

LINEE GUIDA PRIVACY FIBERCOP:

Framework di governance per la protezione dei dati e la privacy di FiberCop

FiberCop si impegna a garantire la protezione dei dati personali e i diritti degli interessati in conformità al **Regolamento generale sulla protezione dei dati dell'UE (GDPR – Regolamento UE 2016/679)** e alla normativa nazionale applicabile. L'azienda ha implementato un **Framework di governance della privacy** strutturato, progettato per assicurare la corretta gestione dei dati personali lungo tutto il loro ciclo di vita.

Governance della privacy e struttura organizzativa

FiberCop agisce in qualità di **Titolare del trattamento** per i dati personali che tratta. In linea con i requisiti del GDPR, il **Consiglio di Amministrazione ha nominato un Data Protection Officer (DPO) il 1° luglio 2024**, responsabile di supervisionare la conformità dell'azienda alla normativa in materia di protezione dei dati e di fornire indicazioni al management e ai dipendenti.

Il DPO opera con il supporto della **Privacy Supervisory Unit all'interno della funzione Legal Governance, Processes & Analysis** e collabora strettamente con il Chief Compliance Officer e con le altre funzioni aziendali per garantire un'implementazione coerente delle politiche privacy in tutta l'organizzazione.

Il modello privacy di FiberCop prevede la designazione di **Internal Privacy Delegates (Delegati Interni Privacy – DIP)** presso le principali unità di business. Tali delegati sono responsabili dell'implementazione operativa dei requisiti del GDPR nei rispettivi dipartimenti e assicurano l'allineamento con le politiche e le procedure privacy dell'azienda.

Questa struttura di governance assicura il monitoraggio degli sviluppi normativi, le verifiche interne di conformità e l'integrazione dei principi di protezione dei dati nei processi operativi.

Processi di conformità privacy

Il framework privacy di FiberCop include una serie di processi pensati per garantire la conformità alle leggi applicabili in materia di protezione dei dati e l'efficace gestione dei dati personali. Tra questi:

- Gestione e aggiornamento periodico del **Registro delle attività di trattamento** ai sensi dell'articolo 30 del GDPR.
- Monitoraggio continuo della normativa applicabile e degli sviluppi regolamentari.
- Implementazione di procedure per la **gestione e la notifica delle violazioni di dati personali**.
- Supporto legale e operativo alle funzioni di business su tematiche privacy, inclusi **assessment del rischio privacy e valutazioni d'impatto**.
- Integrazione delle **Privacy Impact Assessments (PIA)** e delle attività di analisi del rischio nei casi in cui nuove operazioni di trattamento possano presentare rischi per gli interessati.

Il DPO e la struttura di governance privacy supportano inoltre le attività contrattuali con terze parti e assicurano l'adeguata integrazione di clausole e requisiti privacy negli accordi con fornitori e partner.

Diritti degli interessati

FiberCop garantisce che le persone possano esercitare i propri diritti ai sensi del GDPR, inclusi i diritti di **accesso, rettifica, cancellazione, limitazione del trattamento e opposizione**.

Per agevolare l'esercizio di tali diritti, FiberCop mette a disposizione un **canale di comunicazione dedicato con il Data Protection Officer** tramite il seguente punto di contatto:

dpo.fibercop@fibercop.com

Questo canale fornisce un meccanismo diretto e tracciabile attraverso il quale gli interessati possono presentare richieste, ottenere informazioni o segnalare questioni attinenti alla privacy. Un'ulteriore casella di posta interna supporta le comunicazioni privacy all'interno dell'azienda.

Ulteriori informazioni sul trattamento dei dati personali sono disponibili nella **Web Privacy Policy pubblica** di FiberCop, che descrive le finalità della raccolta dei dati, le categorie di dati trattati, le basi giuridiche del trattamento e l'eventuale coinvolgimento di fornitori di servizi terzi:

<https://www.fibercop.com/en/informations/web-privacy-policy-cookies/>

Sicurezza dei dati e protezione delle informazioni

FiberCop integra la protezione dei dati nel proprio più ampio **framework di sicurezza delle informazioni e gestione dei rischi**.

L'azienda ha ottenuto la **certificazione ISO/IEC 27001** per la gestione di tutti gli asset tecnologici e dei processi di ICT risk management e copre il 100% dei siti (2 siti chiave in cui è presente la funzione Security). Tale certificazione conferma la presenza di controlli strutturati per la protezione degli asset informativi e per la gestione dei rischi di cybersecurity associati alle attività di trattamento dei dati. Inoltre, la governance privacy di FiberCop è integrata con le funzioni di cybersecurity e compliance, al fine di garantire il monitoraggio continuo dei rischi e l'implementazione di adeguate misure di salvaguardia per la protezione dei dati personali.

Formazione e consapevolezza

Le attività di formazione e sensibilizzazione rappresentano un elemento chiave del modello di governance di FiberCop in materia di privacy e sicurezza delle informazioni. L'azienda eroga a tutti i dipendenti **formazione obbligatoria sia sulla consapevolezza in ambito cybersecurity sia sulla normativa privacy e sui principi di protezione dei dati**.

Tali programmi sono progettati per garantire che i dipendenti comprendano le proprie responsabilità ai sensi del GDPR e siano in grado di applicare le politiche e le procedure privacy dell'azienda nelle attività quotidiane. Ulteriori iniziative formative sono previste per gli Internal Privacy Delegates e per il personale coinvolto nella gestione operativa dei dati personali.

Monitoraggio dei data breach e supervisione della conformità

FiberCop mantiene procedure interne per l'identificazione, la gestione e la notifica delle violazioni di dati personali in linea con i requisiti del GDPR.

Integrazione con la corporate governance

Il framework privacy è integrato nel più ampio sistema di governance societaria e compliance di FiberCop. Il DPO collabora strettamente con le funzioni aziendali responsabili di compliance, cybersecurity, internal audit e risk management, al fine di garantire che le considerazioni in materia di protezione dei dati siano incorporate nei processi operativi e nelle strutture decisionali.