di gestione del rating del credito a livello nazionale.	Valutazione o assegnazione di un punteggio. - Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto - 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 - Dati riguardanti soggetti interessati vulnerabili. - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto.	SI

Associazione Protezione Diritti e Libertà Privacy

Autore Dott.ssa Gloriamaria Paci

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 - 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. - Valutazione o assegnazione di un punteggio.	- Valutazione o assegnazione di un punteggio	**NO**

Associazione Protezione Diritti e Libertà Privacy

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.

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

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….

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

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

NUOVI OBBLIGHI GENERALI

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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.

Associazione Protezione Diritti e Libertà Privacy

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

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.

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

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

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

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

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

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

CONSULENZE PACI PRIVACY

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

NUOVI DIRITTI

Associazione Protezione Diritti e Libertà Privacy

Autore Dott.ssa Gloriamaria Paci

CONSULENZE PACI PRIVACY

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
Autore Dott.ssa Gloriamaria Paci
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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

INFORMATIVA E CONSENSO

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

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

CONSULENZE PACI PRIVACY

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

IMPIANTO SANZIONATORIO

Autore Dott.ssa Gloriamaria Paci

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

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

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

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

Autore Dott.ssa Gloriamaria Paci

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

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

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

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

CONSIGLI DI CARATTERE GENERALE

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

Autore Dott.ssa Gloriamaria Paci

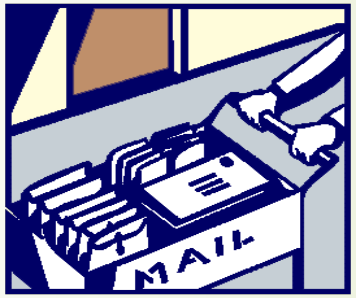
Associazione Protezione Diritti e Libertà Privacy

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

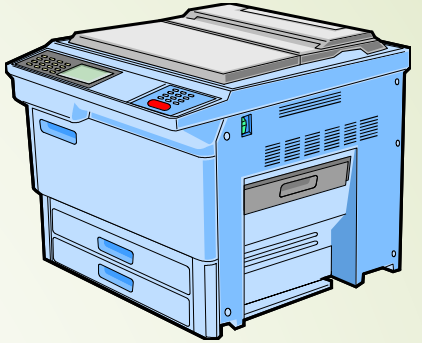


Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

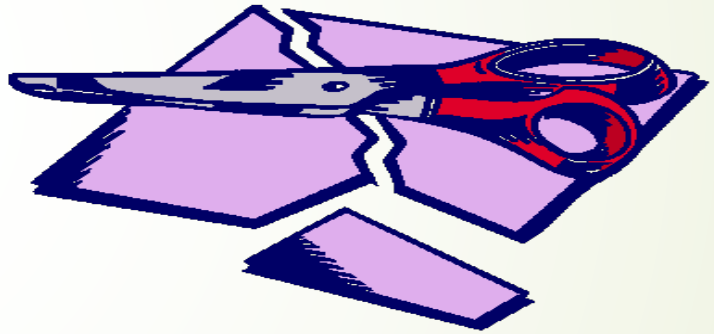
Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

Autore Dott.ssa Gloriamaria Paci

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

Autore Dott.ssa Gloriamaria Paci

CONSULENZE PACI PRIVACY

Privacy in pillole
Accorgimenti per il trattamento dati

3

- 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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

Privacy in pillole
Accorgimenti per il trattamento dati

3

- **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:**

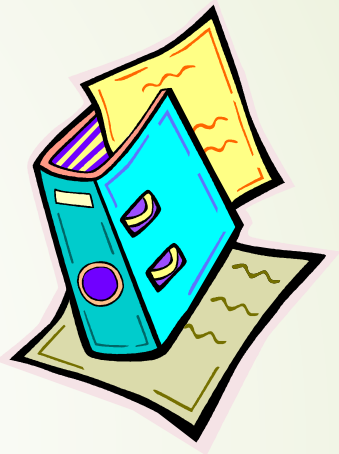
  - mai usare la stessa password per piu servizi e/o account diversi
  - evitare di usare riferimenti personali e/o parole di senso compiuto
  - sceglierle piuttosto lunghe (almeno otto caratteri)
  - aggiungere cifre e caratteri speciali (meglio se non all'inizio o alla fine)
  - cambiarle periodicamente…valgono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

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

MISURE DI SICUREZZA

Associazione Protezione Diritti e Libertà Privacy

Autore Dott.ssa Gloriamaria Paci

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

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

Autore Dott.ssa Gloriamaria Paci

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

Autore Dott.ssa Gloriamaria Paci

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

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'ente a gestire la sicurezza informatica in modo proattivo

Giustificare gli investimenti nel settore della sicurezza informatica

Autore Dott.ssa Gloriamaria Paci

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

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

Autore Dott.ssa Gloriamaria Paci

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**

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

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

Autore Dott.ssa Gloriamaria Paci

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

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

A

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

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

Autore Dott.ssa Gloriamaria Paci

Associazione Protezione Diritti e Libertà Privacy

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

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**

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

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

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

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

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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

CONSULENZE PACI PRIVACY

Autore Dott.ssa Gloriamaria Paci

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;

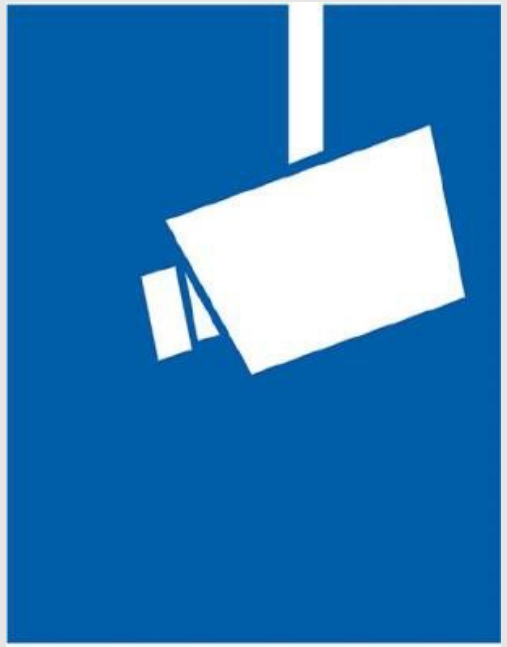
3) L'applicazione dei principi di «privacy by design e by default;

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

Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

Il nuovo cartello della Videosorveglianza



L'informativa completa sul trattamento dei dati è disponibile:

- presso i locali del titolare (reception, casse, ecc.)
- sul sito Internet (URL)...
- altro .....

LA REGISTRAZIONE È EFFETTUATA DA

.....

CONTATTI DEL RESPONSABILE DELLA PROTEZIONE

Le immagini saranno conservate per un periodo di _____

Finalità della videosorveglianza_____

È possibile accedere ai propri dati ed esercitare gli altri diritti riconosciuti dalla legge rivolgendosi a: _____

Associazione Protezione Dirett e Libertà Privacy

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

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. *1. È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.* *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.* *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.* *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). -* *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.* *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.* *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

CONSULENZE PACI PRIVACY