REGIONE PIEMONTE

CSI your digital partner

WEBINAR
SICURI di essere **SICURI?**

Privacy by Design e Data Protection Impact Assessment: dalla teoria alla pratica

Privacy by design

L'importanza della prevenzione

Relatore Avv. Letizia Maria Ferraris

2016-2024
otto anni di cammino nel mondo dei **BIG DATA** e **METADATI**
cosa abbiamo imparato e cosa è ancora da fare

Il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione dei dati

Le applicazioni del GDPR

1. È mutato il paradigma della legge

2. È sorto ineludibile il **concetto di prevenzione** e analisi del rischio per evitare «**danni per i diritti e le libertà**» degli interessati

3. È nato il termine **Accountability**:
ovvero il dovere di dimostrare le scelte adottate e le responsabilità applicate

4. È cambiato il concetto di '**data**' e di trattamento

5. È nato il **concetto di rischio** che è diventato **informatico**, **telematico**, **digitale** e **artificiale**...

Le applicazioni del GDPR

6 Si è innescato il concetto di **protezione della persona** e i **diritti sottesi** alla sua sfera giuridica

7 In questi anni abbiamo compreso l'importanza e l'efficacia della «**Comunicazione**» (l'informativa e la gestione dei diritti), della «**Sicurezza**» (le misure di sicurezza ed i processi di gestione degli incidenti) e della «**Sorveglianza**» (l'audit, i vincoli contrattuali..)

8 È nato il concetto di generazione e condivisione di dati, le nuove regole sulla concorrenza del ***business*** perché ***business di dati***

9 Concetto di '**gestione delle minacce**' nell'ambito della prevenzione

NOVITÀ

Tutte caratterizzate da una unica costante…un tema trasversale: **LA PREVENZIONE** ma soprattutto la **consapevolezza** che dietro i trattamenti si deve evitare **la violazione dei diritti umani**

Una sentenza importante

SENTENZA DELLA CORTE (terza sezione)
14 dicembre 2023

«Rinvio pregiudiziale - Protezione delle persone fisiche con riguardo al trattamento dei dati personali - Regolamento (UE) 2016/679 - Articolo 5 - Principi relativi a tale trattamento - Articolo 24 - Responsabilità del titolare del trattamento - Articolo 32 - Misure adottate per garantire la sicurezza del trattamento - Valutazione dell'adeguatezza di tali misure - Portata del sindacato giurisdizionale - Assunzione delle prove - Articolo 82 - Diritto al risarcimento e responsabilità - Esonero eventuale dalla responsabilità del titolare del trattamento in caso di violazione commessa da terzi - Domanda di risarcimento di un danno immateriale fondata sul timore di un potenziale utilizzo abusivo di dati personali»

Per questi motivi la CORTE dichiara:

1) Gli articoli 24 e 32 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati),devono essere interpretati nel senso che:
una divulgazione non autorizzata di dati personali o un accesso non autorizzato a tali dati da parte di «terzi», ai sensi dell'articolo 4, punto 10, di tale regolamento, non sono sufficienti, di per sé, per ritenere che le misure tecniche e organizzative attuate dal titolare del trattamento in questione non fossero «adeguate», ai sensi di tali articoli 24 e 32.

2) L'articolo 32 del regolamento 2016/679 dev'essere interpretato nel senso che:
l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento ai sensi di tale articolo deve essere valutata dai giudici nazionali in concreto, tenendo conto dei rischi connessi al trattamento di cui trattasi e valutando se la natura, il contenuto e l'attuazione di tali misure siano adeguati a tali rischi.

3) Il principio di responsabilità del titolare del trattamento, enunciato all'articolo 5, paragrafo 2, del regolamento 2016/679 e concretizzato all'articolo 24 di quest'ultimo, deve essere interpretato nel senso che: *nell'ambito di un'azione di risarcimento fondata sull'articolo 82 di tale regolamento, Al titolare del trattamento di cui trattasi incombe l'onere di dimostrare l'adeguatezza delle misure di sicurezza da esso attuate ai sensi dell'articolo 32 di detto regolamento.*

Per questi motivi la CORTE dichiara:

4) L'articolo 32 del regolamento 2016/679 e il principio di effettività del diritto dell'Unione devono essere interpretati nel senso che:
al fine di valutare l'adeguatezza delle misure di sicurezza che il titolare del trattamento ha attuato ai sensi di tale articolo, una perizia giudiziaria non può costituire un mezzo di prova sistematicamente necessario e sufficiente.

