Metodologia per la protezione dei dati e per la valutazione d'impatto (DPIA) del trattamento del Titolare

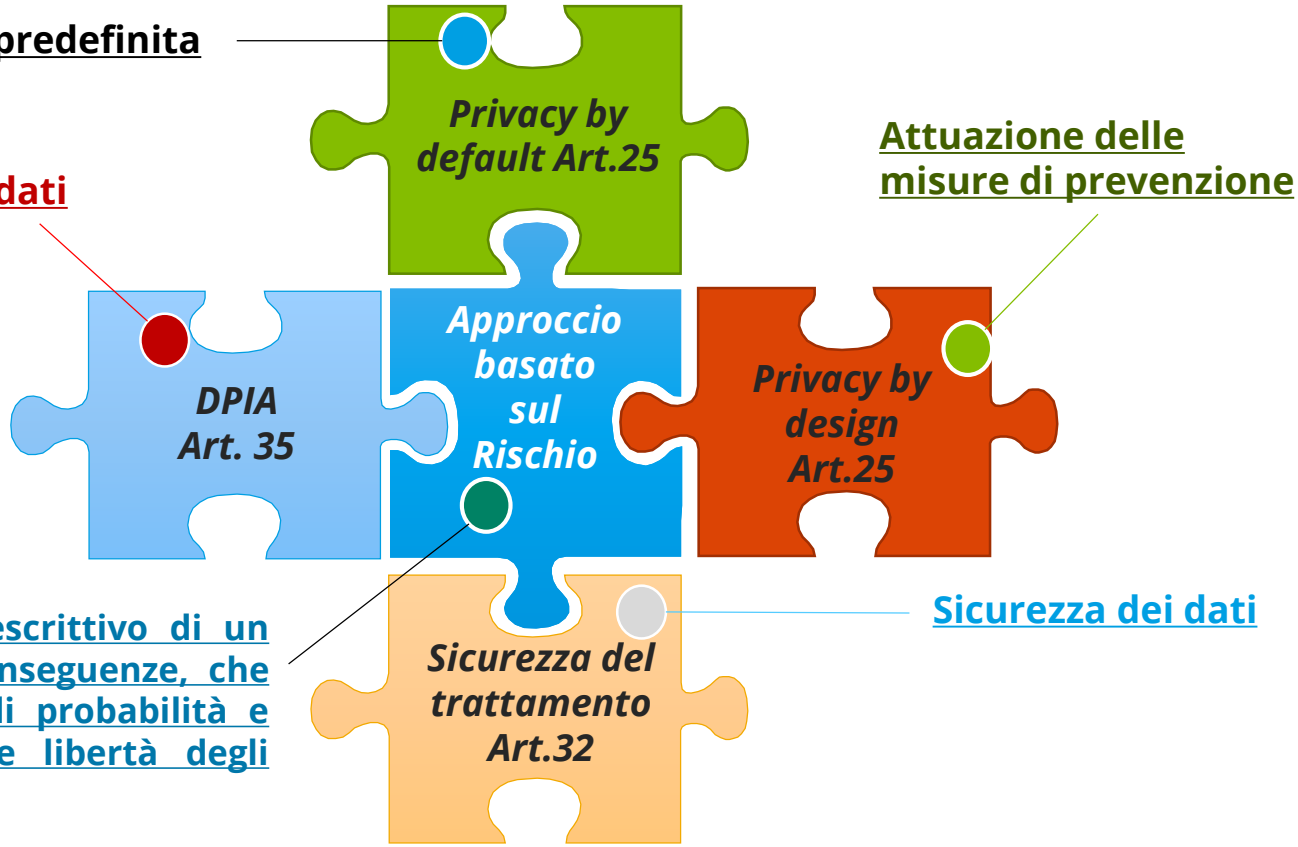
16 marzo 2022

sogei

Approccio innovativo del GDPR

Il titolare del trattamento **mette in atto misure tecniche e organizzative** adeguate per **garantire**, ed **essere in grado di dimostrare**, che il trattamento è effettuato conformemente al GDPR **attraverso**:

