

GDPR INSIGHT

SERIES

PRIVACY BY DESIGN & PRIVACY ENGINEERING

ELEMENTI ESSENZIALI PER L'INTEGRAZIONE
DELLA PRIVACY NELLO SVILUPPO DI SOFTWARE E
SERVIZI



NETPATROL
DATA PROTECTION & CYBER SECURITY

NET PATROL ITALIA

Siamo una società di consulenza specializzata in **privacy** e **cybersecurity**.

La nostra squadra è fatta da giuristi specializzati in data protection e professionisti della sicurezza delle informazioni, in grado di trattare in modo trasversale e organico le complesse tematiche che riguardano la protezione dei dati personali.

Il nostro **obiettivo** è dare alle aziende un interlocutore unico, capace di collaborare con il management per lo sviluppo e miglioramento di processi interni e sistemi di gestione finalizzati ad assicurare nel tempo la conformità alla normativa e un adeguato livello di sicurezza delle attività di trattamento



Privacy law



Data Protection Officer



Cybersecurity & Cyber legal advisory

AFFILIAZIONI E CERTIFICAZIONI





INTRODUZIONE

Dal 25 maggio 2018 è applicabile nell'Unione Europea il Regolamento generale per la protezione dei dati personali (da ora in poi lo chiameremo GDPR).

L'adeguamento nazionale ha avuto completa attuazione con l'entrata in vigore del D.lgs. 101/2018, che ha modificato il Codice Privacy nazionale.

Il GDPR ha innovato tutta la gestione dei dati personali in Europa, dando il via ad un vero e proprio movimento di mercato privacy-centrico.

In questa breve guida della serie GDPR INSIGHT approfondiremo il concetto di **Privacy by design** ed il suo significato per chi tratta dati personali ma anche per chi sviluppa software.

Privacy by design, uno dei pilastri del GDPR

Privacy by design significa adottare le **appropriate** misure tecniche e organizzative per dare attuazione ai principi della protezione dei dati personali e integrare le tutele necessarie per rispettare i diritti dei soggetti interessati.

In sostanza, significa sviluppare progetti, prodotti e servizi in modo tale da assicurare il rispetto della normativa e la tutela dei diritti delle persone, **fin dalle fasi di progettazione**.

L'art. 25 del GDPR prevede che i Titolari del trattamento (chiunque decida di trattare dati personali per perseguire degli scopi precisi) debbano rispettare il principio di privacy by design.

I protagonisti della filiera

Il Titolare del trattamento è però solo uno dei soggetti della "filiera privacy" che tipicamente compone un'attività di trattamento di dati.

Pur se l'obbligo di privacy by design è rivolto espressamente solo al Titolare del trattamento, ci sono delle conseguenze che si riverberano su tutti i protagonisti della filiera. Tra questi, sono compresi gli sviluppatori di software.

Il motivo è semplice: trattare dati personali significa **effettuare operazioni** su insiemi di dati.

Questi dati, tipicamente sono trattati con **software** e **hardware** che viene prodotto e/o gestito da terzi.

Chi fornisce software come servizio (SaaS) o gestisce sistemi informativi o servizi informatici per conto di altri, può essere qualificabile come **Responsabile del trattamento**.

Il Titolare del trattamento ha l'obbligo di scegliere soltanto Responsabili del trattamento in grado di soddisfare i requisiti del GDPR.

In alcuni casi, il Titolare stesso può essere sanzionabile per violazioni di legge realizzate dai suoi fornitori (Responsabili del trattamento).

Per questo motivo è più che mai importante avere sempre ben presente tutta la "filiera privacy", e non limitarsi soltanto a ciò che succede nel proprio cortile.

Perché dovrebbe interessarmi il GDPR se sviluppo software e basta?

Essere in grado di garantire la privacy e sicurezza dei dati nel corso di tutte le attività realizzate da un'organizzazione è ormai un imperativo di **legge** e di **mercato**.

Le persone chiedono sempre più attenzione ai loro dati, e sono disposte a dare **fiducia** a chi sarà in grado di mettere la privacy al primo posto.

Da una parte, le aziende che trattano dati personali saranno sempre più spinte a ricercare strumenti, **software** e servizi in grado di semplificare il rispetto della legge e le richieste dei consumatori.

D'altra parte, i **fornitori** di questi strumenti, software e servizi dovranno essere in grado di innovare e saper dare ai loro clienti un prodotto al passo con le richieste di mercato.

Apple è un esempio palese di come la privacy possa diventare un segno distintivo e un pregio per i prodotti consumer: "*Privacy. That's iPhone.*", recita un recente spot pubblicitario.