5) L'articolo 82, paragrafo 3, del regolamento 2016/679 deve essere interpretato nel senso che:
il titolare del trattamento non può essere esonerato dal suo obbligo di risarcire il danno subito da una persona, ai sensi dell'articolo 82, paragrafi 1 e 2, di tale regolamento, per il solo fatto che tale danno deriva da una divulgazione non autorizzata di dati personali o da un accesso non autorizzato a tali dati da parte di «terzi», ai sensi dell'articolo 4, punto 10, di detto regolamento, dato che tale responsabile deve allora dimostrare che il fatto che ha provocato il danno in questione non gli è in alcun modo imputabile.

6) L'articolo 82, paragrafo 1, del regolamento 2016/679 deve essere interpretato nel senso che:
il timore di un potenziale utilizzo abusivo dei suoi dati personali da parte di terzi che un interessato nutre a seguito di una violazione di tale regolamento può, di per sé, costituire un «danno immateriale», ai sensi di tale disposizione.

Due gli approcci complementari da applicare (art 25 e art 35)

Privacy by Design e Default

Imparare a progettare e scegliere le giuste misure di sicurezza per la protezione dei diritti e minimizzare il trattamento dei dati allo stretto necessario (dati, tempi e persone)

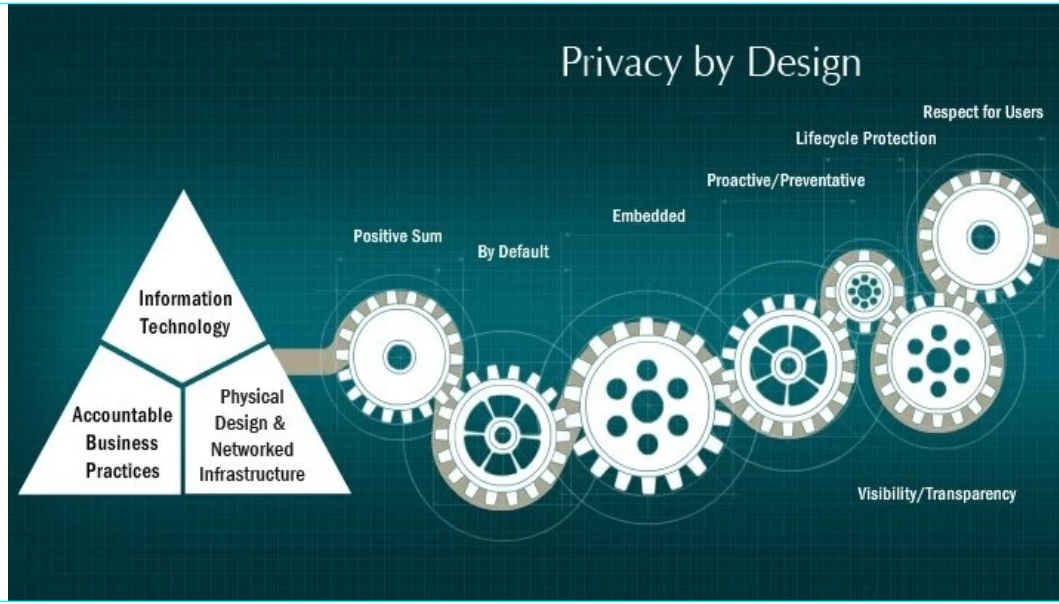
Data Protection Impact Assessment

Imparare a valutare gli effetti ed a mitigare i rischi delle scelte e delle modalità di trattamento dei dati

La Privacy by Design non è una invenzione del **GDPR**

Ann Cavoukian ex commissario per l'informazione e la privacy della provincia canadese dell'Ontario, introdusse il concetto negli anni del suo mandato (dal 1997 al 2014).

L'approccio di **Cavoukian** alla *privacy* appariva però non semplice da imporne l'adozione, difficile da applicare a determinate discipline.