Sistema multilivello di protezione dei dati personali



Responsabilità del titolare – Accountability art. 24

Sistema di valutazione del rischio su tre livelli

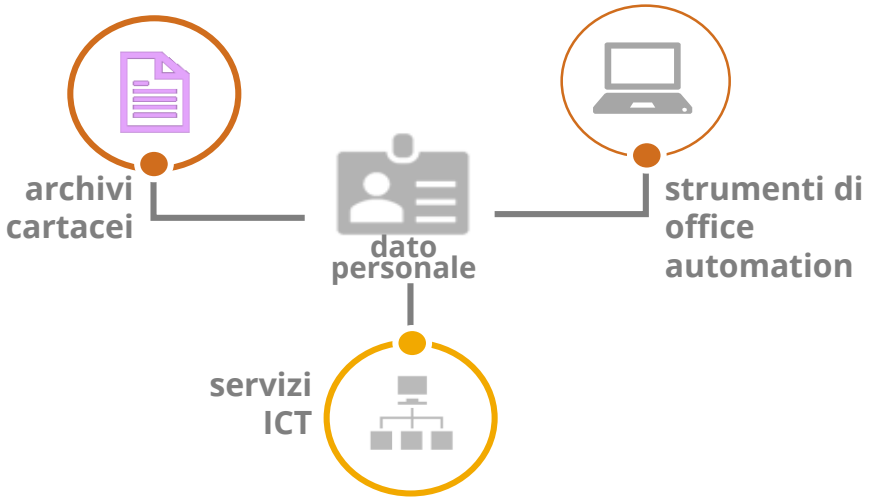
Il primo livello riguarda l'ordinaria valutazione dei rischi prevista dal principio di *privacy by design*, ai sensi dell'art. 24 GDPR, che richiede di adottare quelle misure tecniche e organizzative funzionali a tutelare gli interessati in relazione all'entità e alla concreta probabilità del rischio; dell'art. 25 GDPR, che fornisce le istruzioni per strutturare le misure di garanzia; e dell'art. 32 del GDPR, che prende in esame la disciplina delle misure di sicurezza.

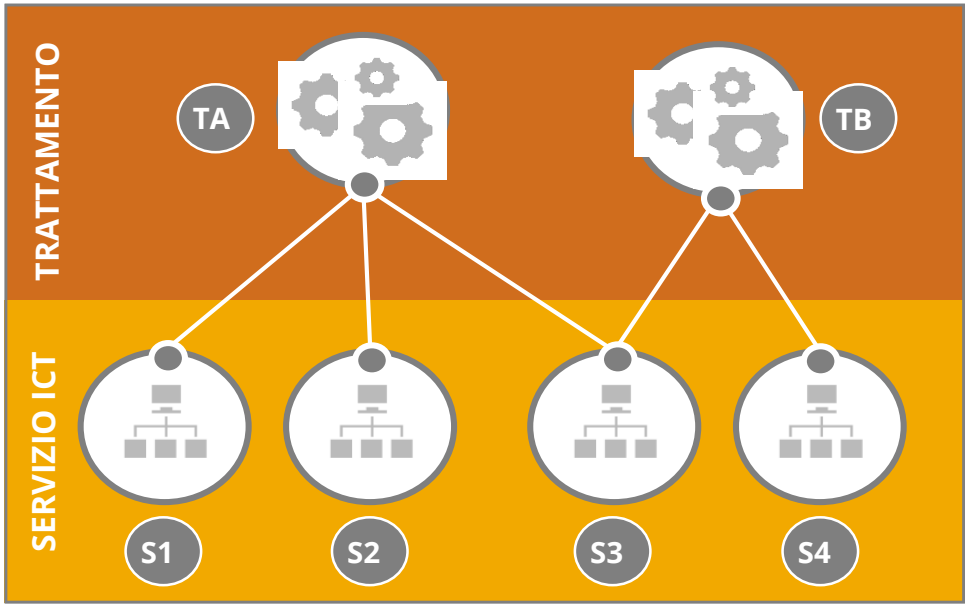
Il secondo livello è quello relativo alla gestione dei trattamenti caratterizzati da un "rischio elevato" e che, pertanto, impongono la previa adozione di una valutazione di impatto secondo il procedimento individuato dall'art 35 GDPR.

