ADVISORY 360 HUB

P4.I

# DPO 360

**DATA PROTECTION** *AS A SERVICE*

## Il servizio tech-based per garantire la compliance aziendale

ADVISORY 360 HUB

P4.I

1

# Perché nasce il nostro servizio

# Quali esigenze ci manifestano le imprese

1. Avere un'**organizzazione interna** della data protection coerente con le norme, la dimensione e il settore di business e **risorse interne** con competenze multidisciplinari

2. Avere un **sistema documentale** in grado di dimostrare la conformità alle normative in materia di privacy

3. Saper affrontare efficacemente un'eventuale **visita ispettiva** dell'autorità Garante e ridurre i **rischi sanzionatori** e i conseguenti **danni d'immagine** per l'organizzazione

4. Aumentare la **sensibilità** in azienda sulle tematiche data protection attraverso percorsi e iniziative ad hoc, favorendo la **corretta applicazione** delle relative **regole** e **procedure**

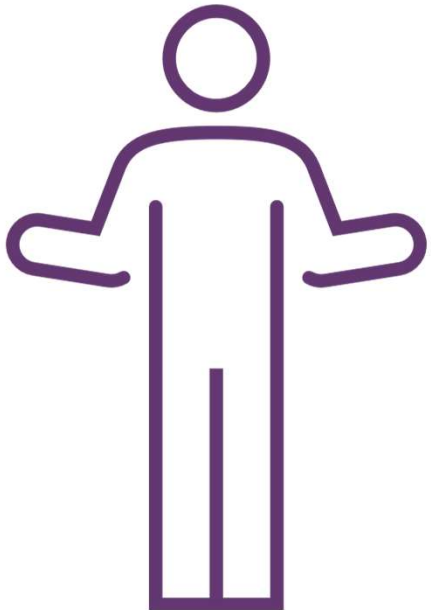
5. Contenere i **costi generali** di gestione dell'ambito data protection, riducendo l'**effort complessivo** e duplicazioni di attività

# Chi è il Data Protection Officer (DPO)

Il responsabile della protezione dei dati personali (DPO) è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679 (GDPR). Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e di controllo, consultive, formative e informative relativamente all'applicazione del GDPR.

## REQUISITI

- Conoscenza della **normativa** e delle prassi in materia di **protezione dei dati personali**
- Competenza nel progettare, verificare e mantenere un **sistema di gestione dei dati personali**
- Deve agire in piena **indipendenza e autonomia** senza ricevere istruzioni in ordine all'esecuzione dei menzionati compiti
- Deve poter disporre delle **risorse necessarie** per l'espletamento dei propri compiti



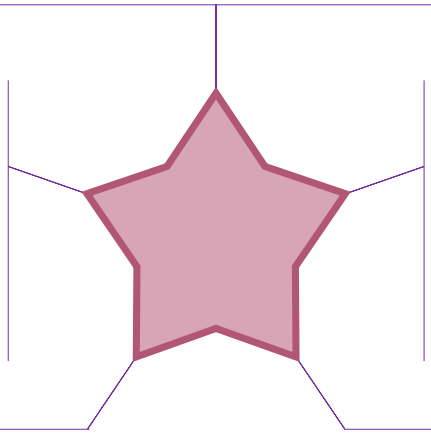
## RESPONSABILITÀ

- **Monitorare costantemente la conformità** alle normative sulla privacy dei dati
- **Gestire e documentare tutte le segnalazioni** di violazioni dei dati
- **Fornire consulenza interna** per garantire che i processi aziendali rispettino le normative sulla privacy
- **Cooperare con le autorità di controllo** in caso di indagini sulla protezione dei dati
- **Educare e formare** il personale sull'importanza della protezione dei dati

# Quali benefici porta la nomina di un DPO

**Disponibilità di un supporto tecnico-giuridico continuo:** Tale aspetto è di fondamentale importanza nell'ottica di una gestione continuativa delle attività GDPR, intesa quindi come parte integrante dell'operatività aziendale e non come sporadica attività burocratica

**Prevenzione contro sanzioni e richieste di risarcimento:** Tutto ciò grazie al miglioramento continuo dei processi interni di privacy tramite attività di pianificazione, verifica e miglioramento, svolte con regolarità e verbalizzate



**Garanzia della compliance aziendale al GDPR:** La presenza di un DPO evita che il Titolare del Trattamento trascuri, per mancanza di tempo o di competenze, le procedure per il corretto trattamento dei dati all'interno della propria attività

