Deloitte.
Legal

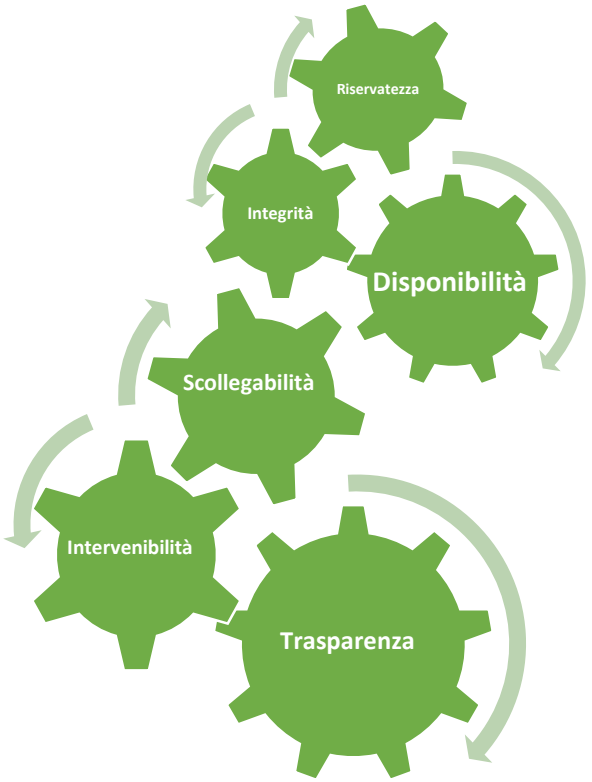
Data Protection | Breaking news

Data Protection Engineering

Marzo 2022

Data Protection Engineering

Il concetto di **Data Protection Engineering** si inserisce nel più generale principio di **Privacy by Design** e **by Default**, centrato sulla configurazione e adozione di misure tecniche e organizzative in ambito privacy. A gennaio 2022 l'ENISA (*European Agency for Cybersecurity*) ha pubblicato un **Report** volto anche alla promozione di *best practices* per dare concretezza ai seguenti **obiettivi**:



I primi 3 obiettivi sono quelli **tradizionalmente** considerati nella **fase di valutazione del rischio**

Gli ultimi 3 obiettivi sono collegati alla **tutela** dell'interessato sotto il profilo privacy

Le **Privacy Enhancing Technologies (PET)** sono un insieme di **tecnologie** o **prodotti software** utili per rafforzare o migliorare la protezione della privacy. Alcuni esempi:

Differential privacy

Algoritmi usati per consentire di effettuare analisi statistiche sui dati proteggendo gli interessati che fanno parte del dataset

On device computation

I modelli allenati con dati locali sono connessi tra loro così da generare un modello combinato

Secure multi-party computation

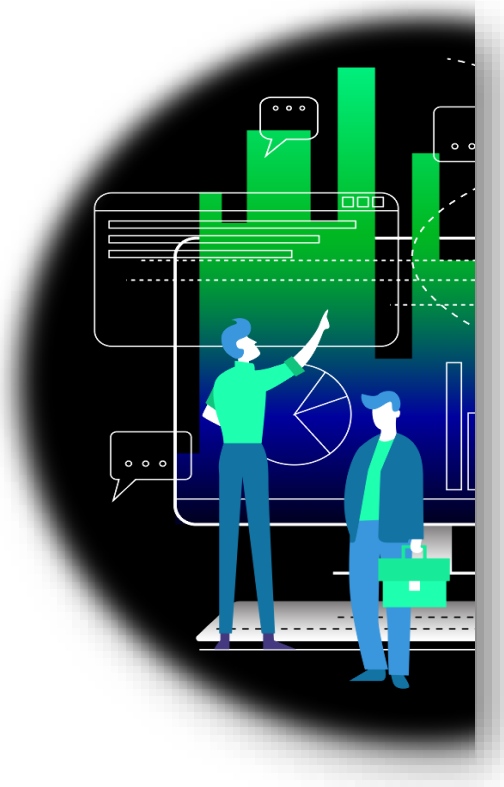
Protocollo volto a gestire il tema del trust nei casi in cui un set di dati sia condiviso tra più parti ognuna delle quali non possa vedere i dati

Le PETs possono essere categorizzate distinguendo tra tecnologie di:

•**Truth-preserving**: permettono di ridurre la possibilità di identificare i dati trattati, preservandone l'accuratezza

Intelligibility-preserving: per conservare i dati in un formato conosciuto ed interpretabile solo dal titolare del trattamento e impedire di rivelare i dati degli interessati

•**Operable Technology**: le operazioni matematiche e logiche sui dati sono eseguibili sui risultati delle loro applicazioni, anche ove i dati non siano intelligibili



L'utilizzo dell'**Intelligenza Artificiale** (IA) è un nuovo metodo per la gestione dei dati personali tramite modelli di **machine learning** di tipo generativo.
Un esempio di tale tecnologia è la **sintetizzazione dei dati**, che consiste nella creazione di dati artificiali da parte di macchine di IA che simulano il «mondo reale»: i dati sintetici non si riferiscono a nessun individuo in particolare.

Alcuni esempi di **tecniche di protezione** dei dati:

Anonimizzazione

- Procedimento che rende l'interessato non riconoscibile mediante un processo irreversibile. Ogni soluzione adottata deve tenere conto del contesto, del tipo di dati e di trattamento e dei possibili rischi di attacco.