Non solo Privacy Design nello sviluppo dei software

La Privacy by Design non è solo un problema tecnologico

La progettazione del trattamento deve mettere **l'individuo al centro**.

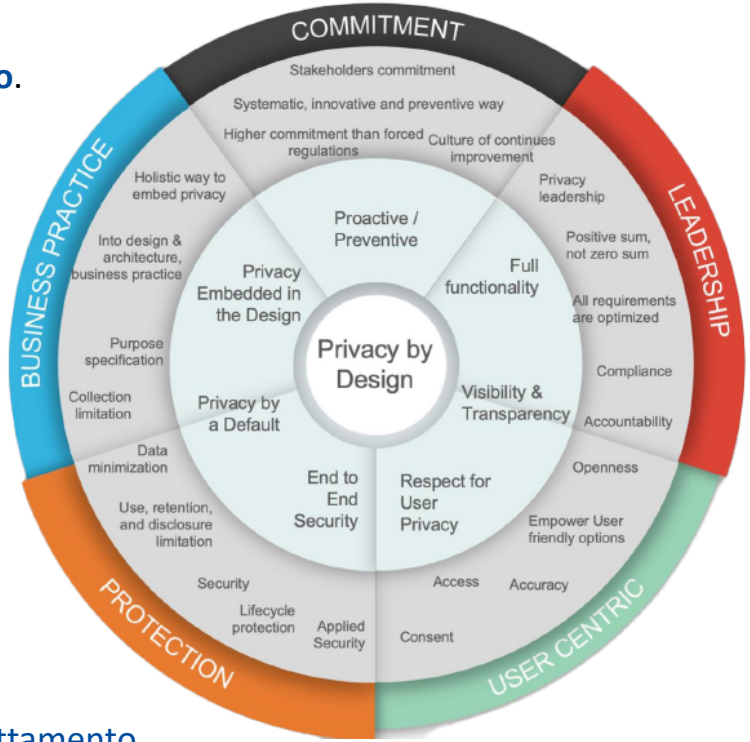
MINIMIZZAZIONE DELLE INFORMAZIONI

ISTRUZIONI PER IL TRATTAMENTO

CONSAPEVOLEZZA DEI PROCESSI

CONSERVAZIONE DEI DATI

MISURE ORGANIZZATIVE



Sono elementi chiave da considerare nella «progettazione» del trattamento

I 7 principi della Privacy by Design

01 **Proattività non reattività**
prevenire non correggere

02 **Privacy**
come impostazione di default

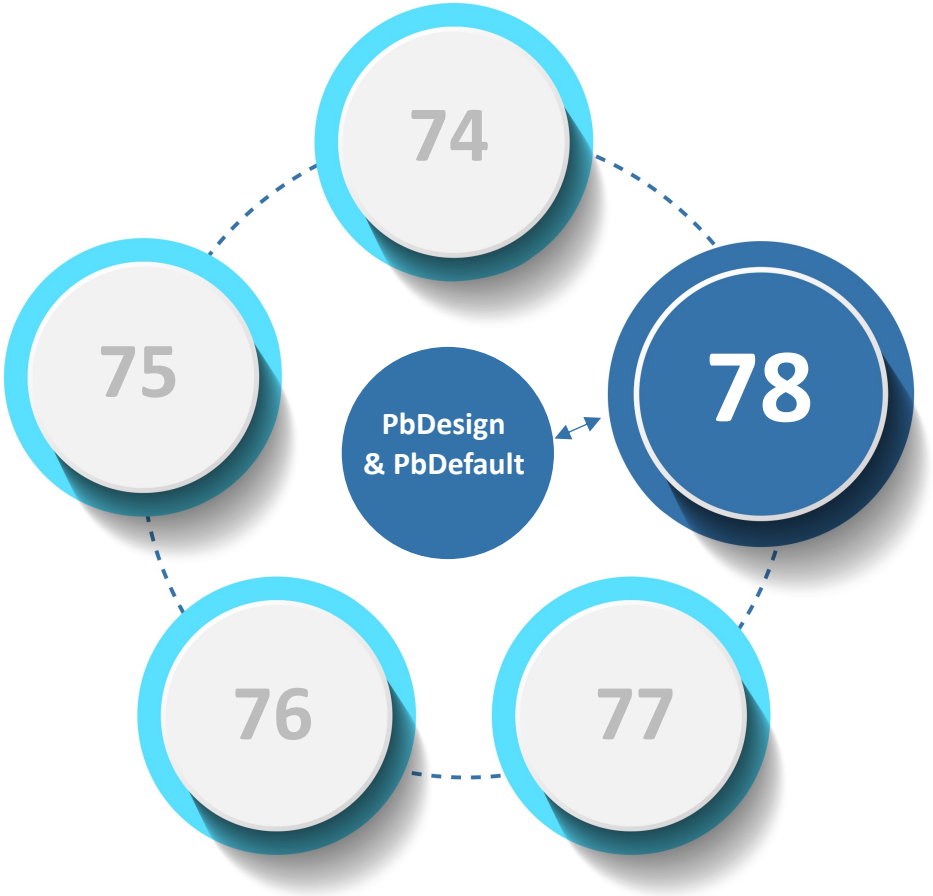
03 **Privacy**
incorporata nella progettazione