GDPR INSIGHT SERIES - PRIVACY BY DESIGN & PRIVACY ENGINEERING

Il ritorno economico sugli investimenti in privacy

Uno **studio benchmark** pubblicato da **Cisco** a gennaio 2020 ("*From privacy to profit: achieving positive returns on privacy investments*") mostra che gli investimenti in privacy, spinti più che altro dalle recenti normative, hanno ottenuto importanti **ritorni economici**.

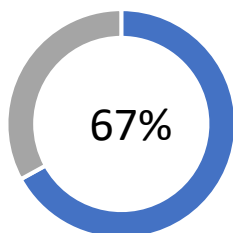
Lo studio è stato realizzato intervistando circa 2800 aziende di ogni dimensione, appartenenti ai principali settori merceologici, in 13 paesi (tra cui anche l'Italia).

Molti degli intervistati hanno affermato che nella fase di **scelta di nuovi fornitori** di prodotti o servizi tengono in considerazione specifiche certificazioni privacy (come la ISO 27701) e garanzie in materia.

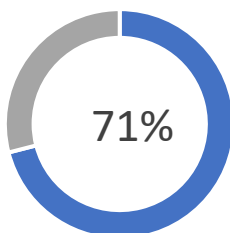
La maggior parte delle aziende intervistate hanno affermato di aver riscontrato un ritorno economico positivo degli investimenti fatti negli ultimi anni. Di queste, circa il 40% ha dichiarato di aver visto un **ritorno di almeno il doppio** di quanto investito.

La stragrande maggioranza delle aziende intervistate ha confermato un **miglioramento** nei seguenti campi, a seguito dello sviluppo di un sistema di gestione privacy:

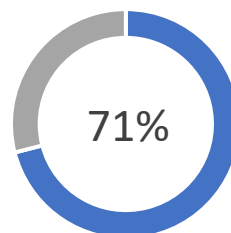
Aumento velocità di
vendita



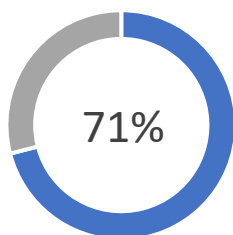
Mitigazione data
breach



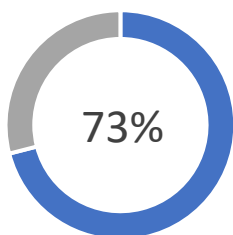
Aumento agilità e
innovazione



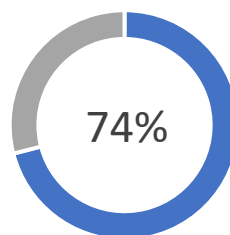
Miglioramento
efficienza



Aumento attrattività
investitori



Aumento fiducia
consumatori

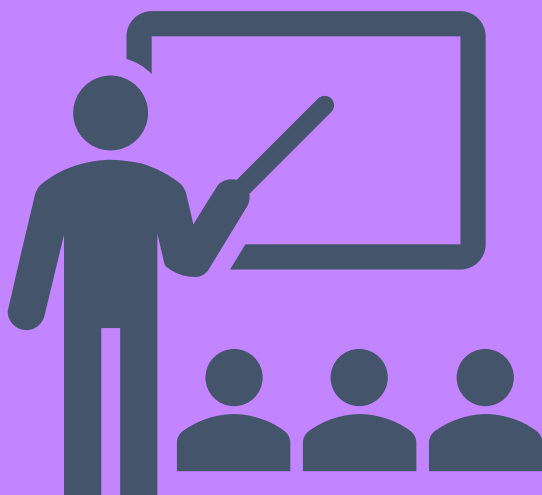


Fonte: Cisco benchmark study "*From privacy to profit: achieving positive returns on privacy investments*", 2020

Lo studio Cisco dimostra che rispettare il GDPR non significa scrivere tonnellate di carta, ma lavorare sulla **governance** aziendale e **innovare i processi** interni, portando in primo piano la protezione dei dati, che sono la linfa vitale di ogni organizzazione, a prescindere dal settore.

PRIVACY BY DESIGN

PRENDIAMO CONFIDENZA CON LE BASI





PRINCIPI E NOZIONI

Il concetto di **privacy by design** esiste da oltre 20 anni, ma è solo con il GDPR che è diventato vincolante.

Incorporare i principi della protezione dei dati fin dalle fasi di progettazione di sistemi, servizi e prodotti è sempre più importante per accrescere la fiducia dei consumatori.

Progettare integrando i principi della protezione dei dati implica la realizzazione di un'analisi orientata alla gestione dei rischi per le persone derivanti dal trattamento dei loro dati personali.

