Application 2.0

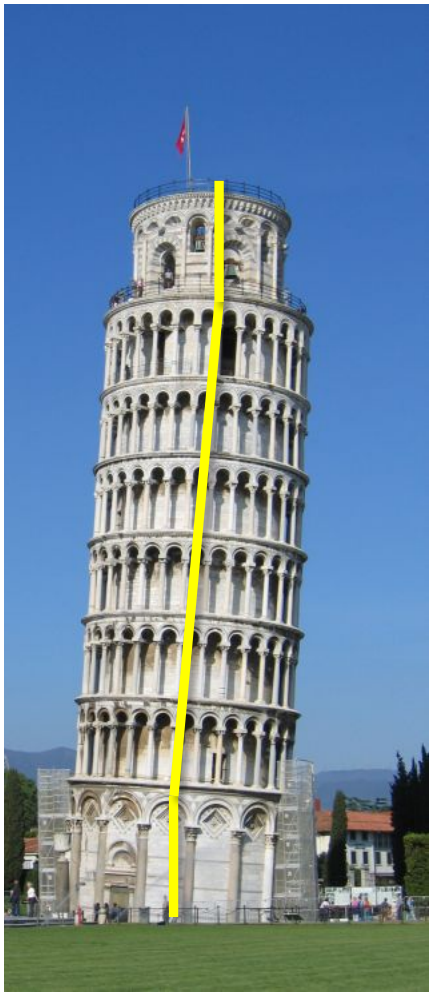
lo sviluppo sicuro delle applicazioni come prevenzione in ambito Cyber Security nell'anno della Privacy by Design