**Integrità e Reputazione:** Lavorando per proteggere i dati personali dei clienti e dei dipendenti, un DPO contribuisce a mantenere l'integrità dell'organizzazione e la sua reputazione nel mercato

**Punto unico di contatto con gli stakeholder:** Il DPO funge da punto di contatto tra l'organizzazione e le autorità di controllo in materia di protezione dei dati, facilitando la comunicazione ufficiale

# Perché avere un DPO esterno

**Difficoltà nella reperibilità di competenze specializzate**: Trovare un DPO interno con competenze specializzate in conformità normativa e privacy può essere una sfida.

**Complessità nell'aggiornamento normativo**: Mantenere il personale interno aggiornato sulle normative privacy è oneroso da un punto di vista economico e richiede tempo

**Gestione del conflitto di interessi**: Un DPO interno potrebbe trovarsi in una situazione di conflitto di interessi se deve fare rapporto direttamente alla direzione aziendale

**Necessità di una gestione e organizzazione autonoma**: Il DPO richiede elevata autonomia nella gestione e nell'organizzazione, e questo è difficile da garantire internamente

**Gestione di situazioni di emergenza**: In situazioni di emergenza, come una violazione dei dati, l'azienda potrebbe non avere un DPO pronto a gestire la situazione

**Vincoli di budget**: L'assunzione e la gestione di un DPO interno possono comportare costi che potrebbero superare il budget disponibile

# Perché P4I è la società giusta: il Team

Il DPO as a Service viene erogato attraverso un **team con competenze multi-disciplinare integrate** che consente di gestire qualsiasi tipologia di richiesta ed eventi

| Legali | Information & Cybersecurity | Organizzative |
|---|---|---|
| +40 Esperti di Norme, Leggi e Provvedimenti | +10 Esperti di Architettura, Sistemi e Sicurezza | +15 Esperti di Organizzazione e Processi |

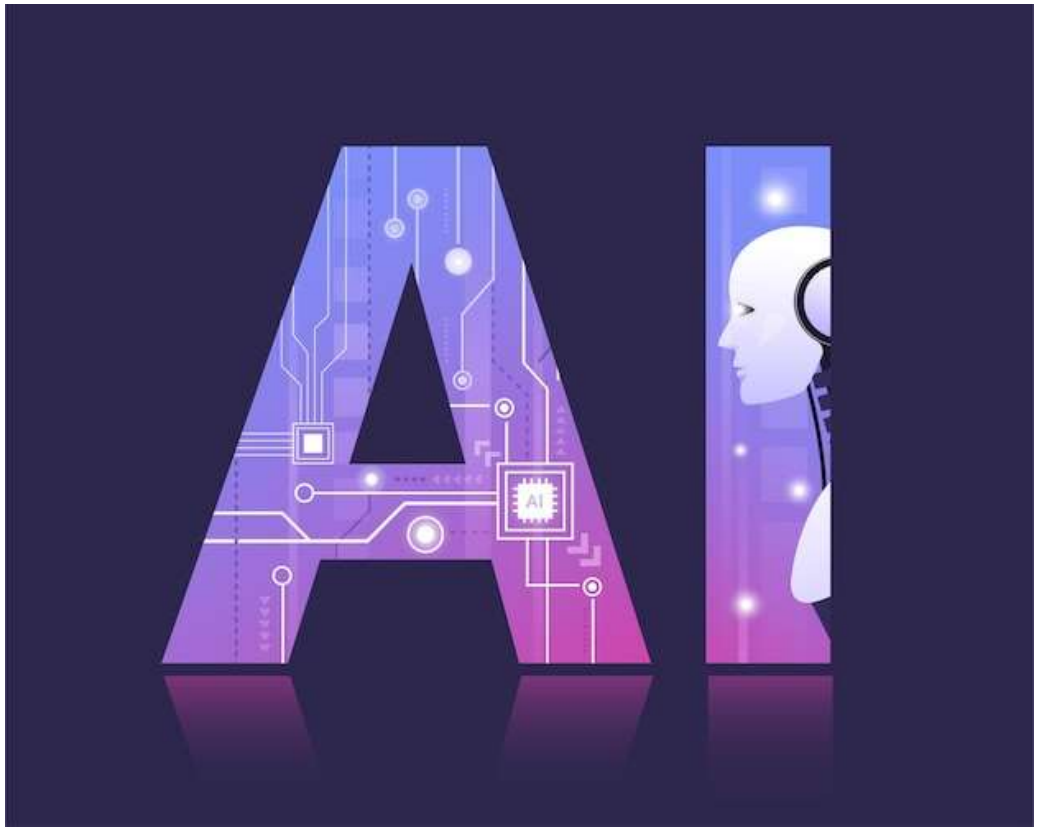
**Dominio** — **Settore**

… Artificial Intellingence | Data Governance | Change Management | VA/PT ← **SME** → Sanità | Banking | GDO | Fashion | …