Accountability: responsabilità proattiva

A coloro che trattano dati personali è richiesta una sorta di "**responsabilità proattiva**".

Il concetto è un'estensione diretta della privacy by design.

Responsabilità proattiva significa essere in grado di governare la propria organizzazione, tenendo in considerazione la protezione dei dati, che ormai sono la linfa vitale di qualsiasi business.

Per questo motivo le organizzazioni dovrebbero **scegliere con cura** gli strumenti con cui trattano dati personali, perché saranno quelli a determinare la qualità del proprio sistema di gestione per la protezione dei dati.

Cosa cambia per le software house?

Quando un'azienda compra o commissiona lo sviluppo di un'app, molto probabilmente si troverà a trattare dati personali in qualità di Titolare del trattamento.

L'azienda dovrebbe essere quindi in grado di rispettare la normativa anche per tutte le attività di trattamento realizzate attraverso l'uso della sua nuova app.

La capacità di rispettare o meno il GDPR non dipende però dall'azienda, ma da chi ha sviluppato l'app. Ciò che può fare l'azienda, al massimo, è scegliere il proprio fornitore sulla base delle garanzie offerte.

Non solo prodotti consumer, ma anche ERP, CRM e CMS

Incorporare i principi di privacy by design nei prodotti e servizi destinati alle aziende è importante tanto quanto per quelli destinati ai consumatori.

Anche **ERP** (Enterprise resource planning), **CRM** (Customer relationship manager) e **CMS** dovrebbero essere in grado di semplificare gli sforzi delle aziende per rispettare il GDPR e tutelare i diritti delle persone.

Capita molto spesso che le aziende siano **sanzionate** a causa dell'inadeguatezza dei software utilizzati.

Le caratteristiche di un CRM

Il CRM è spesso il fulcro delle attività di un'azienda, e altrettanto spesso è il software con cui sono gestiti i flussi di dati.

Un CRM al passo coi tempi e rispettoso del GDPR dovrebbe prevedere almeno queste caratteristiche:

- Data retention granulare
- Sincronizzazione e comunicazione con gli strumenti di raccolta del consenso e CMS
- Capacità di estrazione di dati personali
- Separazione logica degli accessi

Un software che non è in grado di fornire alle aziende queste caratteristiche essenziali, difficilmente troverà mercato nei prossimi anni.

Le persone al centro

L'obiettivo principale della privacy by design è quello di porre al centro dell'attenzione gli **interessi e diritti delle persone**. Questo implica la capacità di sviluppare sistemi, applicazioni e servizi tenendo conto dei rischi derivanti dal trattamento di dati personali delle persone.

Questo non significa svilire altre funzionalità o mettere in secondo piano altre necessità, ma anzi **bilanciare** con la privacy elementi come utilizzabilità, funzionalità, sicurezza e business.



Tra privacy e cybersecurity

Il GDPR non ha soltanto innovato il panorama europeo per la privacy, ma ha anche aumentato l'attenzione alla sicurezza dei dati.

Il Titolare del trattamento è tenuto a adottare misure tecniche e organizzative per **garantire la sicurezza** delle attività di trattamento e la resilienza dei sistemi.

Nessuno può lecitamente trattare dati personali senza curarsi della loro sicurezza.

Come per la privacy, anche in questo caso le aziende non saranno in grado di rispettare i requisiti di legge senza strumenti che permettano di affrontare tutte le necessità relative alla sicurezza dei dati.

Usare strumenti sviluppati senza tener conto della sicurezza dei dati aumenta inevitabilmente il rischio di **data breach**.

Il costo di un data breach

Il costo di un data breach (violazione di sicurezza dei dati) dipende da molti fattori.

Tra i principali certamente deve ricomprendersi l'estensione dei dati compromessi e la natura degli stessi.

Un recente studio realizzato da **IBM e Ponemon Institute** (*"Cost of a data breach", 2018*) su un campione di circa 500 aziende in tutto il mondo stima che il **costo medio di un data breach** si aggira intorno ai 3 milioni di euro, per una media di circa 22.500 dati personali violati.

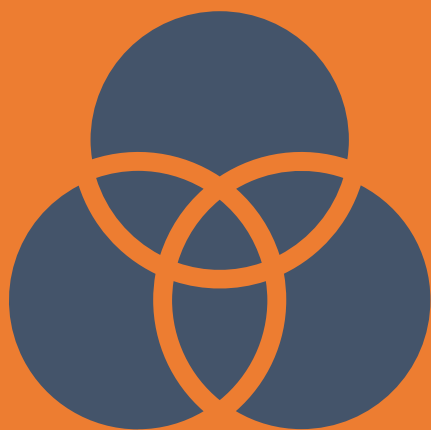
Circa 150 euro per ogni dato personale compromesso.

