CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

SESSIONE FORMATIVA ON LINE CORSO DI PERFEZIONAMENTO

La responsabilizzazione (accountability) quale punto di equilibrio tra sicurezza e diritto alla riservatezza

Autore Dott.ssa Gloriamaria Paci

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

Associazione Protezione Diritti e Libertà Privacy APS
Via Edelweiss Rodriguez Senior, 13
47924 Rimini (Rn)
Tel. 0541-1795431 / Fax 0541-1794118
Cell. Gloriamaria Paci 347-5244264

segreteria@associazionedirittiprivacy.it
posta@pec.associazionedirittiprivacy.it
www.associazionedirittiprivacy.it

Seguici sui social!

https://lintr.ee/apdlp

Gloriamaria Paci

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Nata a Rimini nel gennaio del 1969, dopo alcuni anni dedicati alla carta stampata, nel 1998 Gloriamaria 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.

Luca Di Leo

Consulenza e formazione in materia di protezione dei dati personali dal 2005

Studio Paci & C. Srl
(cda)

Associazione Protezione diritti e libertà privacy APS
(Vice presidente)

Contatti:
dileo@studiopaciecsrl.it
Cell. 3931019939
www.consulenzepaci.it
Linkedin: #luca di leo

Responsabile della Protezione dei Dati (DPO per aziende private, pubbliche, sanità)
certificazione UNI 11697:2017 (Registro Accredia)

Valutatore Privacy
certificazione UNI 11697:2017 (Registro Accredia)

Privacy Officer
Certificazione TUV Italia 2013 – certificazione competenze Federprivacy – Legge n.4/2013

Auditor GDPR
secondo lo schema di certificazione per il GDPR: ISDP@10003 (Registro AICQ SICEV)

Consulente per l'implementazione dello schema di certificazione ISDP@10003
(Ente di certificazione INVEO)

Lead Auditor ISO 27001 , aggiornamento ISO 27701

La base del principio dell'accountability

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

Regolamento Europeo n. 679/2016
Art. 1 – Oggetto e finalità

Paragrafo 2 – Il presente Regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

La protezione delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale.

L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, par. 1, del trattato sul funzionamento dell'U.E. stabiliscono che ogni persona ha diritto alla protezione dei dati personali che lo riguardano

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il Regolamento pone al centro dell'attenzione la tutela della persona umana, delle sue libertà e della sua dignità e il rafforzamento dei diritti fondamentali dei cittadini europei nell'era digitale.
Vista la natura regolamentare della norma, non necessita di recepimento da parte dei Paesi UE ed è attuata allo stesso modo in tutti gli Stati dell'Unione.

Quali diritti e libertà
Privacy ed altri diritti fondamentali quali:

- **La libertà di espressione e di pensiero**
- **La libertà di movimento**
- **Il divieto di discriminazioni**
- **Il diritto alla vita**

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS

Quali diritti e libertà

- ❑ **Il diritto alla libertà di coscienza e di religione**
- ❑ **Il diritto al rispetto della vita privata e familiare**
- ❑ **Il diritto al domicilio e la corrispondenza**
- ❑ **Il diritto del processo equo**
- ❑ **Il diritto al matrimonio**
- ❑ **etc.**

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il GDPR, introducendo una serie di novità in ambito di trattamento di dati personali e di sicurezza del trattamento, modifica il concetto di adempimento privacy a cui si era abituati. Il trattamento non è più soggetto a regole dettagliate e circostanziate e ad adempimenti formali; il Regolamento europeo lascia al Titolare ampio potere decisionale, imponendogli, però, un percorso di adeguamento (*compliance*) efficace, basato sulla minimizzazione del rischio e sul controllo del dato da parte dell'interessato.

Accountability

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

Accountability

Il principio di responsabilizzazione significa che si chiede al Titolare del trattamento di mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento.

