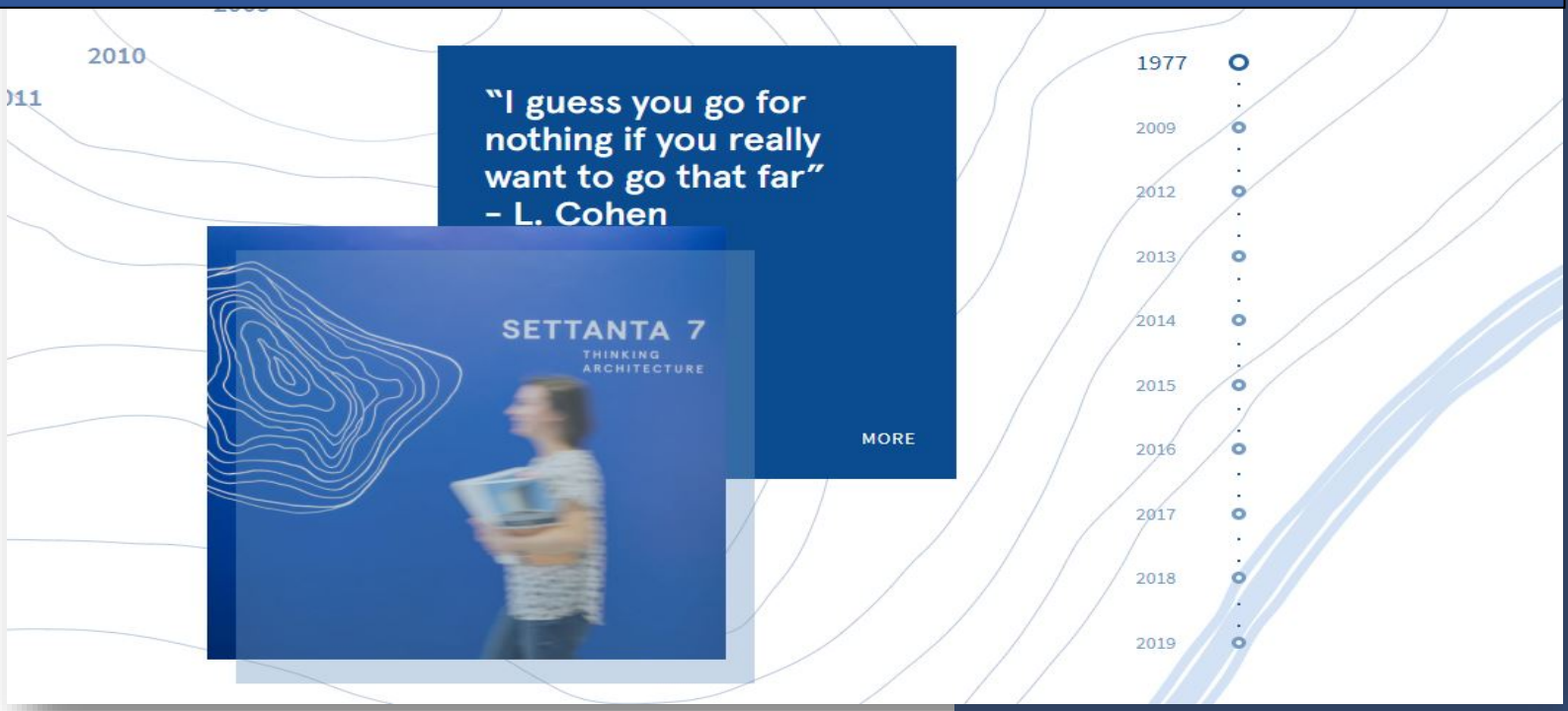
SETTANTA 7
THINKING ARCHITECTURE

2019

POLITICA GENERALE SUL TRATTAMENTO DEI DATI PERSONALI



CONTIENE:

- POLITICA AZIENDALE SULL'UTILIZZO SICURO DEI SISTEMI INFORMATICI E DELLE TECNOLOGIE DIGITALI
- ISTRUZIONI OPERATIVE AI SOGGETTI AUTORIZZATI

DESTINATARI:

- COORDINATORE PRIVACY
- REFERENTI PRIVACY DI AREA
- SOGGETTI AUTORIZZATI
- AMMINISTRATORI DI SISTEMA

SGDP

Sistema Gestione Dati Personali

SOMMARIO

1. Premessa

Il Regolamento (UE) 27 aprile 2016, n. 679 (di seguito anche "Regolamento" o "GDPR"), stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati con lo scopo di proteggere i diritti e le libertà fondamentali delle persone fisiche.
Inoltre, il Regolamento, stabilisce che la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Fatto salvo quanto previsto dagli artt. 2 e 3 del GDPR, in merito a gli ambiti di applicabilità materiale e territoriale del Regolamento, le norme in materia di protezione dei dati personali, si applicano a tutti i trattamenti di dati personali e la loro applicazione ricade esclusivamente sotto la responsabilità del Titolare del Trattamento.
Pertanto, il Regolamento stabilisce che spetti al Titolare del trattamento mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente a tali norme. Dette misure devono essere riesaminate e aggiornate qualora necessario e se ciò è proporzionato rispetto alle attività di trattamento, le misure devono includere l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
Per queste ragioni, **Studio Settanta7** in qualità di Titolare del Trattamento, ha adottato un modello organizzativo, definito Sistema Gestione Dati Personali ("**SGDP**" o "Sistema"), basato anche sulle linee guida degli standard *BS 10012:2017 e* ISO 27001.
Tenendo conto del contesto di business, dei costi, dei rischi connessi, delle esigenze di filiera (Framework Nazionale sulla Sicurezza Cibernetica) e delle aspettative delle parti interessate, che conferiscono i loro dati personali confidando in un trattamento nel rispetto di ogni norma di legge, il Sistema stabilisce le Leadership e l'impegno del Titolare del Trattamento, attraverso la definizione dei ruoli organizzativi, delle responsabilità interne ed esterne e dell'autorità dei soggetti coinvolti. All'interno del SGDP sono individuati gli obiettivi di sicurezza e sono pianificate le politiche e le azioni necessarie per la loro realizzazione; vengono inoltre garantite le risorse e le competenze necessarie al fine di un costante e continuo miglioramento del SGDP nel tempo, verificando periodicamente il suo campo di applicazione e l'allineamento con gli scopi di business e la conformità ai requisiti cogenti.

2. Titolare del Trattamento o "Data Controller"

Ai sensi del GDPR, è Titolare del trattamento la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali
Di seguito sono riportati i dati autorizzati da inserire, se del caso, nelle informative e nelle comunicazioni agli interessati:

*Il titolare del trattamento dei Tuoi dati personali è **Studio Settanta7** – Via Principessa Clotilde, 3 – 10144 Torino (TO) - Partita Iva: 10119920014.*
Il Titolare del trattamento è contattabile, oltre che all'indirizzo postale indicato, all'indirizzo di posta elettronica e privacy@settanta7.com

3. Scopo e ambito di applicazione del sistema di gestione

Questa politica, è da ritenersi il cuore del Sistema SGDP e si pone l'obiettivo di disciplinare il trattamento dei dati personali all'interno di Studio Settanta7 e di individuare le misure tecniche ed organizzative ritenute adeguate per garantire un livello di sicurezza del trattamento dei dati personali proporzionato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle parti interessate coinvolte.
Lo scopo di **Studio Settanta7** è quello di adempiere a qualsivoglia legge in materia di trattamento dei dati personali e di ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, inoltre, **Studio Settanta7** si impegna espressamente per tutta la durata del trattamento a rafforzare, integrare e ottimizzare

le procedure e le misure di sicurezza adottate, allo scopo di mantenere la conformità alle Leggi in materia di protezione dei dati personali.

4. Trattamento lecito dei dati personali

I dati personali devono essere trattati nel rispetto delle leggi, comprese quelle aventi ad oggetto settori specifici, come, ad esempio, lo Statuto dei lavoratori - *Legge 300/1970*.
In particolare, i dati devono essere raccolti per finalità determinate, esplicite e legittime e quindi trattati secondo modalità compatibili con tali finalità.

Studio Settanta7 deve esplicitare e comunicare chiaramente la finalità del trattamento prima che questo abbia inizio in modo da consentire all'interessato, se del caso, di fornire un consenso informato; tale comunicazione all'interessato va fatta a mezzo di apposita documentazione (informativa) che deve essere portata a conoscenza di quest'ultimo e messa a disposizione a fini di ispezione da parte delle autorità di controllo, in assenza della precisazione della finalità al soggetto interessato, il trattamento è sempre illegittimo.

 **Attenzione!**	È vietato raccogliere e trattare dati superflui rispetto agli scopi descritti e l'interessato deve comunque sempre essere informato delle scelte del Titolare.

5. Modalità del trattamento

Il trattamento dei dati personali avviene mediante strumenti cartacei, informatici e telematici con logiche strettamente correlate alle finalità di raccolta e conferimento e, comunque, in modo da garantire sempre la riservatezza, l'integrità e la disponibilità dei dati stessi.

In particolare, i dati personali devono essere:

a. trattati in modo lecito, corretto e trasparente;
b. raccolti per le finalità esplicite e legittime dichiarate e successivamente trattati nel rispetto delle medesime;
c. adeguati, pertinenti e limitati rispetto alle finalità dichiarate ("*c.d. minimizzazione dei dati*");
d. esatti e, se necessario, aggiornati, cancellati e/o rettificati, anche in base alle indicazioni dei soggetti interessati;
e. conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati e, successivamente, per il termine prescrizionale previsto dalla normativa per la tutela dei diritti connessi, fatti salvi in ogni caso periodi di conservazione maggiori previsti da specifiche normative di settore;
f. trattati in maniera da garantirne, mediante misure tecniche ed organizzative adeguate, la protezione rispetto a trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

6. Basi giuridiche del trattamento

Le basi giuridiche applicabili ai principali trattamenti effettuati da **Studio Settanta7** per gli scopi di business sono:

Base Giuridica	Icona	Descrizione
Consenso art. 6.1 lettera **a** GDPR		L'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità.
Contratto art. 6.1 lettera **b** GDPR		Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.
Obbligo di Legge art. 6.1 lettera **c** GDPR		Il trattamento è necessario per adempiere un obbligo legale al quale è soggetta la nostra organizzazione o l'interessato.

