UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Data Protection Engineering: scollegabilità, trasparenza e intervenibilità in rapporto con i diritti degli interessati.

Avv. Federico Alessandri
Studio Legale Alessandri
Corso d'Augusto, 213 – Rimini
alessandri@alessandristudiolegale.com
www.alessandristudiolegale.com

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Il Report ENISA «Data Protection Engineering »del 22 gennaio 2022

Scopo del Report

Il Report ha lo scopo di aiutare consulenti e imprese con l'**implementazione pratica** degli aspetti tecnici della *data protection by design* and *by default*.

Il documento illustra le **tecnologie** e le **tecniche esistenti** e ne valuta la forza e l'applicabilità al fini del raggiungimento dei principi applicabili alla protezione dei dati stabiliti dal GDPR.

In estrema sintesi:

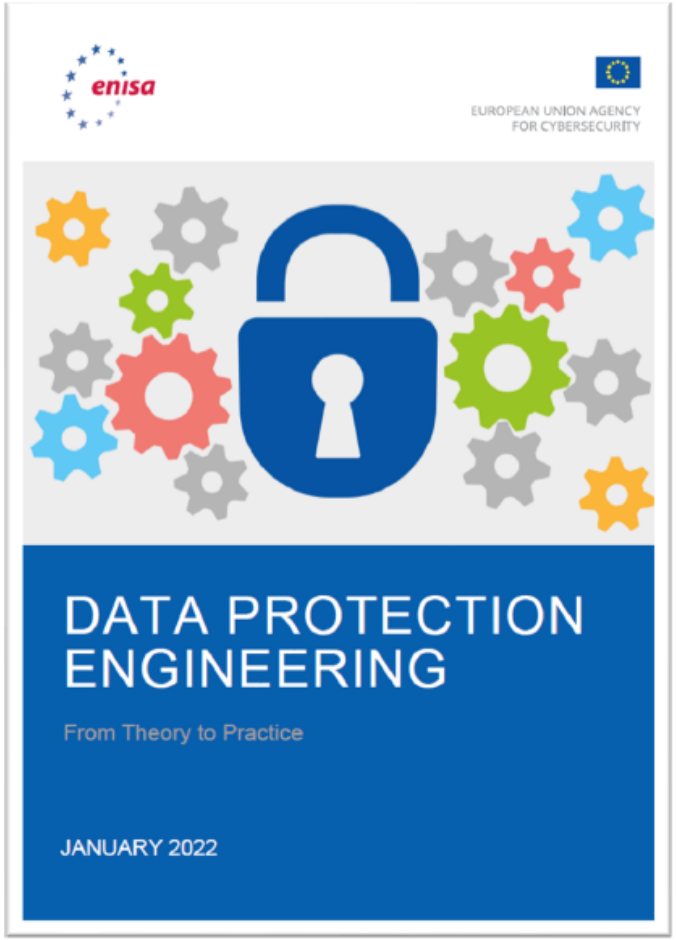
E' possibile declinare l'arte della data protection in tecnicismi ingegneristici?

Obiettivi del Report

I **principi di protezione dei dati**, enunciati nell'articolo 5 del GDPR ed elaborati in termini di misure e garanzie nell'articolo 25 (*data protection by design e by default*), sono gli obiettivi che devono essere raggiunti quando si considera la progettazione, l'attuazione e l'implementazione di un trattamento.

la vera sfida consiste nel **tradurre questi principi in requisiti tangibili** selezionando, implementando e configurando misure e tecniche e organizzative adeguate durante l'intero ciclo di vita del trattamento dei dati previsto.

Le nuove sfide



1. riservatezza
2. integrità
3. disponibilità
4. scollegabilità (unlinkability)
5. trasparenza
6. intervenibilità (intervenability)

Ampliamento delle «canoniche» 3 «dimensioni» dell'**Information Security**, **ICT Security** e **Cyber Security.**

Vecchi e nuovi concetti

Alcune tecniche di sicurezza tradizionali (es. conservazione in archivi e il controllo degli accessi) vengono discusse da ENISA in aggiunta a nuovi concetti come quello dei *synthetic data (*“dati sintetici”) i quali introducono nuove sfide e opportunità.

CONSEGUENZA

Le modalità di trattamento devono quindi essere ripensate anche in maniera radicale (così come sono radicali le minacce), con l’integrazione di opportune salvaguardie e con la definizione di nuovi attori e responsabilità.

.

Il punto chiave: compatibilità della *data protection engineering* con i diritti dell'interessato. Le Privacy Policy

Privacy Policy: quali requisiti devono avere?