Accountability

Il principio di responsabilizzazione significa che il Titolare del trattamento deve adottare approcci e politiche oggetto di una valutazione del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Accountability

Il titolare, quindi, dovrà:

- Definire una politica di gestione, anche in relazione degli strumenti utilizzati;
- Definire gli obiettivi;
- Fornire risorse sia umane che economiche adeguate alla gestione dei processi;
- Formare tutto il personale coinvolto;

Accountability

Il titolare, quindi, dovrà:

- Definire le procedure operative (policy)
- Verificare che vengono effettuati audit sia interni che esterni;
- Verificare che i dati siano sempre protetti per tutto il periodo previsto e riportato nell'informativa;
- Verificare se i responsabili del trattamento siano istruiti sulle attività a loro date in outsourcing;

Il principio **dell'accountability** rappresenta uno dei pilastri su cui si fonda il Regolamento Europeo 2016/679.

In italiano il termine è stato tradotto come "responsabilizzazione" e prende in esame diversi aspetti quali l'affidabilità e la competenza di un'Organizzazione nel gestire il proprio patrimonio informativo

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Una traduzione pertinente, anche se poco pratica, potrebbe essere quella di “rendicontazione”.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

L'accountability è la sintesi di tutto ciò che attiene il GDPR. È quel principio di legge che prefigura per le Organizzazioni l'onere di comprendere e di diventare consapevoli circa i rischi che possono far correre alle persone, trattando i loro dati e il correlato dovere di mitigare tali rischi.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il principio di Accountability

Cenni normativi

Considerando 74 Regolamento Europeo 2016/679

Considerando 85 Regolamento Europeo 2016/679

Articolo 5 Regolamento Europeo 2016/679

Articolo 24 Regolamento Europeo 2016/679

Articolo 32 Regolamento Europeo 2016/679

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il principio di Accountability

Considerando 74 Regolamento Europeo 2016/679

(74) È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto.

In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure.

Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il principio di Accountability

Considerando 85 Regolamento Europeo 2016/679

(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. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il principio di Accountability

Articolo 5 Regolamento Europeo 2016/679 - Principi applicabili al trattamento di dati personali

I dati personali sono: (C39)

1. a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il principio di Accountability

Articolo 5 Regolamento Europeo 2016/679 - Principi applicabili al trattamento di dati personali

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»). (C74)

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il principio di Accountability

Articolo 24 Regolamento Europeo 2016/679 – Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, **ed essere in grado di dimostrare,** che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il principio di Accountability

Certificazioni

E’ importante ricordare che, quando si parla di certificazioni ai sensi dell’articolo 42 del Regolamento Europeo 2016/679, ci si riferisce a certificazioni di processo in base alla ISO 17065, come previsto dall’articolo 43 del Regolamento Europeo 2016/679.

Per evitare fraintendimenti, le certificazioni a partire dalla ISO 27001 non rispondono a quanto previsto dall’articolo 42 del Regolamento Europeo 2016/679.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

inveo
ACCREDITED CERTIFICATION BODY

Data Protection Certification Mechanisms

Study on Articles 42 and 43 of the Regulation (EU) 2016/679

Art. 42	GDPR	Specific ISO/IEC 17065	Aspecific ISO/IEC 17021-1	Out of Scope	Out GDPR
	In scope	ISDP©10003 ©Europrise			
	Aspecific		ISO 27 001 ISO 22301 ISO 27018		
	Out of scope			ISO 27701 (27552) BS 10012	
	Out of GDPR				ISO 9001 ISO 20000 GOODPRIVACY BV GDPR CERTIFICATION JIPDEC DPCO

GDPR	Best practice – ISO guidlines (not certifiable)
	• ISO 31000 • ISO 28590 • ISO 25024 • ISO 29100 • ISO 29134 • ISO 29151 • ISO 25024

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il principio di Accountability

Articolo 32 Regolamento Europeo 2016/679 – Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) a capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il principio di Accountability

2.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Dal principio di Accountability alle disposizioni operative

Articolo 32 Regolamento Europeo 2016/679

Quello dell'accountability che -come ogni principio- è per sua natura generale e astratto, non resta tale ma si concretizza in più di una disposizione del Reg. UE 2016/679.

Un esempio è l'art.32, primo della sezione dedicata alla **sicurezza dei dati**, che recita:

"tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento **mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio** …".

