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/

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Società	Funzione	Scopo
Edenred Italia Srl	General Manager	Accountable
Edenred Italia Srl	CIO - Chief Information Officer	Responsible
Edenred Italia Srl	CISO - Chief Information Security Officer	Responsible
Edenred Italia Srl	Head of Compliance, Governance & Risk	Responsible
Edenred Italia Srl	Head of Legal Affairs- Advisory & Mobility	Responsible
Edenred Italia Srl	Privacy Manager	Responsible
Edenred Italia Srl	DPO & Head of Anti Fraud	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

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

7.0	26/09/2025	Integrazione requisiti ISO/IEC 27017 e ISO/IEC 27018	Information Security Consultant & Privacy Specialist	CISO & DPO	CISO – Chief Information Security Officer
7.1	28/10/2025	Aggiornamento del campo di applicazione	Information Security Consultant	CISO & DPO	CISO – Chief Information Security Officer
7.2	27/02/2026	Aggiornamento annuale	Information Security Consultant	CISO – Chief Information Security Officer	CISO – Chief Information Security Officer
7.3	15/09/2026	Revisione delle Job Description ed integrazione dei ruoli ai fini della sicurezza delle informazioni	Information Security Consultant	CISO – Chief Information Security Officer	CISO – Chief Information Security Officer
7.4	08/10/2026	Integrazione dei requisiti dell'AI Act e aggiornamento del paragrafo 2.2 sull'AI Committee e sull'utilizzo dell'Intelligenza Artificiale nel rispetto dei principi aziendali	Information Security Consultant	CISO – Chief Information Security Officer	CISO – Chief Information Security Officer
7.5	26/10/2026	Aggiornamento del ruolo del General Manager, revisione del documento e integrazione di KPI a supporto degli obiettivi della Politica.	Information Security Consultant	CISO - Chief Information Security Officer	CISO - Chief Information Security Officer

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Sommario

1. Introduzione 6
1.1. Scopo del documento 6
1.2. SGI e ambito di applicazione 6
1.3. Dichiarazione d'intenti 7
1.4. Gestione delle Non Conformità e Azioni Correttive 7
1.5. Conseguenze mancato rispetto 8
1.6. Convenzioni 8
1.7. Termini e definizioni 8
1.8. Acronimi funzioni aziendali 10
1.9. Riferimenti 10
2. Principi, obiettivi e requisiti 12
2.1. Principi guida 12
2.2. AI Committee ed utilizzo dell'intelligenza artificiale nel rispetto dei principi aziendali 14
2.3. Obiettivi e requisiti per la sicurezza delle informazioni e la protezione dei dati personali 15
3. Ruoli e responsabilità 17
3.1. Ruoli 17
3.2. Responsabilità 19
3.2.1. Alta Direzione 19
3.2.2. Chief Legal Officer 19
3.2.3. Chief Financial Officer (CFO) 20
3.2.4. Privacy Manager 20
3.2.5. Chief Information Officer (CIO) 21
3.2.6. Chief Information Security Officer (CISO) 22
3.2.7. Corrispondenti per la Sicurezza delle Informazioni e protezione dei dati personali 23
3.2.8. Direttori e Responsabili di funzione 24
3.2.9. Data Protection Officer (DPO) 24
3.2.10. Chief People & Sustainability Officer 24
3.2.11. Chief Marketing & Product Officer 25
3.2.12. Chief Sales Officer 26
3.2.13. Chief Partnership Officer 26
3.2.14. Chief Strategy Officer 27
3.2.15. Chief Customer Excellence Officer 27
3.2.16. Sales & Customer Success Director Welfare 28
3.2.17. Head of Anti Fraud 28
3.2.18. Head of Employee Relations and Reward 29
3.2.19. Head of Compliance, Governance and Risk 30
3.2.20. Head of Legal Affairs – Advisory & Mobility 30
3.2.21. Head of Demand and Governance 31

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

3.2.22. Head of Enterprise Architecture 31
3.2.23. Head of Core & Digital Solutions Director 32
3.2.24. Head of Testing & Quality Assurance 33
3.2.25. Head of Infrastructure & Operations 33
3.2.26. Head of Product 34
3.2.27. Head of Business Growth Intelligence 35
3.2.28. Privacy Specialist 35
3.2.29. Cyber Security Compliance Specialist 35

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

1. Introduzione

1.1. Scopo del documento

Il presente documento definisce la Politica per la Sicurezza delle Informazioni e la Protezione dei Dati Personali di Edenred Italia S.r.l. (di seguito "Edenred"), stabilendo i principi generali e gli indirizzi di riferimento del Sistema di Gestione Integrato per la Sicurezza delle Informazioni e la Protezione dei Dati Personali (SGI), in conformità ai requisiti delle norme ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27017 e ISO/IEC 27018.

La Politica si applica a tutte le informazioni trattate da Edenred, indipendentemente dal formato, dal supporto utilizzato e dall'ambiente di elaborazione, sia esso on premise o cloud. Le disposizioni contenute nel presente documento si applicano altresì a dipendenti, collaboratori, fornitori e terze parti che, a qualsiasi titolo, trattano informazioni o accedono agli asset aziendali.

La presente Politica costituisce il quadro di riferimento per la definizione degli obiettivi di sicurezza delle informazioni e protezione dei dati personali e supporta l'attuazione, il mantenimento e il miglioramento continuo del SGI.

La Politica è riesaminata almeno annualmente e ogniqualvolta intervengano cambiamenti significativi nel contesto organizzativo, normativo, tecnologico o di rischio, al fine di garantirne la continua adeguatezza, efficacia e coerenza con gli obiettivi aziendali.

1.2. SGI e ambito di applicazione

Edenred Italia ha determinato i confini e l'applicabilità del sistema di gestione per stabilirne il campo di applicazione, nonché l'ambito di validità del sistema.

Nel definire il campo di applicazione del sistema di gestione, si sono considerati:

- I fattori esterni e interni;
- I requisiti relativi alle necessità e aspettative delle parti interessate;
- Le interfacce e le interdipendenze tra le attività da essa svolte e quelle svolte dalle altre organizzazioni.

Edenred Italia ha identificato come campo di applicazione del sistema di gestione tutti i processi di governo, gestione, esercizio e controllo atti a garantire la sicurezza ed il corretto funzionamento delle infrastrutture necessarie all'erogazione dei servizi/prodotti, ovvero, elevati standard di qualità, di sicurezza delle informazioni e protezione dei dati personali correlate e di continuità operativa.
Un campo di applicazione chiaramente definito è fondamentale per garantire efficacia, coerenza e conformità ai requisiti normativi, oltre a facilitare la gestione, la comunicazione ed il miglioramento continuo all'interno dell'organizzazione.
Il SGI si applica a tutto il personale, ai collaboratori e alle terze parti che operano nell'ambito del campo di applicazione definito dall'organizzazione.
Per supportare l'attuazione e il mantenimento del SGI, Edenred ha definito e mantiene un insieme di politiche, procedure, standard e altre informazioni documentate conformi ai requisiti delle norme ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 27017 e ISO/IEC 27018.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Tutto il personale è tenuto a contribuire, nell'ambito delle proprie responsabilità e competenze, alla corretta attuazione, al mantenimento e al miglioramento continuo del SGI.
Ai fini dell'individuazione del campo di applicazione della ISO/IEC 27001:2022, occorre far riferimento al documento **ERIT-SGI- Contesto**.

