Mobile Protection 2.0

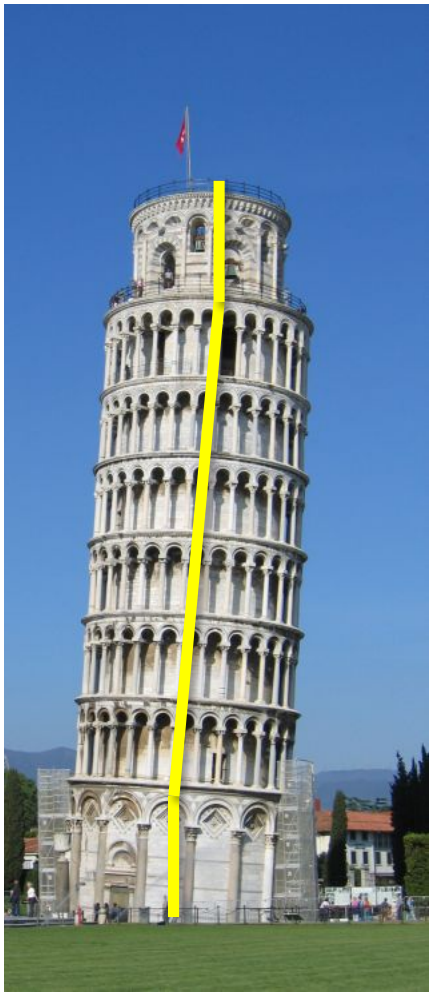
smart working, mobilità e Industry 4.0, la nuova frontiera lavorativa. Facciamolo in sicurezza!!