# Perché P4I è la società giusta: l'esperienza in ambito IA

Il team vanta anche una comprovata esperienza in ambito Intelligenza Artificiale e, visto la proliferazione di soluzioni e delle relative applicazioni all'interno delle aziende, può garantire il corretto indirizzo strategico delle decisioni legate proprio a questo nuovo trend tecnologico.

1. Conoscenza delle **normative** nazionali e internazionali (es. AI Act)
2. Sviluppo di **metodologie** per la valutazione e la gestione dei rischi
3. Utilizzo di **framework** proprietari per la valutazione dei rischi etici
4. Monitoraggio continuo dei **trend** tecnologici e normativi



ADVISORY 360 HUB

P4.I

2

# In cosa consiste il nostro servizio

# Di cosa si tratta

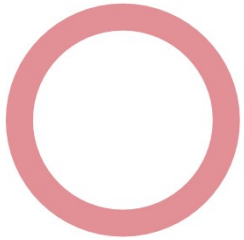
## DPO as a Service

**Governare la protezione dei dati personali** di Imprese e PA, ricoprendo il ruolo di **Data Protection Officer (DPO)** o **supportando il DPO interno**, mettendo a disposizione l'**esperienza e la competenza di un team multidisciplinare** unite ad una **piattaforma tecnologica che integra il nostro know-how.**

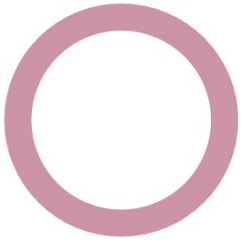
DPO 360
DATA PROTECTION AS A SERVICE

# A chi è rivolto

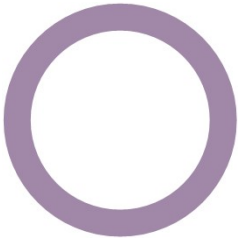
Il DPO as a Service si rivolge a tre tipologie di organizzazioni:



**Autorità/Organismi pubblici e enti governativi**, indipendentemente dalla quantità e tipologia di dati trattati



**Organizzazioni private** che effettuano **trattamenti di monitoraggio regolare e sistematico degli interessati su larga scala**



**Organizzazioni** che hanno come **attività principale il trattamento su larga scala di dati sensibili** o riguardante **condanne penali e reati**, indipendentemente dalla loro dimensione

Inoltre, il servizio si rivolge anche a **tutte quelle organizzazioni che intendono nominare volontariamente un DPO**, anche se non hanno un obbligo di legge, per garantire una **protezione adeguata dei dati personali** che trattano.

# Come funziona

Il DPO as a Service prevede i seguenti servizi, in parte erogati attraverso la Piattaforma Advisory360:

**ATTIVITÀ PROPRIE DEL DPO**
Include le attività di responsabilità del DPO previste dall'art. 39 del Regolamento (UE) 2016/679 (GDPR)

**SUPPORTO PRIVACY**
Include le attività di consulenza specialistica in ambito data protection e privacy per garantire il rispetto delle normative

**SUPPORTO INTELLIGENZA ARTIFICIALE (IA)**
Include le attività che garantiscono la corretta implementazione e adozione di soluzioni aziendali che incorporano l'IA

# Come funziona

## Piattaforma Advisory360


Il Team DPO utilizza la **piattaforma Advisory360** come strumento a supporto del servizio. La piattaforma, all'interno della quale P4I ha incorporato e modellizzato la propria conoscenza ed esperienza in materia data protection, consente al cliente di accedere ai seguenti contenuti:

- contenuti informativi - **News, Magazine, Insights ed Events** – per garantire l'adeguato aggiornamento sulla normativa e le relative evoluzioni
- **questionari** ed **assessment** strutturati e facilmente fruibili per gli utenti, per facilitare il DPO nello svolgimento delle attività di verifica
- metodologie e strumenti quali ad esempio **Template** documentali di informativa, atto di designazione, procedura
- **Documentazione data protection della Società**
- Video per la sensibilizzazione del personale in materia Data Protection attraverso l'area **Education**

DPO 360
DATA PROTECTION AS A SERVICE

# Come funziona

## Piattaforma Advisory360 - Modulo GDPR

### Modulo GDPR


La Piattaforma Advisory360 dispone di un **Modulo specifico per la gestione degli adempimenti** in materia di protezione dei dati personali, che consente di:

- gestire il **Registro dei trattamenti** in qualità di **titolare e di responsabile**
- effettuare l'**Analisi dei rischi dei trattamenti di dati personali**
- effettuare attività di **Assessment sui trattamenti**: Legitimate Interest Assessment (LIA), Data Protection Impact Assessment (DPIA) e Transfer Impact Assessment (TIA)
- generare e conservare **documenti** per garantire il rispetto del principio di accountability
- gestire il **Registro dei Data Breach e il Registro delle richieste degli interessati**

Nel servizio è compreso:

- il **caricamento in Advisory360 della documentazione privacy della Società** (registro dei trattamenti, analisi dei rischi dei trattamenti, ...), ai fini delle attività di indirizzo e monitoraggio del DPO
- la possibilità di download della documentazione privacy della Società**.**

DPO 360
DATA PROTECTION AS A SERVICE

# Come funziona

## Attività di indirizzo del DPO

- Attività di indirizzo del titolare e delle funzioni interne nella gestione di specifici adempimenti in materia di protezione dei dati personali, ad esempio:
  - Supporto nell'analisi preliminare di nuovi trattamenti per definire le azioni da attivare
  - Supporto nella valutazione della necessità di procedere ad una DPIA o rispetto ad una valutazione di impatto effettuato dalla società
  - Analisi di alto livello della documentazione in materia di protezione di dati personali predisposta dalla società (informative, DPA, analisi dei rischi, bilanciamento di interessi)
  - Pareri sulla pertinenza e sul corretto svolgimento dei programmi di formazione interna organizzati dal titolare

# Come funziona

## Verifica della conformità

- Monitoraggio del livello di conformità dell'organizzazione, attraverso attività di verifica organizzate dal DPO:
  - Somministrazione di questionari per valutare il livello di esposizione al rischio e di maturità/conformità dell'organizzazione rispetto ai requisiti previsti dalle normative in materia di protezione dei dati personali
  - Programmazione ed esecuzione di verifiche in modalità self-assessment sui fornitori di servizi del Cliente (Responsabili del trattamento)
  - Programmazione ed erogazione di una campagna di flussi informativi rivolti alle Società del Gruppo e/o alle Unità Organizzative della Società, al fine di intercettare modifiche rilevanti che impattano sulla conformità in materia di protezione dei dati personali

# Come funziona

## Gestione dell'Accountability

- Attività di verifica ed aggiornamento finalizzate alla dimostrazione del livello di conformità dell'organizzazione:
  - Verifica periodica dell'organigramma privacy e della corretta individuazione e designazione dei soggetti previsti
  - Se messo a disposizione di P4I attraverso la Piattaforma Advisory360, aggiornamento del registro dei trattamenti e delle valutazioni dei rischi seguendo una logica «*risk-based*»;
  - Verifica periodica dell'impianto documentale in materia di privacy ad esempio policy, procedure e documentazione di adempimento (es. allineamento delle informative al registro dei trattamenti)
  - Verifica periodica del contenuto dei registri degli eventi, quali ad esempio registro dei data breach, registro delle richieste di esercizio dei diritti degli interessati

# Come funziona

## Valutazione degli eventi

- Supporto al titolare ed alle funzioni interne nella valutazione di eventi occorsi alla Società con impatti in materia di trattamento dei dati personali, ad esempio:
  - Supporto nell'identificazione di violazioni di dati personali (data breach) e nella valutazione preliminare della gravità degli stessi
  - Supporto nella valutazione preliminare di richieste di esercizio dei diritti degli interessati al trattamento
  - Supporto nella valutazione preliminare di richieste avanzate dall'Autorità di Controllo