1.3. Dichiarazione d'intenti

L'Alta Direzione di Edenred, nella figura del General Manager, riconosce la sicurezza delle informazioni e la protezione dei dati personali quali elementi essenziali per il perseguimento degli obiettivi aziendali, la tutela degli asset informativi, il mantenimento della fiducia di clienti, partner e altre parti interessate, nonché per il rispetto dei requisiti normativi, regolamentari e contrattuali applicabili.

L'organizzazione si impegna inoltre a stabilire, attuare, mantenere e migliorare continuamente il Sistema di Gestione per la Sicurezza delle Informazioni e la Protezione dei Dati Personali (SGI), compresi i processi necessari e le relative interazioni, assicurandone l'efficacia e il miglioramento continuo.

A tal fine, l'Alta Direzione si impegna a:

- Assicurare che la politica e gli obiettivi per la sicurezza delle informazioni e la protezione dei dati personali siano stabiliti e compatibili con gli indirizzi strategici dell'organizzazione, con i requisiti normativi, regolamentari e contrattuali applicabili e con le aspettative delle parti interessate rilevanti;
- Assicurare l'integrazione dei requisiti del SGI nei processi aziendali e nelle attività operative di Edenred;
- Assicurare la disponibilità delle risorse umane, tecnologiche, organizzative e finanziarie necessarie al funzionamento, al mantenimento e al miglioramento continuo del SGI;
- Comunicare e promuovere l'importanza di un'efficace gestione della sicurezza delle informazioni e della protezione dei dati personali, in conformità ai requisiti del SGI;
- Fornire guida, supporto, formazione e attività di sensibilizzazione al personale affinché contribuisca attivamente all'efficacia del SGI e operi in modo consapevole rispetto alle proprie responsabilità;
- Assicurare che i rischi relativi alla sicurezza delle informazioni e alla protezione dei dati personali siano identificati, valutati, trattati e monitorati secondo un approccio basato sul rischio e coerente con il contesto organizzativo;
- Promuovere il miglioramento continuo del SGI e sostenere i responsabili delle diverse funzioni aziendali affinché dimostrino leadership e impegno nelle rispettive aree di responsabilità.

1.4. Gestione delle Non Conformità e Azioni Correttive

L'organizzazione si impegna ad identificare e gestire prontamente le non conformità del SGI. Le non conformità vengono 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

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

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 costituiscono inadempimento delle obbligazioni contrattuali, sono intraprese azioni disciplinari specifiche nei confronti dei trasgressori.

1.6. Convenzioni

Le politiche definite nel SGI sono integrazioni ai processi in essere definiti nel Manuale della Qualità secondo la norma UNI EN ISO 9001:2015 e ISO/IEC 27001:2022 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 appartenente alle aziende del Gruppo e professionista/i che forniscono servizi e supporto alle attività aziendali
Data Protection	Termine usato in maniera intercambiabile con privacy e protezione dei dati personali
Personale (Es. personale aziendale, personale Edenred)	La struttura interna di gestione dei progetti (dipendenti Edenred) che comprende tutti gli sviluppatori ed i collaboratori coinvolti nella fornitura di servizi e nel supporto delle attività aziendali
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 ai 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,

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	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 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 [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 GDPR]. 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 ad 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

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

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
KPI	**Key Performance Indicators** – Indicatore chiave di prestazione utilizzato per misurare e monitorare il livello di raggiungimento di un obiettivo definito dall'organizzazione, consentendo di valutarne l'efficacia nel tempo

1.8. Acronimi funzioni aziendali

Acronimi	Definizione
CdA	Consiglio di Amministrazione
GM	General Manager – Direttore Generale
CISO	Chief Information Security Officer – Responsabile della sicurezza delle informazioni
CIO	Chief Information Officer - Direttore Technology
CFO	Chief Financial Officer – Direttore Finanziario
DPO	Data Protection Officer – Responsabile protezione dati personali
CSR	Chief People & Sustainability Officer
PIMS	Privacy Information Management System - Sistema di Gestione delle Informazioni sulla Privacy
RID	Riservatezza; Integrità; Disponibilità

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

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

- 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
- Regolamento (UE) 2024/1689 - AI Act

Interni:

- ERIT-SGI-RelazioneAttivitàValutazioneTrattamentoRischio2026
- ERIT–SEC-22301-BIA 2025
- Allegato A al codice di comportamento

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

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

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

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 SGI, in conformità con la 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 SGI.

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 SGI che implementa tale politica e ricevere opportuna formazione.

Il SGI 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 SGI che è stato progettato in conformità con quanto specificato nella norma ISO/IEC 27001 ed ISO/IEC 27701.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

2.2. AI Committee ed utilizzo dell'intelligenza artificiale nel rispetto dei principi aziendali

Edenred ha istituito un AI Committee con l'obiettivo di garantire un'adeguata governance delle iniziative che prevedono lo sviluppo, l'adozione o l'utilizzo di sistemi di Intelligenza Artificiale. Il Comitato è responsabile delle attività di valutazione, revisione e validazione delle iniziative AI, assicurando che tali soluzioni siano analizzate sotto il profilo legale, normativo, etico, tecnologico, di sicurezza delle informazioni e di protezione dei dati personali. L'AI Committee è composto dalle funzioni di Chief Information Security Officer (CISO), dal Data Protection Officer (DPO), dall'Head of Product, dall'Head of Business Growth Intelligence e dall'Head of Enterprise Architecture. I membri del Comitato contribuiscono, nell'ambito delle rispettive responsabilità, all'analisi e alla valutazione delle iniziative AI, assicurandone la conformità ai requisiti legali, normativi ed etici, nonché la coerenza con i principi di sicurezza delle informazioni, protezione dei dati personali, architettura aziendale e obiettivi di business. Le richieste e le comunicazioni indirizzate al Comitato sono trasmesse alla distribution list dedicata (AI Committee-IT@edenred.com), gestita congiuntamente dalle funzioni che ne fanno parte.

Nell'ambito del processo di governance, il Comitato promuove l'adozione e l'utilizzo delle tecnologie di Intelligenza Artificiale in modo responsabile, trasparente e controllato, nel rispetto dei principi organizzativi, delle normative applicabili e delle linee guida aziendali.

Qualora necessario, l'AI Committee si coordina con le strutture competenti della Capogruppo al fine di ottenere indirizzi, pareri specialistici, validazioni o supporto su specifiche iniziative, tematiche regolamentari o aspetti di governance relativi all'Intelligenza Artificiale.

