UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unimc

Privacy by Design: principi e metodi di attuazione

Gloria Pellizzer

Proattiva s.r.l.

gloria.pellizzer@hotmail.it

Giovedi 2 ottobre 2025

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Cos’è la Privacy by Design?

Le 5 W della Privacy by Design

- Who? - Ann Cavoukian – former Privacy Commissioner of Ontario.
- When? – nel 2010 (ma nato molto prima).
- Where? - 32ª Conferenza Mondiale dei Garanti della Privacy.

Le cinque W della Privacy by Design

- What? – Integrare il concetto di privacy all'interno di sistemi e processi già nella fase di progettazione.
- Why? – Necessità di prevenire i rischi legati alla privacy.

I 7 Principi

- Proattivo non reattivo – La protezione dati deve essere considerata all'inizio del progetto di pianificazione del sistema/processo/trattamento.
- Privacy by default – Privacy al primo posto, impostazione predefinita.
- Privacy integrata nel design – Privacy come parte integrante della funzionalità principale, senza comprometterla.

I 7 Principi

- Funzionalità completa (Approccio Win-Win) - Privacy non può essere un compromesso.
- Sicurezza end-to-end – I dati devono essere sicuri in ogni fase.
- Visibilità e trasparenza – Informare gli interessati è essenziale per creare fiducia e responsabilità.
- Centralità dell'utente – L'utente deve mantenere il controllo dei propri dati e svolgere un ruolo attivo nella loro gestione.

Privacy by Design nel contesto normativo

Art 25 Reg. Ue 2016/679

1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento**, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento** stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Con l’art 25 del GDPR la PbD diventa **OBBLIGATORIA**!

Il titolare del trattamento dovrà implementare i principi previsti dal GDPR nei sistemi e processi già nella fase di progettazione di essi e durante tutto il ciclo di vita del sistema o processo.

Ogni sistema, processo o trattamento deve essere valutato e disegnato in modo da rispettare i principi stabiliti dal Regolamento.

La Privacy by Design viene esaminata e ne viene data importanza anche in altri documenti:

- Linee Guida EDPB 4/2019 sull'art 25 GDPR
- Guide e indicazioni da parte di Garanti Europei (IT, Spagna, Francia etc.)
- Enisa – Privacy and Data Protection by Design (2015)
- ISO standards (IOS/EIC 27701, ISO/EIC 31700)

Quali sono i principi che devono essere attuati?

- TRASPARENZA, LICEITA' E CORRETTEZZA
- LIMITAZIONE DELLE FINALITA'
- MINIMIZZAZIONE DEI DATI
- ESATTEZZA
- LIMITAZIONE DELLA CONSERVAZIONE

ISO/EIC 31700 – PbD diventa STANDARD ISO

ISO/EIC 31700 – 1:2023

La ISO 31700 è stata pubblicata e adottata nei primi mesi del 2023.

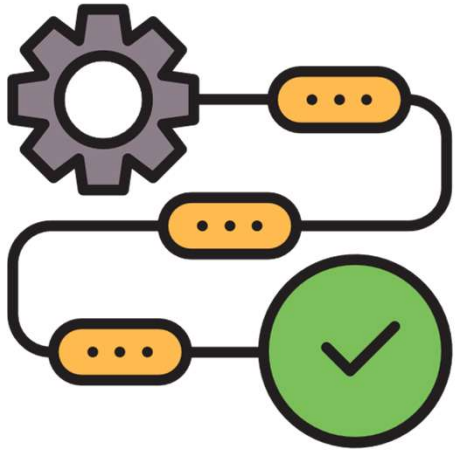
L’obiettivo della norma è fornire un quadro operativo per integrare la protezione dei dati personali fin dalla progettazione di prodotti e servizi di consumo, garantendo che la privacy sia una componente fondamentale e non un'aggiunta successiva.

Lo standard presenta i requisiti necessari ad attuare il principio di PbD all’interno di processi aziendali che prevedano dei trattamenti di dati personali nel fornire servizi e beni a consumatori o utenti.

La ISO/EIC 31700 è strutturata in due parti:

- High Level Requirements – 27 requisiti suddivisi in 5 capitoli.
- Use Cases – esempi che illustrano l'applicazione dei requisiti.

N.B.
La norma non fornisce misure di sicurezza per ottenere la Privacy by Design, ma si applica a processi aziendali.



