	funzionalità principali. La privacy è parte integrante del sistema, senza diminuirne la funzionalità.
Funzionalità completa; somma positiva, non somma zero	La *Privacy by Design* cerca di tutelare tutti i legittimi interessi e gli obiettivi in un'ottica *win-win*, senza prevedere delle soluzioni a somma zero che includano degli inutili trade-off. *Privacy by Design* evita la pretesa di false dicotomie, come la sicurezza a discapito della privacy, in quanto dimostra che è possibile averle entrambe.
Sicurezza end-to-end - Protezione completa del ciclo di vita	La *Privacy by Design* che è stata incorporata in un sistema sin dal primo momento, si estende in modo sicuro durante l'intero ciclo di vita dei dati coinvolti: prevedendo robuste misure di sicurezza - essenziali per la privacy - dall'inizio alla fine di un ciclo di vita. Ciò garantisce che tutti i dati vengano conservati e distrutti – in modo sicuro e tempestivamente - alla fine del processo. Pertanto, la *Privacy by Design* garantisce una gestione delle informazioni sicura end-to-end.
Visibilità e trasparenza - Keep it Open	La *Privacy by Design* cerca di assicurare a tutti gli stakeholder che qualunque sia la pratica aziendale o la tecnologia coinvolta, essa opererà secondo le promesse e gli obiettivi dichiarati, anche assoggettandosi a verifiche indipendenti. Le sue componenti e le sue operazioni rimangono visibili e trasparenti, sia per gli utenti che per i fornitori.
Rispetto per la privacy degli utenti - Mantenerlo incentrato sull'utente	La *Privacy by Design* richiede ai progettisti e agli operatori di garantire gli interessi dei singoli, offrendo robuste misure di privacy per impostazione predefinita. Prevedendo degli avvisi appropriati e potenziando le opzioni user-friendly, pertanto garantendo l'impostazione user-centric.

Tabella 6 - I sette principi della Privacy by Design

Vedere anche il paragrafo 5.8.1.2 dell'*Allegato 4 - Linee Guida per la modellazione delle minacce e individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design.*

10.1.4 Data protection Impact Assessment

La progettazione di qualsiasi software che coinvolga il trattamento dei dati personali deve essere preceduta da un'identificazione dei requisiti di protezione per la privacy, in quanto dal trattamento o dall'elaborazione dei dati personali potrebbero derivare dei rischi. I rischi per la privacy negli applicativi software che comportano il trattamento dei dati personali, dovrebbero essere trattati prima della loro implementazione, ossia sin dalla fase di progettazione (*Engineering Privacy by Design*). Dovranno, quindi, essere analizzati i rischi collegati alle applicazioni software.

In linea con i requisiti di attuazione previsti dal Regolamento (UE) 679 del 2016 (cfr. DR-1), di seguito indicato come **GDPR**, qualora un trattamento dei dati personali possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, i titolari di quest'ultimo dovranno effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali o *Data Protection Impact Assessment*, di seguito indicata come "DPIA" (cfr. Art. 35 DR-1), quest'obbligo è applicabile anche al ciclo di vita del software.