Edenred promuove l'utilizzo responsabile dei sistemi di Intelligenza Artificiale (AI), assicurando che tali tecnologie siano impiegate a supporto delle attività aziendali e dei processi decisionali, senza sostituire il giudizio, la supervisione e la responsabilità umana. L'adozione e l'impiego di soluzioni basate sull'AI avvengono nel rispetto dei principi di sicurezza, trasparenza, affidabilità, equità, protezione dei dati personali, riservatezza delle informazioni e conformità normativa. A tal fine, l'Organizzazione valuta preventivamente gli impatti delle iniziative AI sui processi aziendali, sulle persone e sulle informazioni trattate, assicurandone la coerenza con i requisiti normativi applicabili e con le disposizioni interne.

Edenred si impegna a identificare, valutare e mitigare i rischi connessi all'impiego dell'AI, adottando adeguate misure di controllo volte a garantirne un impiego etico, sicuro ed affidabile. Particolare attenzione è dedicata alla qualità, all'accuratezza e all'integrità dei dati utilizzati, nonché alla prevenzione di errori, bias o risultati non coerenti con le finalità per cui tali sistemi sono adottati.

L'Organizzazione, inoltre, promuove la diffusione della consapevolezza e della formazione del personale coinvolto nello sviluppo, nell'utilizzo o nella gestione di sistemi di Intelligenza Artificiale, al fine di garantire una corretta comprensione delle opportunità, dei rischi e delle responsabilità associate.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

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

Edenred riconosce la sicurezza delle informazioni, la protezione dei dati personali e la continuità operativa quali elementi fondamentali a supporto dei processi di business e delle relazioni con clienti, fornitori e altre parti interessate, al fine di garantire l'erogazione di servizi affidabili, conformi ai requisiti normativi, regolamentari e contrattuali applicabili e coerenti con le esigenze delle parti interessate.

In coerenza con la metodologia Magerit (Risk Analysis & Management) adottata dall'Organizzazione e nell'ottica del miglioramento continuo del Sistema di Gestione, Edenred ha definito i seguenti obiettivi:

1) Contenere i rischi relativi alla sicurezza delle informazioni e alla protezione dei dati personali entro i livelli di accettabilità definiti dall'organizzazione e coerenti con i requisiti normativi applicabili, come indicato all'interno del documento "**ERIT-SGI-RelazioneAttivitàValutazioneTrattamento Rischio2026**";
2) Assicurare la conformità ai requisiti normativi, regolamentari, contrattuali e agli standard di riferimento adottati dall'organizzazione;
3) Garantire la resilienza operativa, la continuità dei servizi e la disponibilità delle informazioni critiche;
4) Supervisionare lo sviluppo e i processi per preservare la privacy e la sicurezza delle informazioni;
5) Garantire attraverso il supporto della funzione HR, la formazione annuale di tutto il personale preposto sulla sicurezza delle informazioni e protezione dei dati personali;
6) Garantire la sicurezza e la resilienza della catena di approvvigionamento attraverso la valutazione periodica e il monitoraggio continuo dei fornitori critici.

Gli obiettivi sopra riportati sono monitorati e misurati attraverso specifici ***Key Performance Indicators* (KPI),** periodicamente riesaminati e sottoposti ad approvazione all'Alta Direzione in fase di Riesame, al fine di valutarne il grado di raggiungimento e l'efficacia delle misure adottate. I risultati delle misurazioni costituiscono un elemento di supporto per il miglioramento continuo del Sistema di Gestione.

La tabella seguente riporta l'associazione tra gli obiettivi definiti ed i relativi KPI di monitoraggio.

Obiettivi	KPI
Contenere i rischi relativi alla sicurezza delle informazioni e alla protezione dei dati personali entro i livelli di accettabilità definiti dall'organizzazione e coerenti con i requisiti normativi applicabili.	1. Percentuale di compliance degli antivirus sui server Windows; 2. Percentuale di compliance degli antivirus sulle postazioni di Lavoro; 3. Percentuale di applicazioni esposte a Internet sottoposte a vulnerability scanner; 4. Percentuale di vulnerabilità critiche e alte risolte; 5. Percentuale di vulnerabilità infrastrutturali critiche e alte con un action plan; 6. Tempo trascorso dall'ultima revisione della procedura di gestione delle vulnerabilità IT; 7. Percentuale dei canali di comunicazione cifrati su un network Edenred; 8. Percentuale di vulnerabilità aperte che sono tracciate; 9. Percentuale di postazioni di lavoro conformi;

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

	10. Percentuale di incidenti di sicurezza IT tracciati ed analizzati; 11. Verificare che la group policy sia attiva sui pc; 12. Percentuale asset IT in cloud correttamente sottoposti a patch di sicurezza; 13. Percentuale attività anomale di utenze ADS rilevate.
Assicurare la conformità ai requisiti normativi, regolamentari, contrattuali e agli standard di riferimento adottati dall'organizzazione.	1. Tempo trascorso dall'ultima revisione della procedura di gestione delle vulnerabilità IT; 2. Tempo dall'ultima revisione IT Risk Assessment.
Garantire la resilienza operativa, la continuità dei servizi e la disponibilità delle informazioni critiche.	1. Percentuale di applicazioni critiche con un'adeguata strategia di backup; 2. Percentuale di applicazioni critiche con backup su cui è stato effettuato un test di ripristino negli ultimi 12 mesi.
Supervisionare lo sviluppo e i processi per preservare la privacy e la sicurezza delle informazioni.	1. Percentuale di sistemi compliant rispetto alla gestione dei cookies; 2. Numero di incidenti di sicurezza informatica con impatto sui dati personali segnalati al DPO entro 24 ore negli ultimi sei mesi; 3. Percentuale change implementate sui servizi cloud coerentemente con il piano definito.
Garantire attraverso il supporto della funzione HR, la formazione annuale di tutto il personale preposto sulla sicurezza delle informazioni e protezione dei dati personali.	1. Percentuale attività di valutazione del trattamento completate su One Trust; 2. Percentuale PIA completate vs identificate; 3. Percentuale nuovi dipendenti formati entro 3 mesi; 4. Percentuale di dipendenti che completano il corso di Data Protection livello 1; 5. Percentuale della popolazione di utenti finali sensibilizzati; 6. Percentuale della popolazione di utenti finali formati; 7. Percentuale di IT Developers formati.
Garantire la sicurezza e la resilienza della catena di approvvigionamento attraverso la valutazione periodica e il monitoraggio continuo dei fornitori critici.	1. Percentuale di questionari di sicurezza ISO 27001 completati dai fornitori totali; 2. Percentuale di controlli di sicurezza valutati come "Satisfied" per i fornitori IT.

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.

Inoltre, al fine di garantire la resilienza operativa, la continuità dei servizi e la disponibilità delle informazioni critiche, Edenred adotta un processo strutturato di Business Impact Analysis (BIA) "**ERIT-**

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

SEC-22301-BIA-2025". I risultati della BIA supportano la definizione ed il periodico riesame delle strategie e dei piani di Business Continuity e Disaster Recovery, nonché dei relativi obiettivi di ripristino.