Il terzo livello riguarda le ipotesi in cui, nonostante lo svolgimento della valutazione di impatto, permanga comunque un "elevato rischio residuale", mitigabile solo attraverso la consultazione preventiva della competente Autorità di controllo (art. 36 GDPR).

Trattamenti

TIPOLOGIE DI TRATTAMENTO





Sogei tratta i dati personali dei dipendenti e di tutte le persone che hanno rapporti con l'azienda (fornitori, consulenti, visitatori, ...) attraverso l'utilizzo di archivi cartacei, strumenti di office automation e servizi ICT.

Ogni trattamento può essere supportato da più servizi ICT e, viceversa, ogni servizio ICT può supportare più trattamenti con finalità e caratteristiche diverse.

Servizio ICT: insieme di applicazioni informatiche omogenee e della relativa infrastruttura tecnologica – nei casi previsti dal GDPR connesse al trattamento dei dati - in grado di supportare lo svolgimento di un processo amministrativo, per le quali sia comunque opportuno esercitare il controllo/monitoraggio (prestazioni, costi, consumi, ecc.) a livello di unica entità.

Le informazioni: Sicurezza e Protezione dati

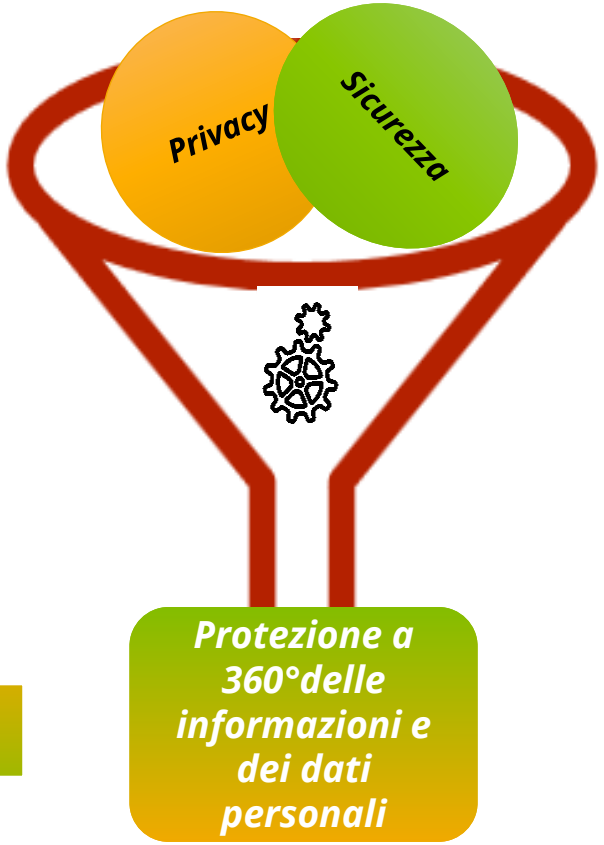
Le informazioni rappresentano il vero patrimonio di un'azienda e di una nazione.

Per **Sogei la protezione delle informazioni**, in ogni sua forma sia cartacea che elettronica, dei dati e delle infrastrutture fisiche e logiche a supporto, **è da sempre un obiettivo strategico**.

Attuazione GDPR anche attraverso la definizione di:

- Specifica organizzazione con ruoli e responsabilità ben definiti;
- Metodologia per la protezione dei dati personali e la valutazione di impatto considerando **tutti i rischi** sia di sicurezza delle informazioni che di privacy, che impattano sui dati personali e sui diritti e le libertà dei cittadini.

