# Aggiornamento della ISO/IEC 29100 “Privacy framework”

**Author :** Cesare Gallotti

**Date :** 10 ottobre 2018


A giugno 2018 è stata pubblicata una correzione (“Amendement 1: Clarifications”) della ISO/IEC 29100 dal titolo “Privacy framework”, lo standard internazionale che si propone come base per le ulteriori attività di normazione in materia di privacy.

La ISO/IEC 29100 fu pubblicata a dicembre 2011 e fino ad oggi è stata usata come base, ad esempio, per la ISO/IEC 29151 “Code of practice for personally identifiable information protection” e la ISO/IEC 27018 “Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”.

Nel prossimo paragrafo è descritta la struttura della ISO/IEC 29100 e in quello successivo si sintetizzano le correzioni apportate.

## La struttura della ISO/IEC 29100

La ISO/IEC 29100 è uno standard molto breve, di 28 pagine.

Dopo la prefazione, l’introduzione e l’ambito di applicazione, il capitolo 2 riporta le definizioni, da adottare negli altri standard basati su questa stessa norma.

Il lettore italiano potrebbe trovare inutili queste definizioni, visto che la normativa europea (in particolare il GDPR) già le fornisce. Bisogna però ricordare che gli standard ISO e ISO/IEC hanno valore anche al di fuori dell’Europa e pertanto alcuni termini e alcune loro definizioni non sono uguali a quelli della normativa, anche se le corrispondenze sono facili da rilevare.

Due esempi eclatanti: la ISO/IEC 29100 non usa il termine “personal data”, ma “personally identifiable information (PII)”; non usa, per gli interessati, il termine “data subject”, ma “PII principal”.

Dopo il brevissimo capitolo dedicato alle abbreviazioni, il capitolo 4 presenta lo “schema di riferimento sulla privacy” vero e proprio. Prima descrive gli attori (principals, controllers,

processors e third parties), poi le loro interazioni e prosegue fornendo indicazioni sulle caratteristiche dei dati personali e sui principi per la loro protezione.

L'ultimo capitolo, il 5, presenta i "privacy principles", divisi in 11 sezioni:

- consenso e scelta;
- legittimità e specifica delle finalità;
- limitazione della raccolta;
- minimizzazione dei dati;
- uso, conservazione e limiti alla comunicazione;
- accuratezza e qualità;
- apertura, trasparenza e informativa;
- partecipazione e accessi da parte degli individui;
- responsabilità;
- sicurezza;
- conformità.

Altre norme internazionali (come le già citate ISO/IEC 29151 e ISO/IEC 27018 e la futura ISO/IEC 27552) usano gli 11 principi per raggruppare i controlli privacy.

Dal 2011 ad oggi i principi sono ancora validi, ma oggi, dopo la pubblicazione nel 2016 del GDPR, se ne vedono alcune carenze. Per esempio: non si parla di privacy-by-default (ma si parla già di privacy-by-design) e si dà maggiore importanza al consenso (presentato come parte del primo principio) rispetto alla legittimità (presentata come parte del secondo principio). Inoltre, l'uso dello standard in situazioni pratiche evidenzia alcune ridondanze.

## Le correzioni del 2018

Le correzioni del 2018 sono molto poche e infatti sono raccolte in 4 pagine.

Alcune correzioni sono di tipo terminologico (per esempio si preferisce usare "questo documento" al posto di "questo standard internazionale"; è stata eliminata la definizione di "identificare"; è stata corretta la circolarità delle definizioni di PII e PII principal). Interessante il fatto che la ISO/IEC 29100 vede come sinonimi "privacy impact assessment" e "privacy risk assessment".

Ulteriori correzioni sono state apportate per allineare il restante del testo alle definizioni aggiornate o per togliere potenziali ambiguità nelle traduzioni in alcune lingue.

Le correzioni sono quindi di bassissimo impatto.

## Ulteriori considerazioni

La ISO/IEC 29100 potrebbe essere aggiornata in modo più ampio, ma questo avrebbe eccessivi impatti su altre norme che si basano su di essa. La scelta di correggere il testo è

quindi condivisibile.

Discutibile invece è il fatto che la ISO/IEC 29100:2011 è disponibile gratuitamente (http://standards.iso.org/ittf/PubliclyAvailableStandards/), mentre la correzione è a pagamento, anche se modesto (https://www.iso.org/standard/73722.html).

A cura di: **Cesare Gallotti**