10 LINEE GUIDA PER L'IMPLEMENTAZIONE DELLA PRIVACY BY DESIGN NEL SDLC

10.1 Introduzione e concetti base

10.1.1 Principi della Privacy

All'interno dalla ISO/IEC 29100:2011 sono descritti undici principi che indirizzano la progettazione, lo sviluppo e l'implementazione dei requisiti di protezione della privacy (10.1.4). Questi principi, sono anche un riferimento per quel che concerne il monitoraggio e la misurazione delle prestazioni del software e per gli aspetti del controllo dei programmi di gestione della privacy in un'organizzazione (vedere anche paragrafo 5.8.1 dell'*Allegato 4 - Linee Guida per la modellazione delle minacce e individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design).*

Principi	**Descrizione**
Consenso e scelta	Secondo questo principio, l'interessato deve poter scegliere se acconsentire o meno al trattamento dei propri dati personali (Consenso Informato). Aderire a questo principio significa fornire all'interessato - in maniera chiara, facilmente comprensibile, accessibile e conveniente - i meccanismi per esercitare la scelta e fornire il consenso in relazione al trattamento dei suoi dati personali al momento della raccolta, al primo utilizzo o non appena possibile.
Scopo legittimo e specifico	Il principio di legittimità e specificità dello scopo assicura che quest'ultimo sia conforme alla legge applicabile e si basi su una base giuridica ammissibile.
Limitazione della raccolta	Limita la raccolta dei dati personali a ciò che è strettamente necessario per gli scopi specificati.
Minimizzazione dei dati	Prevede la progettazione, l'implementazione e l'elaborazione dei dati, attraverso procedure o sistemi ICT, in modo da ridurre al minimo i dati personali che vengono elaborati e il numero di parti interessate dalla privacy.
Limitazione dell'utilizzo, conservazione e divulgazione	Limita l'utilizzo, la conservazione e la divulgazione (incluso il trasferimento) dei dati personali a scopi specifici, espliciti e legittimi del trattamento.
Precisione e qualità	Assicura che i dati personali elaborati siano accurati, completi, aggiornati (a meno che non vi sia una base legittima per mantenere dati obsoleti), e adeguati e pertinenti ai fini del trattamento.
Apertura, trasparenza e preavviso	Tale principio prevede di fornite informazioni chiare e facilmente accessibili sulle politiche stabilite dal titolare del trattamento e sulle procedure relative al trattamento dei dati personali.
Partecipazione individuale e accesso	Stabilisce che agli interessati sia data la possibilità di accedere e di rivedere i propri dati personali, a condizione che la loro identità sia