Luca Bechelli

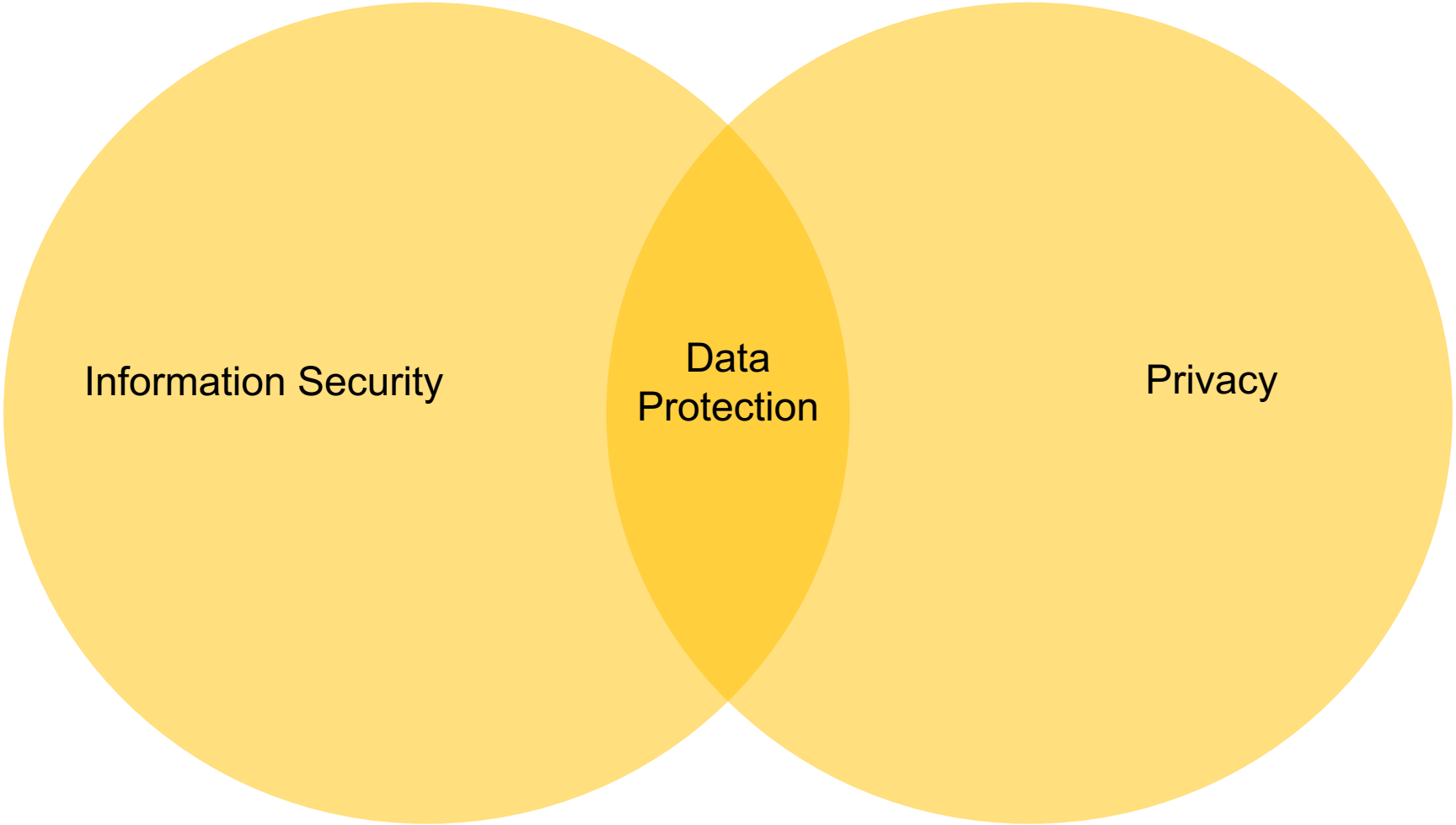
Information & Cyber Security Advisor

Direttivo e Comitato Tecnico - Scientifico CLUSIT

Epic fails… and opportunities



Dall'Information Security alla Data Protection



Privacy by design

Descritta da sette principi, definiti negli anni '90 (in particolare nel 1995):

- Proactive not Reactive: The PbD approach attempts to anticipate and prevent privacy-invasive events before they happen.
- Privacy as the Default Setting: Ensure that personal data is automatically protected in any given IT system or business practice, so that if an individual does nothing, their privacy still remains intact.
- Privacy Embedded into Design: Privacy should be embedded into the design and architecture of IT systems and business practices.
- Full Functionality – Positive-Sum, not Zero-Sum: PbD seeks to accommodate all legitimate interests and objectives in a "win-win" manner, balancing seemly opposing interests, such as security and privacy.
- End-to-End Security – Full Lifecycle Protection: PbD extends throughout the entire lifecycle of the data involved, from start to finish.
- Visibility and Transparency: It seeks to assure all stakeholders that component parts and operations remain visible and transparent, to users and providers alike.
- Respect for User Privacy – Keep it User-Centric: Above all, it puts the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

https://www.ipc.on.ca/privacy/protecting-personal-information/privacy-by-design/

Perché ne parliamo…

- Il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 - *Articolo 24* - Responsabilità del titolare del trattamento:
  - 1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, **nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche,** il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. **Dette misure sono riesaminate e aggiornate qualora necessario.**
  - (…)

Perché ne parliamo…

- "Considerando" 74:
  - (…) In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformita`delle attivita`di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalita`del trattamento, nonche´del rischio per i diritti e le libertà delle persone fisiche.
  - (…)

Quali “fattori” di rischio?

