proteggere i dati trattati da parte delle applicazioni in uso, così come cosa è necessario fare in caso di violazione dei dati personali. I requisiti generali riguardano i concetti di prevenzione, valutazione e monitoraggio. Di seguito i primi cinque punti chiave relativi alle sezioni del GDPR che indirizzano la sicurezza dei dati:

- Al fine di individuare eventuali punti di debolezza nel modo in cui i dati vengono elaborati o gestiti, il GDPR richiede che le organizzazioni valutino i propri sistemi e processi in merito alla capacità di gestire i dati ed eseguire l'analisi delle difettosità al fine di determinare cosa funziona e cosa deve essere cambiato o rimosso.
- Per garantire che i dati siano sempre protetti, da parte dell'applicazione o del sistema, è necessario che vengano considerati gli aspetti di Privacy/Security sin dalla fase di progettazione e per impostazione predefinita. Tale concetto descrive l'idea che la sicurezza e la privacy devono essere entrambe prese in considerazione a partire dalle prime fasi di pianificazione, piuttosto che durante la fase realizzativa.
- Come già precedentemente indicato nel precedente paragrafo, le organizzazioni devono "garantire un livello di sicurezza adeguato al rischio", attraverso le seguenti specifiche:
    - Crittografia e pseudonimizzazione dei dati personali;
    - Capacità nel ripristinare tempestivamente la disponibilità dei dati personali in caso di incidente di sicurezza o problemi tecnici;
    - Garantire la riservatezza, l'integrità e la disponibilità dei sistemi e dei servizi per il trattamento dei dati (il principio di InfoSec).
    - Istituire un processo per effettuare regolarmente test di sicurezza e valutare l'efficacia delle pratiche e delle soluzioni di sicurezza in atto.
- Le organizzazioni devono applicare ove possibile il principio del privilegio minimo, così come attuare specifiche politiche di bonifica periodica e rimozione dei dati che non sono più necessari.
- Infine, si raccomanda alle organizzazioni, soprattutto quelle più grandi, di creare un repository centralizzato di applicazioni e dati per mantenere un miglior controllo sui dati dei propri clienti.

5.8.3 Certificazioni

In accordo con l'articolo 42 del GDPR[41], "Gli Stati membri, le autorità di controllo, il consiglio di amministrazione e la Commissione incoraggiano, in particolare a livello UE, l'istituzione di meccanismi di certificazione della protezione dei dati e di sigilli e marchi di certificazione per la protezione di quest'ultimi, al fine di dimostrare il rispetto del regolamento europeo da parte dei responsabili e degli incaricati al trattamento".
Il regolamento recita come segue: "Al fine di migliorare la trasparenza e il rispetto del presente regolamento, è opportuno incoraggiare l'istituzione di meccanismi di certificazione e di sigilli e marchi di protezione dei dati, consentendo agli interessati di valutare rapidamente il livello di protezione dei propri dati, prodotti e servizi". In tal senso, conformemente al documento di programmazione 2017[42], l'ENISA ha avviato un progetto nell'ambito dei meccanismi di certificazione per la protezione dei dati, sigilli o marchi con l'obiettivo di imprimere il panorama attuale e fornire un orientamento per ulteriori lavori sulla tematica in questione.
Questo progetto è stato realizzato parallelamente alle attività svolte dall'Agenzia nel settore della certificazione riguardo la sicurezza informatica per poter poi trarre conclusioni, esperienze e best practices utili da entrambi i settori.

