La privacy by Design può essere raggiunta applicando i sette principi su cui si basa:

- **Proattivo non reattivo, preventivo non correttivo**: le minacce alla privacy dovrebbero essere anticipate e prevenute, piuttosto che corrette dopo che queste si sono verificate.
- **Privacy come impostazione predefinita ("by default")**: la privacy dovrebbe essere lo standard. I dati personali dovrebbero essere protetti automaticamente, anche senza alcuna azione esplicita da parte dell'individuo interessato.
- **Privacy incorporata nella progettazione ("by design")**: la privacy non dovrebbe essere considerata un elemento aggiuntivo, ma dovrebbe essere integrata nella progettazione e nell'architettura dei sistemi software e delle attività di business in generale.
- **Piena funzionalità - somma positiva, non somma zero**: la privacy dovrebbe coesistere con altri interessi di business. Dovrebbero tuttavia essere evitati compromessi non necessari (ad esempio privacy anziché sicurezza o privacy piuttosto che performance). Si dovrebbe sempre cercare di ottenere una somma positiva.
- **Sicurezza end-to-end - Tutela dell'intero ciclo di vita**: la privacy richiede sicurezza durante l'intero ciclo di vita dei dati personali, garantendo una gestione sicura e completa di tutti i dati.
- **Visibilità e trasparenza**: gli obiettivi di privacy dichiarati dall'organizzazione e conseguentemente adottati dai sistemi informatizzati, devono essere visibili e trasparenti agli utenti.
- **Rispetto per la privacy degli utenti**: devono essere applicate misure adeguate per responsabilizzare l'utente nel processo di trattamento dei propri dati.

Il panorama tecnologico della privacy è stato classificato da Gürses [14] secondo tre paradigmi che tuttavia, non si escludono a vicenda:

- **Privacy come controllo**. In quanto controllo, mira a fornire agli interessati un mezzo per controllare la divulgazione dei propri dati. Rientrano in questa categoria anche gli strumenti adottati dall'organizzazione per definire e applicare politiche di sicurezza dei dati e prevenire l'abuso di accessi non autorizzati. Esempi di tecnologie correlate, includono: le impostazioni relative alla privacy, il controllo dell'accesso e la verifica dei dati.
- **Privacy come riservatezza**. Questo paradigma impedisce la divulgazione delle informazioni o perlomeno ne minimizza il più possibile la divulgazione al fine di evitare di collegarle all'interessato. Le tecnologie di esempio sono: i protocolli di autenticazione anonimi e le reti di comunicazione anonime.
- **Privacy come pratica**. Si concentra maggiormente sull'aspetto sociale della privacy e mira a rendere più trasparenti i flussi di informazioni attraverso strumenti di sensibilizzazione e feedback.

5.8.1.3 Riferimenti normativi

Il 27 aprile 2016 il Parlamento Europeo ha approvato il Regolamento generale sulla protezione dei dati personali afferenti a persona fisica (General Data Protection Regulation[38]) che abroga la direttiva 95/46/CE, al fine di armonizzare le legislazioni dei singoli paesi, consolidare il diritto alla privacy dei cittadini dell'UE e garantire un'adeguata sicurezza dei dati particolari trattati dalle organizzazioni.
Il regolamento si applica a tutti gli enti pubblici e le imprese che trattano dati personali e dati personali classificati (sensibili, biometrici, sanitari e giudiziari, etc.) e/o che raccolgono grandi quantità di dati personali.
Tra gli elementi di maggiore innovazione ed interesse troviamo:

- La responsabilizzazione del Titolare nell'adozione di comportamenti proattivi tali da dimostrare l'attuazione di misure concrete individuate attraverso una valutazione dell'impatto dei trattamenti previsti (Data Protection Impact Analysis – DPIA);

[38] https://gdpr-info.eu/