- “Considerando” 75:
  - I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da:

trattamenti (…) suscettibili di cagionare un danno fisico, materiale o immateriale (…):

- se il trattamento puo`comportare **discriminazioni, furto o usurpazione d’identità, perdite finanziarie, pregiudizio alla reputazione,** perdita di **riservatezza** dei dati personali protetti da **segreto professionale,** decifratura non autorizzata della pseudonimizzazione, o **qualsiasi altro danno economico o sociale significativo;**

se gli interessati rischiano di essere **privati dei loro diritti e delle loro libertà** o venga loro **impedito l’esercizio del controllo sui dati personali** che li riguardano;

(…) dati personali che rivelano l’**origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l’appartenenza sindacale,** nonché **dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale** o a **condanne penali e a reati** o alle relative **misure di sicurezza;**

(…) valutazione di aspetti personali, in particolare mediante l’analisi o la previsione di aspetti riguardanti il **rendimento professionale,** la **situazione economica,** la **salute,** le **preferenze o gli interessi personali, l’affidabilità o il comportamento, l’ubicazione o gli spostamenti,** al fine di creare o utilizzare profili personali;

se sono trattati dati personali di **persone fisiche vulnerabili, in particolare minori;**

se il trattamento riguarda una **notevole quantità** di dati personali e un **vasto numero di interessati.**

Altri rischi…

- Art.5 - Principi applicabili al trattamento di dati personali

1. I dati personali sono:

   a) (…), b) (…), c) (…)

   d) **esatti e, se necessario, aggiornati**; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalita` per le quali sono trattati («esattezza»);

   e) (…)

   f) trattati in maniera da garantire **un'adeguata sicurezza dei dati personali**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o **illeciti e dalla perdita, dalla distruzione o dal danno accidentali** («integrita` e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)

Privacy by Design

- Art.25 – Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita:
  - tenendo conto dello stato dell'arte e dei costi di attuazione, nonche´della natura, dell'ambito di applicazione, del contesto e delle finalita`del trattamento, come anche dei **rischi aventi probabilita`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.

Capo III - Diritti dell'interessato

- Sezione 1 - Trasparenza e modalità
  - Articolo 12 - Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato
- Sezione 2 - Informazione e accesso ai dati personali
  - Articolo 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato
  - Articolo 14 - Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato
  - Articolo 15 - Diritto di accesso dell'interessato
- Sezione 3 - Rettifica e cancellazione
  - Articolo 16 - Diritto di rettifica
  - Articolo 17 - Diritto alla cancellazione («diritto all'oblio»)
  - Articolo 18 - Diritto di limitazione di trattamento
  - Articolo 19 - Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento
  - Articolo 20 - Diritto alla portabilità dei dati
- Sezione 4 - Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche
  - Articolo 21 - Diritto di opposizione
  - Articolo 22 - Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione
- Sezione 5 – Limitazioni
  - Articolo 23 - Limitazioni

Dai diritti agli obiettivi

- **correttezza e trasparenza**: i dati saranno trattati in modo corretto e trasparente nei confronti dell'interessato, in particolare prevedendo informative adeguate prima di intraprendere qualsiasi trattamento e successive comunicazioni riguardo ad eventuali modifiche rispetto a quanto inizialmente indicato;

- **limitazione della finalità**: i dati saranno raccolti esclusivamente per finalità determinate, esplicite e legittime e successivamente trattati in modi che non siano incompatibili con tali finalità;

- **liceità**: i dati saranno raccolti e trattati, ad eccezione dei casi tassativi esplicitamente previsti dal Regolamento, solo in presenza di una o più delle condizioni di liceità da quest'ultimo identificate;

- **esattezza**: i dati devono essere mantenuti esatti e, se necessario, aggiornati. Pertanto, dovranno sussistere tutte le misure necessarie a cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

- **minimizzazione dei dati**: i dati devono essere adeguati, pertinenti e limitati a quanto strettamente necessario alla realizzazione delle finalità per cui saranno raccolti;

- **limitazione della conservazione**: i dati saranno conservati in una forma che consentirà l'identificazione degli interessati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono stati raccolti e trattati;

- **responsabilizzazione**: l'azienda dovrà essere in grado di comprovare l'adozione di misure e processi idonei a garantire il rispetto dei principi descritti ai punti che precedono, delle norme del GDPR (accountability) e delle misure individuate sulla base dell'analisi dei rischi.

Concretamente?