Un elemento chiave della *data protection* è la possibilità per gli interessati di **poter esercitare i loro diritti (Artt. 12 – 22 GDPR).**

consentire l'accesso alle informazioni sul trattamento in modo semplice e chiaro (**principio di trasparenza**).

Fornire informazioni accurate e semplici non è semplice: la semplificazione può creare incomprensioni.

Ad oggi non esistono standard di riferimento che consentono di valutare la comprensibilità (*comprehensibility*) di una *privacy policy*, la valutazione resta in capo al titolare del trattamento.

Privacy Policy: quali elementi vanno considerati quando viene progettata?

- i dispositivi degli utenti e la dimensione degli schermi;
- l’accessibilità deve essere fornita compatibilmente con le tecnologie assistive utilizzate da persone disabili;
- fornire informazioni in forma testuale non rappresenta sempre una soluzione appropriata (es. un'automobile connessa);
- controlli e test di comprensibilità che dovrebbero coinvolgere i DPO e persone con specifiche conoscenze di usabilità.

Le Icone Privacy

Le Icone Privacy

Una migliore comprensibilità può essere ottenuta anche se le informazioni sono veicolate non solo da un testo che richiede capacità e sforzi di lettura, ma anche da simboli grafici (icone).

Le icone sono un metodo ben noto per supportare, o talvolta sostituire, le informazioni testuali.

Art. 12.7 GDPR: *«Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.»*

Le Icone Privacy

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

"Informative privacy più chiare grazie alle icone? E' possibile". Il Garante lancia un contest facendo appello alla creatività collettiva.

English version

VEDI ANCHE: **"Informative chiare": i vincitori del contest lanciato dal Garante privacy**

"Informative privacy più chiare grazie alle icone? E' possibile"
Il Garante lancia un contest facendo appello alla creatività collettiva

"Informative privacy più chiare grazie a simboli e icone? È possibile". Con questo slogan il Garante per la protezione dei dati personali lancia un contest per studiare soluzioni che - attraverso l'uso di icone, simboli o altre soluzioni grafiche - rendano le informative privacy più semplici, chiare e immediatamente comprensibili. In poche parole, facciano in modo che siano davvero utili e adeguate allo scopo per il quale sono state pensate.

Le informative utilizzate da aziende private, enti pubblici, professionisti, siti web, soprattutto social network, motori di ricerca e piattaforme tech, infatti, sono molto spesso troppo lunghe, complesse e quindi non adeguate a rispondere alla loro funzione essenziale. Che è quella di informare gli utenti sull'uso che verrà fatto dei loro dati personali e, di conseguenza, di metterli nella condizione di esprimere in maniera libera e consapevole l'eventuale consenso al trattamento, che si tratti di marketing, di profilazione commerciale o di comunicazione a terzi di determinate informazioni.

Il Garante chiede dunque a sviluppatori, addetti ai lavori, esperti, avvocati, designer, studenti universitari e a chiunque sia interessato, di inviare un set di simboli o icone capaci di rappresentare la totalità degli elementi che, a norma degli articoli 13 e 14 del Regolamento europeo, devono essere contenuti nell'informativa.

Le proposte dovranno essere inviate entro il **30 maggio 2021** all'indirizzo mail: **icone@gpdp.it**

L'Autorità, a proprio insindacabile giudizio, sceglierà i tre dataset di simboli e icone che riterrà più efficaci e li renderà disponibili sul proprio sito a chiunque voglia utilizzarle, indicando il nome dell'autore.

Il Regolamento del contest è consultabile su www.gpdp.it/informativechiare

Roma, 15 marzo 2021

Le Sticky Policies (politiche «appiccicose»)

Policies che «viaggiano» con i dati

Un vantaggio può essere la combinazione dell'organizzazione tecnica del trattamento dei dati e l’obbligo di trasparenza.

Le *policies* sono "attaccate" ai dati e viaggiano con loro in caso di trasferimento dei dati. I metodi crittografici vengono utilizzati per impedire ai destinatari di ignorare le *policies* allegate.

Ad oggi non esistono soluzioni standardizzate di policies leggibili dalle macchine che controllino anche le operazioni di trattamento dei dati.

Privacy Preference Signals

Cosa servono?

Attraverso questi «segnali di preferenza» gli utenti/interessati possono esprimere le loro preferenze in materia di privacy in modo leggibile dalle macchine.

Es. **standard "Global Privacy Control" (GPC)**. utenti possono inviare un segnale di "non vendita o condivisione" tramite il proprio browser a un sito in cui l'utente chiede che i propri dati non vengano venduti o condivisi con terzi diversi da quelli con cui intende interagire, salvo nei casi consentiti dalla legge. Da metà 2021 è regolato dall'adattato *California Consumer Privacy Act* (CCPA).

