Il futuro della privacy: dalla Privacy by Design ad uno standard

Nicola Fabiano

e-privacy 2014
Spring edition

Firenze, 5 aprile 2014

Privacy: cosa accadde nel mondo ?

Gerusalemme, 27-29 Ottobre 2010:

La 32ma Conferenza internazionale dei Garanti privacy ha adottato una risoluzione sulla Privacy by Design proposta dalla Dr. Ann Cavoukian.

Si tratta di una pietra miliare.

La risoluzione

2. Encourage the adoption of Privacy by Design's Foundational Principles, **such as those set out below** as guidance to establishing privacy as an organization's default mode of operation…

Privacy by Design:

The Foundational Principles

- Proactive not Reactive; Preventative not Remedial
- Privacy as the Default
- Privacy Embedded into Design
- Full Functionality: Positive-Sum, not Zero-Sum
- End-to-End Lifecycle Protection
- Visibility and Transparency
- Respect for User Privacy

Privacy by Design

Trilogia di applicazioni

1) sistemi IT
2) pratiche commerciali corrette
3) progettazione strutturale e infrastrutture di rete.

7 Principi fondazionali

1) **Proattivo non reattivo; prevenire per correggere:** L'approccio alla Privacy by Design (PbD) è caratterizzato da interventi di tipo proattivo piuttosto che reattivo. Esso anticipa e previene gli eventi invasivi della privacy prima che essi accadano.

2) **Privacy come impostazione di default:** La Privacy by Design cerca di realizzare il massimo livello di privacy assicurando che i dati personali sono automaticamente protetti in un qualunque sistema IT o di pratica commerciale.

3) **Privacy incorporata nella progettazione:** La PbD è incorporata nella progettazione e nell'architettura dei sistemi IT e delle pratiche commerciali.

4) **Massima funzionalità – Valore positivo, non valore zero:** La Privacy by Design mira a conciliare tutti gli interessi legittimi e gli obiettivi con modalità di valore positivo "vantaggioso per tutti", non attraverso un approccio datato di valore zero, dove sono inutili i compromessi.

7 Principi fondazionali

5) **Sicurezza fino alla fine - Piena protezione del ciclo vitale:** La Privacy by Design essendo stata incorporata nel sistema prioritariamente rispetto alla acquisizione del primo elemento di informazione, si estende in modo sicuro attraverso l'intero ciclo vitale dei dati - solidi interventi di sicurezza sono essenziali per la privacy, dall'inizio alla fine.

6) **Visibilità e trasparenza - Mantenere la trasparenza:** La Privacy by Design cerca di assicurare che tutti i soggetti interessati, qualunque sia la prassi aziendale o tecnologia utilizzata, è di fatto, operativa secondo promesse ed obiettivi stabiliti, soggetti a verifica indipendente.

7) **Rispetto per la privacy dell'utente – Centralità dell'utente:** La centralità dell'utente.

Cosa accadde in Europa ?

25/1/2012

• Proposal for a **REGULATION** OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

• Proposal for a **DIRECTIVE** OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

La PbD in EU: un nuovo scenario

- La nuova proposta europea di riforma della privacy introduce, rispetto alla Direttiva 95/46/EC, un riferimento a "*data protection by design and by default*" (articolo 23 del Regolamento e articolo 19 della Direttiva).
- La Commissione europea ha preferito descrivere le funzioni del responsabile del trattamento invece di impostare lo status giuridico della "*data protection by design and by default*". E' fondamentale chiarire il significato di tale concetto, concentrandosi sul vero senso di questi termini.

Article 23

Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation, **the controller shall,** both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. **The controller shall** implement mechanisms for ensuring that, **by default**, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, **in particular for data protection by design** requirements applicable across sectors, products and services.

4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87.

Riscontri

- L'espressione Privacy by Design è usata per descrivere un metodo per affrontare le questioni afferenti la privacy in questa nuova era (dalla risoluzione PbD in avanti) in cui l'aspetto più importante è stabilire un approccio corretto. Si sottolinea che nel testo europeo il termine "***data protection***" è usato al posto di "***privacy***".
- E' auspicabile che l'espressione "*by design and by default*" non rappresenti un movimento di tendenza o un sistema fondato sul solo supporto tecnologico e sulla sicurezza, ma costituisca un vero approccio metodologico per gestire il futuro della privacy secondo i documenti ufficiali internazionali, in modo da essere presupposto per uno standard privacy valido worldwide.

Quale futuro per la privacy ?

Uno degli aspetti su cui si dovrebbe investire per raggiungere una concreta garanzia per la privacy, soprattutto in ambito internazionale, è la realizzazione di uno ***standard*** che si sottragga alle logiche degli accordi transfrontalieri, alle prassi e ad altri sistemi non codificati.

Gli strumenti ci sono.

Privacy standard ?

OASIS TC - PMRM (Privacy Management Reference Model)

• OASIS PMRM TC opera per fornire un framework basato su standard che aiuterà gli ingegneri dei processi di business, gli analisti IT, gli architetti e gli sviluppatori ad implementare privacy and security policies nelle loro attività.

• Il PMRM interviene dove le privacy policies lasciano fuori altri aspetti. La maggior parte delle politiche descrivono pratiche informative corrette e principi, ma offrono poca attuazione effettiva.

• Il PMRM in sostanza fornisce una linea guida o un modello per lo sviluppo di soluzioni operative ai problemi di privacy. Esso serve anche come uno strumento analitico per valutare la completezza delle soluzioni proposte e come base per stabilire categorie e raggruppamenti di controlli di gestione della privacy.

Privacy standard ?

ISO ?

Gruppo di Lavoro UNINFO sulla serie di norme ISO/IEC 27000

Quaderno dal titolo "La gestione della sicurezza delle informazioni e della privacy nelle PMI"

Dal quaderno:

"La normativa privacy si occupa, come è noto, di sicurezza delle informazioni, anche se limitatamente a quelle di carattere personale. E' quindi naturale volerla associare allo standard internazionale ISO/IEC 27001, che definisce i requisiti di un Sistema di gestione per la sicurezza delle informazioni (SGSI). Questo standard è applicabile in modo generale ad aziende di qualsiasi dimensione e riguarda la sicurezza di qualunque tipo di dato e informazione.
La realizzazione di un SGSI e la sua integrazione con quanto descritto nel presente Quaderno non assicura la completa conformità al Codice privacy né ai diversi Provvedimenti emanati dal Garante; …"

Privacy ≠ Security

Il rispetto della privacy presuppone un'adeguata sicurezza

La sola sicurezza non presuppone il rispetto della privacy

Privacy standard: possibile con la PbD

Utilizzando il metodo della PbD secondo la risoluzione adottata dalla 32ma Conferenza internazionale dei Garanti e l'approccio della Dr. Ann Cavoukian

è possibile realizzare uno schema universale privacy che potrà essere utilizzato adattandolo all'ordinamento giuridico dei singoli Paesi.

La privacy si regge anche sul metodo.

Grazie per l'attenzione

Nicola Fabiano

n.fabiano@studiolegalefabiano.eu

http://www.studiolegalefabiano.eu

 **studiolegalefabiano**  **nfabiano**  **slfabiano**