3. Ruoli e responsabilità

È responsabilità di tutto il personale, dei collaboratori e delle terze parti che operano nell'ambito del SGI essere consapevoli delle politiche, delle procedure e delle regole applicabili alla sicurezza delle informazioni e alla protezione dei dati personali, nonché del proprio contributo all'efficacia del Sistema di Gestione.

Ciascun soggetto è tenuto a svolgere le attività di propria competenza nel rispetto delle responsabilità assegnate, delle disposizioni contenute nella documentazione del SGI e delle misure di sicurezza definite dall'organizzazione, contribuendo attivamente al mantenimento e al miglioramento continuo del sistema.

Di seguito sono riportati i ruoli chiave relativi alla sicurezza delle informazioni e alla protezione dei dati personali definiti da Edenred, con l'indicazione delle principali responsabilità e della relativa collocazione organizzativa.

L'Alta Direzione, nella figura del General Manager, assicura la disponibilità delle risorse necessarie per stabilire, attuare, mantenere e migliorare continuamente il SGI, definendo e comunicando ruoli, responsabilità e autorità necessari al corretto funzionamento del Sistema di Gestione.

3.1. Ruoli

Sigla	Nominativo
GM	Marco Ferrero
CISO	Gianluca Mannella
CIO (BU Technology Leader)	Michele Panigada
CFO	Didier-Vial Maxence
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	Piszczek Agnieszka Monika
Chief Partnership Officer	Fabrizio Ruggiero
Chief Strategy Officer	Daniela De Marco
Chief Customer Excellence Officer	Antonella Mamone
Head of Employee Relations & Reward (HR)	Roberta Monte
Sales & Customer Success Director Welfare	Piszczek Agnieszka Monika
Head of Compliance, Governance and Risk	Valeria Brudaglio

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

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
Head of Product	Luca Melgrati
Head of Business Growth Intelligence	Pasquale Denardo

Per una consultazione più dettagliata della struttura organizzativa aziendale e delle relative attribuzioni, si rinvia al seguente link Organigramma - Workday.

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

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 SGI;
- 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 SGI;
- Approva il budget per la protezione dei dati personali.

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

- Presiede al riesame annuale del SGI;
- Comunica l'importanza dell'efficacia del SGI durante le riunioni aziendali al personale (almeno una all'anno);
- Supervisiona i documenti propri del SGI (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 SGI (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;

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

- 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. Chief Financial Officer (CFO)

Il Chief Financial Officer è responsabile della direzione e della supervisione della funzione Finance, assicurando il presidio della performance economico-finanziaria dell'organizzazione e contribuendo alla definizione e all'attuazione delle strategie aziendali. Garantisce la solidità finanziaria dell'azienda, l'affidabilità delle informazioni economiche, patrimoniali e finanziarie, nonché l'efficacia dei processi di pianificazione, controllo, reporting e gestione dei rischi finanziari.

Principali attività e responsabilità:

- Contribuire alla definizione della strategia aziendale attraverso analisi economico-finanziarie, valutazioni di scenario e previsioni di business;
- Supportare il management nella valutazione di investimenti, iniziative commerciali, nuovi progetti e opportunità di crescita;
- Promuovere una cultura orientata alla performance, all'efficienza operativa e alla sostenibilità economico-finanziaria;
- Monitorare l'andamento economico-finanziario dell'organizzazione attraverso specifici KPI e indicatori di performance;
- Identificare opportunità di ottimizzazione dei costi e di miglioramento dell'efficienza finanziaria;
- Presidiare i rapporti con revisori, consulenti, istituti finanziari e altri stakeholder esterni di competenza;
- Garantire l'efficacia del sistema di controllo interno e dei processi di gestione dei rischi finanziari;
- Assicurare la definizione, l'implementazione e il rispetto delle policy finanziarie e delle procedure aziendali;
- Supervisionare i processi di pianificazione economico-finanziaria e reporting direzionale.

3.2.4. 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.

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.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

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 SGI rispondendo della puntuale applicazione del SGI e dei risultati raggiunti all'Alta Direzione tramite il Chief Legal Officer;
- Coordinarsi con le altre aree aziendali nel raggiungimento degli obiettivi del SGI;
- 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 SGI;
- Pianificare e supportare gli audit interni per verificare lo stato di conformità del SGI;
- 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.

3.2.5. 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;

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

- 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 connessi alla sicurezza delle informazioni e ai dati personali all'interno di Edenred Italia S.r.l.

3.2.6. 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;
- Svolgere 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;

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

- 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 SGI e rende conto della puntuale applicazione del SGI e dei risultati raggiunti all'Alta Direzione tramite il CIO;
- Coordinarsi con le altre aree aziendali nel raggiungimento degli obiettivi del SGI;
- 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 SGI;
- Pianificare ed effettuare audit interni per verificare lo stato di conformità del SGI;
- 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 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 CIO durante il Riesame.

3.2.7. 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;

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

- 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.

3.2.8. Direttori e Responsabili di funzione

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.

3.2.9. 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.

3.2.10. Chief People & Sustainability Officer

Il Chief People & Sustainability Officer è responsabile della definizione e dell'attuazione delle strategie aziendali in materia di gestione delle persone, sviluppo organizzativo, sostenibilità e cultura aziendale,

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

garantendo l'allineamento tra gli obiettivi di business, la valorizzazione del capitale umano e gli impegni ESG (Environmental, Social and Governance) dell'organizzazione.

Tale funzione, supervisiona l'intero ciclo di vita del personale, promuovendo un ambiente di lavoro fondato sui principi di etica, inclusione, responsabilità sociale e conformità normativa. Inoltre, favorisce la diffusione di una cultura aziendale orientata alla sicurezza delle informazioni, alla protezione dei dati personali ed alla continuità operativa, assicurando adeguati livelli di consapevolezza e competenza all'interno dell'organizzazione.

In collaborazione con le funzioni di Governance, Risk, Compliance e Information Security, contribuisce al mantenimento e al miglioramento continuo dei sistemi di gestione adottati dall'organizzazione, supportando la definizione di ruoli, responsabilità e competenze, nonché l'implementazione di iniziative di formazione, sensibilizzazione e sviluppo professionale coerenti con le policy aziendali e gli standard applicabili.

