Politica per la sicurezza delle Informazioni e la protezione dei dati personali

Politica

Edenred Italia Srl

Via GB Pirelli 18
20124 Milano
Italy
☎ +39 (0) 2 26 904 1
+39 (0) 2 21 309 1
https://www.edenred.it/

Società	Funzione	Scopo
Edenred Italia Srl	General Manager	Accountable
Edenred Italia Srl	Head of Corporate Compliance & Legal	Responsible
Edenred Italia Srl	CISO - Chief of Information Security Officer	Responsible
Edenred Italia Srl	CIO - Chief Information Officer	Responsible
Edenred Italia Srl	Privacy Manager	Responsible
Edenred Italia Srl	DPO - Data Protection Officer	Consulted

Revisioni					
#	**Data**	**Descrizione**	**Autore**	**Rivisto da**	**Approvato da.**
1.0	12/07/2019	Prima versione	Information Security Consultant	CISO - Chief of Information Security Officer	General Manager
2.0	15/03/2021	Seconda versione	Information Security Consultant	CISO - Chief of Information Security Officer	General Manager
3.0	10/09/2021	Terza versione	Information Security Consultant	CISO - Chief of Information Security Officer	General Manager
4.0	28/09/2022	Quarta versione	Information Security Consultant	CISO - Chief of Information Security Officer	General Manager
5.0	12/12/2023	Integrazione con privacy policy secondo i requisiti dello standard ISO/IEC 27701	Information Security & Privacy Consultant	CISO&DPO	General Manager
6.0	08/10/2024	Integrazioni secondo la nuova normativa ISO/IEC 27001:2022	Information Security Consultant & Privacy Specialist	CISO & DPO	CISO

7.0	26/09/2025	Integrazione requisiti ISO/IEC 27017 e ISO/IEC 27018	Information Security Consultant & Privacy Specialist	CISO & DPO	CISO
7.1	28/10/2025	Aggiornamento del campo di applicazione	Information Security Consultant	CISO & DPO	CISO

Sommario

1. Introduzione

1.1. Scopo del documento

Il presente documento di politica esplicita le linee di indirizzo di più alto livello decise dall'Alta Direzione di Edenred Italia Srl (in breve Edenred), in materia di sicurezza delle informazioni e protezione dei dati personali al fine di poterle comunicare in maniera ottimale al suo interno e ai soggetti esterni rilevanti.
La presente politica si applica a tutte le informazioni trattate da Edenred all'interno del suo sistema di gestione per la sicurezza delle informazioni e protezione dei dati personali (in breve PIMS), indipendentemente dagli strumenti utilizzati per tali operazioni di trattamento e dai supporti su cui le informazioni sono memorizzate o trasmesse sia On Premise che in Cloud. Sono inoltre espressamente inclusi in questo contesto i fornitori e i collaboratori che ne trattano le informazioni o che hanno comunque accesso ad esse.
La Politica di sicurezza delle informazioni e la protezione dei dati personali viene revisionata e aggiornata annualmente per garantire la sua adeguatezza ed efficacia di fronte alle mutevoli minacce in continua evoluzione. Qualora emergessero cambiamenti significativi per l'azienda, la politica verrà aggiornata o modificata all'occorrenza, per garantire la sua adeguatezza anche in caso di specifiche esigenze aziendali.

L'organizzazione, inoltre, si impegna a stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni e della protezione dei dati personali, compresi i processi necessari e le loro interazioni, come indicato nel documento "ERIT-SEC-22301-BIA 2024".

1.2. PIMS e suo ambito di applicazione

Trattamento di dati personali in regime di titolare/responsabile del trattamento per la gestione di servizi personalizzati per aziende private ed enti pubblici mediante l'applicazione norma ISO/IEC 27701:2019, consistenti in servizi sostitutivi di mensa aziendale, servizi alla persona, servizi per incentivare la produttività, erogati ed organizzati mediante un network di affiliati utilizzando "titoli di legittimazione" attraverso software di gestione in modalità SaaS tramite l'applicazione delle Linee Guida ISO/IEC 27017:2015 e ISO/IEC 27018:2019.
Il campo di applicazione è riferito alle seguenti sedi di Edenred:

- Edenred Milano - Via G.B.Pirelli, 18, 20124;
- Edenred Torino - C.so Marconi, 15, 10125;
- Edenred Genova - V.le Brigata Bisagno, 2/6, 16129;
- Edenred Trento - Via Trener 8, 38121;
- Edenred Padova - Piazza Luigi da Porto, 8, 35131;
- Edenred Firenze - Via Aretina, 167/B, 50136;
- Edenred Roma - Via Delle Sette Chiese, 142, 00145;
- Edenred Napoli - Viale Gramsci, 17/B, 80122;
- Edenred Bari - Executive Center Via G. Amendola, 166/5, 70126.

In questo contesto le parti interessate, interne ed esterne a Edenred definite nel documento di contesto sono qui sinteticamente riportate:

1. la struttura interna di gestione dei progetti che comprende tutti gli sviluppatori;
2. le aziende del gruppo, i professionisti che forniscono servizi e supporto alle attività di sviluppo;
3. le aziende e i professionisti esterni che forniscono prodotti, servizi e risorse negli ambiti previsti.

Considerando le modalità operative e la cultura aziendale i dipendenti delle aziende del gruppo e i professionisti sono trattati alla stregua di personale interno, a cui vengono pertanto applicate le stesse regole e indicazioni di sicurezza e data protection. Inoltre, i fornitori sono legati dalle contromisure predisposte per la gestione dei rapporti con i fornitori. Si specifica, pertanto, che in tutta la documentazione relativa al PIMS il termine "personale" (es. personale aziendale, personale Edenred) definisce le parti interessate del punto 1 e 2.