Saranno sempre più importanti con adozione di massa dei dispositivi IOT.

Dashboard Privacy («cruscotti»)

Cosa consentono di fare?

- aumentano la trasparenza e anche la possibilità di intervento per gli utenti/interessati.
- 2 tipi: **dashboard lato servizi** e **lato utente** → sviluppati nell'ambito di progetti di ricerca e mirano a migliorare la trasparenza dell'utente nella divulgazione di dati personali a diversi titolare e a supportare l'utente nella gestione delle identità.

Es. Google. Punto di accesso centrale per gli utenti per gestire privacy (*«Perché vedo questa pubblicità?»*).
Trasparenza parziale.

Sistemi di gestione del consenso.

È fondamentale gestirlo correttamente nell'ambito dei servizi internet.

Se il consenso deve essere raccolto per un sistema o un servizio in evoluzione permanente, le modifiche del servizio devono essere documentate e riflesse nelle condizioni di utilizzo.

- In molti casi il consenso deve essere ottenuto prima ancora che esista un profilo utente, e dunque una password o un token di autenticazione. Tuttavia, l'associazione tra il profilo dell'utente (cioè i dati personali) e l'espressione del consenso (cioè il clic sul pulsante di consenso) deve essere in qualche modo documentata e conservata a prova di manomissione.
- utilizzo **firme elettroniche qualificate** rispetto a quelle autografe

I vantaggi di un sistema di gestione del consenso basato ad es. su *token* di autenticazione come le carte d'identità personali e tecnologie come la *blockchain*:

- riduce gli sforzi di gestione del titolare del trattamento e degli incaricati del trattamento. Il compito di raccogliere il consenso viene automatizzato, lasciando le costose e scarse risorse umane esperte libere di concentrarsi su altri compiti (ad es. determinare se è necessario raccogliere un nuovo consenso o meno).

- possibilità di integrare il sistema di gestione del consenso con altri strumenti di gestione (es. CRM). In questo caso, a seconda dell'entità dell'integrazione, esiste un enorme potenziale di minimizzazione degli sforzi, in quanto l'alternativa sarebbe quella di implementare procedure di gestione manuali, che richiedono costose competenze umane.

Misure tecniche e diritto di accesso, cancellazione e rettifica dell’interessato.

Implementazione misure tecniche sul diritto di accesso

Se implementate, cosa consentono di fare?

- Elaborare la richiesta automaticamente sugli archivi di dati all'interno dell'organizzazione raccogliendo tutti i dati personali relativi all'individuo richiedente fornendogli l'insieme completo dei dati raccolti.
- Non richiedono interazioni manuali da parte dell'organizzazione.
- Riducono notevolmente gli sforzi manuali quando si tratta di quantità massive di richieste di diritto di accesso.
- Le richieste ai partner commerciali coinvolti nell'elaborazione dei dati (responsabili, sub-responsabili e così via) possono essere soddisfatte in modo piuttosto semplice dalle infrastrutture di flusso dei dati esistenti create e gestite per il servizio di diritto di accesso.

Profili di criticità e rischi:

- *Autorizzazioni*
- *Deleghe*
- *Rischio violazione dati*
- *Completezza*
- *Correttezza*
- *Volume*

Conclusioni

Obiettivi futuri

- La comunità di ricerca dovrebbe continuare a esplorare l'impiego di tecniche e tecnologie (di sicurezza) che possano sostenere l'attuazione pratica dei principi *data protection*, con il sostegno politico e finanziario delle istituzioni dell'UE.
- Le iniziative volte a sostenere gli ingegneri dovrebbero essere ulteriormente sostenute da professionisti, ricercatori e università.
- Le **autorità politiche e di regolamentazione UE** – nei loro rispettivi campi di competenza - dovrebbero:
  - **diffondere i vantaggi di tali tecnologie e tecniche** fornendo indicazioni sulla loro applicabilità e diffusione.
  - discutere e promuovere le buone prassi in tutta l'UE in relazione alle soluzioni all'avanguardia delle tecnologie e delle tecniche pertinenti anche attraverso pubblicazioni.
  - promuovere l'istituzione di schemi di certificazione pertinenti (art. 42 GDPR) per garantire una corretta progettazione della protezione dei dati.
  - garantire che gli approcci normativi su nuove tecnologie tengano conto di tutte le possibili entità e ruoli dal punto di vista della *data protection* rimanendo tecnologicamente neutrali.