Legittimo Interesse art. 6.1 lettera **f** GDPR		Il trattamento è necessario per il perseguimento di un nostro legittimo interesse o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali del soggetto interessato.

7. Istruzioni sull' utilizzo del Consenso come base giuridica del trattamento

Nel valutare se il consenso sia la corretta base giuridica del trattamento che si intende iniziare si devono prendere in considerazione le "***Linee guida sul consenso ai sensi del regolamento (UE) 2016/679"*** rilasciate dal Gruppo di Lavoro Articolo 29 (WP29). In particolare, si deve anche tener conto che l'elemento della manifestazione di volontà "libera" implica che l'interessato abbia una scelta effettiva e il controllo sui propri dati. Come regola generale, se l'interessato non dispone di una scelta effettiva, si sente obbligato ad acconsentire o subirà conseguenze negative se non acconsente, il consenso non sarà considerato valido, se il consenso è parte non negoziabile delle condizioni generali di contratto/servizio si presume che non sia stato prestato liberamente; di conseguenza, il consenso non sarà considerato libero se l'interessato non può rifiutarlo o revocarlo senza subire pregiudizio.
In termini generali, qualsiasi azione di pressione o influenza inappropriata sull'interessato (che si può manifestare in svariati modi) che impedisca a quest'ultimo di esercitare il suo libero arbitrio, rende il consenso invalido.
È altamente inopportuno "accorpare" il consenso all'accettazione delle condizioni generali di contratto/servizio o "subordinare" la fornitura di un contratto o servizio a una richiesta di consenso al trattamento di dati personali che non sono necessari per l'esecuzione del contratto o servizio stesso.

Disposizioni specifiche sul Consenso dei dipendenti

Al fine di garantire la regolarità del consenso occorre tenere sempre presente che il WP29 stabilisce che, per la maggior parte delle attività di trattamento svolte sul posto di lavoro, la base legittima non può e non dovrebbe essere il consenso del dipendente (articolo 6, paragrafo 1, lettera a) in considerazione della natura del rapporto tra datore di lavoro e dipendente (subordinato).
Ciò non significa che **Studio Settanta7** non possa mai basarsi sul consenso come base legittima per il trattamento dei dati dei dipendenti ma semplicemente che, qualora lo prescelga, dovrà essere in grado di dimostrare che il consenso è stato effettivamente espresso liberamente. In ogni caso, dato lo squilibrio di potere tra il datore di lavoro e il suo personale, i dipendenti possono manifestare il loro consenso liberamente soltanto in casi eccezionali nei quali **Studio Settanta7** deve essere in grado di garantire, e dimostrare loro, che non subiranno alcun pregiudizio o ripercussione negativa per il fatto che esprimano il loro consenso o meno.

Dimostrazione del consenso

Per i trattamenti basati sul consenso dell'interessato, **Studio Settanta7** deve essere in grado di dimostrare che quest'ultimo ha acconsentito al trattamento attraverso l'adozione di metodi opportuni e proporzionati al rischio per i diritti e le libertà del soggetto interessato. In particolare, deve essere limitata allo stretto necessario l'acquisizione di ulteriori dati dell'interessato per dimostrare il consenso e l'eventuale revoca.
Studio Settanta7, quando possibile e opportuno, adotta idonee tecnologie per la gestione automatizzata dei consensi (registrazione non opinabile) e delle revoche in modo da trasferire all'interessato il controllo diretto dei propri dati e dell'esercizio dei diritti connessi.
Ad esempio, l'eventuale iscrizione ad un servizio di newsletter deve sempre consentire la cancellazione automatica da parte dell'interessato in modo da evitare ulteriori procedure gestionali.

8. Ulteriori informazioni sul legittimo interesse di Studio Settanta7

Una delle principali espressioni del principio di «responsabilizzazione» introdotto dal nuovo Regolamento, prevede che spetti al Titolare del Trattamento stabilire se, nel bilanciamento fra legittimo interesse del Titolare o del terzo e diritti e libertà dell'interessato, prevalga l'interesse legittimo.
Studio Settanta7 può, pertanto, trattare i dati personali qualora ciò sia necessario a difendere o a far valere un Interesse Legittimo (o quelli di un terzo collegato).
Ciò include le seguenti ipotesi di trattamento, a scopo esemplificativo ma non esaustivo:

- difendersi in sede giudiziaria, finalizzare le procedure contrattuali e precontrattuali, prevenire le frodi, gestire i pagamenti e gli insoluti, raggiungere gli scopi di business nel rispetto di qualsivoglia legge o normativa vigente;

- trasmissione di dati personali a fini amministrativi interni e con gli enti o soggetti collegati;
- gestire la sicurezza delle reti informatiche e dei sistemi elettronici, trattando anche i dati personali relativi al traffico sul sito web e sui servizi cloud gestiti direttamente, nella misura strettamente necessaria e proporzionata per garantirne la sicurezza (cioè la capacità di resistere a eventi imprevisti o atti illeciti o dolosi che possano compromettere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi);
- utilizzare i servizi offerti o resi accessibili, da autorità pubbliche, organismi di intervento in caso di emergenza informatica, gruppi di intervento per la sicurezza informatica in caso di incidente, fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi anche di sicurezza;
- impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, nonché porre termine agli attacchi da "blocco di servizio" e ai danni ai sistemi informatici e di comunicazione elettronica.

9. Soggetti a cui è consentito trattare i dati personali di Studio Settanta7

Studio Settanta7 si avvale delle attività di soggetti esterni con i quali ha stipulato appositi accordi per regolare i rapporti di **Titolarità/Responsabilità** ai sensi del Regolamento.
Al suo interno, invece, i soggetti coinvolti nelle attività di trattamento dei dati personali, sono identificati come soggetti "**Autorizzati**" al trattamento, compresi i soggetti individuati quali "**Amministratori di Sistema**" o "**AdS**" ai sensi del Provvedimento a carattere generale del Garante per la protezione dei dati personali: ''*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema- del 27 novembre 2008".*

10. Responsabile del Trattamento o "Processor"

Qualora un trattamento debba essere effettuato da un soggetto esterno alla sua organizzazione, **Studio Settanta7** ricorre unicamente a soggetti che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la corretta tutela dei diritti delle parti interessate. Viene identificato come Responsabile del Trattamento ai sensi dell'art. 28 del GDPR ogni soggetto appartenente a tale categoria.
I trattamenti eseguiti da parte di un Responsabile del Trattamento devono essere disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del Trattamento a **Studio Settanta7**; tale contratto deve disciplinare il tipo di Trattamento dei Dati personali, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di soggetti interessati, gli obblighi del Responsabile del Trattamento e i diritti di Studio Settanta7.

 **Attenzione!**	È necessario svolgere controlli periodici al fine di vigilare sulle operazioni di trattamento condotte dal soggetto Responsabile e garantire il rispetto delle prescrizioni contenute nel contratto, nonché degli obblighi stabiliti dalla normativa in materia di trattamento dei dati personali; inoltre è necessario svolgere controlli e verifiche con riferimento al livello di sicurezza applicato dal Responsabile, chiedendone, se del caso, eventuali integrazioni. Il Responsabile si deve impegnare a conformarsi alle prescrizioni contenute nel contratto e a rispettare gli obblighi di legge previsti in materia di trattamento e sicurezza dei dati personali con riferimento alle attività di propria pertinenza. In ogni caso, il Responsabile deve astenersi dall'adottare autonome decisioni in merito alle finalità e alle modalità del trattamento; in caso di urgenza e necessità, dovrà provvedere a informare, senza ingiustificato ritardo, **Studio Settanta7** affinché possa assumere le opportune decisioni.

Studio Settanta7 adotta un modello di contratto standard (DPA-SGDP-01_Accordo per l'elaborazione dei dati personali_Generale) e due modelli specifici (DPA-SGDP-02_Accordo per l'elaborazione dei dati personali_Consulente Lavoro e DPA-SGDP-03 - Accordo per l'elaborazione dei dati personali_Amministratore di Sistema).

Soggetto Responsabile:

Il **Delegato del Titolare** è Responsabile della stipula dei contratti con i **Data Processor.**

Il **Coordinatore Privacy** è la funzione preposta alla conservazione dei contratti.

11. Responsabile Protezione Dati (RPD) o Data Protection Officer (DPO)

Tra i principali obblighi previsti dal nuovo regolamento europeo sulla privacy c'è quello, per alcune organizzazioni, di adeguare il proprio organigramma privacy inserendo all'interno dello stesso la figura del DPO, acronimo di Data Protection Officer ovvero Responsabile Protezione Dati.
Il Data Protection Officer, se nominato, deve essere profondo conoscitore del "Core Business" dell'organizzazione, con particolari competenze in campo informatico, giuridico, di valutazione del rischio e di analisi dei processi, il cui compito principale è l'osservazione, la valutazione e la gestione del trattamento dei dati personali allo scopo di far rispettare le normative europee e nazionali in materia di privacy. La funzione di DPO può essere rivestita, oltre che da un libero professionista o consulente esterno, anche da un dipendente del titolare del trattamento.
Il DPO oltre che figura di riferimento per i soggetti interessati, svolge anche il ruolo di interfaccia tra Studio Settanta7 e l'autorità di controllo.

Studio Settanta7 ai sensi dell'art. 24, paragrafo 1 GDPR, con l'intento di dimostrare l'adozione di misure adeguate a garantire la conformità al Regolamento, ha valutato la sussistenza delle condizioni di obbligatorietà di nomina del DPO.
Al fine di determinare una scelta ponderata e corretta sulla necessità di nomina del DPO, **Studio Settanta7** ha provveduto ad analizzare tutte le condizioni previste dall' art. 37 paragrafo 1 del GDPR al fine di escludere, in modo oggettivo, ogni singola condizione di obbligatorietà di nomina.