04 **Massima funzionalità**
Valore positivo, non valore zero

05 **Sicurezza fino alla fine**
Piena protezione del ciclo vitale

06 **Visibilità e trasparenza**
Mantenere la trasparenza

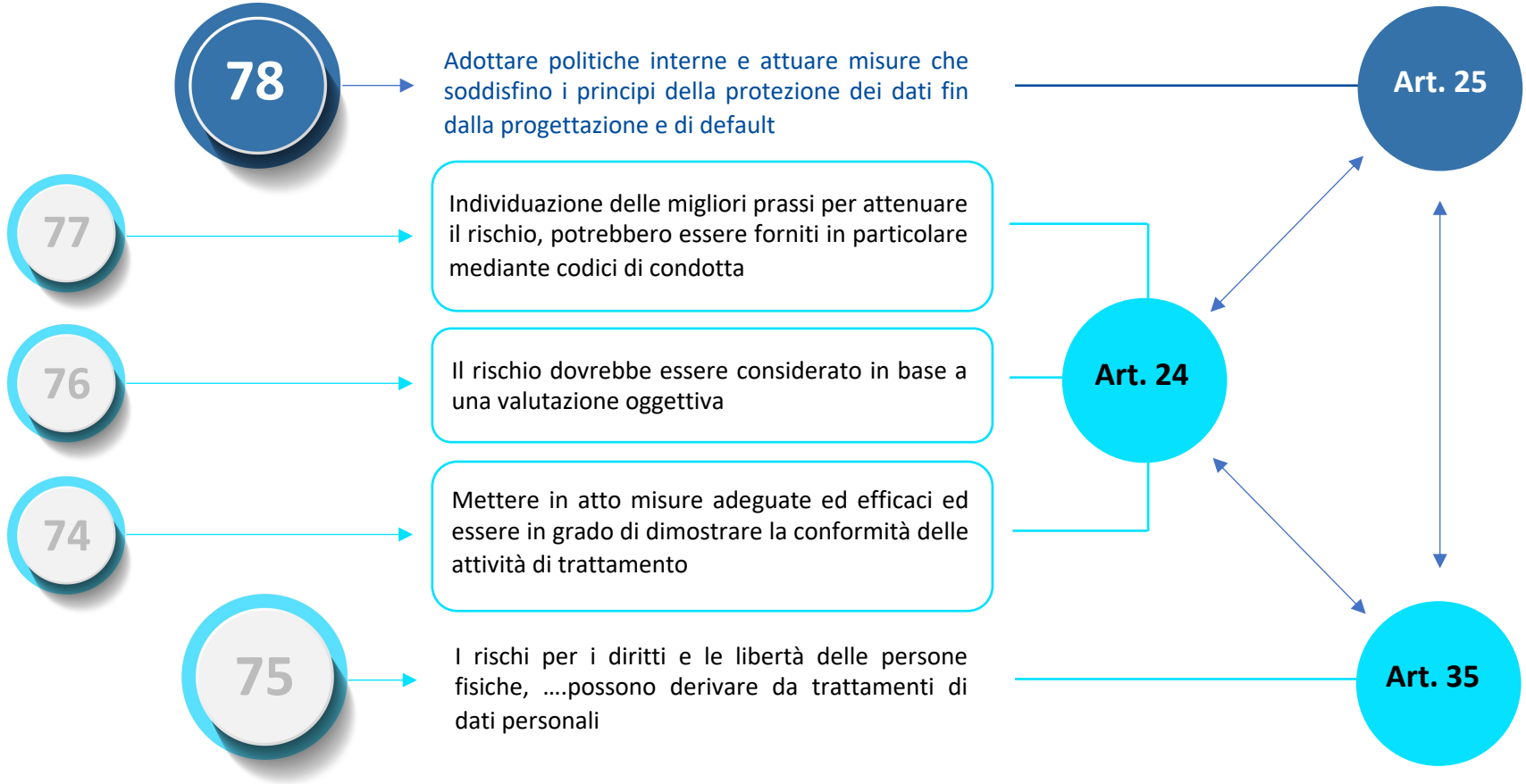
07 **Rispetto per la privacy dell'utente** Centralità dell'utente