Principali attività e responsabilità:

- Definire e attuare le strategie aziendali in materia di gestione delle persone, sviluppo organizzativo, cultura aziendale e sostenibilità, in linea con gli obiettivi di business;
- Guidare l'evoluzione del modello organizzativo, assicurando che ruoli, responsabilità, competenze e strutture di riporto siano adeguatamente definiti e aggiornati;
- Supervisionare l'intero ciclo di vita dei dipendenti, inclusi i processi di selezione, assunzione, onboarding, sviluppo professionale, valutazione delle performance, mobilità interna e cessazione del rapporto di lavoro;
- Assicurare la definizione e l'attuazione delle strategie ESG, monitorando le iniziative e gli obiettivi correlati alle tematiche ambientali, sociali e di governance;
- Garantire che il personale disponga delle competenze necessarie per lo svolgimento delle proprie attività, attraverso adeguati programmi di formazione e sviluppo;
- Assicurare che i processi di assunzione, variazione di ruolo e cessazione del rapporto di lavoro prevedano l'applicazione dei controlli definiti dalle policy aziendali e dai sistemi di gestione;
- Collaborare con le funzioni Governance, Risk, Compliance, Legal e Information Security per garantire il rispetto dei requisiti normativi, contrattuali e degli standard adottati dall'organizzazione;
- Supportare il mantenimento e il miglioramento continuo dei sistemi di gestione aziendali, contribuendo alla definizione delle competenze, delle responsabilità e dei requisiti di consapevolezza del personale.

3.2.11. Chief Marketing & Product Officer

Il Chief Marketing & Product Officer è responsabile della definizione e dell'attuazione delle strategie di marketing, nonché della gestione e dell'evoluzione del portafoglio prodotti e servizi dell'organizzazione. Assicura l'allineamento tra le esigenze dei clienti, le opportunità di mercato e gli obiettivi aziendali, promuovendo l'innovazione, la competitività dell'offerta e la crescita sostenibile del business. Coordina le attività di marketing e product management, garantendo il continuo sviluppo di soluzioni in grado di generare valore per clienti e stakeholder.

Principali attività e responsabilità:

- Definire e attuare le strategie di marketing e di posizionamento dei prodotti e servizi aziendali;
- Supervisionare la progettazione, l'evoluzione e la gestione del ciclo di vita dei prodotti e delle soluzioni offerte;

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

- Garantire la coerenza tra le esigenze dei clienti, i trend di mercato e gli obiettivi strategici dell'organizzazione;
- Promuovere iniziative di innovazione, trasformazione e sviluppo dell'offerta;
- Collaborare con le funzioni Sales, Operations, IT e Customer Excellence per favorire la crescita del business e l'evoluzione dell'offerta;
- Analizzare il mercato, il contesto competitivo e i bisogni emergenti dei clienti;
- Monitorare le performance di prodotti, servizi e iniziative di marketing attraverso specifici indicatori e KPI;
- Supportare l'identificazione di nuove opportunità di sviluppo, differenziazione e valorizzazione dell'offerta aziendale.

3.2.12. Chief Sales Officer

Il Chief Sales Officer è responsabile della definizione e dell'attuazione della strategia commerciale dell'organizzazione, assicurando il raggiungimento degli obiettivi di crescita, sviluppo del business e consolidamento della presenza sul mercato. Tale funzione, guida e coordina le attività commerciali, promuovendo l'acquisizione di nuovi clienti, la valorizzazione del portafoglio esistente e l'espansione dell'offerta di Edenred. Opera in stretta collaborazione con le altre funzioni aziendali per massimizzare le performance commerciali e supportare il conseguimento degli obiettivi strategici dell'organizzazione.

Principali attività e responsabilità:

- Definire e implementare la strategia commerciale in coerenza con gli obiettivi aziendali;
- Garantire il raggiungimento degli obiettivi di crescita, acquisizione e fidelizzazione della clientela;
- Coordinare e supervisionare le strutture commerciali e di business development;
- Individuare nuove opportunità di mercato e sostenere l'evoluzione dell'offerta commerciale;
- Promuovere iniziative finalizzate all'incremento dei ricavi e allo sviluppo del business;
- Collaborare con le funzioni Marketing, Product e Operations per ottimizzare le performance commerciali e la customer value proposition;
- Monitorare l'andamento del mercato, il posizionamento competitivo e le esigenze della clientela;
- Misurare e analizzare le performance di vendita attraverso specifici indicatori e KPI, definendo eventuali azioni correttive.

3.2.13. Chief Partnership Officer

Il Chief Partnership Officer è responsabile della definizione e dell'attuazione della strategia di partnership aziendale, finalizzata allo sviluppo e al consolidamento dell'ecosistema di partner che contribuiscono all'erogazione e alla diffusione dei servizi dell'organizzazione, inclusi esercenti convenzionati, merchant, partner commerciali e fornitori di servizi. Supervisiona la creazione, la gestione e il rafforzamento delle relazioni con i partner strategici e gli altri stakeholder dell'ecosistema, promuovendo opportunità di collaborazione e sviluppo del business. Opera con l'obiettivo di ampliare la rete di accettazione dei servizi, incrementare il valore generato dalle partnership e supportare la crescita sostenibile dell'organizzazione.

Principali attività e responsabilità:

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

- Definire la strategia di sviluppo e gestione delle partnership;
- Garantire la crescita della rete di partner e convenzionati;
- Sviluppare e mantenere relazioni con partner strategici;
- Identificare nuove opportunità di collaborazione e sviluppo commerciale;
- Assicurare il raggiungimento degli obiettivi di crescita e copertura della rete;
- Sviluppare nuove collaborazioni strategiche;
- Monitorare la performance e qualità delle partnership;
- Coordinare le iniziative volte all'espansione della rete di accettazione dei servizi Edenred.

3.2.14. Chief Strategy Officer

Il Chief Strategy Officer è responsabile della definizione, del coordinamento e del monitoraggio della strategia aziendale, assicurando l'allineamento tra gli obiettivi di business, le opportunità di mercato e i piani di sviluppo dell'organizzazione. Supervisiona le iniziative strategiche e i programmi di trasformazione e innovazione, supportando il management nell'individuazione di opportunità di crescita, miglioramento delle performance e creazione di valore sostenibile nel lungo periodo.

Principali attività e responsabilità:

- Definire, aggiornare e promuovere la strategia aziendale in coerenza con gli obiettivi organizzativi;
- Supportare il management nei processi decisionali e nella pianificazione strategica;
- Coordinare programmi di trasformazione, innovazione e sviluppo organizzativo;
- Monitorare l'evoluzione del mercato, il contesto competitivo e i principali trend di settore;
- Identificare opportunità di crescita, efficientamento e sviluppo del business;
- Valutare iniziative strategiche, partnership e opportunità di investimento a supporto degli obiettivi aziendali;
- Garantire l'allineamento delle iniziative strategiche con le priorità e gli obiettivi dell'organizzazione;
- Monitorare l'avanzamento dei programmi strategici e misurarne i risultati attraverso specifici indicatori di performance.

3.2.15. Chief Customer Excellence Officer

Il Chief Customer Excellence Officer è responsabile della definizione e dell'attuazione delle strategie volte a garantire un'esperienza cliente eccellente lungo l'intero ciclo di vita dei prodotti e dei servizi aziendali. Coordina e supervisiona le attività di Customer Care, Customer Experience e Customer Success, assicurando elevati livelli di soddisfazione, fidelizzazione e qualità dei servizi erogati a clienti, utenti e partner. Promuove il miglioramento continuo dei processi e monitora le performance dei servizi attraverso specifici indicatori di qualità e customer satisfaction, contribuendo alla creazione di valore e al rafforzamento delle relazioni con i clienti.