Ciò comporterà che ogni soggetto dovrà autonomamente scegliere **come ed in che misura mettere in sicurezza i trattamenti:**

- quali antivirus installare
- quali sistemi di salvataggio dati adottare
- ecc.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il principio di Accountability

L'accountability è oggi considerata come un approccio pratico alla privacy e al trattamento dei dati personali; essa punta, pertanto, allo sviluppo di strumenti che possano essere utilizzati dalle organizzazioni per valutare la compliance (conformità) e renderne conto alle Autorità Garanti per la protezione dei dati personali.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

In linea generale accountability si basa sulla concezione che gli individui siano responsabili per le proprie azioni e devono renderne conto ai terzi che ne facciano richiesta (interessati).

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Nell'ottica moderna, introdotta dal legislatore europeo, responsabilizzazione parte dall'idea che **nessuno, meglio del titolare, possa individuare sistemi di protezione e metodi adeguati** a garantire la sicurezza dei dati che non rallentino o impediscano le normali e attività quotidiane

Il concetto di **accountability** presuppone l'educazione e la consapevolezza del Titolare che deve individuare validi strumenti di adeguamento al GDPR per garantire la protezione dei dati.

Le sanzioni, molto più pesanti da quelle previste dai singoli Paesi UE, rappresentano invece **il mezzo correttivo residuale** utilizzato di fronte all'evidenza di una grave assenza di rispetto di qualsiasi principio normativo.

Il regolamento pone con forza l'accento sulla "responsabilizzazione" di titolari e responsabili – ossia, **sull'adozione di comportamenti proattivi** e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Principio di accountability ovvero **responsabilizzare il titolare di un trattamento dati** che non è più mero esecutore di un elenco di misure imposte ad una norma, ma diviene ***responsabile delle misure operative e tecniche*** che riterrà opportune, efficaci e dunque adeguate per salvaguardare il patrimonio informativo.

L'obiettivo di ogni titolare, responsabile e addetto al trattamento dei dati, sarà quello di **essere compliance con il regolamento.** Questo significa sostanzialmente non solo divenire responsabile delle scelte di mezzi, operazioni, procedure, finalità, ecc. in materia di trattamento dei dati, ma anche ***essere in grado di "dare conto" delle valutazioni svolte alla base delle scelte poi operate***.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il termine “accountability” richiama almeno due accezioni o componenti fondamentali:

- Dar conto all’esterno ed in particolare al complesso degli stakeholder (interessati), in modo esaustivo e comprensibile, del corretto utilizzo delle informazioni;

- L’esigenza di introdurre logiche e meccanismi di maggiore responsabilizzazione interna alle aziende

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il Titolare sarà, quindi, "responsabilizzato", se riuscirà a dar conto:

- ✓ Attività svolta
- ✓ Finalità delle scelte adottate
- ✓ Gli strumenti e le modalità con cui vengono trattate e tutelate le banche dati

La ***responsabilizzazione è un processo*** che inizia dalla fase di progettazione del trattamento, attraverso un approccio strutturato, dimostrando competenza e capacità gestionale.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il principio di responsabilizzazione richiede al titolare del trattamento di porre in essere ***misure tecniche e organizzative adeguate*** per garantire, potendolo anche dimostrare, che il trattamento sia effettuato in modo conforme al GDPR . Si tratta di un punto cruciale nel nuovo assetto previsto per la protezione dei dati in quanto è affidato ai titolari del trattamento il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative vigenti, ***tenendo conto di alcuni criteri specifici indicati dal GDPR stesso***.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Il primo fra tali criteri è sintetizzato nell'espressione inglese **Data protection by default and by design**, ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del GDPR e "tutelare i diritti degli interessati", considerando il contesto complessivo nel quale si inserisce il trattamento e i rischi per i diritti e le libertà degli interessati

La capacità di effettuare **una adeguata analisi preliminare** o di dimostrare a **posteriori il proprio livello di sicurezza**, e dunque anche di conformità, risulta essere una necessità ineludibile, che richiede l'uso di adeguati **modelli di analisi e di gestione.**

L'obiettivo sarebbe quello di abbandonare il tradizionale modello passivo, basato sulla concezione di "regole da rispettare", per giungere ad un modello attivo, basato su una gestione proattiva del rischio, che si ponga la questione di "quali obiettivi raggiungere", andando a definire in modo chiaro la direzione che si vuole prendere, e cioè il risultato che si vuole ottenere unitamente al rischio che ragionevolmente può considerarsi accettabile.