Il GDPR prevede che il Titolare del Trattamento e il responsabile del trattamento designino sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a)	*il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; ex art 37 paragrafo 1 Lettera a) GDPR*
b)	*le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;* ex art 37 paragrafo 1 Lettera b) GDPR
c)	*le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 del GDR o di dati relativi a condanne penali e a reati di cui all'art. 10 del GDPR.* ex art 37 paragrafo 1 Lettera c) GDPR

Analisi del Titolare del Trattamento

Analisi del punto a)

Clausola di obbligatorietà di nomina del DPO
Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali - ex art 37 paragrafo 1 Lettera a) GDPR

Risultato dell'analisi del Titolare del Trattamento:
CLAUSOLA DI OBBLIGATORIETA' NON APPLICABILE

Considerazioni del Titolare:

Studio Settanta7 non è un'autorità pubblica o un organismo pubblico.

Analisi del punto b)

Clausola di obbligatorietà di nomina del DPO

Le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala - ex art 37 paragrafo 1 Lettera b) GDPR

_____

Considerazioni del Titolare:

Studio Settanta7 non effettua trattamenti di tale natura

ULTERIORI APPROFONDIMENTI SULL'ATTIVITA' DI MONITORAGGIO

Quanto alla definizione di monitoraggio regolare e sistematico, le Linee guida forniscono alcune indicazioni elencando degli esempi di tipologie di attività che comportano tale forma di monitoraggio quali:

- curare il funzionamento di una rete di telecomunicazioni;
- la prestazione di servizi di telecomunicazioni;
- il re-indirizzamento di messaggi di posta elettronica;
- attività di marketing basate sull'analisi dei dati raccolti;
- profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio);
- tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili;
- programmi di fidelizzazione;
- pubblicità comportamentale;
- monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili;
- utilizzo di telecamere a circuito chiuso;
- dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

ULTERIORI APPROFONDIMENTI SUL TRATTAMENTO SU LARGA SCALA

Al fine di verificare la sussistenza del trattamento su larga scala, il Gruppo di Lavoro Articolo 29 raccomanda di tenere conto dei seguenti fattori:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Attualmente, nessuno di questi fattori risulta essere rilevante per i trattamenti effettuati da **Studio Settanta7**

Risultato dell'analisi del Titolare del Trattamento:
CLAUSOLA DI OBBLIGATORIETA' NON APPLICABILE

Analisi del punto c)

Clausola di obbligatorietà di nomina del DPO *le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 del GDR o di dati relativi a condanne penali e a reati di cui all'art. 10. ex art 37 paragrafo 1 Lettera c) GDPR* **_____** **Considerazioni del Titolare:** **Studio Settanta7** non effettua trattamenti su larga scala di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10. I suddetti dati vengono trattati esclusivamente per finalità inerenti il mantenimento del rapporto di lavoro secondo le disposizioni di legge.	**Risultato dell'analisi del Titolare del Trattamento:** **CLAUSOLA DI OBBLIGATORIETA' NON APPLICABILE**

Considerando quanto sopra evidenziato, si ritiene che attualmente non esistano i presupposti per l'obbligatorietà della nomina del DPO da parte della **Studio Settanta7**
Tuttavia, Studio Settanta7 continuerà ad avvalersi di soggetti interni ed esterni (consulenti) al fine di ottemperare compiutamente a quanto previsto dal GDPR.
Tali soggetti pur avendo talvolta compiti ed incarichi simili al Data Protection Officer, di fatto non saranno mai identificati con le sigle **DPO** o **RDP**.

Soggetto Responsabile:
Il **Delegato del Titolare**, valuta periodicamente la sussistenza delle condizioni di obbligatorietà di nomina del DPO o la necessità di provvedere comunque alla nomina al fine di garantire una corretta vigilanza sulla compliance dell'organizzazione.

12. Organigramma Privacy

Il Delegato del Titolare è la persona fisica delegata ad esercitare, con pieni poteri esecutivi, tutti gli obblighi e le responsabilità derivanti dalla normativa in materia di protezione dei dati personali. Stabilisce leadership e impegno del Titolare del Trattamento attraverso la definizione dei ruoli organizzativi, delle responsabilità interne ed esterne e dell'autorità dei soggetti coinvolti. Ha il inoltre il compito di fornire le risorse necessarie a garantire adeguate misure tecniche e organizzative a tutela della sicurezza dei trattamenti, dei diritti e delle libertà fondamentali delle parti interessate.

Coordinatore Privacy	Referenti Privacy	Autorizzati al trattamento
Il Coordinatore privacy funge da punto di coordinamento delle attività legate alla protezione dei dati personali. Si relaziona direttamente con il Titolare del trattamento e con i Referenti Privacy ed è incaricato di rispondere ai soggetti interessati.	I Referenti Privacy sono i singoli responsabili indicati nell'organigramma; hanno funzioni di indirizzo e controllo nei confronti dei soggetti autorizzati al trattamento nelle rispettive aree. Si relazionano direttamente con il Coordinatore privacy e collaborano all'applicazione delle politiche di sicurezza stabilite dal Titolare del trattamento.	I membri del nostro personale, dipendenti o collaboratori, operano internamente alla nostra struttura sui dati personali in qualità di soggetti autorizzati al trattamento e agiscono sotto la supervisione dei relativi Referenti Privacy relazionandosi direttamente con questi.

L'organigramma privacy, completo dei nominativi di tutti i soggetti coinvolti, è contenuto nel documento **ORG-SGDP-01** allegato alla presente politica.

13. Autorizzati al Trattamento

Tutti i soggetti autorizzati devono essere adeguatamente istruiti, formati e vincolati alla riservatezza; in caso contrario è fatto divieto loro di procedere a qualunque trattamento dei dati personali.
Le autorizzazioni al trattamento devono essere formalizzate per iscritto dai Referenti Privacy e il soggetto, nella veste di persona autorizzata al trattamento dei dati personali, si impegna a trattare i dati in modo lecito, corretto e nel pieno rispetto di tutte le disposizioni in materia di trattamento dei dati personali, nonché delle specifiche istruzioni impartite dal Titolare del trattamento.

Azioni procedurali:

Tutte le attivazioni, modifiche o revoche di risorse informatiche al soggetto Autorizzato, devono rispettare le azioni procedurali riportate nella Politica sull'utilizzo delle risorse informatiche (PO-SGDP-02 - Politica sull'utilizzo delle risorse informatiche) e, in particolare:

- attivazione di nuovi soggetti autorizzati;
- perdita del diritto di accesso;
- verifica delle mansioni;
- accesso ai dati in caso di emergenza;
- disattivazione delle credenziali inutilizzate;
- salvataggio dei dati;
- riassegnazione, smaltimento e gestione RAEE;
- custodia delle credenziali tecniche per l'amministrazione dei sistemi.

Soggetto Responsabile:

Il **Referente Privacy** svolge il compito di controllo e indirizzo delle attività connesse alla formazione e all'istruzione dei soggetti autorizzati dell'area di pertinenza e vigila che nessun soggetto non adeguatamente istruito e formato tratti i dati personali.
Il **Coordinatore Privacy** fornirà tutto il supporto necessario al Referente Privacy per far fronte alle richieste e alle segnalazioni dei soggetti Autorizzati.

14. Amministratore di Sistema - AdS

Gli Amministratori di Sistema o "**AdS**" vanno identificati e designati per iscritto, in conformità a quanto stabilito dal Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008, previa valutazione in ordine alle caratteristiche di capacità, affidabilità ed esperienza. Tale Provvedimento estende gli adempimenti previsti per gli Amministratori di Sistema anche alle funzioni (soggetti autorizzati) per le quali le operazioni di trattamento comportano particolari e più ampi privilegi per l'accesso ai dati personali, ovvero quando le attività siano esercitate in un contesto che renda tecnicamente possibile l'accesso, anche fortuito, a dati personali.

Per questi motivi **Studio Settanta7** stabilisce quanto segue:

a) quali "*Amministratori di Sistema*" devono essere individuate sia le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, sia le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;
b) alcune delle attività tecniche svolte possono comportare un'effettiva capacità di azione sulle informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; e ciò, anche quando non siano consultate in chiaro le informazioni medesime;
c) devono essere analizzate le operazioni di trattamento svolte dall'AdS, nel contesto del suo profilo di incarico;
d) alcune delle operazioni di trattamento svolte dall' AdS possono comportare, anche involontariamente, particolari rischi;
e) deve essere valutata l'adeguatezza del candidato al ruolo di AdS in funzione della sua esperienza, capacità e affidabilità, anche ai fini di garantire che il trattamento dei dati personali sia svolto nel pieno rispetto delle disposizioni vigenti e delle misure di sicurezza mediante gli elementi indicati nel suo curriculum ed in particolare:

- la tipologia di studi effettuati;
- la partecipazione a corsi qualificanti, in particolare nell'area di sicurezza informatica, nonché sui temi riguardanti le misure di sicurezza in materia di protezione dei dati personali;
- le certificazioni acquisite, in particolare nell'area di sicurezza informatica, nonché sui temi riguardanti le misure di sicurezza in materia di protezione dei dati personali;
- gli anni di esperienza maturata in qualità di incaricato alla gestione e manutenzione di sistemi informatici.

f) vanno identificate le persone fisiche preposte alla funzione di Amministratori di Sistema riportando i loro dati identificativi, di contatto e la loro funzione, in un apposito elenco reso disponibile alle parti interessate per qualsiasi evenienza e aggiornato ad ogni modifica;

g) va garantita, altresì, la tracciabilità e la registrazione dell'attività di accesso da parte degli Amministratori di Sistema; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. Le registrazioni, inoltre, devono comprendere i riferimenti allo "username" utilizzato, i riferimenti temporali e la descrizione dell'evento (log in e log out) che le ha generate e devono essere conservate per un periodo congruo, non inferiore a sei mesi;

h) l'AdS dovrà rispettare le vigenti disposizioni in materia di trattamento dei dati personali, ivi compresi i profili di sicurezza, nonché le modificazioni ed integrazioni della normativa in materia. Ciò con particolare riferimento alle disposizioni vigenti che impongono limiti e divieti all'azione degli Amministratori di Sistema in funzione di altri diritti ed interessi di lavoratori e di terzi (ad esempio, la legge n. 300/1970 Statuto dei lavoratori, e così via). Tali norme, in effetti, non sempre consentono di effettuare attività ed azioni che, pure sotto il profilo meramente tecnico, potrebbero essere valutate come utili e/o opportune;

i) è necessario provvedere, almeno annualmente, a verificare le attività svolte dagli Amministratori di Sistema al fine di valutarne la rispondenza rispetto alle misure organizzative, tecniche e di sicurezza predisposte a garanzia dei trattamenti dei dati personali.