# Come funziona

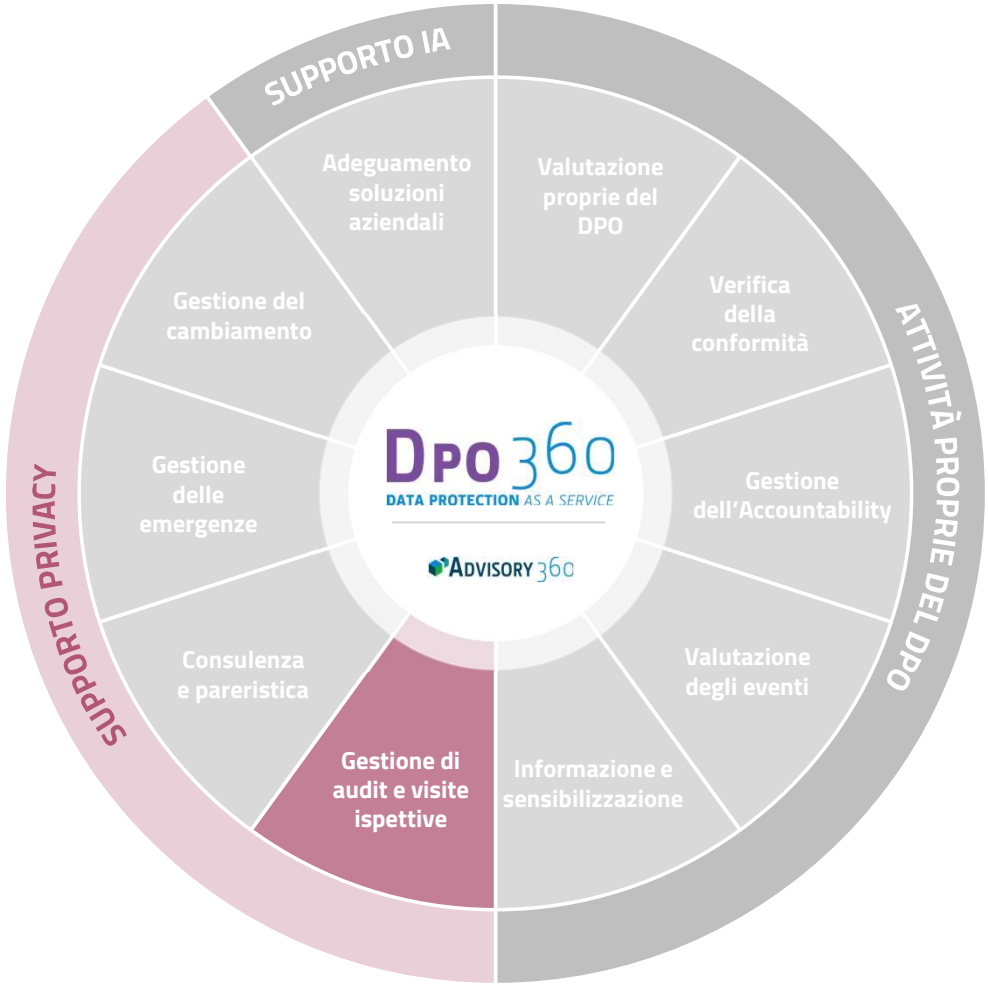
## Informazione e sensibilizzazione

- Condivisione di comunicazioni, flash news, articoli del Network di Digital360 e approfondimenti in merito a tematiche rilevanti in materia di protezione dei dati personali
- Segnalazione di eventi di interesse tenuti dai nostri esperti direttamente o all'interno di eventi organizzati da soggetti terzi
- Partecipazione a survey per confrontare le scelte effettuate dalla Società con quelle di altre realtà di mercato (benchmarking)
- Messa a disposizione di video-pillole e/o video-percorsi che coprono aspetti legati alla protezione dei dati personali e alla sicurezza delle informazioni
- Pianificazione di campagne per la valutazione del livello di conoscenza dell'azienda o di singole aree funzionali rispetto ad ambiti coperti dalla normativa

# Come funziona

## Gestione di audit e visite ispettive

- Programmazione ed esecuzione di audit verticali - interni e/o esterni - per la verifica della conformità di specifici trattamenti, processi aziendali, sistemi informativi
- Progettazione e conduzione di simulazioni di verifiche ispettive dell'Autorità Garante e di simulazioni di eventi critici quali attacchi di phishing e ransomware (data breach), al fine di valutare oltre alla conformità della documentazione e dei processi, anche il livello di preparazione del personale.