- Il principio è di non pensare a proteggere i dati, ma di progettare in modo da non avere bisogno di proteggerli
  - Da qui deriva il concetto più utilizzato, che è quello della minimizzazione
  - Anche la pseudonimizzazione segue la stessa logica: la domanda non è quando sia necessaria, ma quando sia invece necessario avere l'identificazione

- Dove possibile, si usano dati anonimi
  - Che non vuole dire non avere accesso ai dati identificativi, vuole proprio dire dati anonimi

Ciclo di vita del trattamento e analisi del rischio

Trattamenti ad alto Rischio

Art.35 (DPIA):

- Un insieme di azioni, tra cui l'Analisi del rischio:
  - Valutazione impatti e probabilità
  - Identificazione misure
- eventuale "consultazione preventiva"

Art.35 (DPIA), comma 11:

- *"**Se necessario**, il titolare del trattamento procede a un **riesame** per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento"*
- Il WP29 suggerisce una frequenza al più triennale

In tutti i casi

Art.25 (privacy by design / default):

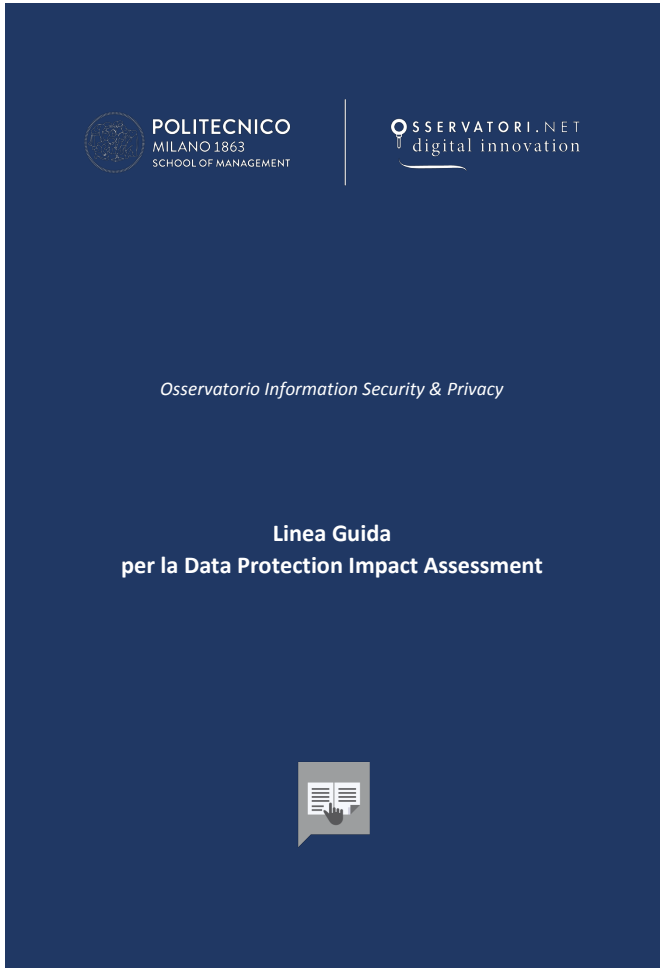
- Analisi del rischio:
  - Valutazione impatti e probabilità
  - Identificazione misure
- Implementazione

Art.32 (sicurezza del trattamento):

- Aggiornamento **periodico** dell'Analisi del rischio per determinare la necessità di adeguare le misure al variare delle minacce e degli impatti per l'interessato

Linea guida DPIA

- Liberamente scaricabile dal sito:
- https://www.osservatori.net/it_it/pubblicazioni/linea-guida-per-la-data-protection-impact-assessment



GRAZIE

Domande?

Luca Bechelli
Direttivo e Comitato Tecnico Scientifico Clusit
luca@bechelli.net
www.bechelli.net
https://twitter.com/luca_bechelli
https://www.facebook.com/bechelli.luca
http://www.linkedin.com/in/lucabechelli