1.3. Dichiarazione d'intenti

L'**Alta Direzione** di Edenred nella figura del GM ha deciso di stabilire ed attuare un sistema di gestione per la sicurezza delle informazioni e la protezione dei dati personali (**PIMS**) per preservare la riservatezza, l'integrità e la disponibilità delle informazioni aziendali sia On Premise che in Cloud. Il PIMS si basa sull'applicazione di un processo di gestione del rischio integrato con i processi aziendali in essere, perseguendo i seguenti obiettivi quale impegno dell'Alta Direzione:

A. Assicurando che la politica e gli obiettivi per la sicurezza delle informazioni e la protezione dei dati personali siano stabiliti e siano compatibili con gli indirizzi strategici dell'organizzazione e con la normativa vigente
B. Assicurando l'integrazione dei requisiti del PIMS nei processi di Edenred;
C. Assicurando le disponibilità delle risorse necessarie PIMS;
D. Comunicando l'importanza di un'efficace gestione della sicurezza delle informazioni e della protezione dei dati personali in conformità ai requisiti del PIMS
E. Fornendo guida e sostegno alle persone per contribuire all'efficacia del PIMS;
F. Promuovendo il miglioramento continuo;
G. Fornendo sostegno ad altri pertinenti ruoli gestionali nel dimostrare la propria Leadership come opportuno nelle rispettive aree di responsabilità.

Il **PIMS** si applica a tutto il personale Edenred compreso nell'ambito di applicazione. Al fine di rendere operativo il PIMS sono state formalizzate le informazioni documentate Edenred rispetto la norma ISO/IEC 27001 e ISO/IEC 27701 nonché delle estensioni ISO/IEC 27017 e ISO/IEC 27018.

Alla corretta attuazione e al miglioramento del PIMS deve concorrere, ciascuno nell'ambito delle proprie competenze, tutto il personale aziendale ricompreso nell'ambito di applicazione.
Il Chief Legal Officer ha il dovere di informare periodicamente l'Alta Direzione sullo stato di attuazione, efficacia ed adeguatezza del PIMS dell'azienda sotto la stretta sorveglianza del Data Protection Officer (DPO) ed interagendo con le altre funzioni aziendali (Compliance, Legal, Information Security etc.) e proponendo azioni nell'ottica di miglioramento continuo.

1.4. Gestione delle Non Conformità e Azioni Correttive

L'organizzazione si impegna a identificare e gestire prontamente le non conformità nel sistema di gestione della sicurezza delle informazioni e di protezione dei dati personali. Le non conformità vengo documentate e analizzate per determinarne le cause. Vengono intraprese azioni correttive al fine di superare le non conformità e prevenire il loro ripetersi. L'efficacia delle azioni correttive viene verificata e monitorata regolarmente. Le responsabilità per la gestione delle non conformità e delle azioni correttive sono assegnate ai responsabili della sicurezza delle informazioni e protezione dei dati personali.

1.5. Conseguenze Mancato Rispetto

In generale, la normativa aziendale prevede una serie di misure comportamentali che i dipendenti sono tenuti a rispettare, come indicato nell' "Allegato A al codice di comportamento".

In particolare, si precisa che l'utilizzo degli strumenti informatici e telematici assegnati deve avvenire nel rispetto delle leggi e delle normative vigenti e nel rispetto dei regolamenti, policy e procedure interne. Si ricorda infatti che in caso di violazione delle norme di Sicurezza delle informazioni e della Protezione dei dati personali, disciplinate nell'ambito della normativa interna, che costituissero inadempimento delle obbligazioni contrattuali, sono intraprese azioni disciplinari specifiche nei confronti dei trasgressori.

1.6. Convenzioni

Le politiche definite nel PIMS sono integrazioni ai processi in essere definiti nel Manuale della Qualità secondo la norma UNI EN ISO 9001:2015 e ISO/IEC 27001 integrati con i requisiti del Regolamento Europeo per la protezione dei dati personali (GDPR).

Per tale motivo sono previste per tutte le attività operative una descrizione dei compiti e delle responsabilità da seguire ogni qualvolta si trattano dati personali.

Tale area è presidiata dal Chief Legal Officer che supporta il Compliance Manager ed il CISO, con il coinvolgimento del DPO, in tutte le fasi di revisione ed introduzione di nuovi processi.

1.7. Termini e definizioni

Termine	Definizione
Collaboratore	Persona/e delle aziende del gruppo e professionista/i che forniscono servizi e supporto alle attività
Data Protection	Termine usato in maniera intercambiale con privacy e protezione dei dati personali
Personale (Es. personale aziendale, personale Edenred)	La struttura interna (dipendenti Edenred) di gestione dei progetti che comprende tutti gli sviluppatori e i collaboratori che forniscono servizi e supporto alle attività
PIMS	Privacy Information Management System - Sistema di Gestione delle Informazioni sulla Privacy
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato») [art. 4.1 GDPR]
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione [art. 4.2 GDPR];
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica,

	in particolare per analizzare o prevedere aspetti riguardanti il rendiment professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica [art. 4.4 GDPR]
Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile [art. 4.5 GDPR]
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 [art. 4.7 DPR]. Ai fini di queste Linee Guida, Edenred Italia S.r.l. opera in qualità di Titolare del trattamento
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento [art. 4.8 GDPR]
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento [art. 4.11 GDPR]
Categorie particolari di dati personali	Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona [art. 9 GDPR]
Violazione di sicurezza	Per violazione di sicurezza ci si riferisce a un qualsiasi incidente che causa o possa causare un'interruzione della disponibilità, riservatezza o integrità degli asset dell'organizzazione
Disponibilità	Assicura che l'Informazione sia accessibile ed utilizzabile quando necessario, dal personale autorizzato a farlo, secondo le modalità e i tempi previsti
Informazione	Dato o elemento che consente di avere conoscenza più o meno esatta di fatti, situazioni, modi di essere. L'Informazione può essere composta a sua volta da un insieme di dati e/o Informazioni tra loro correlabili. L'Informazione può essere registrata su supporti cartacei o elettronici (supporti di memorizzazione informatici), ed essere comunicata in forma orale tra più individui, o essere in trasmissione o elaborazione tra sistemi elettronici
Integrità	Assicura che le Informazioni non possano essere alterate o manipolate accidentalmente o intenzionalmente. Le stesse devono essere trattate solo attraverso processi adeguatamente autorizzati e controllati
Riservatezza	Assicura che le Informazioni siano accessibili solo al personale autorizzato
RID	Riservatezza Integrità Disponibilità
On Premise	Indica soluzioni e infrastrutture gestite internamente dall'organizzazione nelle proprie sedi fisiche, con controllo diretto su sicurezza, dati e sistemi, secondo i requisiti dell'ISMS (ISO/IEC 27001) e del sistema di gestione della privacy (ISO/IEC 27701).
Cloud	Si riferisce a servizi e risorse erogati da fornitori esterni tramite internet, con responsabilità condivise tra cliente e cloud provider. Le norme ISO/IEC 27017 (sicurezza nei servizi cloud) e ISO/IEC 27018 (protezione dei dati personali in cloud pubblici) definiscono controlli specifici per garantire sicurezza, privacy e conformità in questi ambienti.