Soggetto Responsabile:
Il **Delegato del Titolare** è responsabile della designazione degli AdS, della loro adeguatezza e della verifica annuale delle attività svolte.

15. Piano di Formazione

Studio Settanta7 predispone un piano di formazione specifico sulla sicurezza del trattamento dei dati personali, definendo obiettivi, metodi didattici, strumenti di erogazione dei contenuti e procedure di monitoraggio e di valutazione degli interventi formativi effettuati.

Soggetto Responsabile:
Il **Coordinatore Privacy** è responsabile della formazione sul trattamento dei dati personali**.**

16. Informativa al soggetto interessato

Il trattamento di dati personali deve svolgersi entro gli stessi limiti inseriti nell'informativa. In altri termini, una volta che l'interessato è stato informato delle modalità del trattamento dei suoi dati personali, detta informativa costituisce il limite del trattamento stesso.
Ciascuna persona autorizzata al trattamento deve pertanto conoscere le informative predisposte in relazione ai trattamenti che effettua. È chiaro che ogni persona autorizzata al trattamento avrà cura di valutare con maggiore attenzione le informative che più direttamente riguardano la sua attività.

Soggetto Responsabile:
I soggetti autorizzati al trattamento sono responsabili del rispetto dei limiti di trattamento riportati nelle specifiche informative.

Struttura dell'informativa

Studio Settanta7 adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del GDPR e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Soggetto Responsabile:
Il **Coordinatore Privacy e i Referenti Privacy** sono responsabili di fornire all'interessato tutte le informazioni necessarie per il rispetto di qualsivoglia normativa vigente in materia di trattamento dei dati personali.

17. Comunicazione e diffusione dei Dati Personali

Studio Settanta7 potrà sempre comunicare i dati personali per il raggiungimento degli scopi legati alle finalità di raccolta, ai seguenti soggetti:

Autorizzati al trattamento	Responsabili del trattamento	Titolari del trattamento
Dipendenti, collaboratori, Amministratori di Sistema.	Società/Studi professionali che prestano attività di assistenza e/o consulenza a Studio Settanta7 in materia contabile, amministrativa, fiscale, legale, tributaria e finanziaria, nonché a terzi fornitori di servizi cui la comunicazione sia necessaria per l'adempimento delle prestazioni oggetto di contratto.	Autorità amministrative, istituzionali e/o giudiziarie e ogni altro soggetto al quale la comunicazione sia obbligatoria per legge e/o per l'espletamento delle finalità di raccolta e conferimento.

L'elenco completo dei destinatari dei dati personali è sempre reso disponibile presso il Coordinatore privacy, che ha il compito di tenerlo costantemente aggiornato.

Ipotesi di comunicazione e diffusione dei dati

Una specifica attenzione va dedicata alle ipotesi di comunicazione o diffusione dei dati. In altri termini, ogni qual volta si prospetti l'eventualità di divulgare (in qualsiasi forma o modo) dati personali, è necessario procedere alle seguenti verifiche, specie se riguardano categorie particolari di dati personali:

- verifica della legittimità della divulgazione alla luce della informativa fornita all'interessato;
- verifica di eventuali normative che consentano/rendano obbligatoria la divulgazione.

 **Attenzione!**	Fatti salvi gli obblighi di legge, in nessun caso i dati personali trattati da **Studio Settanta7** potranno essere diffusi senza esplicito consenso dell'interessato.

Soggetto Responsabile:
Il **Coordinatore Privacy** e i **Referenti Privacy** sono responsabili della comunicazione dei dati personali.

18. Requisiti per il trasferimento dei Dati Personali verso un paese terzo

Per gli scopi pertinenti alle finalità di raccolta e conferimento, nel rispetto del principio di liceità del trattamento, i dati personali possono essere trasferiti verso paesi situati al di fuori dell'Unione europea, alcuni dei quali potrebbero non fornire garanzie adeguate di protezione dei dati (vedere elenco completo dei Paesi che forniscono garanzie adeguate di protezione dei dati sul sito web del Garante per la Protezione dei Dati Personali https://www.garanteprivacy.it). In tali casi Studio Settanta7 farà in modo di garantire tutele appropriate per proteggere i dati personali in quei Paesi. Alcune delle tutele da adottare, ove opportuno, includono: l'utilizzo di clausole contrattuali standard approvate dalla Commissione Europea con i nostri fornitori, contratti di trasferimento infra-gruppo (in modo che possiamo trasferire in sicurezza i dati personali) e la stipula di contratti con società certificate Privacy Shield negli Stati Uniti.

19. Finalità diversa del trattamento

Qualora **Studio Settanta7** intendesse trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento dovrà fornire all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

Soggetto Responsabile

Il **Referente Privacy** informerà il **Coordinatore Privacy** della necessità dell'ulteriore trattamento. Il Coordinatore Privacy avrà il compito di provvedere a sottoporre all'interessato l'informativa. Se del caso, il **Coordinatore Privacy** predisporrà l'acquisizione del consenso dei soggetti interessati per quello specifico trattamento e sarà cura del **Referente Privacy** ottenerlo regolarmente dall'interessato.

20. Provenienza e tempo di conservazione dei dati personali

L'interessato ha il diritto di conoscere le finalità del trattamento, le categorie di dati personali in questione, la base giuridica che rende lecito il trattamento stesso e, qualora i dati non siano stati raccolti presso di lui, tutte le informazioni disponibili sulla loro origine. Inoltre, ha il diritto di conoscere la natura obbligatoria o facoltativa del conferimento dei suoi dati personali e l'eventuale conseguenza del suo rifiuto a rispondere alla richiesta di conferimento.

Studio Settanta7 conserva i dati personali solo per il tempo necessario a raggiungere gli scopi per i quali i medesimi dati sono stati raccolti, anche al fine di soddisfare eventuali requisiti legali, contabili o di segnalazione, identificando sempre, quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo. Spetta al Referente che intende attivare un trattamento di dati personali stabilire, con la collaborazione del Coordinatore Privacy, le finalità e le modalità del trattamento per conto del Titolare del trattamento e determinare con il medesimo i tempi o la logica di conservazione prevista.

21. Profilazione

Per profilazione si intende qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo degli stessi per valutare determinate caratteristiche esclusive riconducibili alla sfera personale relativa ad una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Ogni necessità di profilazione deve essere valutata in funzione dell'impatto sui diritti e le libertà dei soggetti interessati.

Decisioni automatizzate

Nessun soggetto interessato deve essere sottoposto ad una qualunque decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che possa produrre effetti in grado di incidere in modo significativo sulla sua persona.

Soggetto Responsabile:

Il Coordinatore Privacy ha il compito di valutare, con il Titolare, l'opportunità di procedere alla profilazione.

22. Marketing diretto e comunicazioni indesiderate

Le attività di marketing diretto devono svolgersi nel rispetto di qualsivoglia legge in materia comprese quelle sulla protezione dei dati personali.

In particolare, le attività devono essere svolte nel rispetto del Titolo X del D.lgs. 196/2003 (modificato dal D.lgs. 101/2018) e delle linee guida della direttiva CE 2002/58.

L'uso di sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi automatici di chiamata), del telefax o della posta elettronica a fini di commercializzazione diretta è consentito soltanto nei confronti di soggetti che abbiano espresso preliminarmente il loro consenso.

Attenzione!	**Studio Settanta7** può utilizzare le coordinate elettroniche di un cliente, acquisite nel contesto dello svolgimento della propria attività, a scopi di commercializzazione diretta di propri analoghi prodotti o servizi a condizione che al cliente sia stata offerta (attraverso idonea informativa ai sensi dell'art. 13 GDPR) in modo chiaro e distinto, al momento della raccolta dei dati e ad ogni messaggio inviato, la possibilità di opporsi gratuitamente e in maniera agevole all'utilizzo dell'indirizzo di posta elettronica per tale finalità, sempre che il cliente non abbia già rifiutato inizialmente il servizio.

Studio Settanta7 stabilisce quanto segue:

a. l'invio di comunicazioni non deve essere invasivo;
b. nell'ottica del miglioramento continuo deve essere monitorato il numero delle cancellazioni al fine di determinarne le cause (es. informazioni inutili, invii troppo numerosi, ecc.);
c. nel caso si richieda la compilazione di un sondaggio elettronico sulle ragioni della cancellazione, questo non deve essere obbligatorio al fine di ottenerla;
d. bisogna informare in modo chiaro e trasparente il soggetto destinatario, in merito alla politica e alla logica utilizzata per l'invio, riportando sempre nei moduli di richiesta di consenso il numero approssimativo delle comunicazioni inviate e la cadenza temporale, in modo diversificato a seconda dello strumento di comunicazione utilizzato;
e. le campagne di invio di qualunque genere che coinvolgono strumenti di comunicazione quali Telefax, SMS, MMS o similari, devono essere autorizzate in modo specifico dal Coordinatore Privacy;
f. tutti i contenuti delle comunicazioni inviate via mail, devono essere sottoposte a scansione antivirus/malware.

23. Anonimizzazione dei dati

In alcune circostanze potremmo rendere anonimi i dati personali, cosicché non potranno più essere associati al soggetto interessato; in tali casi sarà possibile utilizzare detti dati senza ulteriore avviso nei confronti delle parti interessate e potranno essere conservati per un tempo indeterminato.