A questo, devono aggiungersi eventuali sanzioni e danno d'immagine.

Come mostra lo studio di Cisco, un modo per **mitigare i costi** di un data breach è applicare i principi di privacy by design e sviluppare un sistema di gestione per la protezione dei dati in grado di sopperire alle necessità aziendali e ai rischi derivanti dal contesto di operatività.

I PILASTRI DELLA PRIVACY

UNLINKABILITY, TRASPARENZA, CONTROLLO





I TRE PILASTRI DELLA PRIVACY

La protezione dei dati personali si fonda su **tre parametri** fondamentali:



Unlinkability

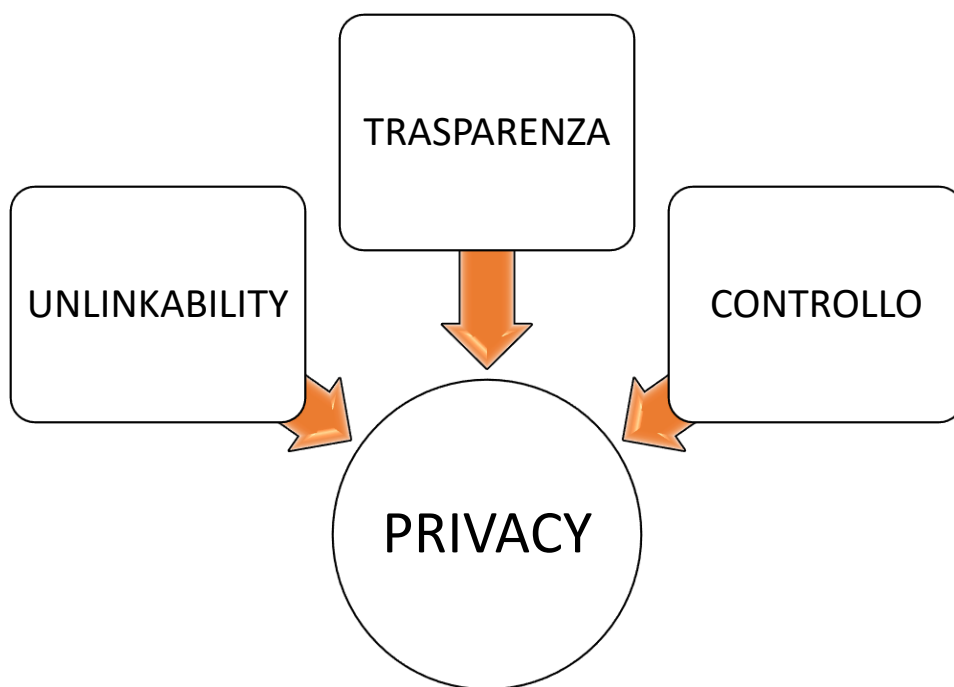


Trasparenza



Controllo

Lo scopo di questi parametri è quello di fornire un sufficiente grado di astrazione per consentire lo sviluppo di sistemi di trattamento in grado di soddisfare i complessi requisiti di legge in materia di privacy.



Questi parametri devono essere intesi come **punti di riferimento astratti** per sviluppare servizi e prodotti in grado di rispettare la normativa e tutelare i diritti dei soggetti interessati.

Il GDPR, attraverso specifiche prescrizioni di legge, definisce ulteriormente questi tre principi, pur mantenendo volutamente un certo livello di astrazione.

Chiunque tratti dati personali è tenuto a garantire che in ogni fase del trattamento siano rispettati questi tre parametri fondamentali.



IN DETTAGLIO

Vediamo insieme nel dettaglio il significato dei tre parametri.

Unlinkability

Il parametro della unlinkability potrebbe essere tradotto in italiano con minimizzazione, anche se non sarebbe del tutto corretto, poiché la minimizzazione è solo una proprietà dell'unlinkability.

Questo parametro intende mitigare il rischio di **uso non autorizzato** di dati personali e **l'interconnessione** eccessiva di informazioni appartenenti a diversi insiemi di dati.

I riferimenti del GDPR sono:

- Limitazione delle finalità (art. 5, lett. b)
- Minimizzazione dei dati (art. 5, lett. c)
- Limitazione della conservazione (art. 5, lett. e)

È utile notare che il rispetto del parametro di unlinkability può essere di supporto anche per la sicurezza dei dati: segmentare reti e sistemi, o amministrare le utenze secondo i principi di "need to know" e "least privilege" sono strategie che aiutano a raggiungere sia obiettivi di privacy che di sicurezza.