Capitoli ISO 31700

Capitolo I – GENERALI

- Gestione dei diritti interessati
- Determinazione di ruoli e responsabilità
- Formazione del personale
- Documentazione dei controlli (accountability)

Capitolo II – REQUISITI DI COMUNICAZIONE

- Informative, canali di comunicazione dedicati
- Gestione di reclami, richieste degli interessati
- Gestione e comunicazione di violazione di dati

Capitolo III – GESTIONE DEL RISCHIO

- Valutazione dei rischi ponendo al centro l'utente
- Valutazione e gestione terze parti
- Documentazione per requisiti, controlli e monitoraggio continuo

Capitolo IV – CONTROLLI PRIVACY

- Definire e Integrare controlli privacy nello sviluppo e gestione del prodotto
- Misurare efficacia dei controlli
- Implementare e testare controlli

Capitolo V – FINE CICLO VITA INFORMAZIONI PERSONALI

- Definire e implementare controlli per la gestione del rischio dei dati personali in caso di ritiro o fine vita del prodotto o dell'utente
- Valutazione di eventuali terze parti coinvolte nel trattamento

La seconda parte riporta tre esempi:

- Sito di e-commerce B2C
- una palestra (con un servizio aggiuntivo di raccolta dati delle prestazioni e invio su un'applicazione per dispositivo mobile)
- uno smart lock (con relativa app per dispositivo mobile).

Gli esempi dimostrano quale può essere l'applicazione dei requisiti della prima parte a ciascun caso. Anche gli esempi fanno riferimento a PROCESSI e non a misure di sicurezza.

Come si attua il principio di Privacy by Design?

È come costruire una casa!!

Quando si decide di costruire una casa, non si parte subito a scavare, ma ci sono delle fasi di preparazione e pianificazione che sono fondamentali.

Lo stesso ragionamento deve essere applicato allo sviluppo di prodotti, nuovi servizi, trattamenti e processi pensati in compliance con il principio di Privacy by Design.

L'EDPB, con le Linee Guida 4/2019 sull'art 25 GDPR, ha cercato di spiegare come rendere operativa la Privacy by Design, fornendo degli esempi concreti per l'applicazione dei principi del Regolamento.

Alcune Autorità Garanti Europee (AEPD, CNIL, DPA Norvegese, ICO etc.) si sono rese conto della necessità di produrre una guida pratica per supportare i titolari del trattamento nell'applicazione concreta del principio.
Attuare il principio di PbD significa costruire un sistema strutturato, ma soprattutto **EFFICACE**.

Vediamo come applicare concretamente il principio di Privacy by Design nel processo di sviluppo di un prodotto tecnologico.

1) DEFINIRE UNA STRUTTURA ORGANIZZATIVA

È necessario individuare tutti gli attori e assegnare a ciascuno le attività da svolgere in base alle proprie competenze, stabilendo delle procedure ben precise:

a) Figure apicali in azienda
b) DPO e Legal Team
c) Sviluppatori e Team IT
d) Eventuali altre figure.

Fondamentale è la **FORMAZIONE**.

2) ANALISI DEL CONTESTO

Ogni prodotto è diverso, perciò ne va analizzato il contesto. Le principali domande da porsi sono:

a) Quali trattamenti di dati personali?
b) Quali dati vengono raccolti e con quali basi giuridiche?
c) Come vengono elaborati?
d) Chi deve accedere a tali dati? Sono coinvolti soggetti terzi?
e) Quanto li conservo?
f) Quali sono i rischi?
g) Quali misure di sicurezza in funzione dei rischi individuati?

3) PROGETTAZIONE E DESIGN

Nella fase di progettazione oggettiva si dovrà:

a) Prevedere di raccogliere meno dati possibili (select before you collect)

b) Valutare le misure idonee per la gestione degli accessi da parte degli incaricati (tracciabilità dei log, principio «need to know» etc.)

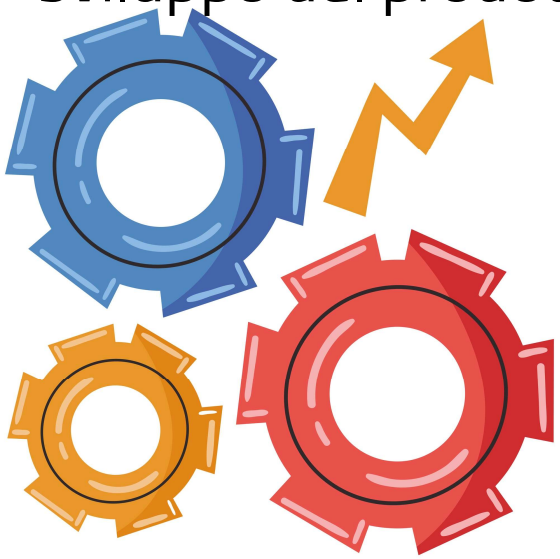
c) Definire tempi di conservazione per ciascuna categoria di dati

d) Prevedere meccanismi di informazione per l'utente e per la gestione dei diritti degli interessati.