24. Diritti che Studio Settanta7 deve garantire alle parti interessate

Tutti i trattamenti di dati personali devono essere effettuati garantendo in ogni momento, al soggetto interessato, la possibilità di esercitare i suoi diritti, con particolare attenzione alla rettifica, alla cancellazione, alla limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, nelle modalità di seguito indicate:

Diritto di accesso (art. 15 GDPR)	L'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle informazioni di cui all'art. 15 del Regolamento. Qualora i dati personali siano trasferiti ad un paese terzo, l'interessato ha, inoltre, diritto di essere informato dell'esistenza di garanzie adeguate relative al trasferimento ai sensi dell'art. 46 del Regolamento.
Diritto di rettifica (art. 16 GDPR)	L'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
Diritto alla cancellazione (art. 17 GDPR)	L'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali quando: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'art. 6, paragrafo 1, lett. a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'art. 21, paragrafo 1 del Regolamento e non sussiste alcun motivo legittimo prevalente per procedere

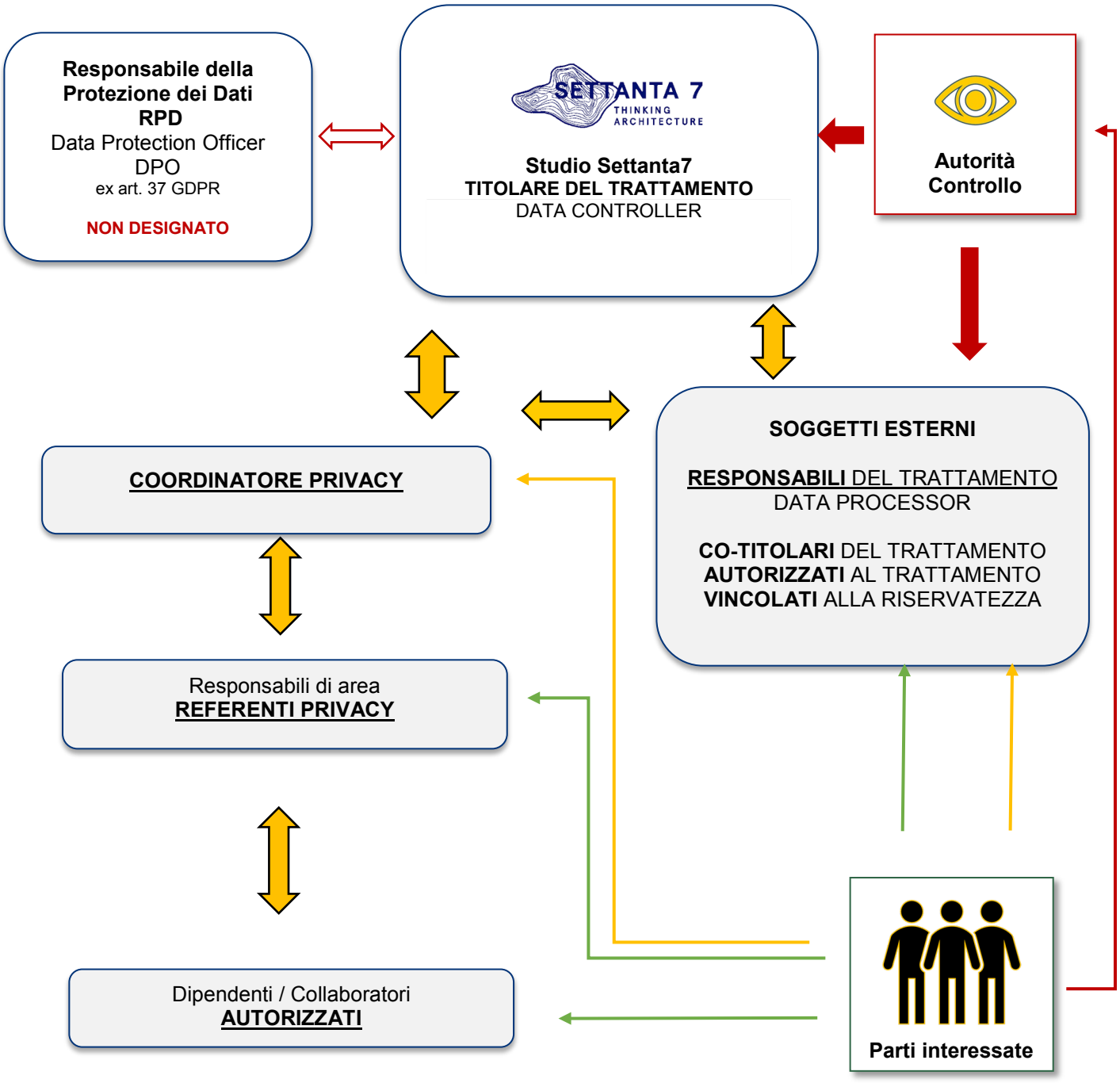
	al trattamento oppure si oppone al trattamento ai sensi dell'art. 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento; f) [*lettera omessa in quanto non applicabile ai trattamenti di dati effettuati da Studio Settanta7*]
Diritto di limitazione di trattamento (art. 18 GDPR)	L'interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi: a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; c) benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si è opposto al trattamento ai sensi dell'art. 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.
Obbligo di notifica (art. 19 GDPR)	Il Titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il Titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.
Diritto alla portabilità dei dati (art. 20 GDPR)	L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti.
Diritto di opposizione (art. 21 GDPR)	L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'art. 6, paragrafo 1, lettera f), compresa la profilazione. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
Diritto di proporre reclamo all'Autorità (art.77 GDPR)	Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il Regolamento ha il diritto di proporre reclamo dinanzi all'Autorità amministrativa indipendente competente nello Stato Membro dell'Unione europea dove risiede abitualmente, dove lavora ovvero dove si è verificata la presunta violazione.
Diritto al risarcimento (art.82 GDPR)	Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento.

Elenco dei diritti da garantire al soggetto interessato		
	Garante per la protezione dei dati personali	**Modulistica per l'esercizio dei diritti**

Centralino: Indirizzo +39 06.696771 e-mail: garante@gpdp.it Indirizzo protocollo@pec.gpdp.it PEC: https://www.garanteprivacy.it Sito Web:	Per esercitare i suoi diritti verso **Studio Settanta7**, l'interessato deve identificarsi (autenticarsi) e deve utilizzare il seguente modulo MOD-SGDP-01_Istanza di esercizio dei diritti degli interessati, anche reperibile attraverso il seguente link **https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924**

Soggetto Responsabile:
La gestione dell'esercizio dei diritti dell'interessato, all'interno di **Studio Settanta7**, avverrà secondo quanto stabilito nell'apposita procedura operativa (PR-SGDP-01_Procedura per la risposta alle istanze di esercizio dei diritti degli interessati); tale procedura riporta i soggetti responsabili e le istruzioni a loro impartite.

25. Gestione dei diritti e rapporti con le parti interessate e l'autorità di controllo



icona	Natura della richiesta
	Normale rapporto di trattamento ed esercizio diritti. L'interessato richiede operazioni ordinarie a garanzia dei suoi diritti o chiarimenti su specifici trattamenti a cui può tranquillamente rispondere l'autorizzato al trattamento. Vengono considerate richieste ordinarie: a. ottenere l'accesso ai dati personali attraverso i sistemi elettronici preposti allo scopo; b. ottenere la rettifica dei dati personali inesatti che riguardano l'interessato senza ingiustificato ritardo; c. ottenere l'integrazione dei dati personali incompleti, fornendo una dichiarazione integrativa; d. revocare il consenso ad uno specifico trattamento attraverso un sistema automatizzato; e. ottenere la cancellazione di specifici dati personali, se tale operazione rientra nell'ambito di attività/compiti del soggetto Autorizzato; f. ottenere tutte le informazioni presenti nell'informativa del trattamento. **Soggetto Responsabile:** Il **Referente Privacy** è responsabile della corretta gestione delle richieste di esercizio dei diritti dell'interessato nella propria area di competenza. Fatto salvo quanto stabilito nella procedura per l'esercizio dei diritti dell'interessato (PR-SGDP-01_Procedura per la risposta alle istanze di esercizio dei diritti degli interessati), tutte le richieste straordinarie o non pertinenti alla propria gestione devono essere immediatamente dirottate al **Coordinatore Privacy**.
	Reclamo - Esercizio dei diritti – Chiarimenti L'interessato richiede operazioni straordinarie a garanzia dei suoi diritti e/o richiede chiarimenti su specifici trattamenti che coinvolgono più aree di competenza, a cui per rispondere è necessario un coordinamento più ampio tra le aree interessate e/o l'intervento del Titolare del Trattamento. Tutte le richieste sopra citate devono essere gestite nel rispetto dell'apposita procedura (PR-SGDP-01_Procedura per la risposta alle istanze di esercizio dei diritti degli interessati). Su questo punto si precisa che è considerata richiesta straordinaria: a. ottenere la conferma che sia o meno in corso, da parte nostra, un trattamento di dati personali che riguarda l'interessato e in tal caso, ottenere l'accesso ai dati personali trattati; b. ricevere in un formato strutturato, se il trattamento è effettuato con mezzi elettronici, di uso comune e leggibile da dispositivo automatico, i dati personali che riguardano l'interessato; c. trasmettere dati a un altro titolare del trattamento senza impedimenti da parte nostra; d. opporsi al trattamento dei dati personali basato su di un nostro legittimo interesse; e. revocare il consenso ad uno specifico trattamento attraverso una procedura manuale cartacea; f. ottenere la cancellazione dei propri dati personali ai sensi dell'art. 17 del GDPR; g. ottenere la limitazione del trattamento dei dati personali ai sensi dell'art.18 del GDPR; h. ottenere la comunicazione da parte nostra agli altri soggetti Titolari della richiesta di esercizio dei diritti da parte dell'interessato ai sensi dell'art.19 del GDPR (es. Oblio); i. ottenere maggiori informazioni rispetto a quelle comunicate o presenti nell'informativa. **Soggetto Responsabile:** Il **Coordinatore Privacy** è responsabile della corretta gestione delle richieste di esercizio straordinario dei diritti, degli ulteriori chiarimenti e dei reclami dell'interessato.
	Reclamo - Violazione dei diritti e delle libertà fondamentali L'interessato presenta all'Autorità di controllo un reclamo di qualunque tipo sulla correttezza, trasparenza o liceità di un qualsivoglia trattamento effettuato da noi.