1.8. Acronimi funzioni aziendali

Termine	Definizione
CdA	Consiglio di Amministrazione
GM	General Manager – Direttore Generale
CISO	Chief Information Security Officer – Responsabile della sicurezza delle informazioni
CIO (BU Technology Leader)	Chief Information Officer - Direttore Technology
CFO	Chief Finacial Officer – Direttore Finanziario
DPO	Data Protection Officer – Responsabile protezione dati personali
Head of Anti Fraud	Antifrode
Chief Legal Officer	Legal Affairs Director - Direttore Affari Legali
Chief People & Sustainability Officer	Human Resources Director & CSR – Direttore Risorse Umane & CSR
Chief Marketing & Product Officer	Direttore Marketing, Communication & Distant Sales
Chief Sales Officer	Direttore Commerciale Customers
Chief Partnership Officer	Direttore Commerciale Merchants
Chief Strategy Officer	Direttore Progetti Innovativi e strategici
Chief Customer Excellence Officer	Direttore Customer Operations
Sales & Customer Success Director Welfare	Direttore Welfare
Head of Compliance, Governance and Risk	Compliance, Governance & Risk Manager
Head of Legal Affairs & Advisory	Legal & Advisory
Head of Enterprise Architecture	Responsabile della Governance dei processi IT
Head of Core &	Responsabile delle Architetture Informatiche

Digital Solutions	
Head of Testing & Quality Assurance	Responsabile della supervisione e gestione del testing e della qualità
Head of Infrastructure & Operations	Responsabile delle infrastrutture IT
PIMS	Privacy Information Management System - Sistema di Gestione delle Informazioni sulla Privacy

1.9. Riferimenti

Normativi:

- ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
- ISO/IEC 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27701 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.
- ISO/IEC 29100 Information technology — Security techniques — Privacy framework.
- ISO 9001 Quality management systems — Requirements.
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito “GDPR”).
- D.lgs. 30 giugno 2003, n.196 “Codice in materia di protezione dei dati personali” aggiornato dal D.lgs. 10 agosto 2018, n. 101.
- Linee Guida 4/2019 sull’Articolo 25, Protezione dei Dati by Design e by Default, Versione 2.0, European Data Protection Board.
- Privacy and Data Protection – from policy to engineering, December 2014, European Union Agency for Network and Information Security.
- Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati, 4 aprile 2017.
- Linee guida sul trattamento di dati personali dei lavoratori privati - 23 novembre 2006, Garante per la Protezione dei Dati Personali.
- WP29 – Opinione 2/2017 – Trattamento dei dati sul posto di lavoro.
- Provvedimento in materia di videosorveglianza - 8 aprile 2010 e successive modifiche e integrazioni, Garante per la Protezione dei Dati personali.

Interni:

- ERIT-SGI-Relazione Attività Valutazione Trattamento Rischio 2025;
- ERIT–SEC-22301-BIA 2024;
- Allegato A al codice di comportamento;

2. Principi, obiettivi e requisiti

2.1. Principi guida

Tutte le misure per la sicurezza delle informazioni e la protezione dei dati personali adottate devono essere sempre progettate, implementate e gestite tenendo in considerazione i principi chiave in materia di sicurezza e di protezione dei dati personali.
Nello specifico Edenred garantisce relativamente alla sicurezza delle informazioni e della protezione dei dati personali:

- **Riservatezza:** garantire che le informazioni e i dati personali gestiti da Edenred siano accessibili esclusivamente ai soggetti autorizzati. Salvaguardare la riservatezza significa proteggerli da accessi, intenzionali o accidentali, da parte di persone non autorizzate;
- **Integrità:** garantire che le informazioni e i dati personali siano completi, accurati e non alterati da modifiche non autorizzate o da errori accidentali. Salvaguardare l'integrità significa proteggerli da cancellazioni, alterazioni o manomissioni causate da soggetti non autorizzati o da eventi imprevisti e non controllabili;
- **Disponibilità:** garantire che le informazioni e i dati personali siano accessibili agli utenti autorizzati ogniqualvolta necessario, in funzione delle esigenze di continuità operativa e nel rispetto degli obblighi normativi di conservazione. Salvaguardare la disponibilità significa proteggerli da eventi, dolosi o accidentali, che possano comprometterne l'accesso o la fruibilità.

Inoltre, per completezza sono indicati anche i principi previsti dalla ISO/IEC 29100 ed ereditati dalla ISO/IEC 27701.