Trasparenza

Trasparenza significa prima di tutto **essere consapevoli** di ciò che si fa. Non possiamo garantire trasparenza a clienti e utenti senza conoscere i flussi di dati, le attività di trattamento e i soggetti coinvolti.

Il parametro di trasparenza intende assicurare che i soggetti interessati (le persone a cui si riferiscono i dati personali trattati) abbiano cognizione dell'uso che si farà dei loro dati, in modo **semplice**, comprensibile e conciso.

I riferimenti del GDPR sono:

- Principio di liceità e correttezza (art. 5, lett. a)
- Informazioni ai soggetti interessati (artt. 12, 13, 14, 34)
- Registro delle attività di trattamento (art. 30)

Il rispetto del parametro di trasparenza implica che tutte le scelte effettuate in merito al trattamento dei dati (legali, tecniche, organizzative) debbano essere **ricostruibili** e **tracciabili** in ogni momento.

Trasparenza significa quindi anche **dimostrabilità** delle proprie azioni.

Controllo

Il parametro del controllo garantisce la possibilità che tutte le parti coinvolte nel trattamento di dati personali, e principalmente i soggetti interessati, possano **intervenire nel trattamento** quando necessario.

La possibilità di intervento è strettamente correlata all'esercizio dei diritti dei soggetti interessati, ma non solo. Mantenere il controllo sulle attività di trattamento significa che chi tratta dati personali deve avere il polso della situazione per tutto ciò che accade, anche quando sono coinvolti strumenti informatici o soggetti terzi.

I riferimenti del GDPR sono:

- Diritti dei soggetti interessati e consenso (artt. 7, 15, 16, 17, 18, 19, 20, 21, 22)
- Accountability e Responsabili del trattamento (artt. 24, 28)
- Sicurezza del trattamento (art. 32)



GDPR INSIGHT SERIES - PRIVACY BY DESIGN & PRIVACY ENGINEERING

Privacy e sicurezza: due facce della stessa medaglia

Non bisogna dimenticare che il GDPR richiede anche di garantire la **sicurezza** dei dati trattati.

Chiunque tratta dati personali è tenuto a garantire un livello di sicurezza adeguato al rischio, in ogni fase del trattamento.

Anche la sicurezza delle informazioni ha i suoi **tre parametri** fondamentali:



Riservatezza

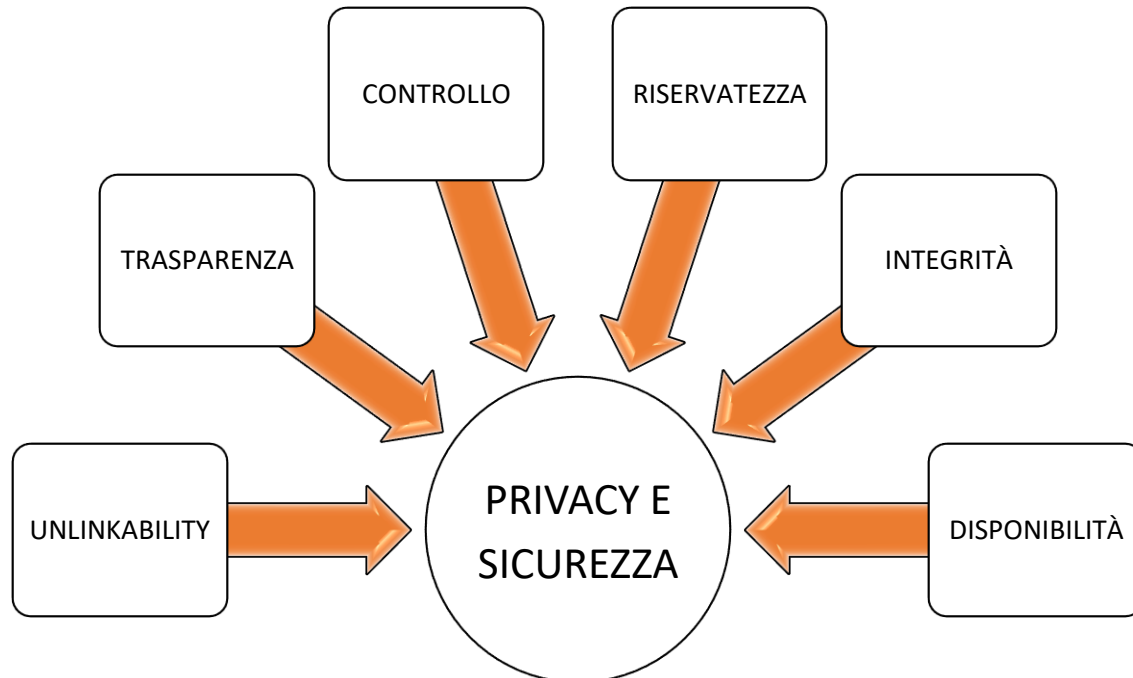


Integrità



Disponibilità

Oggi è opportuno parlare in modo trasversale di **sei parametri**, per la privacy e sicurezza dei dati, che devono essere tenuti in considerazione durante lo sviluppo di prodotti, software e servizi.