Non c'è Privacy senza Sicurezza



GDPR

Privacy by design, by default e DPIA

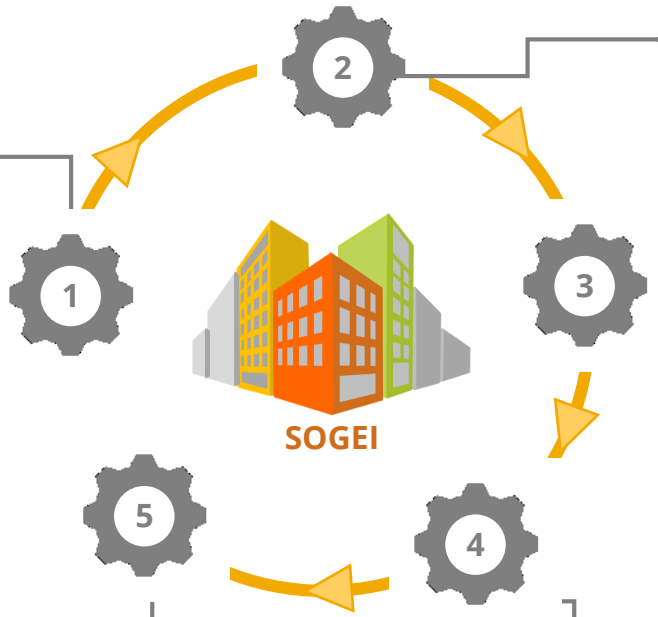
SPECIFICHE DEL TRATTAMENTO

L'owner del trattamento valuta la **necessità**, **proporzionalità** e **non eccedenza** dei dati rispetto alle finalità e alla base giuridica in modo da trattare solo i dati minimi e per un arco temporale definito (*privacy by default*).
Individua inoltre le categorie di dati personali e i mezzi utilizzati per trattarli (archivi cartacei, strumenti di office automation, servizi ICT), gli interessati, i destinatari di comunicazione e l'eventuale trasferimento di dati extra Ue, dimostrando di aver definito le **garanzie per l'esercizio dei diritti degli interessati**.

VALUTAZIONE RISCHIO RESIDUO

Sogei ha definito un algoritmo per il calcolo del rischio residuo che pesa le misure individuate sulla base del loro grado di attuazione e del rischio per gli interessati precedentemente calcolato.
L'owner del trattamento definisce una **soglia di accettabilità** del rischio residuo, superata la quale è necessario ridefinire gli elementi del trattamento, adottare ulteriori misure di sicurezza o ricorrere alla consultazione del'Autorità di controllo.

Metodologia per la protezione dei dati personali e la valutazione di impatto



RISCHI PER GLI INTERESSATI

L'owner del trattamento effettua la **valutazione di impatto (DPIA)** determinando se il trattamento rientra in almeno una delle categorie ad elevato rischio delle linee guida WP248 e stimando i rischi per i diritti e le libertà degli interessati (combinazione di probabilità di accadimento e danno per le persone fisiche).

RISCHI PER L'ORGANIZZAZIONE

L'owner del trattamento stima i rischi per l'organizzazione sulla base della perdita di **riservatezza**, **integrità** e **disponibilità** dei dati.

SELEZIONE MISURE ADEGUATE

Sulla base dei livelli di rischio per gli interessati e l'organizzazione, l'owner del trattamento seleziona dal framework FOURSec le misure tecniche e organizzative adeguate relativamente ai trattamenti svolti su **archivi cartacei** e **strumenti di office automation**, fornendone la modalità di implementazione. Se il trattamento utilizza **servizi ICT** di supporto, il responsabile di ogni servizio individua, sulla base dei rischi specifici ricalcolati sul servizio, le misure ICT adeguate.