Pseudonimizzazione

- Procedimento che impedisce che i dati personali possano essere attribuiti a un individuo specifico senza l'utilizzo di informazioni aggiuntive.

Crittografia

- Principale tecnica di **data masking** usata per proteggere la riservatezza dei dati da accessi non autorizzati.

⓾ **Crittografia omomorfica**: consente di operare calcoli su dati crittografati senza che siano previamente decrittografati.

⓾ **Calcolo multiparte sicuro**: protocolli crittografici che distribuiscono un calcolo fra più parti, nessuna delle quali può vedere i risultati delle altre.

⓾ **Ambienti di esecuzione affidabili**: proteggono i dispositivi da accessi non autorizzati.

⓾ **Private information retrieval**: consente di recuperare una voce in un database senza svelare al data owner quale dato sia stato attenzionato.

1)Accesso - Autenticazione

- Tecniche che prevengono il verificarsi di attività non autorizzate e/o indesiderate. Tra queste vi sono:

⓾ **Controllo discrezionale degli accessi (DAC)**: limitazione dell'accesso ad un determinato contenuto.

⓾ **Attribute-based credentials (ABC)**: autenticazione degli interessati attraverso diversi attributi non collegabili tra loro.

⓾ **Zero Knowledge Proof**: metodo interattivo per dimostrare di essere a conoscenza di un'informazione segreta, senza rivelarla.

1)Comunicazione e conservazione

- Le tecniche di **conservazione** perseguono il duplice fine di:

⓾ **proteggere la riservatezza** dei dati personali inattivi;

⓾ **informare i titolari** del trattamento in caso di violazione.

-
- In merito alle **comunicazioni**:

⓾ **Crittografia end-to-end**: sistema di comunicazione cifrata per cui solo le parti coinvolte possono accedere alle chiavi di decriptazione;

⓾ **Proxy & onion routing**: tecnica di anonimizzazione delle comunicazioni in cui il traffico degli utenti viene incanalato con diversi server di inoltro, in cui ciascuno di essi riceve dati crittografati a più livelli senza conoscere né il mittente né il destinatario.

Sono molteplici i possibili strumenti di **trasparenza, intervenibilità e controllo** in ambito privacy, tra cui anche i seguenti:

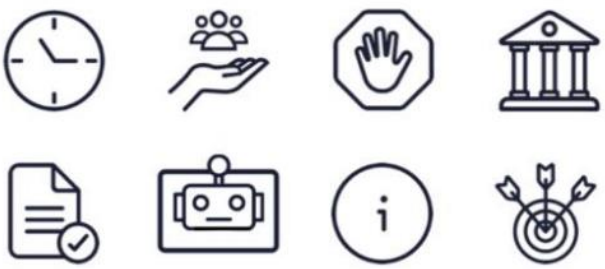
Privacy policy	Il titolare del trattamento deve elaborare informative chiare, semplici e complete.
Sticky Policy	Policy «attaccate» ai dati affinché le regole di trattamento seguano i dati anche in caso di trasferimenti a terzi.
Espressioni di preferenze sulla privacy	Per tenere traccia delle preferenze dell'utente in modo standardizzato.
Dashboard sulla privacy	Per illustrare agli interessati le modalità di trattamento dei dati.
Raccolta del consenso	Esempio il form «ho letto e compreso i termini di utilizzo», da accettare nei siti.
Gestione del consenso	Tecnologie con cui archiviare in modo permanente le manifestazioni di consenso
Diritto di accesso, cancellazione, rettifica	Automatizzazione dell'esercizio dei diritti dell'interessato per ridurre i costi.

Al fine di rendere le informative privacy più semplici, chiare ed immediatamente comprensibili viene sempre più valorizzato l'utilizzo di **simboli** ed **icone**. Si tratta di una possibilità prevista dal GDPR che il Garante Privacy ha deciso di promuovere lanciando recentemente un contest finalizzato ad individuare un set di immagini che esemplifichino gli elementi che devono essere obbligatoriamente contenuti nelle informative ai sensi degli articoli 13 e 14 del GDPR. Di seguito, i vincitori del contest:

Osservatorio579

Athlantic

Maastricht European Centre on Privacy and Cybersecurity



Experience the future of law, today

Today, you need smart lawyers who bring even more to the table than legal advice and memorandums. You need to work better, faster and with lower total cost. That takes someone who knows your business and your industry, yet thinks and works in new ways. A steady hand at the center of the transformation all around us. An expert in law, commerce and technology, who is able to serve you globally.

To make an impact that matters, you need an accomplished confidante who is both pragmatic and pioneering.

Deloitte Legal invites you to experience the future of law, today. Meet current obligations more effectively while anticipating future opportunities.

To make an impact that matters, you need an accomplished confidante who is both pragmatic and pioneering.

Deloitte Legal invites you to experience the future of law, today. Meet current obligations more effectively while anticipating future opportunities.

Automate complicated and time-consuming legal activities. Benefit from a commercial mindset that integrates legal, business and industry expertise. Draw upon our experience with business operating model transformation.

As you lead your enterprise through unprecedented complexity and change, we'll work with you not just for you. Working together, you're empowered to make confident decisions, guide your business and take advantage of possibilities.

Experience the future of law, today.

Key contacts Data Protection Team

Ida Palombella

Partner

ipalombella@deloitte.it

Pietro Boccaccini

Director

pboccaccini@deloitte.it

Simone Prelati | Federico Vota

Camilla Torresan | Lidia Letterelli | Benedetta Antonelli

Deloitte.
Legal