Osservandoli in una visione d'insieme, i sei requisiti di privacy e sicurezza sono tra loro **complementari** e in alcuni casi si sovrappongono.

Per questo motivo è sempre più necessario integrare fin dalle fasi di progettazione le necessarie valutazioni per privacy e sicurezza, in modo tale da ponderare preventivamente i rischi e **bilanciare** tutti gli obiettivi (senza dimenticare quelli di business!).

PRIVACY ENGINEERING

STRATEGIE E TECNICHE PER LA PRIVACY BY
DESIGN





TECNICHE E STRATEGIE DI PRIVACY BY DESIGN

L'implementazione dei requisiti normativi all'interno di processi e progetti complessi non è semplice.

I parametri brevemente affrontati nella sezione precedente sono degli utili **obiettivi** da tenere in considerazione, ma il processo di sviluppo di un prodotto o servizio non può accontentarsi semplicemente di obiettivi astratti. In questa sezione vedremo alcune **strategie** e **tecniche** per implementare nella pratica gli obiettivi privacy in un progetto.

Privacy engineering

Per privacy engineering si intende il processo sistematico e diretto, attraverso la valutazione dei rischi, che ha come obiettivo quello di **tradurre in termini pratici e operativi** i principi della privacy by design nel ciclo vita di sistemi, prodotti e servizi utilizzati per trattare dati personali.

In breve, il processo di privacy engineering si compone almeno di tre punti essenziali:

- Definizione dei requisiti privacy
- Progettazione e implementazione dei requisiti
- Verifica e validazione dei requisiti

L'obiettivo è che i requisiti privacy (e di sicurezza) siano integrati come parte del progetto, così da definirli e implementarli prima del lancio sul mercato del prodotto o del servizio.

Le metodologie utilizzate per integrare la privacy by design nel processo di sviluppo cambiano molto a seconda delle necessità e del contesto, ciò che conta è avere obiettivi ben definiti, anche in riguardo alle richieste di mercato.

Data protection impact assessment

Un modo per raggiungere gli obiettivi di privacy e sicurezza è la **Data protection impact assessment (DPIA)**.

Per DPIA si intende il processo con cui è possibile **valutare i rischi** relativi alla privacy e sicurezza di uno specifico trattamento.

A prescindere dalla metodologia utilizzata, ogni DPIA dovrebbe almeno seguire i seguenti step logici:

- Identificazione del contesto
- Identificazione di minacce, eventi negativi e rischio
- Identificazione delle soluzioni
- Implementazione delle soluzioni
- Review

Una DPIA può avere ad oggetto qualsiasi attività, prodotto o servizio con cui saranno trattati dati personali.

L'art. 35 del GDPR obbliga i Titolari del trattamento a svolgere DPIA.

In alcuni casi però può essere conveniente anche per una software house sottoporre a DPIA il software che si sta sviluppando, in modo tale da fornire **garanzie** in più e preziose informazioni ai clienti che vorranno usarlo (e che eventualmente saranno tenuti a fare DPIA).

Quali sono i rischi da valutare?

Per rischi si intendono gli eventi negativi che potrebbero **impattare** sui diritti e le libertà dei soggetti interessati.

Ricorda che con una DPIA non stiamo valutando i rischi per l'organizzazione ma per i diritti e libertà delle persone di cui stiamo trattando i dati personali.

Esempi di questa tipologia di rischi possono essere il furto d'identità, il danno reputazionale, ma anche la discriminazione o la manipolazione.



GDPR INSIGHT SERIES - PRIVACY BY DESIGN & PRIVACY ENGINEERING

Una DPIA per un'app mobile

Come accennato, una DPIA può avere molte forme e metodologie. Può essere un documento di poche pagine o di centinaia di pagine con allegati.

Ciò che conta, è seguire un filo logico che permetta di valutare il più oggettivamente possibile i rischi per i diritti e libertà delle persone e identificare le possibili soluzioni.