FourSEC

Valutazione di impatto sulla protezione dei dati personali per un trattamento della Pubblica Amministrazione

Il documento sulla valutazione di impatto - Indice

1. *EXECUTIVE SUMMARY*
2. *ACRONIMI E GLOSSARIO*
3. *DOCUMENTAZIONE CORRELATA*
4. *SPECIFICHE DEL TRATTAMENTO*
5. *VALUTAZIONE DI IMPATTO*
6. *RISCHI PER PERDITA DI RISERVATEZZA, INTEGRITÀ, DISPONIBILITÀ DELLE INFORMAZIONI*
7. *RISCHI COMPLESSIVI E MISURE DI SICUREZZA ADEGUATE*
8. *VALUTAZIONI FINALI*
9. *PROTEZIONE DELL'INFRASTRUTTURA*
10. ALLEGATO TECNICO – ARCHITETTURA DEL SISTEMA

Focus - Valutazione del rischio intrinseco e il framework FourSEC

Valutazione del rischio intrinseco

RISCHIO INTRINSECO
Si calcola combinando la **probabilità di accadimento** di una **minaccia** sui dati personali e il **danno** che il suo concretizzarsi potrebbe causare all'interessato e all'organizzazione.

MINACCE SUI DATI

- ✓Accesso non autorizzato e/o trattamento illecito.
- ✓Divulgazione non autorizzata o accidentale.
- ✓Modifica non autorizzata o accidentale.
- ✓Indisponibilità temporanea o prolungata.
- ✓Perdita, distruzione accidentale o illecita.

PROBABILITÀ DI ACCADIMENTO

La probabilità che si concretizzi la minaccia, da valutare sulla base di:

- ✓appetibilità del dato;
- ✓contesto di riferimento;
- ✓serie storiche.

LA VALUTAZIONE NON TIENE CONTO DELLE MISURE DI PROTEZIONE GIÀ ESISTENTI (es. data center sicuro, sistemi di protezione perimetrale, cifratura, ecc.).

DANNO

PER L'INTERESSATO:

- ✓ fisico-biologico;
- ✓ finanziario;
- ✓ reputazionale;
- ✓ di identità.

PER L'ORGANIZZAZIONE:

- ✓ Finanziario;
- ✓ compromissione attività di business;
- ✓ Immagine;
- ✓ sanzioni amministrative.

Il framework FourSEC - Struttura e utilizzo

Tipologia di misure
- Procedurali
- Infrastrutturali
- Archivi cartacei
- Office automation
- ICT

Minacce sui dati
- Accesso non autorizzato e/o trattamento illecito
- Divulgazione non autorizzata o accidentale
- Modifica non autorizzata o accidentale
- Indisponibilità temporanea o prolungata
- Perdita, distruzione accidentale o illecita

Rischi
- Livello di rischio per i diritti e le libertà degli interessati (B/M/A)
- Livello di rischio per l'organizzazione (B/M/A)
- Livello di rischio complessivo (B/M/A)

Ambito di sicurezza
- Asset
- Controlllo accessi
- Erogazione del servizio
- Gestione eventi
- Organizzazione
- Risorse umane e terze parti
- Sicurezza fisica
- Sviluppo e manutenzione
- Tracciamento

Norme/standard
- GDPR
- Codice privacy
- Provvedimenti Garante
- MM AgID per la PA
- ISO 27001
- NIST Cybersecurity Framework
- Framewokk Nazionale Cybersecurity Data Protection
- Istruzioni titolari MEF
- Politiche aziendali

FourSEC 2.2 - 340 misure di sicurezza

PRIVACY BY DESIGN/DPIA TRATTAMENTI

Le misure di tipo procedurale, archivi cartacei e office automation proteggono i dati personali trattati in funzione del livello di rischio (interessati e organizzazione) valutato su ogni minaccia.