L’art. 25 sulla Privacy by Design e Privacy by Default

è spiegato al **CONS. 78**, ma ci sono altri Considerando che possono essere utili per comprendere come individuare le misure adeguate e i rischi da gestire nell’attuazione della protezione sin dalla progettazione

Nel GDPR tutto segue un filo logico…



In pratica quindi…

Processi di autenticazione sicura, barriere verso possibili attacchi informatici, visualizzazioni degli ultimi accessi effettuati dall'utente medesimo…

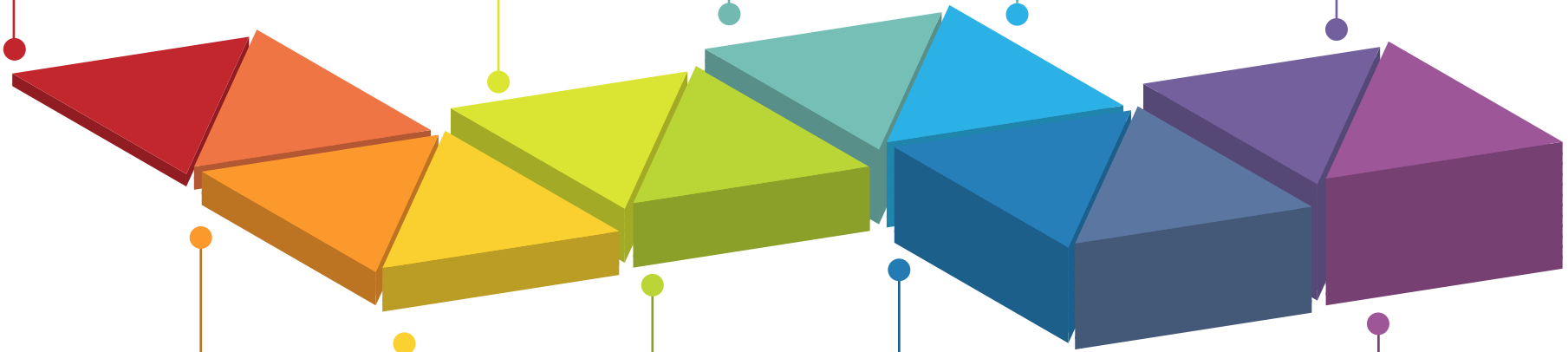
Limitazione alla raccolta dei dati (personali) strettamente necessari all'attività di trattamento sulla base delle finalità e basi giuridiche identificate

Creazione di ambienti di sviluppo sicuri

Log relativi alla tracciatura di tutte le attività effettuate dagli utenti (non solo degli Amministratori di Sistema, ma anche dei semplici utilizzatori/utenti interessati)

Introduzione di moduli software in grado di facilitare l'esercizio dei diritti degli interessati (diritto alla rettifica, alla cancellazione/oblio, come da artt. 15-22)

Piattaforme hardware/cloud sicure, utilizzate per ospitare il software



Cifratura del data base

Utilizzo di tecniche di pseudonimizzazione o anonimizzazione (più o meno sofisticate)