Principio	Definizione	Principi ISO/IEC 29100
Liceità del trattamento	I dati personali devono essere trattati legalmente e devono quindi fondarsi su una base giuridica (consenso delle persone interessate, trattamento necessario per l'esecuzione di un contratto, il rispetto di un obbligo legale, legittimo interesse, ecc.) [art. 6 GDPR]	2. Purpose legitimacy and specification
Correttezza e Trasparenza	Il trattamento dei dati personali deve essere eseguito con trasparenza e correttezza nei confronti dei soggetti interessati. Edenred Italia S.r.l. deve informare i soggetti coinvolti nel trattamento, in merito alle caratteristiche principali dello stesso e ai diritti loro riconosciuti [art. 5.1 (a) GDPR]	7. Openness, transparency and notice
Limitazione della finalità	I dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo compatibile con tali finalità [art. 5.1 (b) GDPR]	3. Collection limitation
Minimizzazione dei dati	I dati personali devono essere adeguati, pertinenti e limitati a ciò che è necessario in relazione agli scopi per i quali sono trattati [art. 5.1 (c) GDPR]	4. Data minimization
Esattezza	I dati personali devono essere accurati e, se necessario, aggiornati [art. 5.1 (d) GDPR]	6. Accuracy and quality

Limitazione della conservazione	I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo che non supera il conseguimento delle finalità per le quali sono trattati [art. 5.1 (e) GDPR]	5. Use, retention and disclosure limitation
Integrità e riservatezza	Deve essere garantita un'adeguata sicurezza dei dati personali da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali [art. 5.1 (f) GDPR]	10. Information security
Responsabilizzazione	Edenred Italia S.r.l., in qualità di Titolare del trattamento è competente per il rispetto dei principi sopra esposti [art. 5.1 (g) GDPR]	9. Accountability
Sicurezza del trattamento	Edenred Italia S.r.l. deve integrare la protezione dei dati mettendo in atto adeguate misure di sicurezza durante tutto il periodo di trattamento dei dati personali. La sicurezza deve essere presa in considerazione quando si sviluppano nuovi sistemi informatici o non informatici, servizi, soluzioni applicative e processi che implicano l'elaborazione di dati personali e/o quando si sviluppano politiche organizzative, processi, pratiche commerciali e/o strategie organizzative che hanno implicazioni per la privacy	11. Privacy compliance

I requisiti per la sicurezza delle informazioni sono pienamente allineati con gli obiettivi strategici di Edenred e sono attuati attraverso il PIMS, che incorpora il SGSI conforme alla ISO/IEC 27001.
Il processo di gestione del rischio, integrato nei processi aziendali, consente di identificare, valutare e trattare i rischi relativi sia alla sicurezza delle informazioni sia alla protezione dei dati personali, contribuendo all'efficacia complessiva e al miglioramento continuo del PIMS.

La valutazione del rischio "**Relazione attività di gestione del rischio**", lo "**Statement of Applicability**" ed il "**Piano di trattamento del rischio**" identificano le modalità con le quali vengono controllati i rischi relativi alla sicurezza delle informazioni e la protezione dei dati personali.
In particolare, sono fondamentali per tale politica il backup di dati e processi, la capacità di evitare virus informatici e attacchi da parte di hacker, il controllo degli accessi ai sistemi ed i registri per gli incidenti relativi alla sicurezza delle informazioni.
La continuità operativa del business è assicurata da un piano di Business Continuity coadiuvato attraverso la logica di Smart & Remote Working e di Disaster Recovery supportato dalla logica multi-sito.

Tutto il personale Edenred che fornisce servizi e supporto alle attività di sviluppo, dovrà conformarsi con la presente politica e con il PIMS che implementa tale politica e ricevere opportuna formazione.

Il PIMS è soggetto a revisioni e miglioramenti continui e sistematici discussi ed approvati dall'Alta direzione. Edenred garantisce che tale politica dovrà essere revisionata al fine di rispondere a qualsiasi cambiamento nella valutazione del rischio o nel piano del trattamento del rischio in sede di "Riesame della Direzione" annuale o straordinario.
Le politiche per la sicurezza delle informazioni e la protezione dei dati personali fanno parte del PIMS che è stato progettato in conformità con quanto specificato nella norma ISO/IEC 27001 ed ISO/IEC 27701.

2.2. Obiettivi e requisiti per la sicurezza delle informazioni e la protezione dei dati personali

Edenred ha stabilito che l'obiettivo principale per la sicurezza delle informazioni e la protezione dei dati personali deve essere quello di supportare l'offerta sul mercato con prodotti con alto profilo di sicurezza, garantendo un appropriato e uniforme livello di protezione.

Nel perseguimento di questo obiettivo principale, e supportati dall'adozione della metodologia Magerit (Risk Analisys & Management), Edenred si aspetta che il PIMS sia un elemento abilitante per:

1) Contenere il rischio IT a livelli accettabili, mantenendo il livello di rischio alla soglia 4 "molto alto", come indicato all'interno del documento "**ERIT-SGI-Relazione Attività Valutazione Trattamento Rischio 2025**";
2) Contenere il rischio DP a livelli accettabili rispetto ai requisiti della normativa vigente, mantenendo il livello di rischio alla soglia 2 "medio", come indicato all'interno del documento "**ERIT-SGI-Relazione Attività Valutazione Trattamento Rischio 2025**";
3) Il mantenimento della certificazione formale;
4) Supervisionare lo sviluppo e i processi per preservare la privacy e la sicurezza delle informazioni;
5) Supportare l'area vendite per le gare d'appalto e le richieste dei clienti;
6) Supervisionare gli audit dei clienti;
7) Garantire attraverso il supporto della funzione HR la formazione annuale di tutto il personale preposto sulla sicurezza delle informazioni e protezione dei dati personali;
8) Supervisionare gli audit dei fornitori in ambito IT e non IT.

I sopracitati obiettivi sono soggetti a misurazione, controllo e riesame da parte dell'Alta Direzione con cadenza periodica, venendo fissati puntualmente ad ogni aggiornamento della presente politica.
In tal senso è assicurato il raggiungimento degli obiettivi attraverso il monitoraggio costante dei relativi KPI.

Nei requisiti principali inerenti all'attività di sviluppo del software (indicati sia dalle parti interessate interne che da quelle esterne) vista la sensibilità del loro ambito d'impiego, sono incluse le caratteristiche di sicurezza degli applicativi sviluppati. I requisiti di sicurezza costituiscono pertanto parte integrante di quelli specificati per la gestione della qualità dei prodotti aziendali.