Principali attività e responsabilità:

- Definire e sviluppare la strategia di Customer Experience, in coerenza con gli obiettivi aziendali;
- Garantire l'efficacia e la qualità dei servizi di assistenza e supporto alla clientela;
- Monitorare la soddisfazione dei clienti attraverso l'analisi di KPI e indicatori di performance;
- Coordinare i processi di raccolta, analisi e gestione dei feedback dei clienti;

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

- Identificare e promuovere iniziative di miglioramento continuo dell'esperienza cliente;
- Collaborare con le funzioni Marketing, Sales, Operations e Product per assicurare un'esperienza cliente integrata, efficace e coerente su tutti i canali di contatto;
- Supportare la definizione di strategie volte ad aumentare la fidelizzazione e la retention della clientela.

3.2.16. Sales & Customer Success Director Welfare

Il Sales & Customer Success Director Welfare è responsabile della definizione e dell'attuazione delle strategie commerciali e di Customer Success relative ai servizi Welfare. Coordina le attività di acquisizione, sviluppo e gestione del portafoglio clienti, assicurando il raggiungimento degli obiettivi di business, la crescita sostenibile del mercato di riferimento e il mantenimento di elevati livelli di soddisfazione e fidelizzazione della clientela.

Principali attività e responsabilità:

- Definire e implementare le strategie commerciali per i servizi Welfare;
- Coordinare e supervisionare i team Sales e Customer Success;
- Garantire elevati livelli di soddisfazione, fidelizzazione e retention della clientela;
- Monitorare le performance commerciali attraverso specifici indicatori e KPI;
- Individuare opportunità di sviluppo del business e di valorizzazione dell'offerta Welfare;
- Supportare la definizione e il miglioramento continuo di prodotti e servizi;
- Collaborare con le funzioni Marketing, Product, Operations e Customer Care per garantire un'esperienza cliente efficace, coerente e orientata alla creazione di valore.

3.2.17. 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;

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

- 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 e promuovere una cultura di miglioramento continuo all'interno del team antifrode.

3.2.18. Head of Employee Relations and Reward

L'Head of Employee Relations and Reward è responsabile della definizione, dell'implementazione e del presidio delle strategie aziendali in materia di relazioni con il personale, gestione dei rapporti di lavoro, sistemi di remunerazione e programmi di incentivazione. Tale funzione, assicura l'adozione di politiche e pratiche HR coerenti con gli obiettivi dell'organizzazione, promuovendo un ambiente di lavoro basato su equità, valorizzazione delle persone, conformità normativa e sostenibilità organizzativa. Tale funzione supporta il management nella gestione delle tematiche giuslavoristiche e nell'assunzione delle decisioni relative al personale, garantendo la corretta applicazione della normativa vigente, delle policy aziendali e delle linee guida definite a livello di Gruppo. Contribuisce inoltre allo sviluppo di sistemi di reward finalizzati ad attrarre, motivare e trattenere i talenti, favorendo l'allineamento tra performance individuali e obiettivi aziendali.

Principali attività e responsabilità:

- Definire ed aggiornare le politiche aziendali in materia di Employee Relations, Compensation & Benefit e reward;
- Fornire supporto e consulenza specialistica al management su tematiche giuslavoristiche e di gestione del personale;
- Supervisionare gli aspetti contrattuali relativi al rapporto di lavoro e garantire la conformità alla normativa vigente;
- Coordinare le iniziative relative alla remunerazione, ai sistemi incentivanti, ai benefit ed ai programmi di riconoscimento delle performance;
- Gestire le relazioni con i dipendenti e supportare la risoluzione di questioni organizzative e disciplinari;
- Collaborare con le funzioni HR, Legal, Finance e con il management aziendale per supportare i processi decisionali inerenti al personale;
- Monitorare l'evoluzione delle normative del lavoro ed assicurarne il recepimento nei processi e nelle policy aziendali;
- Garantire l'allineamento delle pratiche HR alle linee guida e agli indirizzi definiti dal Gruppo.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

3.2.19. Head of Compliance, Governance and Risk

L'Head of Compliance, Governance and Risk è responsabile della definizione, implementazione e supervisione del framework aziendale di governance, gestione dei rischi e conformità normativa, assicurandone l'allineamento agli obiettivi strategici dell'organizzazione e ai requisiti legislativi, regolamentari e contrattuali applicabili. Tale funzione supporta il management nell'identificazione, valutazione, mitigazione e monitoraggio dei rischi aziendali, promuovendo una cultura orientata alla compliance, al controllo interno e al miglioramento continuo. Inoltre, assicura il coordinamento delle attività di governance e dei sistemi adottati dall'organizzazione, contribuendo alla tutela del patrimonio aziendale nonché, alla resilienza organizzativa ed alla conformità ai requisiti normativi ed agli standard di riferimento.

L'Head of Compliance, Governance and Risk collabora trasversalmente con tutte le aree aziendali, fornendo indirizzo metodologico e supporto specialistico in materia di gestione dei rischi, compliance, continuità operativa, sicurezza delle informazioni e controlli interni.

Principali attività e responsabilità:

- Definire e mantenere il framework di Governance, Risk and Compliance dell'organizzazione, assicurandone la coerenza con gli obiettivi aziendali e le best practice di settore;
- Coordinare i processi di identificazione, valutazione, trattamento e monitoraggio dei rischi aziendali, inclusi i rischi operativi, tecnologici, normativi e reputazionali;
- Supportare il management nella definizione delle strategie di mitigazione e nella valutazione dell'efficacia dei controlli interni;
- Monitorare l'evoluzione del contesto normativo e regolamentare, valutandone gli impatti sull'organizzazione e promuovendo le necessarie azioni di adeguamento;
- Definire, mantenere e promuovere policy, procedure e standard aziendali volti a garantire la conformità ai requisiti applicabili;
- Collaborare con le funzioni Legal, Information Security, Privacy, Procurement ed HR per garantire un approccio integrato alla gestione del rischio ed alla conformità normativa;
- Verificare la conformità ai requisiti normativi, regolamentari e contrattuali applicabili in materia di sicurezza delle informazioni;
- Supportare il mantenimento ed il miglioramento continuo dei sistemi di gestione e delle certificazioni aziendali.

3.2.20. Head of Legal Affairs – Advisory & Mobility

La funzione Head of Legal Affairs è responsabile del presidio e del coordinamento delle attività legali dell'organizzazione, garantendo supporto specialistico alle diverse funzioni aziendali ed al management nella gestione delle tematiche contrattuali, normative, regolamentari e di compliance. La funzione assicura la tutela degli interessi aziendali attraverso la valutazione dei rischi legali, la predisposizione e revisione della documentazione contrattuale, il supporto alle iniziative commerciali e strategiche, nonché l'interpretazione delle normative applicabile alle attività aziendali.