Facciamo un esempio semplificato di DPIA per una semplice app mobile:

Contesto	App che indica il meteo in tempo reale all'utente, rilasciata gratuitamente per l'uso.
Minaccia	L'app developer ha utilizzato per lo sviluppo SDK che consentono l'installazione di trackers di terze parti che raccolgono dati sulla localizzazione degli utenti che usano il servizio. L'utente non è consapevole del tracking perché non sono date informazioni in merito e non è chiesto il suo consenso.
Evento	Vendita dei dati di geolocalizzazione a società di advertising all'insaputa del soggetto interessato.
Rischio	Profilazione nascosta da parte degli advertisers per profilare l'utente e proporre pubblicità mirata. Potenzialmente, quei dati potrebbero essere utilizzati anche per finalità di propaganda politica (cfr. Cambridge Analytica).
Soluzione	Informare e chiedere il consenso, o evitare di usare librerie di terze parti che permettono il tracking dell'utente.

Come si può notare, in questo caso la fonte di minaccia è l'app developer stesso, che per avere un ritorno economico ha scelto di utilizzare librerie di sviluppo di terzi che consentono di localizzare a scopo di lucro gli utenti finali, senza il loro consenso e a loro insaputa.

Talvolta, anche le **API** utilizzate sono fonte di rischio.

Una recente ricerca¹ ha dimostrato che moltissime API Android possono essere utilizzate per fingerprinting dei dispositivi mobili, identificare app vulnerabili e dati personali riservati. In questo caso però, la minaccia è al di fuori della portata di uno sviluppatore.

¹ A. Yerukhimovich, R. Balebako, A. E. Boustead, R. K. Cunningham, W. Welser and R. Housley, "Can Smartphones and Privacy Coexist?," RAND Corporation, 2016



Strategie di design della privacy

La privacy engineering si compone di diverse **strategie di design**, che descrivono l'approccio necessario a raggiungere determinati obiettivi di progettazione.

Le principali strategie di design possono dividersi in due gruppi:



Strategie orientate ai dati

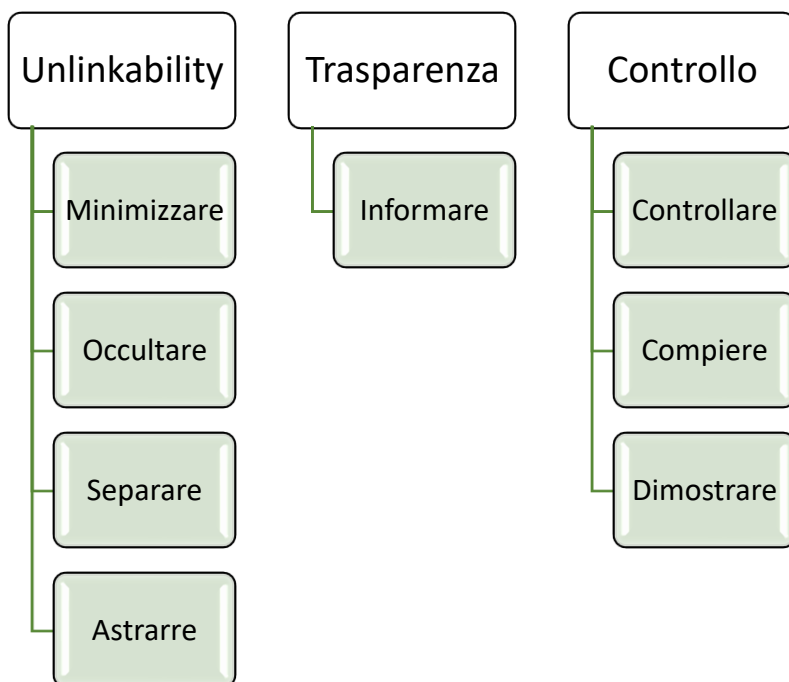


Strategie orientate ai processi

Le prime sono di carattere tecnico, orientate a definire le modalità di acquisizione dei dati ed il loro ciclo vita.

Le seconde sono di carattere organizzativo, orientate alla definizione dei processi che governeranno il trattamento dei dati in tutte le sue fasi.

A seconda del contesto e del progetto determinate strategie possono essere più idonee di altre, ma in generale deve ritenersi che il momento migliore per applicare queste strategie sia quello di **concept development** del software.



Ognuna di queste strategie comprende al suo interno delle specifiche **tecniche** che, se adottate durante la fase di sviluppo di un prodotto o servizio, permettono di raggiungere gli obiettivi desiderati.

Un esempio pratico di tecnica di **astrazione** è la **differential privacy**.