Luca Bechelli

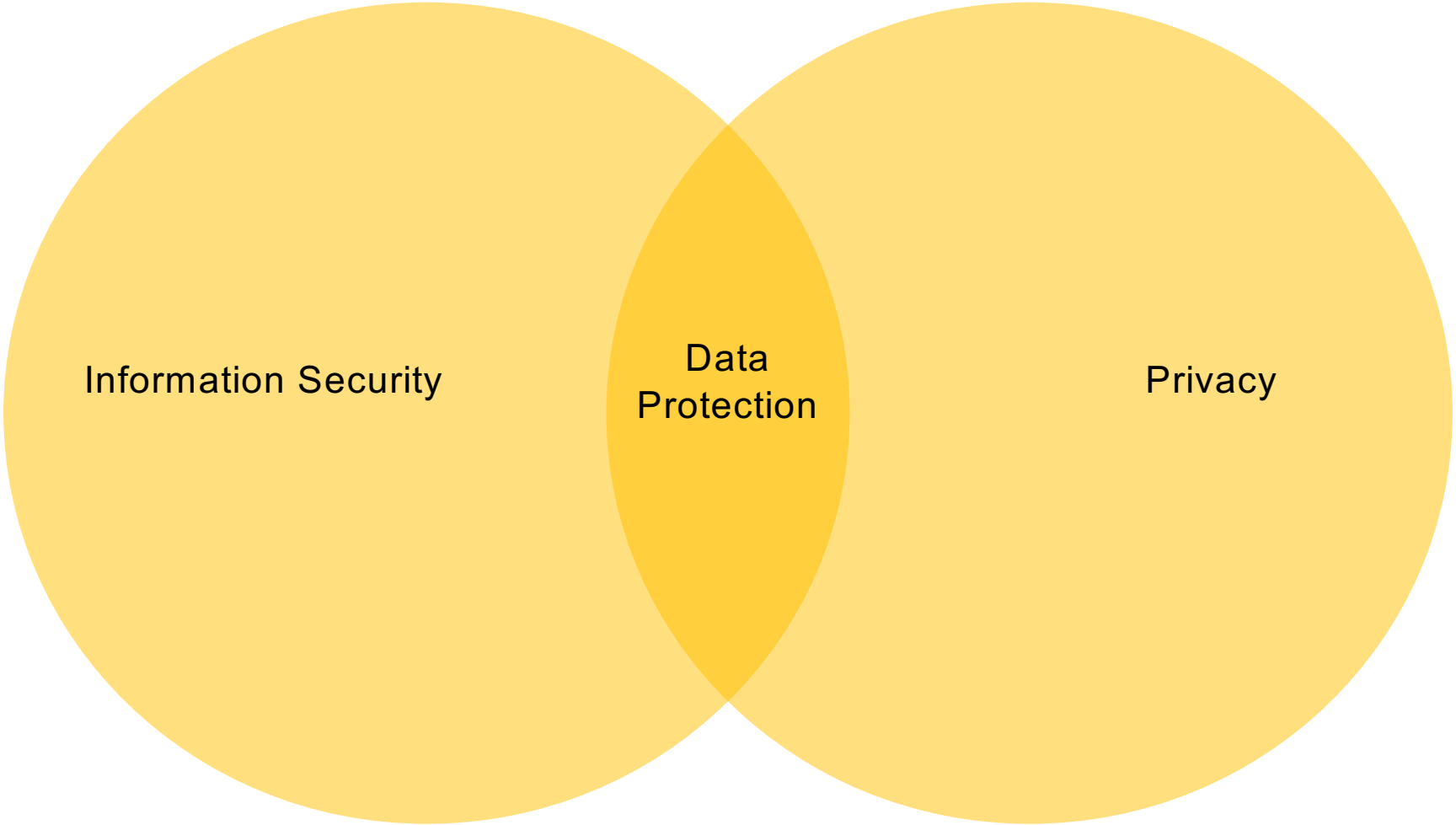
Information & Cyber Security Advisor

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/

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;

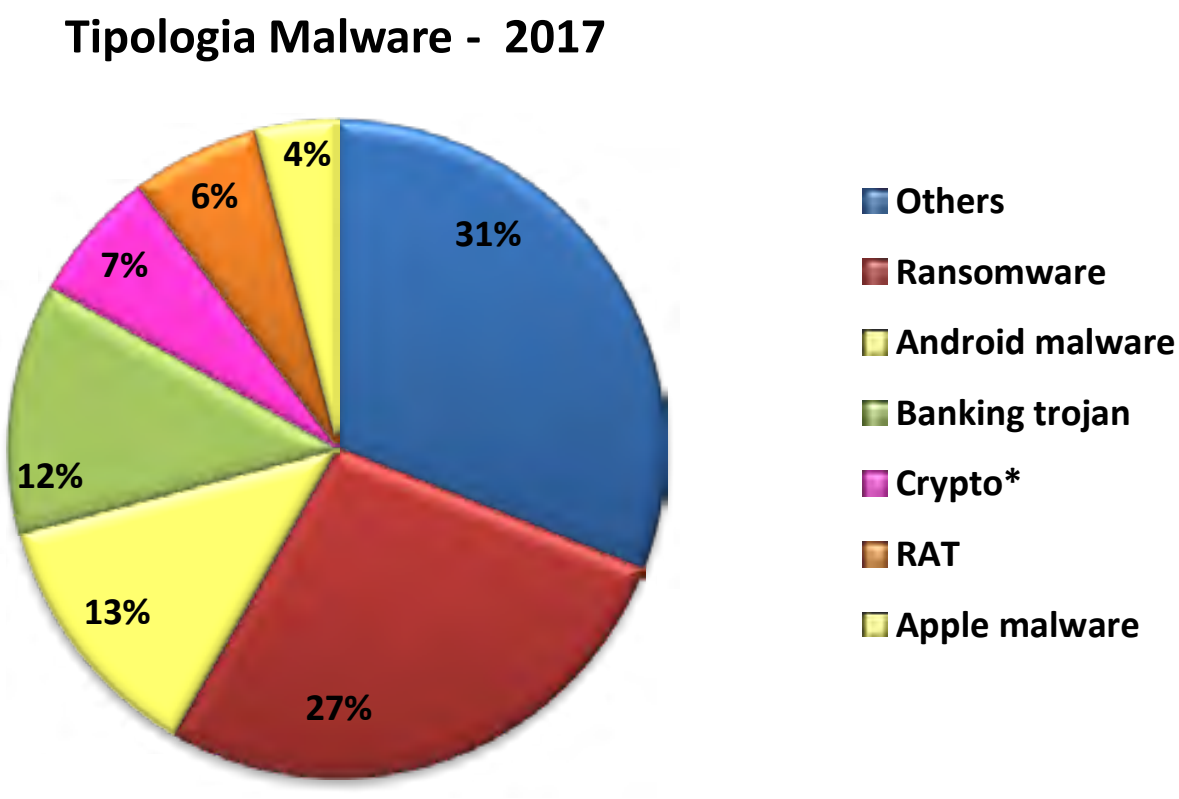
- **responsabilizzazione**: l'azienda dovrà essere in grado di comprovare l'adozione di misure e processi idonei a garantire il rispetto dei principi descritti ai punti che precedono, delle norme del GDPR (accountability) e delle misure individuate sulla base dell'analisi dei rischi.