Tale funzione fornisce inoltre consulenza legale continuativa alle strutture interne, supportando i processi decisionali e contribuendo alla definizione di soluzioni conformi ai requisiti normativi e agli obiettivi di business. Tra le principali responsabilità rientrano anche il coordinamento delle attività di contenzioso e precontenzioso, la gestione dei rapporti con i consulenti legali esterni ed il supporto nella definizione e nell'aggiornamento di procedure e modelli contrattuali.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Nell'ambito della Direzione Legal Affairs, le responsabilità risultano articolate tra un presidio trasversale di consulenza e supporto legale aziendale, affidato all'Head of Legal Affairs & Advisory, e un presidio specialistico dedicato alle attività della business unit Mobility, affidato all'Head of Legal Affairs - Mobility, con particolare riferimento agli aspetti legali connessi ai servizi, ai contratti e alle iniziative di business afferenti a tale area.

Con riferimento alla funzione Legal Affairs, le responsabilità risultano dunque articolate in due ambiti distinti di competenza:

- **Head of Legal Affairs & Advisory:** Responsabile del coordinamento delle attività legali e consulenziali a supporto delle diverse funzioni aziendali. Il ruolo fornisce indirizzo e assistenza su questioni contrattuali, societarie, regolamentari e di contenzioso, assicurando un supporto trasversale al business ed al management nelle attività decisionali;
- **Head of Legal Affairs – Mobility:** Responsabile del presidio delle tematiche legale afferenti alla business unit Mobility. Il ruolo supporta le attività operative e commerciali della divisione mediante la gestione della contrattualistica con clienti, partner e fornitori, l'assistenza nelle procedure pubbliche, il supporto ai nuovi progetti ed il coordinamento delle attività di precontenzioso e contenzioso.

3.2.21. Head of Demand and Governance

L'Head of Demand and Governance è responsabile della gestione della domanda di evoluzione dei servizi e delle soluzioni IT, assicurando che le esigenze del business siano raccolte, valutate, prioritizzate e tradotte in iniziative coerenti con gli obiettivi strategici dell'organizzazione. Supervisiona inoltre i processi di governance finalizzati a garantire un efficace coordinamento tra le funzioni aziendali e tecnologiche, promuovendo il miglioramento continuo dei processi e l'ottimizzazione delle risorse.

Principali attività e responsabilità:

- Raccogliere, analizzare e qualificare le richieste provenienti dalle diverse funzioni aziendali;
- Garantire l'allineamento delle iniziative progettuali con la strategia aziendale, le priorità di business e la roadmap tecnologica;
- Definire, implementare e presidiare i processi di Demand Management e Governance, assicurando una corretta valutazione, prioritizzazione e pianificazione delle iniziative progettuali;
- Favorire il coordinamento tra le funzioni di business e le strutture IT, garantendo la raccolta, l'analisi e la traduzione dei requisiti aziendali in soluzioni efficaci e sostenibili;
- Promuovere il miglioramento continuo attraverso attività di analisi, ottimizzazione e standardizzazione dei processi aziendali e tecnologici;
- Supportare i processi decisionali relativi agli investimenti e alle priorità progettuali mediante analisi di impatto, valutazioni costi-benefici ed identificazione dei rischi associati;
- Garantire la conformità ai modelli di governance aziendale, alle policy interne e agli standard organizzativi applicabili, assicurandone la corretta applicazione.

3.2.22. Head of Enterprise Architecture

L'Head of Enterprise Architecture fa parte del Technology Leadership Team di Edenred Italia e riporta funzionalmente all'EMEA (Employee Benefits Architecture Head). La figura collabora con il Team Centrale di Architettura del Gruppo ed è coinvolta nelle iniziative di business e tecnologiche di Edenred

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

Italia, con l'obiettivo di guidare l'evoluzione dell'architettura aziendale, supportare il programma di trasformazione digitale e promuovere l'adozione di soluzioni innovative e condivise a livello di Gruppo.

Principali attività e responsabilità:

- Definire e governare l'architettura di riferimento del Sistema Informativo, assicurandone l'allineamento con la strategia aziendale, le esigenze di business, gli obiettivi ed il piano di trasformazione digitale;
- Mantenere ed aggiornare il repository architetturale relativo ai processi, applicazioni, tecnologie e relative interdipendenze;
- Definire i principi architetturali, la struttura tecnologica del Sistema Informativo e le modalità di integrazione tra sistemi interni ed esterni;
- Rappresentare la funzione Enterprise Architecture nei processi di governance aziendale e nelle community di architettura del Gruppo, contribuendo alla definizione, promozione e diffusione di standard, metodologie, best practice e soluzioni condivise, nonché supportando le decisioni relative ad investimenti IT, iniziative progettuali, sicurezza delle informazioni, continuità operativa, interoperabilità, selezione delle soluzioni e gestione dei fornitori;
- Tradurre gli indirizzi strategici aziendali in requisiti tecnologici, identificando le evoluzioni necessarie del Sistema Informativo e proponendo percorsi di sviluppo sostenibili dal punto di vista tecnico, operativo ed economico;
- Governare l'evoluzione dell'architettura del Sistema Informativo, monitorando l'architettura corrente e target, le obsolescenze tecnologiche, il debito tecnico, i rischi ed i relativi impatti sui servizi e sul business;
- Assicurare l'attuazione delle iniziative necessarie alla convergenza del Sistema Informativo verso l'architettura di riferimento, promuovendo il miglioramento continuo ed il riutilizzo delle soluzioni definite a livello di Gruppo;
- Garantire che i nuovi progetti, le iniziative tecnologiche e le soluzioni adottate siano conformi ai principi e agli standard architetturali aziendali, valutando eventuali soluzioni transitorie e definendo i relativi piani di adeguamento;
- Supportare i processi di governance e le attività decisionali aziendali, fornendo indirizzo architetturale e valutazioni sugli impatti delle iniziative strategiche.

3.2.23. Head of Core & Digital Solutions Director

Il Core & Digital Solutions Director è responsabile della governance, dell'evoluzione e della gestione delle applicazioni digitali e dei sistemi core di Edenred Italia. Coordina la realizzazione delle iniziative tecnologiche, garantisce la continuità e l'evoluzione del patrimonio applicativo aziendale e supporta il percorso di trasformazione digitale, assicurando l'allineamento tra esigenze di business, architettura applicativa ed obiettivi strategici dell'organizzazione.