	Soggetto Responsabile: Il **Delegato del Titolare** è responsabile della corretta gestione dei rapporti con l'autorità di controllo.

26. Registro dei trattamenti

Come specificato nelle FAQ del Garante per la protezione dei dati personali (8 ottobre 2018), sono tenuti a redigere il Registro le imprese o le organizzazioni con almeno 250 dipendenti e - al di sotto dei 250 dipendenti - qualunque titolare o responsabile che effettui trattamenti che possano presentare rischi, anche non elevati, per i diritti e le libertà delle persone o che effettui trattamenti non occasionali di dati oppure trattamenti di particolari categorie di dati (come i dati biometrici, dati genetici, quelli sulla salute, sulle convinzioni religiose, sull'origine etnica etc.), o anche di dati relativi a condanne penali e a reati. Nelle FAQ vengono indicate, tra l'altro, quali informazioni deve contenere il Registro e le modalità per la sua conservazione e il suo aggiornamento.

Il registro deve essere tenuto in forma scritta oppure in formato elettronico, e va esibito all'autorità di controllo (Garante) in caso di verifiche.

Il Registro dei titolari del trattamento deve elencare almeno queste informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, se nominati, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati (DPO);
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie dei dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o di Studio Settanta7 internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49 del GDPR, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, paragrafo 1 del GDPR.

Soggetto Responsabile:
La funzione preposta alla conservazione e alla compilazione del registro è il **Coordinatore Privacy.** Il registro deve essere conservato con diligenza e cura e può essere richiesto in sede ispettiva dall'Autorità di controllo.

27. Valutazione d'impatto sulla protezione dei dati – DPIA (Data Protection Impact Assessment)

È una procedura prevista dall'articolo 35 del Regolamento che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.
È obbligatorio redigere una DPIA in tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
In particolare, è obbligatorio condurre una DPIA per:

- trattamenti valutativi o di scoring, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);

- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è obbligatoria in presenza di almeno due di questi criteri, ma tenendo conto delle circostanze, il **Delegato del Titolare,** anche su richiesta del **Coordinatore Privacy**, può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta **Studio Settanta7** non soltanto a rispettare le prescrizioni del GDPR, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali. Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria.

Studio Settanta7 attualmente non effettua trattamenti che necessitano di una valutazione di impatto sulla protezione dei dati ma, qualora fosse necessario redigere una DPIA, si riserva di adottare le linee guida WP248rev.1 "Linee-guida concernenti la valutazione di impatto sulla protezione dei dati, nonché i criteri per stabilire se un trattamento possa presentare un rischio elevato ai sensi del regolamento 2016/679".
La CNIL, l'Autorità francese per la protezione dei dati, ha messo a disposizione un software di ausilio ai titolari, in vista della effettuazione della valutazione d'impatto sulla protezione dei dati (DPIA). La versione in italiano è stata messa a punto anche con la collaborazione del Garante per la protezione dei dati personali: https://www.garanteprivacy.it/regolamentoue/DPIA. Studio Settanta7, se del caso, utilizzerà tale software per condurre la DPIA.

Soggetto Responsabile:
Il **Coordinatore Privacy** informerà il **Delegato del Titolare** sulla necessità di svolgere una DPIA.

28. Sicurezza e Conformità

Conformità all'Art. 24 GDPR
Studio Settanta7 tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, ha l'obbligo di mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento UE 2016/679. Dette misure sono riesaminate e aggiornate qualora necessario. Esse includono, inoltre, l'attuazione di politiche e procedure operative adeguate in materia di protezione dei dati, in grado di garantire che siano trattati per impostazione predefinita 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. Tutti i trattamenti sono censiti e registrati nel Registro delle attività di trattamento, redatto anche ai sensi dell'art.30 del GDPR. Studio Settanta7 adotta, inoltre, una specifica politica di sicurezza sull'utilizzo degli strumenti informatici contenente le istruzioni per l'utilizzo corretto delle risorse informatiche in dotazione e le informazioni sui controlli di sicurezza applicati ad ogni singolo strumento.

Conformità all'Art. 25 GDPR
Tutti i sistemi informatici adibiti al trattamento dei dati personali devono essere progettati sin dall'inizio tenendo conto della sicurezza dei trattamenti per impostazione predefinita (Privacy e Security by Design). Tutte le configurazioni predefinite devono essere cambiate in configurazioni iniziali sicure in modo da ottenere impostazioni predefinite in grado di privilegiare sempre la privacy e la Security, anche a scapito di una condizione di maggiore produttività (Privacy e Security by Default). È compito del progettista o dell'installatore dei sistemi fornire sempre una relazione progettuale che dimostri che si è tenuto conto di questi principi fin dalla progettazione del sistema installato.

Conformità all'Art. 32 GDPR
Fatto salvo quanto stabilito per la compliance all'art. 25 del GDPR, tutti i sistemi informatici che trattano dati personali o informazioni critiche devono essere dotati di tecnologie di sicurezza in grado di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni trattate. Tali sistemi di protezione devono essere

dotati di idonei sistemi di registrazione eventi (LOG) in grado di consentire a Studio Settanta7 di dimostrare l'efficacia delle misure di sicurezza, il rispetto delle politiche di sicurezza e il corretto operato degli Amministratori di Sistema. Tutte le tecnologie di sicurezza devono essere scelte tra le migliori presenti sul mercato e particolare attenzione va posta ai software di protezione da virus, malware, ecc. che verranno installati sui Server e sugli Endpoint; questi ultimi devono essere valutati in base ai test effettuati da laboratori indipendenti certificati, ad esempio: https://selabs.uk/ per i prodotti Endpoint Security (specifiche AMTSO). I report dei test che ne provano l'efficacia vanno salvati e allegati alla documentazione tecnica. Anche i sistemi di backup, Gestione Vulnerabilità, Gestione Log e i firewall perimetrali devono garantire adeguati livelli di sicurezza dimostrabili attraverso certificazioni o report tecnici.

29. Rischio

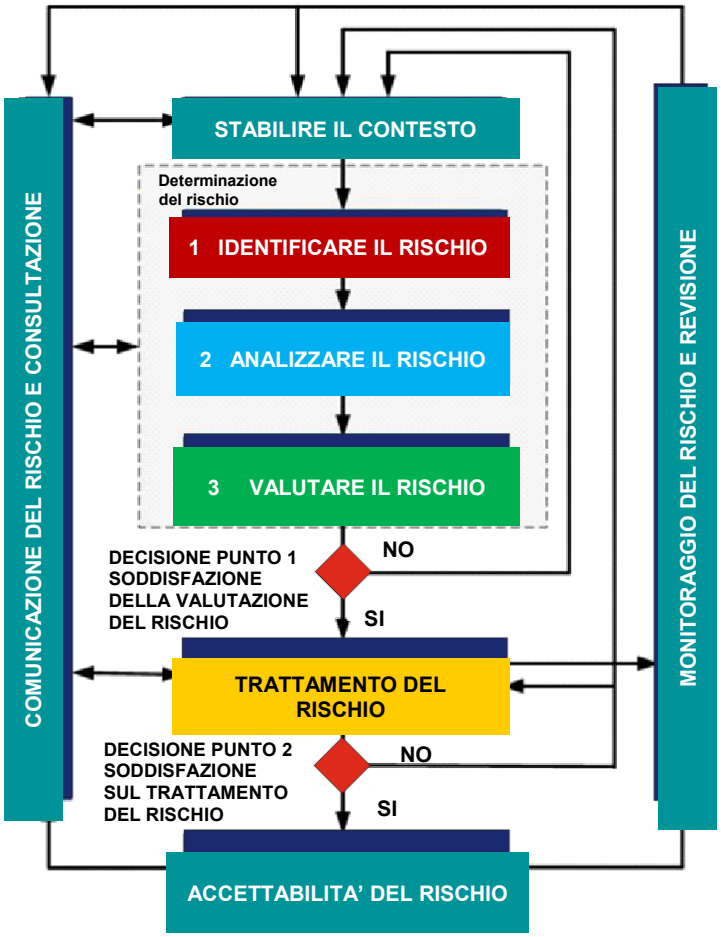
In materia di protezione dei dati personali per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità, per i diritti e le libertà.
Al fine di una corretta gestione del rischio **Studio Settanta7** adotta le apposite Linee guida del Gruppo di lavoro Articolo 29 WP248rev.1.

30. Analisi e valutazione del rischio

L'analisi del rischio si applica a tutti i sistemi, processi e servizi in ambito IT, utilizzati e/o erogati da **Studio Settanta7** che sono coinvolti in qualsivoglia trattamento di dati personali.

Descrizione del processo di analisi

L' analisi viene condotta valutando il livello di impatto sulla libertà, dignità e diritti del soggetto interessato, analizzando le dimensioni della **r**iservatezza (divulgazione, accesso), **i**ntegrità (alterazione) e **d**isponibilità (distruzione, indisponibilità, perdita) dei dati personali, seguendo i seguenti passi fondamentali:



Elementi da considerare nella valutazione del rischio privacy

La valutazione del rischio deve riguardare non solo la sicurezza del trattamento ma anche gli effetti complessivi del trattamento.

Errori da evitare:

- non bisogna confondere la gestione dei rischi con il tema delle misure di sicurezza;
- il rischio non si riferisce al titolare ma al soggetto interessato.

La valutazione del rischio si compone di tre processi principali:

1. **Identificazione dei rischi**
2. **Analisi dei rischi**, consiste nel valutare tutti gli aspetti del tipo:
   - parti interessate coinvolte e possibili impatti;
   - valutazione di adeguatezza dei controlli già presenti (analisi delle contromisure già implementate e gestite);
   - impatti, possibili conseguenze e relativi costi (impatti di tipo operativo, di compliance sulle norme e sui regolamenti vigenti e sulla continuità di servizio);
   - probabilità che un evento (cioè che una minaccia riesca a sfruttare una vulnerabilità) si realizzi.
3. **Valutazione dei rischi,** viene calcolata moltiplicando gli impatti per le probabilità che l'evento si realizzi. Questa operazione restituisce un valore numerico che sarà usato per classificare il rischio.