Perché ne parliamo…

- Le minacce*:
  - **Variety of data & multiple sensors**
  - **Personal device, always ‘on’**
  - **Different types of identifiers**
  - **Mobile and connected**
  - **Possibility of tracking**
  - **Limited physical security**
  - **Limited user interfaces**
  - **Limitations of app developers**
  - **Use of third-party software**
  - **App market**
  - **Cloud storage**
  - **Online Social Networks**

* Fonte: Privacy and data protection in mobile applications - Enisa

20% del totale…



© Clusit - Rapporto 2018 sulla Sicurezza ICT in Italia

Privacy Risk Management

…mobile apps may hide risks (and accountability obligations), dependingon the overall context of the processing of personal data…(*)

GDPR PRINCIPLES	INDICATIVE PRIVACY RISKS	INDICATIVE REQUIREMENTS
Lawfulness, fairness and transparency Art.5(1)(a)	Unlawful, excessive and incorrect processing (e.g. due to permissions to unauthorised parties to access personal data through the app).	App providers/developers should make sure that they have a legal basis for the processing of personal data. App providers/developers should inform the data subjects properly about their data processing activities. This may help the users to understand what personal data is collected by them and why. App providers/developers should be aware of data subject rights such as rights to access, rectification, erasure, data portability. They should implement appropriate processes to support these rights.
Purpose limitation Art.5(1)(b)	Excessive collection and sharing of data (e.g. due to multiple sensors of mobile devices that are activated without need).	App providers/developers should use the data for a specific purpose that the data subjects have been made aware of and no other, without further consent. If the personal data is used for purposes other than the initial, they should be anonymised or the data subjects must be notified and their consent must be re-obtained.
Data minimisation Art.5(1)(c)	Excessive processing (e.g. due to use of third party libraries).	The minimum amount of data for specific processing should be processed by app providers/developers. For instance, they should not store the exact location point when a generic location area is sufficient for their app functionalities.
Accuracy Art.5(1)(d)	Outdated data pose identity theft risks.	Rectification processes into data management should be embedded in the app design.
Storage limitation Art.5(1)(e)	Undue data disclosure (e.g. due to cloud storage services used by mobile app developers).	Personal data must not be stored longer than necessary. App providers/developers should provide the "right to be forgotten" to the data subjects. This data must be kept only for a certain period of time for non-active users.
Integrity and confidentiality Art.5(1)(f)	Unlawful data processing, data loss, data breach, data destruction or damage .	App providers/developers should ensure that the security requirements of the personal data and the processing systems are met. This encompasses integrity and confidentiality as well as availability and resilience (Art. 35(1)(b) GDPR). For instance, the appropriate control access mechanisms should be embedded into the apps infrastructure in order to detect or monitor unauthorized access to the data.

* Fonte: Privacy and data protection in mobile applications - Enisa

Data Protection Goals… by design

Confidentiality, Integrity & Availability…
&
Unlinkability, Transparency, and Intervenability

- Unlinkability:
  - privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context,
  - privacy-relevant data are unlinkable to any other set of privacy-relevant data outside of the domain
  - is related to the principles of necessity and data minimisation as well as purpose binding

Si realizza mediante: data minimisation, separation of contexts (physical separation, encryption, usage of differentidentifiers, access control), anonymisation (aggregation or adding noise for ensuring that the data cannot be linked to a person and that persons cannot be singled out), pseudonymisation, erasure of data.

Data Protection Goals… by design

Confidentiality, Integrity & Availability…
&
Unlinkability, Transparency, and Intervenability

- Transparency:
  - all privacy-relevant data processing including the legal, technical and organisational setting can be understood and reconstructed at any time
  - the actual, the planned and the time after the processing, to know what exactly happened
  - it is a prerequisite for **accountability**

Si realizza mediante: logging, reporting, understandable documentation covering technology, organisation, responsibilities, source code, privacy policies, notifications, information of and communication with the persons whose data are being processed

Data Protection Goals… by design

Confidentiality, Integrity & Availability…
&
Unlinkability, Transparency, and Intervenability

- Intervenability:
  - intervention is possible … by those persons whose data are processed
  - individuals' rights: the rights to rectificationand erasure of data, the right to withdraw consent or the right to lodge a claim or to raise a dispute to achieve remedy
  - control the data processor and the used IT systems to influence or stop the data processingat any time

Si realizza mediante: processes for influencing or stopping the data processing, manually overturning an automated decision, data portability to prevent lock-in at a data processor, single points of contact, switches for users to change a setting (e.g. changing to a non-personalised, empty-profile configuration), deactivating an auto pilot or a monitoring system for some time.

By design… e oltre!

- Ciò che è considerato «by design» è assimilabile alla misura minima
- E' necessario accompagnare alle misure di sicurezza ormai note, di mercato, un approccio specifico di valutazione e gestione dei rischi legati alla privacy
- La buona notizia: non dobbiamo «inventarci» quasi niente di nuovo! E' fondamentalmente l'approccio alla sicurezza che deve essere esteso, sia dentro che fuori il mondo IT

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