Principali attività e responsabilità:

- Governare il portafoglio dei progetti applicativi e digitali, monitorandone obiettivi, priorità, pianificazione, budget, rischi e costi;
- Assicurare la realizzazione ed il coordinamento dei progetti tecnologici relativi ai canali digitali ed ai sistemi core aziendali;
- Garantire la manutenzione evolutiva e correttiva delle applicazioni aziendali, incluse le attività di supporto applicativo di secondo e terzo livello;

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

- Definire e promuovere soluzioni software coerenti con le best practice di settore;
- Guidare le iniziative di trasformazione IT, favorendo l'adozione di soluzioni innovative e l'evoluzione tecnologica del Sistema Informativo;
- Assicurare la gestione e l'implementazione delle azioni correttive e di miglioramento derivanti dai processi di supporto e gestione dei ticket;
- Collaborare con il team Infrastructure per identificare e definire gli ambienti tecnologici più idonei a supportare l'esercizio, le prestazioni e l'evoluzione delle applicazioni aziendali;
- Rappresentare la funzione Core & Digital Solutions nei principali comitati di coordinamento e governance, partecipando alle attività di pianificazione, definizione delle iniziative progettuali ed indirizzo tecnologico.

3.2.24. Head of Testing & Quality Assurance

L'Head of Testing & Quality Assurance è responsabile della definizione, dell'implementazione e del presidio delle strategie, metodologie e processi di Testing e Quality Assurance adottati dall'organizzazione. Garantisce che le soluzioni applicative soddisfino i requisiti di qualità, affidabilità e conformità prima del rilascio in esercizio, coordinando le attività di verifica e validazione e promuovendo il miglioramento continuo degli standard di qualità aziendali.

Principali attività e responsabilità:

- Definire e governare il framework aziendale di Testing e Quality Assurance, assicurandone l'applicazione coerente all'interno dell'organizzazione;
- Garantire la qualità, l'affidabilità e la conformità delle soluzioni applicative attraverso processi strutturati di verifica e validazione;
- Coordinare i team di testing interni e fornitori esterni coinvolti nelle attività di Quality Assurance;
- Supervisionare la gestione delle anomalie, dei rischi e delle non conformità rilevate durante il ciclo di test, monitorandone la risoluzione;
- Assicurare la produzione e l'aggiornamento della documentazione di test, della reportistica e delle evidenze necessarie a supporto dei processi di rilascio;
- Promuovere l'adozione di metodologie, strumenti e pratiche finalizzate all'incremento dell'efficienza e dell'efficacia delle attività di Quality Assurance.

3.2.25. Head of Infrastructure & Operations

L'Head of Infrastructure & Operations è responsabile della governance, della gestione e dell'evoluzione delle infrastrutture tecnologiche e dei servizi IT di Edenred Italia. Coordina le attività operative ed infrastrutturali garantendo la disponibilità, la resilienza, la sicurezza e l'efficienza dei sistemi e dei servizi IT, assicurando il supporto alle esigenze di business, ai programmi di trasformazione tecnologica e all'adozione degli standard definiti a livello di Gruppo.

Principali attività e responsabilità:

- Definire e governare la strategia infrastrutturale di Edenred Italia, assicurandone l'allineamento con gli obiettivi aziendali e le direttive tecnologiche del Gruppo;

Pubblico

Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

- Garantire la disponibilità, la continuità operativa, le prestazioni e l'affidabilità delle infrastrutture tecnologiche e dei servizi IT aziendali;
- Gestire e coordinare le attività di IT Operations e di supporto agli utenti, assicurando adeguati livelli di servizio e la continuità operativa delle soluzioni tecnologiche;
- Pianificare e governare l'evoluzione delle infrastrutture tecnologiche, inclusi sistemi, reti, telecomunicazioni, servizi cloud, data center, piattaforme di collaborazione e postazioni di lavoro;
- Assicurare il mantenimento e l'adeguatezza degli ambienti tecnologici a supporto delle attività di sviluppo, collaudo e produzione delle applicazioni aziendali;
- Condurre attività di analisi e revisione delle infrastrutture e dei servizi IT, promuovendo il miglioramento continuo dei processi, delle metodologie e degli standard operativi;
- Definire e gestire la roadmap infrastrutturale, inclusi i programmi di rinnovamento tecnologico e la sostituzione dei sistemi giunti a fine ciclo di vita;
- Collaborare con il CISO e con le altre funzioni aziendali per la gestione dei rischi IT, l'implementazione delle remediation di sicurezza e il rafforzamento delle misure di protezione delle infrastrutture;
- Definire e gestire i piani di Disaster Recovery, coordinandone l'aggiornamento e l'esecuzione periodica dei test;
- Supportare le iniziative di trasformazione aziendale, i progetti strategici e le operazioni di fusione e acquisizione, per gli ambiti di competenza infrastrutturale;
- Gestire il budget OPEX e CAPEX dell'area Infrastructure & IT Operations, nonché gli acquisti IT, i rapporti con i fornitori e la gestione dei relativi contratti;
- Monitorare le performance operative attraverso KPI e reporting periodici, fornendo visibilità agli stakeholder locali e di Gruppo;
- Collaborare con i team Global Technology per promuovere l'adozione degli standard, delle architetture e delle soluzioni tecnologiche condivise;
- Gestire, coordinare e sviluppare le risorse interne ed esterne della funzione, garantendone l'allocazione ottimale sulle attività di esercizio e sui progetti, in linea con le priorità aziendali e gli obiettivi assegnati.

3.2.26. Head of Product

L'Head of Product è responsabile della definizione, dell'evoluzione e della gestione del portafoglio prodotti e servizi dell'Organizzazione, assicurandone l'allineamento con la strategia aziendale, le esigenze dei clienti e gli obiettivi del business.

Principali attività e responsabilità:

- Definire la strategia e la roadmap di prodotto;
- Raccogliere e valutare i requisiti di business e le esigenze degli stakeholder;
- Coordinare lo sviluppo, l'evoluzione ed il miglioramento continuo dei prodotti e servizi;
- Valutare l'impatto di nuove tecnologie ed iniziative strategiche, incluse quelle basate sull'Intelligenza Artificiale;
- Promuovere l'innovazione e l'introduzione di nuove funzionalità e soluzioni.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.

3.2.27. Head of Business Growth Intelligence

L'Head of Business Growth Intelligence è responsabile dell'analisi dei dati e delle informazioni di business finalizzate a supportare la crescita dell'Organizzazione, l'identificazione di nuove opportunità ed il miglioramento delle performance aziendali. Assicura la disponibilità di analisi ed evidenze a supporto dei processi decisionali strategici.

Principali attività e responsabilità:

- Definire e coordinare le attività di Business Intelligence e analisi dei dati;
- Raccogliere, analizzare e interpretare dati provenienti da fonti interne ed esterne;
- Individuare trend, opportunità di mercato e aree di miglioramento delle performance;
- Supportare il management nelle decisioni strategiche attraverso analisi e reporting;
- Valutare l'utilizzo di tecnologie avanzate, incluse soluzioni di Intelligenza Artificiale e analisi predittiva, per generare valore per il business.

3.2.28. 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.

3.2.29. Cyber Security Compliance Specialist

Il Cyber Security Compliance 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.

Pubblico
Questo documento contiene informazioni classificate come Pubbliche (C1). Le informazioni contenute possono essere utilizzate, condivise e distribuite liberamente, nel rispetto delle normative applicabili e dell'integrità del contenuto. Il documento è di proprietà di Edenred Italia S.r.l.