# Come funziona

## Consulenza e pareristica

- Supporto specialistico e gestione degli adempimenti privacy dell'azienda da parte di P4I, ad esempio:
  - Stesura ex-novo dell'organigramma privacy, delle procedure o policy interne dell'organizzazione, del registro dei trattamenti e della valutazione dei rischi
  - Gestione di specifici adempimenti, tra cui a titolo esemplificativo e non esaustivo:
    - Analisi di privacy by design e by default
    - valutazioni di impatto sul trattamento dei dati personali (DPIA)
    - valutazioni sui trasferimenti di dati personali extra UE (TIA)
    - test di bilanciamento di interessi (LIA)
    - nomine di Responsabili del trattamento (DPA)
  - Redazione di pareri legali in relazione a specifici temi o ambiti di applicazione della normativa (es. definizione del ruolo privacy ricoperto dall'Organizzazione nell'ambito del rapporto con un soggetto terzo che svolge un trattamento)

# Come funziona

## Gestione delle emergenze

- Supporto specialistico consulenziale nella gestione di specifici eventi, tra cui a titolo esemplificativo e non esaustivo:
  - ✓ violazioni di dati personali (data breach)
  - ✓ richieste di esercizio dei diritti degli interessati
  - ✓ richieste dell'Autorità di Controllo

- Assistenza nella gestione dei rapporti con l'Autorità di controllo e con i soggetti interessati al trattamento

# Come funziona

## Gestione del cambiamento

- Definizione di un piano di sensibilizzazione, formazione e affiancamento del personale in materia di protezione dei dati personali
- Progettazione ed erogazione di attività di formazione e affiancamento del personale in presenza e/o a distanza e/o attraverso percorsi personalizzati
- Attivazione dell'applicazione hi di Digital Attitude per cambiare la mentalità e i comportamenti delle persone e far conoscere e implementare policy le procedure definite dall'organizzazione

# Come funziona

## Adeguamento soluzioni aziendali

- Mappatura di norme e leggi - vigenti e in fase di sviluppo - in ambito AI che si applicano alle organizzazioni e supporto nella definizione ed attuazione del percorso di adeguamento
- Valutazione dei potenziali rischi etici per l'azienda connessi allo sviluppo e/o utilizzo di soluzioni IA, dalla valutazione dei bias algoritmici, alla trasparenza degli algoritmi, alla protezione dei dati personali fino alla valutazione delle possibili conseguenze in termini di privacy e discriminazione legata al set di dati utilizzati e all'addestramento a cui è sottoposto l'algoritmo
- Redazione e diffusione di policy che ne identifichino i confini, consentendo il corretto indirizzamento di rischi (ad es. brand reputation, sicurezza informatica, utilizzo improprio dei dati) e agevolando l'adozione sostenibile delle nuove soluzioni di IA
- Supporto a 360° per la contrattualistica relativa a servizi e soluzioni basate sull'IA, incluso il supporto per la tutela dei diritti di proprietà intellettuale, industriale e commerciale

# Come viene gestito

Il DPO as a Service prevede molteplici meccanismi di coordinamento:

- **Monitoraggio della casella di posta elettronica del DPO e segnalazione delle mail da gestire** (es. richieste degli interessati)

- Elaborazione e condivisione di **reportistica in favore del Cliente**:
  - con cadenza trimestrale, un report con la **rendicontazione delle attività svolte**
  - con cadenza annuale, una **relazione al Top Management** sulle attività del DPO ed i principali punti di attenzione

- Predisposizione e messa a disposizione di:
  - una **dashboard riepilogativa dello stato di conformità del Cliente** rispetto ai principali adempimenti in materia di protezione dei dati personali
  - uno **scadenziario delle azioni da condurre** per il miglioramento/mantenimento della conformità

- Svolgimento di **incontri ricorrenti** con i referenti del Cliente:
  - incontri **operativi** per attività di indirizzo, monitoraggio e aggiornamento della roadmap di adeguamento del Cliente, svolgimento di attività operative e/o aggiornamento in merito a novità significative
  - incontri **strategici** per attività di condivisione del livello di conformità del Cliente e raccolta di feedback in merito al servizio offerto da P4I

- Il servizio prevede, per i periodi di chiusura aziendale, un'assistenza da parte di P4I in modalità ***best effort***

ADVISORY 360 HUB

P4.I

Per maggiori informazioni

**https://www.advisory360hub.it/**