È inoltre necessario **DOCUMENTARE** ogni modifica, adempimento etc.

4) IMPLEMENTAZIONE

Tenuto conto di quanto valutato fin ora, si potrà procedere alla fase di implementazione delle cosiddette «PETS» (privacy-enhancing techlogies) e delle misure individuate nel processo di sviluppo del prodotto. Ad esempio:



a) Sistemi di autenticazione e autorizzazione
b) Crittografia
c) Tecniche di Anonimizzazione
d) Log delle modifiche e backup
e) Protocolli di trasmissione sicura (ad es. HTTPS, FTPS, SSH etc.).

5) TESTING

TEST DI SVILUPPO	TEST DI SICUREZZA
Verificare congruenza tra le strategie, specifiche adottate e le funzionalità del prodotto. Per superare il test, la funzionalità non può essere compromessa dalle strategie a protezione dei dati né viceversa (win-win).	Verificare che le misure di sicurezza applicate funzionino correttamente (VA/PT, etc.) e che l'integrazione dei requisiti per la protezione dei dati diano una buona user experience.

La fase di testing non deve essere svolta su dati reali. Questo comporterebbe un innalzamento dei rischi sui dati e anche l'uso degli stessi per una finalità diversa da quella per cui sono stati raccolti.

6) LANCIO DEL PRODOTTO

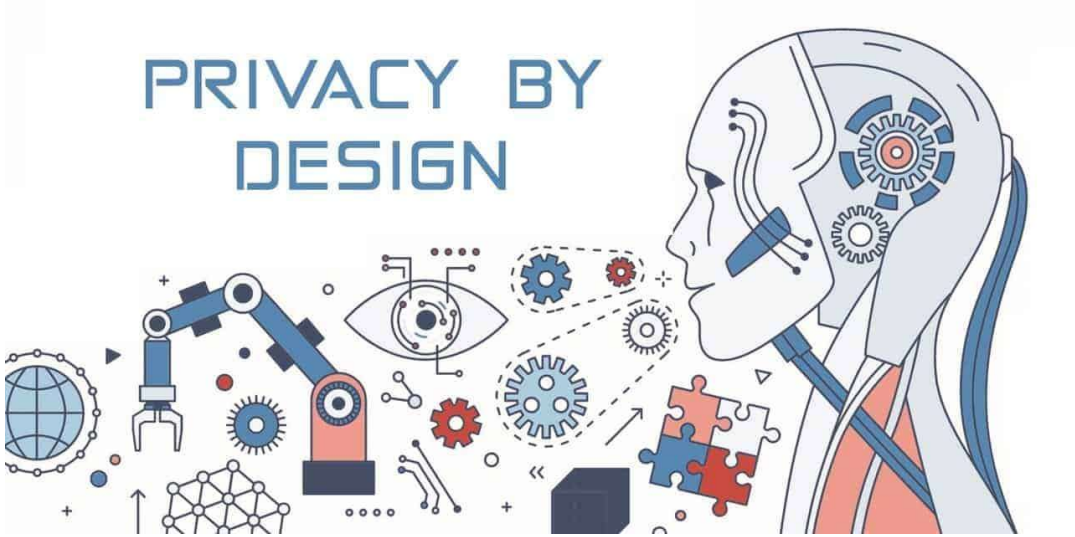
Devono essere implementati dei **CONTROLLI** privacy e sistemi di **MONITORAGGIO** per assicurarsi che le tecnologie utilizzate e il prodotto in generale funzionino in compliance con la normativa.

7) MANTENIMENTO

La fase post-lancio è altrettanto essenziale, in quanto è il primo momento in cui l'utente ha contatto con il prodotto (software, sito web etc.). È necessario verificare l'interazione dell'utente con le informazioni a lui rese accessibili.

È importante mantenere il sistema aggiornato e monitorato lungo tutto il suo ciclo di vita.

È essenziale che le aziende lavorino sullo sviluppo di nuove tecnologie cercando di garantire allo stesso tempo la sicurezza delle informazioni e la tutela dei diritti fondamentali.



La Privacy by Design è lo strumento ideale per raggiungere questo obiettivo.

«Give me **six hours to chop down a tree** and I will spend the **first four** sharpening the ax»

Grazie a tutti per l’attenzione!