3. Ruoli e responsabilità

È responsabilità di ogni risorsa del personale e collaboratore, istruita e formata per competenze (vedi mansionario), essere consapevole delle politiche e delle procedure del PIMS e del proprio contributo all'efficacia dello stesso, svolgendo le proprie attività nell'osservanza e applicazione pratica di quanto stabilito nei documenti dei processi del PIMS. I soggetti hanno ruolo esecutivo sul processo indicato.
Sono di seguito riportati e descritti i ruoli chiave rispetto alla sicurezza delle informazioni e la protezione dei dati personali definiti da Edenred, indicando le loro funzioni principali e la loro collocazione organizzativa all'interno della struttura organizzativa.

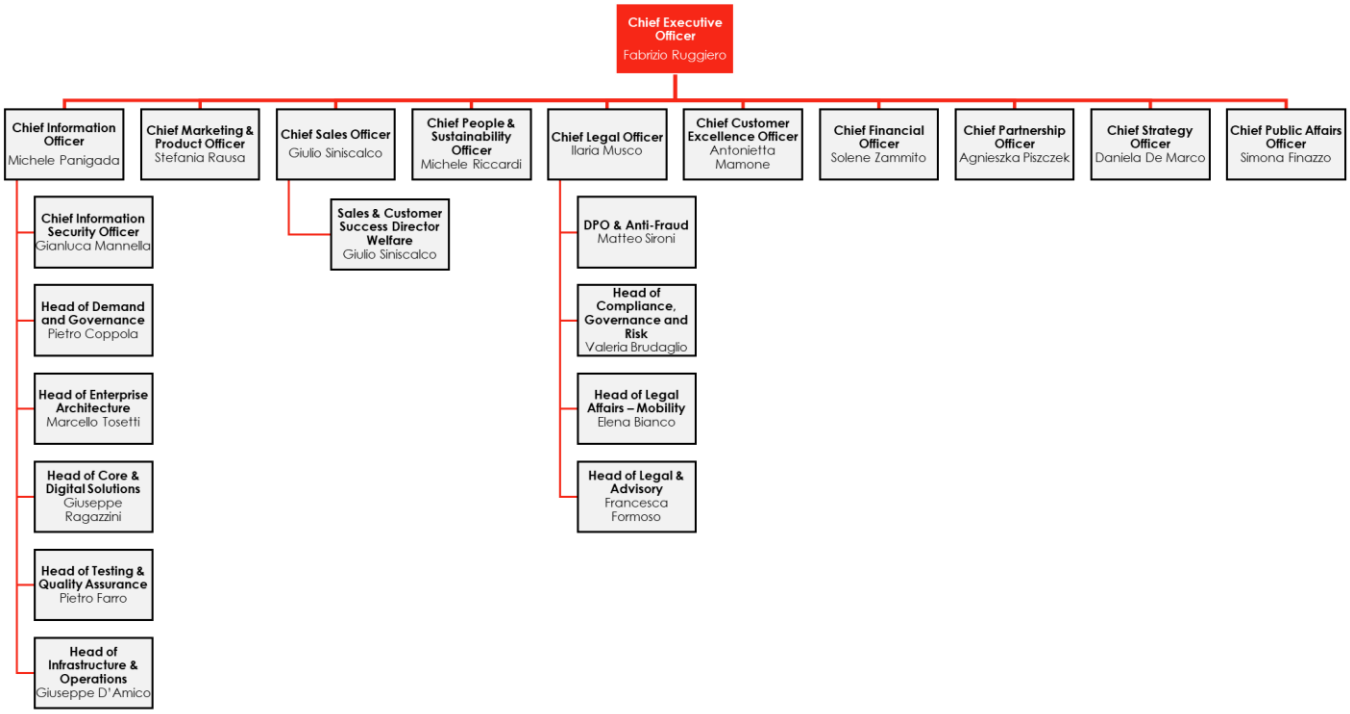
L'Alta Direzione nella figura del GM ha determinato e messo a disposizione le risorse necessarie per stabilire, attuare, mantenere e migliorare in modo continuo il PIMS, definendo responsabilità ed autorità per i ruoli ad esso pertinenti.

3.1. Ruoli

Sigla	Nominativo
GM	Fabrizio Ruggiero
CISO	Gianluca Mannella
CIO (BU Technology Leader)	Michele Panigada
CFO	Solene Zammito
DPO & Head of Anti Fraud	Matteo Sironi
Chief Legal Officer	Ilaria Musco
Chief People & Sustainability Officer	Michele Riccardi
Chief Marketing & Product Officer	Stefania Rausa
Chief Sales Officer	Giulio Siniscalco
Chief Partnership Officer	Agnieszka Piszczek
Chief Strategy Officer	Daniela De Marco
Chief Customer Excellence Officer	Antonella Mamone
Sales & Customer Success Director Welfare	Giulio Siniscalco

Head of Compliance, Governance and Risk	Valeria Brudaglio
Head of Legal Affairs - Mobility	Elena Bianco
Head of Legal Affairs & Advisory	Francesca Formoso
Privacy Manager	Francesca Formoso
Head of Demand and Governance	Pietro Coppola
Head of Enterprise Architecture	Marcello Tosetti
Head of Core & Digital Solutions	Giuseppe Ragazzini
Head of Testing & Quality Assurance	Pietro Farro
Head of Infrastructure & Operations	Giuseppe D'Amico

Di seguito l'organigramma aziendale con focus sulle funzioni inerenti alla politica:



3.2. Responsabilità

3.2.1. Alta Direzione

L'Alta direzione è la massima autorità all'interno di Edenred Italia S.r.l. e rappresenta il titolare del trattamento.
Le sue responsabilità sono le seguenti:

- Approva le azioni di trattamento del rischio;
- Approva la politica e gli obiettivi per la sicurezza delle informazioni in modo che siano compatibili con gli indirizzi strategici dell'organizzazione e nell'ottica di miglioramento continuo del PIMS;
- Approva le azioni di reazione ad incidenti relativi alla privacy di gravità alta;
- Approva l'organigramma, definendo ruoli e responsabilità nel mansionario. Assicura la disponibilità del personale al PIMS;
- Approva il budget per la protezione dei dati personali.