Da qui, la **pianificazione di azioni** che potrebbero incrementare la responsabilità (accountability) ed arrivare a un contenimento dei costi e a possibili vantaggi competitivi, oltre che ad una maggiore tempestività nell'individuazione e nella gestione delle nuove emergenti minacce.

La forma si sposa con la sostanza e porta alla creazione di una serie di **policy o procedure interne**, che accompagnano l'attività quotidiana del Titolare attraverso una loro ampia condivisione a livello interno.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Una delle definizioni più pregnanti di questo concetto è rinvenibile nel sito dell'Information Commissioner's Office (ICO) – l'Autorità di controllo inglese:

"Accountability is not a box-ticking exercise. Being responsible for compliance with the GDPR means that you need to be proactive and organised about your approach to data protection, while demonstrating your compliance means that you must be able to evidence the steps you take to comply".

"L'accountability non consiste in una mera spunta di caselle. Una compliance responsabile al GDPR significa essere proattivi e avvicinarsi alla protezione dei dati personali secondo modalità strutturate. Per contro, dar prova della propria compliance significa essere in grado di dimostrare i passi che vengono intrapresi per rendersi compliant".

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Le 10 azioni da intraprendere secondo ICO

Approcciandosi al Regolamento ***con la regola del buon senso***, il titolare del trattamento ***può evitare sanzioni garantendo*** che i dati personali archiviati nei flussi aziendali siano adeguatamente protetti.

Essere proattivi è comunque considerato l'atteggiamento migliore da adottare, al fine di non rispondere in futuro di un danno derivante da trattamento dei dati personali attraverso la dimostrazione (inversione dell'onere della prova) di aver fatto tutto il possibile per evitarlo.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Le 10 azioni da intraprendere secondo ICO

Information Commissioner's Office – l'Autorità di controllo inglese

1) "**Adozione e implementazione di policy a tutela dei dati personali"** ossia proceduralizzazione, registrazione delle operazioni di trattamento, previa una esatta mappatura dei trattamenti effettuati. Le singole policy potranno essere più o meno stringenti e rigorose in relazione al volume ed alle categorie di dati trattati e alla dimensione dell'organizzazione.

2) **"Adozione di un approccio basato sui principi della privacy by design e della privacy by default"** durante tutto il ciclo di vita dei trattamenti. Un mero monitoraggio dei trattamenti in essere non è sufficiente. Occorrerà prestare una costante attenzione, volta all'individuazione di nuovi trattamenti per renderli privacy-oriented.

3) "**Definizione e regolamentazione scritta dei rapporti con i Responsabili esterni del trattamento"**. L'espressa esclusione di una natura puramente formalistica dell'approccio al GDPR porta ad escludere che i contratti con i Responsabili esterni possano essere mere riproduzioni dei requisiti prescritti dall'art. 28, favorendo invece una redazione *ad hoc* di tali documenti, avuto riguardo al contenuto del rapporto in essere e con particolare (ma non esclusivo) riferimento alle misure tecniche e organizzative, senza tralasciare la verifica di eventuali trasferimenti di dati verso Paesi extra UE.

Le 10 azioni da intraprendere secondo ICO

Information Commissioner's Office – l'Autorità di controllo inglese

Conservazione dei documenti comprovanti le attività di trattamento di dati personali". Nonostante il dibattito dottrinario circa la necessità minimizzazione della produzione documentale, a parere di chi scrive e alla luce della situazione delineatasi, l'opzione documentale rimane la soluzione preferibile, anche in una prospettiva assicurativa.

5) "**Implementazione di misure di sicurezza adeguate**" in relazione alle categorie di dati trattati e alla tipologia di trattamenti effettuati.