Protocolli di connessione e trasmissione dati sicuri

Procedure operative relative ai processi di backup e disaster recovery, inclusive di tutele rispetto ai diritti libertà fondamentali degli interessati

Protezione perimetrale e sui server ospitanti i software da attacchi e malware

Esecuzione continuativa di vulnerability assessment

L'Autorità Garante italiana dedica sul suo sito una sezione di approfondimento proprio sul tema della Privacy By Design , ove richiama le **Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, emesse dall'EPDB**

Un approccio pratico: esempi del Garante Spagnolo

Il Garante Spagnolo tratta con particolare attenzione le strategie riguardanti il trattamento dei dati, di natura tecnica con un focus specifico su un trattamento rispettoso della privacy dei dati raccolti.

01. MINIMIZZARE

Raccogliere e trattare la minima quantità di dati possibile. Ad esempio: attraverso la selezione di un campione pertinente di soggetti.

02. NASCONDERE

Limitare l'esposizione dei dati, impostando le misure necessarie per garantire la tutela degli obiettivi di riservatezza e separazione, ad esempio rendendo incomprensibili i dati personali a chi non è autorizzato ad accedervi

03. DISTACCARE

Mantenere contesti di trattamento autonomi che rendano difficile correlare gruppi di dati che dovrebbero essere disgiunti al fine di evitare, o almeno minimizzare, il rischio che, durante il trattamento di dati personali diversi appartenenti allo stesso individuo e utilizzati in trattamenti autonomi, possa essere effettuata una profilazione completa del soggetto.

04. ASTRARRE

Limitare al massimo il dettaglio dei dati personali che vengono trattati, usando, ad esempio, parole generiche oppure gruppi di valori.

FONTE https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

Fondamentali le **attività di natura organizzativa** con lo scopo di definire i processi che attuino una gestione responsabile dei dati personali. Ad esempio:

01. INFORMARE

Garantire che gli Interessati siano pienamente informati del trattamento dei loro dati in modo tempestivo, fornendo informazioni sul trattamento in forma concisa, trasparente, comprensibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice.

02. CONTROLLARE

Fornire agli interessati il controllo sulla raccolta, l'elaborazione, gli usi e le comunicazioni dei loro dati personali, comprese misure quali l'attuazione di meccanismi che consentano agli utenti di cancellare o richiedere la cancellazione dei dati personali

03. ADEMPIERE

Definire un modello di privacy e una struttura di *governance* che includa una politica di protezione dei dati supportata dall'alta dirigenza, nonché ruoli e responsabilità per garantire la conformità.

04. DIMOSTRARE

Mostrare agli interessati e alle autorità di controllo il rispetto della politica di protezione dei dati che si sta attuando, nonché degli altri requisiti e obblighi legali imposti dal Regolamento attraverso misure come la verifica sistematica, effettuata in modo indipendente e documentato, del livello di conformità alla politica di protezione dei dati.

FONTE https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

In sintesi applicare la **Privacy by Design significa:**

prevenire, **proteggere** e **saper gestire i rischi quotidiani degli interessati** in qualunque settore del business o della quotidianità di un ente.
Questa è la vera sfida per ogni titolare o responsabile che svolga attività di trattamento.

Un’analisi che andrà svolta step by step, perché le tecnologie mutano i loro asset chiedono un continuo adeguamento rispetto all’attività di prevenzione.

Dobbiamo esigere la Privacy by Design... per proteggere noi stessi

Tutto ciò deve essere fatto poiché dietro a ogni dato personale vi è una ***persona umana 'in carne e ossa'****, con le sue vulnerabilità e fragilità, così come dietro all'informazione del dato a lui riconducibile vi è la conoscenza intima del medesimo e del suo patrimonio identitario.*

Egli è così esposto a una crescente pluralità di situazioni, potenzialmente a lui cagionevoli o dannose.

La protezione del dato assurge quindi a difesa dell'essere umano, sino conseguirne il fine ultimo di conservarne la dignità*.*

Avv. Letizia Maria Ferraris

GRAZIE
per l’attenzione

presidente@csi.it