Compiti (molti dei quali almeno 1 volta l'anno):

- Presiede al riesame annuale del PIMS;
- Comunica l'importanza dell'efficacia del PIMS durante le riunioni aziendali al personale (almeno una all'anno);
- Supervisiona i documenti propri del PIMS (politiche, istruzioni, etc.) redatti per soddisfare i requisiti della norma ISO/IEC 27701, definendo eventuali modifiche.
- Analizza i risultati degli audit interni ed esterni e i documenti che evidenziano l'efficacia o le carenze del PIMS (es. i dati degli indici di misurazione, azioni di miglioramento e correttive);
- Analizza l'efficacia delle azioni intraprese, apportando e deliberando le modifiche che ritiene necessarie;
- Verifica le competenze e le responsabilità delle figure aziendali;
- Approva eventuale extra budget per la protezione dei dati personali.

3.2.2. Chief Legal Officer

Chief Legal Officer è responsabile della governance in ambito Legal e Compliance di Edenred Italia S.r.l.; le sue responsabilità principali sono:

- Governance della privacy:
  - Definizione e aggiornamento della strategia di data protection, per mantenerla allineata alle esigenze di business e ai requisiti di legge;
  - Definizione degli standard di data protection di Edenred;
  - Monitoraggio della data protection e definizione degli obiettivi annuali per garantire il controllo ed il contenimento dei rischi ad un livello accettabile;
  - Conduzione di audit regolari per la valutazione della conformità;
  - Revisione regolare degli incidenti di sicurezza e privacy più rilevanti e, se del caso, proposta di azioni di miglioramento al fine di indirizzare le cause originali dell'incidente;
  - Reporting regolare all'Alta Direzione.

- Fornitura di servizi e soluzioni in ambito privacy:
  - Definizione dell'approccio e degli strumenti per la sensibilizzazione al fine di diffondere e rafforzare la cultura della privacy;

- Competenze sull'analisi dei rischi e le strategie di controllo e attenuazione degli stessi;
- Gestione degli incidenti relativi alla privacy (analisi, comunicazione, miglioramento);
- Competenze sulla gestione degli incidenti di privacy più gravi;
- Soluzione e servizi di ricerca delle vulnerabilità (sonde, scansioni);
- Consulenza e supporto per la messa in produzione di soluzioni in ambito data protection raccomandate dal Gruppo.

3.2.3. Privacy Manager

Il privacy Manager è il responsabile di massimo livello per la privacy all'interno di Edenred Italia S.r.l. Risponde direttamente al Chief Legal Officer in ambito privacy anche se a livello funzionale riferisce all'Alta Direzione. Le sue responsabilità più importanti e i compiti principali che è chiamato ad assolvere sono riportati di seguito.

Responsabilità:

- assolvere il ruolo di punto di riferimento aziendale in materia di privacy;
- garantire un corretto e costante presidio della privacy a tutte le attività svolte dall'azienda;
- supportare il Chief Legal Officer per la gestione della data protection;
- gestire il budget per la privacy;
- coordinare il personale dell'azienda con responsabilità in materia di data protection;
- svolge il ruolo di punto di riferimento per la segnalazione degli incidenti relativi alla privacy;
- mantenere la conformità a leggi, regolamenti, contratti e norme tecniche applicabili per la loro componente di privacy;
- gestire le comunicazioni in materia di privacy interne ed esterne all'azienda.

Compiti principali:

- organizzare le responsabilità relative alla privacy;
- effettuare e aggiornare la valutazione del rischio relativo alla protezione dei dati personali;
- proporre all'Alta Direzione, tramite il Chief Legal Officer:
  - le azioni di trattamento del rischio;
  - la politica e gli obiettivi per la privacy;
  - le azioni di reazione ad incidenti relativi alla privacy di gravità alta;
- proporre la strategia per la gestione della privacy alla Direzione;
- controllare periodicamente il livello complessivo della protezione dei dati personali trattati dall' organizzazione;
- informare periodicamente la Direzione sullo stato della protezione dei dati personali;
- coordinare la gestione degli incidenti relativi alla privacy;
- partecipare al Riesame della Direzione in cui predispone gli elementi in ingresso ed in uscita del PIMS rispondendo della puntuale applicazione del PIMS e dei risultati raggiunti all'Alta Direzione tramite il Chief Legal Officer;
- coordinarsi con le altre aree aziendali nel raggiungimento degli obbiettivi del PIMS;
- coordinarsi con il CISO per le verifiche e supporto ai requisiti di privacy in ambito sicurezza delle informazioni;
- coordinarsi con il DPO nelle verifiche relative all'ottemperanza degli obblighi normativi in ambito data protection;
- coordinarsi con la funzione di Procurement nelle fasi di stesura ed aggiornamento degli accordi contrattuali relativi alla data protection con partner e fornitori;

- redigere, revisionare, distribuire ed archiviare le istruzioni di lavoro, i moduli relativi ai documenti obbligatori della privacy; redigere i documenti di sua competenza come da specifiche nelle Politiche del PIMS;
- pianificare e supportare gli audit interni per verificare lo stato di conformità del PIMS;
- definire le necessità formative in materia di privacy;
- supportare tutta l'azienda nell'individuazione delle misure di data protection adeguate;
- identificare eventuali problemi, rilevare le non conformità, raccogliere e analizzare quelle redatte dalle altre figure aziendali.

Attiva e/o controlla l'attuazione delle soluzioni definite e/o approvate dal GM. Verifica l'efficacia delle stesse, comunicando gli esiti all'Alta Direzione tramite il Chief Legal Officer.