6) **"Registrazione e, se necessario, comunicazione di eventi di Data Breach".**

7) **"Effettuazione di una valutazione di impatto,** nel caso in cui il trattamento di dati personali possa implicare un alto rischio per i diritti e le libertà degli interessati".

8) **"Nomina di un Data Protection Officer"** se necessario e, se possibile,

9) **"Adesione a codici di condotta o a schemi di certificazione".**

10) **"Monitoraggio, aggiornamento delle misure poste in essere** e creazione di una cultura della privacy all'interno della propria organizzazione".

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Principio Accountability e buon senso

Il Titolare **ha dunque l'obbligo di essere responsabile nella gestione dei dati personali**, e deve essere consapevole che di quelle informazioni raccolte, deve essere responsabile non solo per il Regolamento Europeo, ma anche per **etica** e buon senso.

I dati personali che tratta e custodisce il Titolare non gli appartengono, ma gli sono stati affidati unitamente al dovere di proteggerli.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

Principio Accountability e buon senso

Il Titolare ha il compito di agire **vale a dire che** dovrà essere in grado di rendere conto delle azioni fatte o delegate, con ***valutazioni*** svolte alla base **delle scelte** operate. Ma soprattutto deve essere in grado di dimostrare in quale maniera, passibile di verifica, venga esercitata la responsabilità.

Il rispetto del principio di accountability è fondamentale per il raggiungimento della compliance al GDPR.

Essere responsabilizzato vuol dire **testimoniare**, dare delle prove concrete ed essere in grado di **documentare** la consapevolezza, la competenza e la responsabilità, riportando nel registro dei trattamenti tutto ciò che si svolge e in maniera dettagliata, comprese le contromisure adottate e le motivazioni alla base di tali adozioni.

Si deve inoltre dimostrare di riuscire a **governare l'intero processo**, gestendolo nella sua interezza, avendo il pieno controllo su di esso.

Principio Accountability e buon senso

La stretta aderenza al principio di accountability si rivela dunque fondamentale nella gestione di un eventuale data breach.

Qualora fosse necessario procedere con la notifica al Garante ed eventualmente anche agli interessati, il Titolare sarebbe in grado di testimoniare che i dati sono stati trattati nel rispetto del **principio di privacy by design** e con rischio residuale basso, che è stata svolta la **DPIA** e che sono state messe in atto tutte le contromisure necessarie, **avendo quindi fatto tutto il possibile** per minimizzare i rischi.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

In conclusione …..

Consapevolezza del cambio di approccio: il nuovo modello previsto dal Regolamento Europeo 2016/679 richiede la responsabilizzazione del titolare. Va da se che la sua accountability non può mai essere demandata a qualcun altro. Avere consapevolezza che i dati vanno trattati in un'ottica di *minimizzazione*: non si deve e non si può eccedere la raccolta dei dati rispetto alle finalità che ci si pone.

Mappatura dei trattamenti, ovvero effettuare una valutazione per proteggere tutti i tipi di dati trattati, individuando per ciascuno dato tutte le elaborazioni (trattamenti) effettuati o da effettuare, le finalità, le basi giuridiche, la durata del trattamento, la provenienza e destinazione dei dati, le modalità di raccolta e di conservazione (retention), i soggetti coinvolti (responsabili del trattamento).

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

In conclusione …..

Redazione degli atti di nomina degli addetti designati e di nomina dei responsabili esterni del trattamento con l'istituzione di ruoli e responsabilità in materia di trattamento dei dati e previsione di procedure di formazione ai dipendenti sulle tematiche

Redazione di un modello utile alla ideazione e realizzazione di prodotti e servizi in conformità ai principi di privacy by design e by default al fine di fornire il più possibile informazioni per testimoniare l'impegno della struttura nell'approcciare correttamente i trattamenti dati come previsto dall'articolo 25 del GDPR. Il modello, in particolare, deve contenere le analisi dei rischi residuali sui trattamenti e sugli archivi; l'elenco di tutte le misure di sicurezza implementate (articolo 32 GDPR, "Sicurezza del trattamento"); l'elenco delle misure consigliate seguendo la falsariga dell'Allegato B al vecchio Codice Privacy e quelle eventualmente implementate; i piani di ripristino dei dati; i piani di formazione degli addetti.