Attraverso questa tecnica è possibile anonimizzare set di dati attraverso l'introduzione di "rumore" casuale, pur mantenendone il valore intrinseco. La differential privacy per sua natura funziona soltanto in presenza di grandi dataset, il cui valore statistico non viene influenzato dall'introduzione di elementi casuali.

La tecnica è molto utile in ambito medico o scientifico, dove è necessario acquisire enormi quantità di dati preservando la privacy di coloro a cui si riferiscono i dati.



Ciclo di sviluppo o ciclo di vita dei dati?

L'applicazione delle strategie e tecniche viste finora può avere ad oggetto il **ciclo di sviluppo** di un software o servizio, o il **ciclo di vita dei dati**, talvolta anche con effetti molto diversi tra loro.

Ad esempio, la **minimizzazione** dei dati può essere raggiunta scegliendo di non raccogliere dati non strettamente necessari. Questa è una decisione che riguarda il ciclo di vita dei dati (raccolta).

Lo stesso obiettivo può essere però raggiunto utilizzando **protocolli di crittografia** che rendono possibile raccogliere uno spettro più ampio di dati, pur limitando il data-flow ai soli soggetti o sistemi che necessitano di certi dati. Questa è una decisione che riguarda il ciclo di sviluppo (design e implementazione).

Un modo per coadiuvare l'esigenza di fare attenzione al ciclo vita dei dati, pur mantenendo una precisa metodologia di sviluppo, può essere quello di integrare metodi di sviluppo software, come l'**Agile Secure Development Lifecycle** (SDLC)², con metodologie per la valutazione dei rischi privacy sul ciclo vita dei dati, come il metodo **LINDDUN**.³

Le privacy enhancing technologies

Oltre alla definizione di strategie e tecniche di design per prodotti e servizi secondo il principio di privacy by design, è anche possibile implementare delle **soluzioni tecnologiche** in grado di mitigare alcuni rischi e semplificare il raggiungimento dei propri obiettivi.

Il termine **privacy enhancing technologies (PETs)** è stato introdotto per definire una categoria di soluzioni tecnologiche sviluppate per raggiungere determinati obiettivi di privacy.

Oggi, il campo delle PETs è diventato una vera e propria materia che si pone a metà tra la computer science, la giurisprudenza e l'economia.

Nonostante la loro indubbia utilità, queste soluzioni tecnologiche da sole non possono sopperire a tutti i rischi privacy.

Per questo motivo è necessario sviluppare ogni prodotto e servizio che tratterà dati personali secondo i principi di privacy by design che abbiamo affrontato.

Le PETs possono essere anche delle **soluzioni stand-alone** utilizzabili da chiunque.

Uno degli esempi più famosi di PET stand-alone è certamente **TOR**⁴ (The Onion Router), un software open-source che permette comunicazioni anonime tramite Internet.

Tra le PETs che possono essere d'aiuto durante lo sviluppo di un **software** possono citarsi gli strumenti e algoritmi di **hashing**, utilissimi per **pseudonimizzare** i dati e per preservarne l'integrità, così come gli strumenti di **cifratura**, utili a preservare la riservatezza dei dati sia a riposo che in transito.

² Il Secure Development Lifecycle è un metodo nato per integrare requisiti di sicurezza all'interno del ciclo di sviluppo software. Il SDLC può essere utilizzato allo stesso modo per integrare requisiti privacy e attuare le tecniche di privacy engineering.

³ <https://www.linddun.org/>

⁴⁴ <https://www.torproject.org/>



Net Patrol Italia

www.netpatrol.it - info@netpatrol.it – 02 87165913

Sede di Milano

Via Napo Torriani, 31 | 20124 Milano

Sede di Udine

Via Giovanni Paolo II, 3 | 33100 Udine

GDPR INSIGHT SERIES

PRIVACY BY DESIGN & PRIVACY ENGINEERING

ELEMENTI ESSENZIALI PER L'INTEGRAZIONE DELLA PRIVACY NELLO SVILUPPO DI PRODOTTI E SERVIZI

Febbraio 2020

© Net Patrol Italia s.r.l.

Disclaimer:

Questa guida non intende sostituire le fonti legali e riflette unicamente le opinioni degli autori.

Le azioni intraprese dalle organizzazioni non possono basarsi esclusivamente sulla lettura di questa pubblicazione. In nessun modo la presente pubblicazione può sostituire il lavoro prestato da persone specializzate e competenti nella materia della protezione dei dati personali.

Net Patrol Italia s.r.l. non può essere ritenuta responsabile per i danni o le violazioni del Regolamento UE 2016/679 realizzate dalle organizzazioni che fondino le proprie decisioni esclusivamente sulla base di questa pubblicazione.