31. Valutazione della Gravità o Impatto

La valutazione della gravità del rischio va calcolata tenendo conto delle conseguenze del rischio sull'organizzazione (impatto sull'organizzazione) e le conseguenze del rischio sui soggetti interessati (impatto sugli interessati).

Impatto sull'organizzazione:

Va valutato tenendo conto dei seguenti effetti complessivi:

a. perdita di controllo sui servizi e conseguenze in termini di efficacia, efficienza o continuità di servizio dell'organizzazione;
b. perdita della capacità di raggiungere gli obiettivi di servizio dell'organizzazione;
c. perdita di capacità operativa del personale.

Impatto sugli interessati:

Va valutato in funzione delle conseguenze a cui potrebbero andare incontro gli individui e la loro capacità di superarle, tenendo conto dei seguenti effetti complessivi del trattamento:

a. danno per la reputazione;
b. discriminazione;
c. furto d'identità;
d. perdite finanziarie;
e. danni fisici o psicologici;
f. perdita di controllo dei dati;
g. altri svantaggi economici o sociali;
h. impossibilità di esercitare diritti, servizi o opportunità.

Attenzione!

Non bisogna confondere la valutazione dell'impatto del rischio sull'interessato con il tema della valutazione d'impatto sulla protezione dei dati DPIA di cui al punto 27.

Se la valutazione dell'impatto del rischio sull'organizzazione e la valutazione dell'impatto del rischio sull'interessato producono risultati qualitativamente diversi, al fine della classificazione del rischio, bisogna prendere in considerazione il valore qualitativo peggiore.

Punteggio	Impatto	Descrizione
1	Basso	**Impatto sull'organizzazione:** ▪ perdita di controllo assente o trascurabile su una singola parte del servizio, con conseguenze trascurabili in termini di efficacia, efficienza o continuità di servizio dell'organizzazione; ▪ perdita assente o trascurabile della capacità di raggiungere gli obiettivi di servizio dell'organizzazione; ▪ perdita assente o trascurabile di capacità operativa del personale; ▪ improbabili richieste di danni da parte degli interessati per le conseguenze del mancato rispetto delle norme sulla privacy; ▪ improbabili sanzioni da parte delle autorità di controllo per la violazione delle leggi sul trattamento dei dati personali o altri requisiti cogenti.
		Impatto sugli interessati: Gli individui possono andare incontro a disagi minimi, superabili senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
2	Medio	**Impatto sull'organizzazione:** ▪ moderata perdita di controllo su parti del servizio, con limitate conseguenze in termini di efficacia, efficienza o continuità di servizio dell'organizzazione; ▪ moderata perdita della capacità di raggiungere gli obiettivi di servizio dell'organizzazione; ▪ moderata perdita di capacità operativa del personale; ▪ poco probabili richieste di danni da parte degli interessati per le conseguenze del mancato rispetto delle norme sulla privacy; ▪ poco probabili e/o modeste sanzioni da parte delle autorità di controllo per la violazione delle leggi sul trattamento dei dati personali o altri requisiti cogenti.
		Impatto sugli interessati: Gli individui possono andare incontro a significativi disagi, superabili nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
3	Alto	**Impatto sull'organizzazione:** ▪ notevoli conseguenze sulla capacità del servizio di raggiungere risultati in termini di efficacia, efficienza o continuità di servizio dell'organizzazione; ▪ significativa perdita della capacità di raggiungere gli obiettivi di business o di servizio dell'organizzazione; ▪ significativa perdita di capacità operativa del personale; ▪ penali applicate dal cliente per mancato rispetto delle SLA o dei termini contrattuali; ▪ probabili richieste di danni da parte degli interessati per le conseguenze del mancato rispetto delle norme sulla privacy; ▪ probabili e/o elevate sanzioni da parte delle autorità di controllo per la violazione delle leggi sul trattamento dei dati personali o altri requisiti cogenti.
		Impatto sugli interessati: Gli individui possono andare incontro a conseguenze significative, probabilmente superabili, anche se con gravi difficoltà, (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).

Punteggio	Impatto	Descrizione
4	Molto Alto	**Impatto sull'organizzazione:** ▪ perdita di controllo del servizio con gravi conseguenze sul raggiungimento dei risultati in termini di efficacia, efficienza o continuità di servizio dell'organizzazione; ▪ grave perdita della capacità di raggiungere gli obiettivi di servizio dell'organizzazione; ▪ grave perdita di capacità operativa del personale; ▪ Elevate richieste di danni da parte degli interessati per le conseguenze del mancato rispetto delle norme sulla privacy; ▪ elevate sanzioni da parte delle autorità di controllo per la violazione delle leggi sul trattamento dei dati personali o altri requisiti cogenti; ▪ gravi o ripetute penali applicate dal cliente per mancato rispetto delle SLA o termini contrattuali.
		Impatto sugli interessati: Gli individui possono subire conseguenze gravi o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Classificazione Probabilità

La probabilità di accadimento è definita dalla seguente tabella:

Punteggio	Probabilità	Descrizione
1	Improbabile	Quando si ritiene che il controllo in atto sia efficace e l'evento non si è mai verificato.
2	Poco Probabile	Quando si ritiene che il controllo in atto sia sufficientemente robusto e comunque l'evento non si è mai verificato.
3	Probabile	Quando si ritiene che il controllo non sia sufficientemente robusto e/o l'evento si è verificato sporadicamente in passato.
4	Frequente	Quando si ritiene che il controllo sia assente o palesemente inefficace, e/o l'evento si è verificato frequentemente.

Classificazione dei rischi

La classificazione dei rischi è definita dalla seguente matrice:

Probabilità → **Impatto ↓**	**Improbabile (1)**	**Poco Probabile (2)**	**Probabile (3)**	**Frequente (4)**
Basso (1)	**Trascurabile (1)**	**Basso (2)**	**Basso (3)**	**Medio (4)**
Medio (2)	**Basso (2)**	**Medio (4)**	**Medio (6)**	**Medio (8)**
Alto (3)	**Basso (3)**	**Medio (6)**	**Alto (9)**	**Alto (12)**
Molto Alto (4)	**Medio (4)**	**Medio (8)**	**Alto (12)**	**Critico (16)**

Classi di rischio

La classe di rischio determina l'accettabilità del rischio in funzione della seguente tabella:

Punteggio	Esposizione	Gestione azione di controllo (MCA)
1	**Trascurabile**	Rischio che non richiede alcun controllo o misure aggiuntiva in quanto non ha nessun impatto sul soggetto interessato.

Punteggio	Esposizione	Gestione azione di controllo (MCA)
2-3	Basso	Rischio che rientra nei parametri accettabili di servizio e continuità di servizio; in questo caso le misure ed i controlli implementati sono ritenuti sufficienti a contenere gli impatti sull'interessato in un ambito accettabile e facilmente superabile. Non ci sono presupposti per la richiesta di risarcimento danni ai sensi dell'art. 82 del GDPR; non ci sono rischi oggettivi di sanzioni.
4-8	Medio	Il Rischio deve essere gestito perché costituisce un punto di criticità; può essere mitigato estendendo il campo di applicazione delle misure e controlli esistenti, oppure può essere trasferito. In ogni caso il monitoraggio e le revisioni del rischio devono tener conto di questo livello. Gli impatti sul soggetto interessato possono essere superati con alcune difficoltà. Esistono i presupposti per la richiesta di risarcimento danni ai sensi dell'art. 82 del GDPR anche se circoscritta ad un numero di soggetti limitato; il rischio di sanzioni è di lieve entità.
9 to 12	Alto	Il Rischio può compromettere la continuità di servizio e i rapporti con i clienti e gli individui, si possono avere ricadute sui vincoli contrattuali, legislativi e normativi; per tali motivi il rischio deve essere mitigato con controlli e misure esistenti o introdotte ad hoc. Deve essere stabilito un piano del trattamento del rischio dove indicare tempi, modi e risorse per mitigarlo. Gli impatti sul soggetto interessato possono essere superati con molte difficoltà. Sono probabili le richieste di risarcimento danni ai sensi dell'art. 82 del GDPR da parte di un numero considerevole di soggetti; le sanzioni sono probabili e possono essere molto elevate.
13 to 16	**Critico**	Il Rischio può distruggere i servizi e le informazioni ed avere un impatto non sostenibile dall'organizzazione; per tali motivi il rischio deve essere mitigato ed il piano del trattamento deve avere priorità su tutte le altre attività. Gli impatti sul soggetto interessato non possono essere superati se non con enormi difficoltà. Sono certe le richieste di risarcimento danni ai sensi dell'art. 82 del GDPR da parte di un numero considerevole di soggetti; le sanzioni sono certe e possono essere elevatissime.

Soggetto Responsabile:
Il **Coordinatore Privacy,** avvalendosi della collaborazione dei **Referenti Privacy** e degli **AdS**, è la funzione preposta all'analisi dei rischi.

32. Trattamento del rischio e Accountability

L'organizzazione adotta le seguenti misure per il trattamento del rischio e la gestione dell'accountability.

Misure Generali:	Misure Tecnologiche:	Misure Organizzative:
Gestione della Qualità dei dati, conservazione adeguata, pseudonimizzazione dei dati, anonimizzazione dei dati, minimizzazione dei dati.	Policy di sicurezza logiche e fisiche, aggiornamenti servizi e software, test, controllo accessi e tracciamento operazioni, cifratura dei dati.	Ruoli, governance, istruzioni, formazione, procedure, audit, strumenti di controllo per gli interessati, contatti.

Soggetto Responsabile:
Il **Delegato del Titolare**, con la collaborazione del **Coordinatore Privacy,** stabilisce e adotta le misure generali, tecnologiche e organizzative necessarie alla corretta gestione e mitigazione del rischio in conformità a quanto previsto dal Regolamento.