Compilazione dei registri attività dei trattamenti (articolo 30 GDPR).

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

In conclusione …..

Redazione DPIA (Data Protection Impact Analysis) che contiene una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento, una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Eventuale identificazione e nomina del RPD. Il GDPR prevede la possibilità di dotarsi di un RPD e in alcuni casi lo obbliga. È necessario quindi verificare l'art. 37 del GDPR e poi scegliere.

Rivalutazione periodica di tutte le misure istituite in ottica di aggiornamento e miglioramento.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

In conclusione …..

Inventario degli asset. È necessario istituire e aggiornare un inventario degli asset (PC e altri dispositivi di informatica individuale, server, applicazioni informatiche, middleware, utenti e impianti) per valutarne le vulnerabilità che può influenzare l'analisi di rischio. Per ogni asset devono essere definite le misure di sicurezza applicabili sui dati secondo la capacità di garantire la riservatezza, integrità e disponibilità (RID) dei dati.

Individuare i responsabili esterni e gli addetti interni ovvero coloro che trattano i dati e che utilizzano gli asset; in quest'ambito è opportuno che il titolare li informi e li formi con uno specifico programma.

Analisi dei rischi e misure di sicurezza. Si effettua la stima del rischio per ogni tipo di trattamento e, di conseguenza, di dato gestito, valutando le minacce incombenti e l'impatto come danno reputazionale, quindi economico.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

In conclusione …..

Mitigazione dei rischi: significa valutare l'adozione delle misure di sicurezza adeguate a diminuire il rischio di problemi sui dati.

Policy e procedure aziendali sulla security: è necessario stabilire almeno quelle relative ai data breach ed alla gestione di incidenti informatici, alla Business Continuity e Disaster Recovery.

Redazione delle informative sul trattamento dei dati personali rivolte agli interessati e la conseguente gestione del consenso da parte degli interessati stessi.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

---- CONSERVAZIONE DEI DATI ----

DANIMARCA

Il garante danese ha aperto una procedura contro un'azienda di arredi per non avere cancellato i dati di 385 mila clienti, conservati in un vecchio sistema informativo, non più in uso, perché sostituito da altro aggiornato.

Il garante danese ha anche aperto un procedimento per l'applicazione di una sanzione di 160 mila euro alla compagnia di taxi, per mancata cancellazione dei dati della prenotazione delle corse. La società aveva la regola interna di distruzione dei dati dopo due anni. Ma questo non è avvenuto, in quanto la società cancellava solo i nomi, ma non i numeri di telefono dei clienti.

---- PROCEDURE PER L'ACCOUNTABILITY ----

INDAGINE INTERNAZIONALE SUL RISPETTO DELLA PRIVACY

SINTESI DEI RISULTATI ITALIANI
19 soggetti pubblici (Regioni e Provincie autonome) e 54 società in-house analizzate.

1. Politiche per la protezione dei dati personali

Un quinto delle regioni non ha ancora adottato una procedura interna per la gestione dei dati personali nell'organizzazione o non l'ha applicata correttamente nelle attività quotidiane. Quasi tutte, però, hanno incaricato una o più persone competenti in materia di governance e gestione della protezione dei dati personali, a un livello gerarchico sufficientemente elevato nell'organizzazione.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

---- PROCEDURE PER L'ACCOUNTABILITY ----

2. Formazione, monitoraggio e consapevolezza

La maggior parte delle regioni e delle società in-house riconoscono l'importanza di un'adeguata formazione dei dipendenti in materia di protezione dei dati personali.

Nel 40% dei casi, però, le organizzazioni non hanno posto in essere alcun monitoraggio in merito all'attuazione di corrette pratiche nel trattamento dei dati personali.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

---- PROCEDURE PER L'ACCOUNTABILITY ----

3. Trasparenza

E' garantita un'adeguata trasparenza nel trattamento dei dati, attraverso specifiche informative agli interessati sul trattamento dei dati personali. Tali informative, di solito, sono costantemente aggiornate e facilmente accessibili, sebbene alcune organizzazioni appaiono limitarsi a presentare la sola privacy policy del sito web.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

---- PROCEDURE PER L'ACCOUNTABILITY ----

4. Capacità di risposta e gestione degli incidenti di sicurezza

Appare grave che il 24% delle società e il 48% delle Regioni non abbiano definito policy e procedure per la gestione delle richieste e dei reclami da parte degli interessati, o delle stesse Autorità.

