- La nomina del Responsabile della protezione dei dati (Data Protection Officer – DPO o Responsabile della Protezione dei Dati – RPD) con il compito di vigilare, sui processi interni alla struttura, l'osservanza del Regolamento, fornire pareri in merito alla DPIA, indicare le misure tecniche e organizzative per attenuare i rischi per i diritti e gli interessi delle persone interessate, servire da punto di contatto con l'autorità di controllo;
- La comunicazione all'Autorità Garante di eventuali violazioni della sicurezza dei dati personali (Data Breach);
- Il principio di "privacy by design" che prevede l'integrazione delle attività volte alla protezione dei dati personali in tutte le fasi del ciclo di vita dei sistemi e delle applicazioni IT, dalla fase di progettazione, messa in esercizio, utilizzo e dismissione finale;
- Il principio di "privacy by default" che prevede il rispetto dei principi generali della protezione delle informazioni, quali la minimizzazione dei dati e la limitazione delle finalità, nelle impostazioni dei servizi e dei prodotti che trattato dati personali.

La protezione della privacy richiesta dal GDPR presuppone quindi programmi di conformità sostenuti da tutta l'organizzazione, in modo da integrare i requisiti di sicurezza dei dati in tutte le fasi di ogni processo aziendale, dalla progettazione al rilascio.
L'Articolo 25 del GDPR[39] – **Data protection "by default" "by design"** – chiede al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate:

- volte ad attuare in modo efficace i principi di protezione dei dati, quali la pseudo-anonimizzazione e la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati (by design);
- per garantire che siano trattati, by default, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, di base (by default), non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza previo intervento dell'interessato.

Nel ciclo di vita del software sicuro, deve essere posta quindi maggiore attenzione quando si sviluppano applicativi che dovranno trattare dati personali, inserendo controlli mirati per ciascuna fase, secondo le best practices di sicurezza e secondo le indicazioni fornite dall'analisi dei rischi privacy (DPIA). Tali controlli devono essere formalmente verificati in fase di test e collaudo.
Altri elementi da considerare durante le fasi del ciclo di sviluppo del software, si evincono dall'Articolo 32 del GDPR[40] – **Sicurezza del trattamento** – nel quale viene chiesto al titolare e al responsabile del trattamento di mettere in atto le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre cose:

- la pseudo-anonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative messe in campo al fine di garantire la sicurezza del trattamento.

5.8.2 Requisiti di sicurezza applicativi nel GDPR

Per ciò che riguarda i requisiti di AppSec nel GDPR, gli articoli 25, 32, 33, 34 e 35 contengono la maggior parte delle indicazioni di dettaglio, da seguire affinché le organizzazioni sappiano come

[39] https://gdpr-info.eu/art-25-gdpr/

[40] https://gdpr-info.eu/art-32-gdpr/