3.2.4. Chief Information Officer (CIO)

Il Chief Information Officer (BU Technology Leader) è responsabile della governance della sicurezza delle informazioni di Edenred Italia S.r.l.; le sue responsabilità principali sono:

- Governance della sicurezza delle informazioni:
  - Definizione e aggiornamento della strategia di sicurezza, per mantenerla allineata alle esigenze di business;
  - Definizione degli standard di sicurezza di Edenred;
  - Monitoraggio della sicurezza e definizione degli obiettivi annuali di sicurezza per garantire il controllo ed il contenimento dei rischi IT ad un livello accettabile;
  - Audit regolare delle varie sedi Edenred per la valutazione del livello di rischio IT a cui sono esposte;
  - Revisione regolare degli incidenti di sicurezza IT più rilevanti e, se del caso, proposta di azioni di miglioramento al fine di indirizzare le cause originali dell'incidente;
  - Reporting regolare all' Alta Direzione.

- Fornitura di servizi e soluzioni di sicurezza:
  - Definizione dell'approccio e degli strumenti per la sensibilizzazione al fine di diffondere e rafforzare la cultura della sicurezza;
  - Competenze sull'analisi dei rischi e le strategie di controllo e attenuazione degli stessi;
  - Gestione degli incidenti di sicurezza (analisi, comunicazione, miglioramento);
  - Competenze sulla gestione degli incidenti di sicurezza più gravi;
  - Soluzione e servizi di ricerca delle vulnerabilità (sonde, scansioni);
  - Consulenza e supporto per la messa in produzione di soluzioni di sicurezza raccomandate dal Gruppo.

Il CIO è nominato Approver in ambito alle attività svolte sul Sistema di Gestione per la Sicurezza delle Informazioni, con il supporto del Team DPO relativamente alla protezione dei dati personali. Tali figure hanno, l'autorità necessaria affinché si assicuri, di concerto con il Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni, e con l'area privacy, compliance e legal, l'applicazione dei processi e delle procedure in ambito al sistema di gestione in conformità allo schema internazionale di riferimento ISO/IEC 27001 e ISO/IEC 27701 , promuovendo le azioni di awareness e fornendo adeguato endorsment alle iniziative di sviluppo.
In forza di tale nomina, all'Approver composta da CIO e dal Team DPO, viene richiesta la partecipazione nelle attività connesse al Riesame della Direzione ed alla revisione dell'analisi dei rischi IT e dei rischi DP (data protection) all'interno dell'Organizzazione Edenred Italia S.r.l.

3.2.5. Chief Information Security Officer (CISO)

Il Chief Information Security Officer è il responsabile di massimo livello per la sicurezza delle informazioni all'interno di Edenred Italia S.r.l risponde direttamente al CIO in ambito security anche se a livello funzionale riferisce all' Alta Direzione.
Le sue responsabilità più importanti e i compiti principali che è chiamato ad assolvere sono riportati di seguito.

Responsabilità:

- assolvere il ruolo di punto di riferimento aziendale in materia di sicurezza delle informazioni;
- garantire un corretto e costante presidio della sicurezza delle informazioni relativamente a tutte le attività svolte dall'azienda;
- supportare il CIO per la gestione rispettivamente dell'IT Security e della sicurezza delle informazioni;
- gestire il budget per la sicurezza delle informazioni;
- coordinare il personale dell'azienda con responsabilità in materia di sicurezza delle informazioni;
- svolge il ruolo di punto di riferimento per la segnalazione degli incidenti relativi alla sicurezza delle informazioni;
- mantenere la conformità a leggi, regolamenti, contratti e norme tecniche applicabili per la loro componente di sicurezza delle informazioni;
- gestire le comunicazioni in materia di sicurezza delle informazioni interne ed esterne all'azienda.

Compiti principali:

- organizzare le responsabilità relative alla sicurezza delle informazioni;
- effettuare e aggiornare la valutazione del rischio IT relativo alla sicurezza delle informazioni;
- proporre all'Alta Direzione, tramite il CIO:
  - le azioni di trattamento del rischio IT;
  - la politica e gli obiettivi per la sicurezza delle informazioni;
  - le azioni di reazione ad incidenti relativi alla sicurezza delle informazioni di gravità alta;
- proporre la strategia per la gestione della sicurezza delle informazioni alla Direzione;
- controllare periodicamente il livello complessivo di sicurezza delle informazioni aziendale;
- informare periodicamente la Direzione sullo stato della sicurezza delle informazioni;
- coordinare la gestione degli incidenti relativi alla sicurezza delle informazioni;
- partecipare al Riesame della Direzione in cui predispone gli elementi in ingresso ed in uscita del PIMS e rende conto della puntuale applicazione del PIMS e dei risultati raggiunti all'Alta Direzione tramite il CIO;
- coordinarsi con le altre aree aziendali nel raggiungimento degli obbiettivi del PIMS;
- coordinarsi con i responsabili delle architetture e dello sviluppo nelle verifiche dei prerequisiti dei progetti di sviluppo software e remediation a seguito dei test di sicurezza;
- coordinarsi con il DPO nelle verifiche relative all'ottemperanza degli obblighi normativi in ambito data protection;
- coordinarsi con la funzione di Procurement nelle fasi di stesura ed aggiornamento degli accordi contrattuali relativi alla sicurezza delle informazioni con partner e fornitori;
- redigere, revisionare, distribuire ed archiviare le istruzioni di lavoro, i moduli relativi ai documenti obbligatori della sicurezza delle informazioni; redigere i documenti di sua competenza come da specifiche nelle Politiche del PIMS;
- pianificare ed effettuare audit interni per verificare lo stato di conformità del PIMS;

- definire le necessità formative in materia di sicurezza delle informazioni;
- supportare tutta l'azienda nell'individuazione delle misure di sicurezza delle informazioni adeguate;
- identificare eventuali problemi, rilevare le non conformità, raccogliere ed analizzare quelle redatte dalle altre figure aziendali.

Attiva e/o controlla l'attuazione delle soluzioni definite e/o approvate dal GM. Verifica l'efficacia delle stesse, comunicando gli esiti all'Alta Direzione tramite il CIO durante il Riesame.