Si evidenziano ancora carenze in merito alla gestione degli incidenti di sicurezza – i cosiddetti Data Breach – tanto che un quinto delle organizzazioni non ha ancora implementato una procedura di risposta agli incidenti di sicurezza che includa, tra l'altro, la notifica all'Autorità e, in caso di alto rischio per le libertà e i diritti degli interessati, anche la comunicazione a questi ultimi. Un quarto delle organizzazioni, inoltre, sembra non disporre di un registro per documentare le violazioni subite.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

---- PROCEDURE PER L'ACCOUNTABILITY ----

5. Valutazione e monitoraggio dei rischi

Il 24% delle società in-house,

ma addirittura il 58% delle Regioni,

non hanno processi documentati per la valutazione dei rischi sulla protezione dei dati personali (DPIA), in relazione all'utilizzo di nuovi prodotti, tecnologie o servizi.

La maggior parte dei soggetti analizzati ha creato un registro dei trattamenti effettuati. Un quinto delle Regioni, però, dovrebbe fare uno sforzo maggiore per tenere traccia anche dei dati personali comunicati o trasmessi a terzi.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

PROCEDURE PER L'ACCOUNTABILITY
IMPLEMENTAZIONE

Politica di sicurezza e procedure per la protezione dei dati personali

- L'organizzazione dovrebbe documentare la propria politica in merito al trattamento dei dati personali come parte della sua politica di sicurezza delle informazioni.

- La politica di sicurezza dovrebbe essere revisionata e rivista, se necessario, su base annuale.

- La policy di sicurezza dovrebbe almeno riferirsi a**: i ruoli e le responsabilità del personale**, **le misure tecniche e organizzative** di base adottate per la sicurezza dei dati personali, **i responsabili del trattamento** dei dati o altre terze parti coinvolte nel trattamento dei dati personali.

- Dovrebbe essere creato e mantenuto **un inventario di policy / procedure specifiche** relative alla sicurezza dei dati personali, **basato sulla policy generale di sicurezza.**

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

PROCEDURE PER L'ACCOUNTABILITY
IMPLEMENTAZIONE

Ruoli e responsabilità

- I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza

- Dovrebbe essere effettuata una chiara nomina delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza.

Politica di controllo degli accessi

- I diritti specifici di controllo degli accessi dovrebbero essere assegnati **a ciascun ruolo** (coinvolto nel trattamento di dati personali) in base al principio della stretta pertinenza e necessità per il ruolo di accedere e conoscere i dati.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

PROCEDURE PER L'ACCOUNTABILITY
IMPLEMENTAZIONE

Gestione risorse/asset

- L'organizzazione dovrebbe disporre di un registro/censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (hardware, software e rete).

- Il registro dovrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. Server, workstation), posizione (fisica o elettronica). Dovrebbe essere assegnato ad una persona specifica il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT).

PROCEDURE PER L'ACCOUNTABILITY
IMPLEMENTAZIONE

Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)

- È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.

- Gestione degli incidenti / Personal data breaches
Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

PROCEDURE PER L'ACCOUNTABILITY
IMPLEMENTAZIONE

Gestione degli incidenti / Violazione dei dati personali (Personal data breaches)

- È necessario definire un piano di risposta agli incidenti (Incident Response Plan) con procedure dettagliate per garantire una risposta efficace e ordinata al verificarsi di incidenti o violazioni di dati personali.

- Gestione degli incidenti / Personal data breaches

Il piano di risposta degli incidenti (Incident Response Plan) dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli.

CONSULENZE PACI PRIVACY

Associazione Protezione Diritti e Libertà Privacy APS

GRAZIE PER L'ATTENZIONE

CONSULENZE PACI PRIVACY

Associazione
Protezione Diritti e Libertà
Privacy APS