33. Scelta dell'adeguato livello di sicurezza dei sistemi informativi

Basandosi sulle linee guida dettate dall' *Agenzia per l'Italia Digitale* (AGID) in merito all'attuazione della Direttiva UE 2016/1148 (*Network Information Security),* **Studio Settanta7** adotta un insieme ordinato e ragionato di

"controlli", ossia azioni puntuali di natura tecnica od organizzativa, predisposto al fine di fornire un riferimento pratico per valutare e innalzare il livello di sicurezza informatica di Studio Settanta7. Tali controlli sono a loro volta ispirati dalle norme ISO27001 (sicurezza delle informazioni) e dalle norme americane NIST (*National Institute of Standard and Technology*). I controlli da verificare sono stati mappati con le specifiche del Framework Nazionale sulla Sicurezza Cibernetica.
Il livello di adozione dei controlli è graduato rispetto ai seguenti livelli di maturità:

M - **minimo,** ovvero il livello al di sotto del quale il rischio è ritenuto inaccettabile;
S - **standard,** ovvero il livello ottimale verso cui Studio Settanta7 dovrebbe tendere;
A - **alto,** ovvero il livello da raggiungere per il trattamento dei dati personali più critici.

Le misure previste nei controlli sono state selezionate dalle seguenti 8 categorie:

1. inventario dei dispositivi autorizzati e non autorizzati;
2. inventario del software autorizzato e non autorizzato;
3. configurazione sicura di hardware e software;
4. adozione di un processo di gestione delle vulnerabilità;
5. utilizzo controllato dei privilegi amministrativi;
6. adozione di difese contro i programmi malware;
7. capacità di recuperare l'operatività in caso di incidente, (Business Continuity);
8. protezione generale dei dati personali e delle informazioni critiche.

34. Controlli di sicurezza e livello di Maturità

In riferimento al modello AGID descritto precedentemente, **Studio Settanta7** dopo una attenta analisi dei trattamenti di dati personali effettuati e tenuto conto delle leggi e delle ragionevoli aspettative delle parti interessate coinvolte, ha stabilito che l'obiettivo di sicurezza e il relativo livello di controlli applicato, è quello **STANDARD**, anche se, per alcuni trattamenti specifici, potranno essere adottati controlli di sicurezza appartenenti al livello di maturità **ALTO.**
Studio Settanta7 non effettua trattamenti di dati personali particolarmente rischiosi. Le categorie particolari di dati trattati sono esclusivamente quelli dei propri dipendenti, quindi certi nella quantità e comunque numericamente non rilevanti rispetto al concetto di larga scala evidenziato dal Gruppo di lavoro ex articolo 29 - European Data Protection Supervisor 16/EN(IT) nelle Linee Guida WP 243- *Orientamenti in materia di Data Protection Officers* (DPO).
Tenuto conto dei rischi e dell'analisi effettuata sulle parti interessate, in particolar modo su dipendenti e clienti, non si sono rilevate particolari situazioni critiche. **Studio Settanta7** non si ritiene un obiettivo particolarmente sensibile ad attacchi informatici mirati, pertanto intende adottare un modello di sicurezza Standard, in grado di proteggerla da tutte le minacce "automatiche", cioè dagli attacchi portati in larga scala attraverso internet, e dalle altre tecnologie comunemente utilizzate. Studio Settanta, anche alla luce dei risultati dell'analisi dei rischi cibernetici effettuata, ritiene che questo modello di sicurezza possa rispondere adeguatamente alle proprie esigenze; tale modello di sicurezza innalza notevolmente il costo da sostenere per portare un attacco mirato alle infrastrutture informatiche di Studio Settanta7.
I controlli applicati, e le modalità di applicazione di ogni singolo controllo, sono elencati nel seguente documento: PO-SGDP-03_Punti di controllo per la sicurezza IT
Il documento è approvato dal **Delegato del Titolare** e revisionato almeno una volta all'anno.

Soggetto Responsabile:
Il **Coordinatore Privacy,** avvalendosi della collaborazione del Responsabile IT e degli AdS, è la funzione preposta all'applicazione dei controlli di sicurezza stabiliti dal Titolare del trattamento.

35. Violazione dei dati personali

Ogni violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati viene analizzata, documentata e gestita anche ai sensi di quanto previsto dell'art. 33 del GDPR. Per questi motivi **Studio Settanta7** si è dotata di un Registro delle violazioni, costantemente aggiornato, a cura del Coordinatore Privacy (con l'aiuto degli AdS) in cui viene documentata qualsiasi violazione riguardante i dati personali trattati, comprese le circostanze, le conseguenze e i provvedimenti adottati per porvi rimedio. Per ovvie ragioni di sicurezza il registro non deve essere messo a disposizione di nessun soggetto interessato ma può essere consegnato solamente all'Autorità di Controllo.
Le violazioni di dati personali sono identificate attraverso i seguenti tre principi:

Violazione della riservatezza	Violazione dell'integrità	Violazione della disponibilità
Quando vi è una divulgazione o un accesso non autorizzato o accidentale ai dati personali.	Quando vi è un'alterazione non autorizzata o accidentale dei dati personali.	Quando vi è l'impossibilità di accedere ai dati personali o è avvenuta, anche accidentalmente, la loro distruzione.

A seconda delle circostanze, è possibile che ogni singola violazione possa riguardare uno o più principi contemporaneamente.
A meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà dell'interessato, Studio Settanta7 procederà, senza ingiustificato ritardo, a notificare al Garante per la protezione dei dati personali le eventuali violazioni di dati subite entro 72 ore dal momento in cui ne è venuto a conoscenza.
Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà del soggetto interessato, Studio Settanta7 comunicherà a tale soggetto l'avvenuta violazione senza ingiustificato ritardo; ciò non è necessario qualora siano state applicate ai dati personali, oggetto della violazione, misure adeguate di protezione destinate a rendere i dati incomprensibili, come ad esempio la cifratura, o qualora **Studio Settanta7** fosse riuscita ad adottare, in tempo utile, misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati coinvolti.
Studio Settanta7 ha adottato un'apposita procedura di gestione del Data Breach (PR-SGDP-02_Procedura per la gestione delle violazioni di dati personali).

Soggetto Responsabile:
I soggetti responsabili sono individuati nell'apposita procedura PR-SGDP-02_Procedura per la gestione delle violazioni di dati personali.

36. Registro delle violazioni dei dati

Studio Settanta7 è tenuta a documentare ai sensi dell'art. 33 GDPR qualsiasi violazione di dati ("violazione dei dati personali") che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Il registro deve essere aggiornato costantemente e costituisce uno strumento utile, in coerenza con il principio di accountability, per dimostrare l'adeguamento al regolamento privacy europeo.
Le finalità del registro e le modalità di alimentazione dello stesso sono illustrate nelle sessioni informative e formative organizzate in modo periodico.
Il registro deve essere conservato con diligenza e cura e può essere richiesto in sede ispettiva dal Garante per la protezione dei dati personali e dalla Guardia di Finanza che, di recente, ha stipulato una specifica convenzione con il Garante per la protezione dei dati personali.

Contenuto del registro

Il registro deve riportare i seguenti campi:

a. tipologia di violazione di dati;
b. data, oggetto, contesto e descrizione della violazione;
c. categorie e numero approssimativo di interessati;
d. conseguenze (descrizioni per tipologie: danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica);
e. provvedimenti adottati per porre rimedio alle violazioni.

Soggetto Responsabile:
Il **Coordinatore Privacy** è la funzione preposta alla conservazione e alla compilazione del registro.

37. Ricezione di *curricula*

Nei casi di ricezione di *curricula* spontaneamente trasmessi dagli interessati al fine dell'instaurazione di un rapporto di lavoro, **Studio Settanta7** fornirà apposita informativa (INF-SGDP-03_Informativa per i candidati al lavoro) al momento del primo contatto utile successivo all'invio del curriculum medesimo. Nei limiti delle finalità di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei *curricula* non è dovuto.

38. Sanzioni in caso di inosservanza

Un soggetto dipendente che abbia violato le disposizioni riportate nel presente documento può essere sottoposto ad azioni disciplinari per i possibili riflessi negativi cagionati dalla sua negligenza sulla sicurezza relativa alla protezione dei dati personali. In particolare, ogni infrazione alle suddette disposizioni da parte del personale dipendente di **Studio Settanta7** costituisce grave inadempimento contrattuale, che potrà essere sanzionata secondo le norme disciplinari previste dal C.C.N.L. applicato.
Per i soggetti non dipendenti, l'eventuale inosservanza delle disposizioni contenute nel presente documento, in quanto da considerare grave inadempimento ai sensi dell'art. 1456 Codice civile, potrebbe comportare la risoluzione del rapporto di collaborazione.

39. Impegno del Titolare del Trattamento

Il **Delegato del Titolare** sostiene attivamente la sicurezza di Studio Settanta7 tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza delle informazioni.
L'impegno del Titolare si attua tramite una struttura i cui compiti sono:

a. **garantire** che siano identificati tutti gli obiettivi relativi alla sicurezza dei dati personali;
b. **stabilire** i ruoli operativi i e le responsabilità per lo sviluppo e il mantenimento del SGDP;
c. **fornire** risorse sufficienti alla pianificazione, implementazione, controllo, revisione, gestione e miglioramento continuo del SGDP;
d. **controllare** che il SGDP sia integrato in tutti i processi interni e che procedure e controlli siano sviluppati efficacemente;
e. **monitorare** i cambiamenti dell'esposizione alle minacce incombenti sui trattamenti dei dati personali e analizzare gli incidenti (alla loro sicurezza), rivedendo i criteri per l'accettazione del rischio ed i livelli di rischio accettabili;
f. **approvare** e **sostenere** tutte le iniziative volte al miglioramento della sicurezza dei dati personali trattati;
g. **attivare** programmi per la diffusione della consapevolezza e della cultura della sicurezza dei dati personali.

40. Efficienza del processo e riesame del Titolare del trattamento

Il **Delegato del Titolare** verificherà periodicamente e regolarmente, in concomitanza di cambiamenti significativi, e comunque con cadenza almeno annuale, l'efficacia e l'adeguatezza del SGDP in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della presente politica, in risposta ai cambiamenti dell'ambiente di lavoro, dell'innovazione tecnologica, del business e delle condizioni legali.

Torino, 06/06/2019
Studio Settanta7