PRIVACY BY DESIGN/DPIA SERVIZI ICT DI SUPPORTO

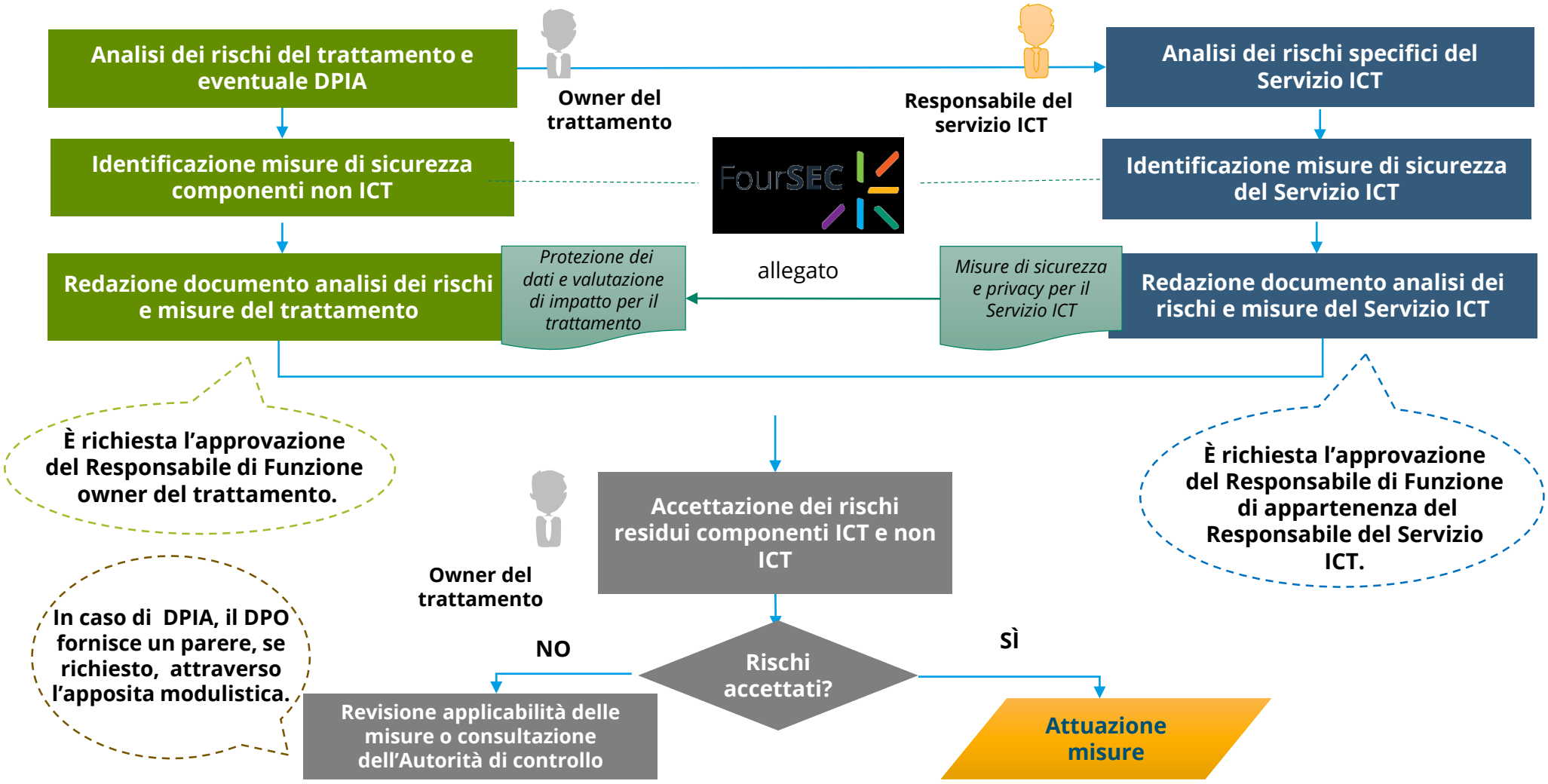
Le misure di tipo ICT proteggono i servizi informatizzati erogati da Sogei in funzione del livello di rischio (interessati e organizzazione) valutato su ogni minaccia.

MISURE INFRASTRUTTURALI

Proteggono il data center Sogei a prescindere dal livello di rischio stimato per i servizi ICT. Sono allegate al registro dei trattamenti di Sogei in qualità di responsabile del trattamento.

Privacy by design, by default, DPIA

Riepilogando: Flusso di privacy by design e valutazione d'impatto (DPIA)



GRAZIE PER L'ATTENZIONE