41 Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), L 119/1 4.5.2016

42 ENISA (2016) Documento di programmazione ENISA 2017-2019: disponibile all'indirizzo web https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019/view

Il regolamento generale sulla protezione dei dati introduce disposizioni sulla certificazione per migliorare la trasparenza delle operazioni di trattamento da parte dei responsabili e degli incaricati a quest'ultimo. Il legislatore ha inoltre previsto un ruolo di certificazione nell'assistenza ai controllori e agli incaricati del trattamento per dimostrare la conformità al regolamento.
Di seguito si descrivo i principali aspetti della pratica di certificazione esistente, applicabile al regime di certificazione della protezione dei dati istituito nell'ambito del GDPR.
La certificazione è un'attività di valutazione della conformità. Questa comporta "la presentazione di una valutazione e di un'attestazione imparziale da parte di terzi che certifichi che è stato dimostrato il rispetto dei requisiti specificati". I requisiti sono generalmente derivati da norme tecniche o legislative. Quest'ultimo è il caso della certificazione nel settore della protezione dei dati, in cui la legislazione secondaria dell'UE che tutela il diritto alla protezione dei dati personali fornisce il quadro normativo come base per i requisiti di valutazione. È anche possibile che i requisiti siano incorporati in una direttiva tecnica ispirata alle disposizioni del GDPR. Le disposizioni del GDPR devono essere ulteriormente elaborate per essere idonee alla certificazione.
Poiché la norma ISO/IEC 17067:2013 prevede che "laddove sia necessario elaborare i requisiti per eliminare l'ambiguità, le motivazioni dovrebbero essere formulate da persone competenti e messe a disposizione di tutte le parti interessate".
Secondo la terminologia proposta da ISO e IEC, un requisito di certificazione è un requisito "che il cliente deve soddisfare come condizione per stabilire o mantenere la certificazione". Il termine comprende sia i requisiti sostanziali (chiamati anche requisiti "prodotto/processi/persona") sia i requisiti procedurali. I requisiti sostanziali derivano dalla base normativa. I diritti delle persone interessate (art. 15-22 GDPR), la sicurezza dei dati (art. 32 GDPR), la protezione dei dati fin dalla progettazione (art. 25 (1) GDPR) e la protezione dei dati per default (art. 25(2) GDPR) offrono, ad esempio, una base normativa che può essere ulteriormente specificata nei requisiti sostanziali di certificazione.
Al tempo stesso, anche i requisiti procedurali fanno parte di un sistema di certificazione e devono essere soddisfatti dalla parte che richiede la certificazione[43]. Tali requisiti procedurali dovrebbero ad esempio specificare a quali condizioni il responsabile del trattamento dei dati può utilizzare il certificato acquisito, quali sono i periodi di sorveglianza, la struttura compensativa, ecc. Alcuni degli aspetti procedurali sono già chiariti dal GDPR - ad esempio la durata di validità della certificazione è di 3 anni (art. 42(7)).
Alcuni schemi di certificazione esistenti potrebbero usare il termine "criteri" per indicare i requisiti sostanziali (prodotto/processi/persona)[44]. Il GDPR sembra indicare i requisiti sostanziali come "criteri" e i requisiti procedurali come "requisiti".
La certificazione Privacy by Design non si basa né sulla legislazione né su uno standard tecnico, ma su un quadro di riferimento di sette principi fondamentali per la Privacy by Design.
Riguardo l'aspetto di garanzia di conformità con la legislazione, possono esistere tre approcci principali di seguito elencati:

- **Certificazioni indipendenti dalla legislazione**: Si tratta delle certificazioni basate sulle norme ISO/IEC o su altri documenti normativi, come il quadro normativo Privacy by Design Principles. La certificazione Privacy by Design fornita da Ryerson University e Deloitte Canada non sta' a significare la conformità alle leggi sulla privacy dell'Ontario. La norma ISO/IEC 27018, ad esempio, "stabilisce obiettivi di controllo, controlli e linee guida comunemente accettati per l'attuazione di misure volte a proteggere le informazioni personali (PII) in conformità ai principi di riservatezza contenuti nella

[43] La norma ISO/IEC 17065:2012 fornisce esempi di tali requisiti. Un esempio è il pagamento della tassa da parte dell'organizzazione richiedente all' organismo di certificazione.

[44] Un esempio è la certificazione EuroPrise.