3.2.6. Corrispondenti per la Sicurezza delle Informazioni e protezione dei dati personali

La responsabilità del monitoraggio operativo della sicurezza delle informazioni e della protezione dei dati personali deve essere identificata chiaramente all'interno delle diverse Business Unit di Edenred. Deve comprendere la messa in opera di un piano d'azione che deve essere definito successivamente alla valutazione della sicurezza della singola BU.
Questa responsabilità si traduce nell'individuazione e designazione di un Corrispondente per la Sicurezza delle Informazioni e della protezione dei dati personali per ogni singola BU o di un'altra figura adeguata all'organizzazione considerata.

Il Corrispondente ha le responsabilità seguenti:

- essere l'interlocutore privilegiato per la governance della sicurezza dei sistemi e delle informazioni e della protezione dei dati personali per la sua BU;
- elaborare, in collaborazione con il Responsabile della Sicurezza delle Informazioni e delle funzioni Privacy, un piano di azione che consenta di ridurre i rischi identificati e pertinenti;
- mettere in opera il piano di riduzione dei rischi e seguirne l'implementazione al fine di garantirne la corretta ed efficace esecuzione;
- assicurare un reporting circa l'avanzamento delle varie attività sia alla Direzione della propria BU sia al Responsabile della Sicurezza delle Informazioni che alle funzioni Privacy;
- sensibilizzare i collaboratori della propria BU sulla sicurezza delle informazioni e protezione dei dati personali dei sistemi con il supporto del Responsabile della Sicurezza delle Informazioni e delle funzioni Privacy;
- effettuare un monitoraggio costante del livello di sicurezza e protezione dei dati personali della propria BU;
- gestire le richieste operative relative alla sicurezza per la propria BU.

Per gestire correttamente le proprie responsabilità, il Corrispondente si appoggia e fa riferimento alla struttura di governance relative alla compliance, privacy e della sicurezza dei sistemi e delle informazioni di Edenred.

3.2.7. Direttori e Responsabili di funzione

Quindi, i Direttori ed i Responsabili di funzione ad ogni livello sono responsabili dell'implementazione dei principi della presente Politica di Sicurezza delle Informazioni all'interno delle loro strutture. Dimostrano il loro impegno e coinvolgimento:

1. Facendosi promotori presso i propri collaboratori della diffusione della cultura della sicurezza e della privacy, incentivando la conoscenza, la lettura ed il rispetto delle politiche e delle procedure di sicurezza aziendali;
2. Fornendo risorse adeguate e sufficienti per gestire correttamente la sicurezza all'interno delle aree di loro responsabilità;
3. Agendo in modo appropriato per garantire la protezione degli asset aziendali;
4. Applicando e facendo rispettare ogni decisione in materia di sicurezza e protezione dei dati personali, facendo eventualmente riferimento ai ruoli aziendali competenti.

3.2.8. Data Protection Officer (DPO)

Il Data Protection Officer (DPO) ha il compito di supportare, coordinare e collaborare con tutte le strutture organizzative aziendali nella gestione di tematiche data protection e di sorvegliare l'osservanza dei requisiti normativi applicabili e delle politiche di Edenred.
Alla luce dell'art. 39 GDPR, il DPO svolge i seguenti compiti e funzioni:

- informare e fornire consulenza al titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- sorvegliare l'osservanza del Regolamento, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'Autorità di Controllo;
- fungere da punto di contatto con l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

3.2.9. Head of Anti Fraud

L'Head of Anti Fraud è inserito all'interno della Direzione Legal a diretto riporto del Chief Legal Officer ed è responsabile dello sviluppo e dell'implementazione di strategie per prevenire, rilevare e investigare attività fraudolente, guidando un team specializzato per la gestione del rischio di frode e collaborando con gli stakeholder interni ed esterni per proteggere il patrimonio e la reputazione dell'organizzazione.
Le principali responsabilità includono la creazione di policy di prevenzione delle frodi, l'analisi dei dati per individuare modelli di frode, la collaborazione con gli enti legali e normativi e la promozione di una cultura aziendale di consapevolezza delle frodi.

Principali attività e responsabilità:

- Sviluppo di strategie e policy - Progettare e attuare strategie, policy e procedure antifrode per prevenire e rilevare proattivamente attività fraudolente.
- Indagine sulle frodi - Guidare e gestire le indagini su attività sospette, raccogliendo prove e analizzando i dati per identificare tendenze e modelli.
- Analisi dei dati e tecnologia - Analizzare i dati sulle frodi utilizzando conoscenze statistiche e strumenti tecnologicamente avanzati per identificare nuove minacce e migliorare i sistemi di rilevamento, in stretto contatto con la Direzione Technology.
- Gestione degli stakeholder - Collaborare con i team interni (ad esempio Technology, Finance, Risk & Compliance) e con enti esterni (ad esempio autorità di regolamentazione, forze dell'ordine, banche) per garantire un'efficace gestione delle frodi.
- Reporting – Presentare report completi all'Amministratore Delegato e ad ExCom sull'esposizione al rischio di frode, sugli incidenti e sulle misure di mitigazione.
- Formazione e sensibilizzazione - Sviluppare e implementare programmi di formazione per i dipendenti al fine di aumentare la consapevolezza sui rischi di frode e sulle tecniche di prevenzione.

- Conformità - Garantire che le misure antifrode siano conformi alle normative e agli standard di settore pertinenti.
- Leadership di team - Guidare, guidare e promuovere una cultura di miglioramento continuo all'interno del team antifrode.

3.2.10. Privacy Specialist

Il Privacy Specialist è ingaggiato e supporta il DPO in tutte le attività di verifica dell'osservanza dei requisiti normativi applicabili e delle politiche di Edenred.

3.2.11. Cyber Security Compliance Specialist

Il Cyber Security Specialist è ingaggiato e supporta il CISO in tutte le attività di verifica dell'osservanza dei requisiti di sicurezza applicabili e delle politiche di Edenred.