FIBERCOP PRIVACY GUIDELINES:

FiberCop Data Protection and Privacy Governance Framework

FiberCop is committed to ensuring the protection of personal data and the rights of data subjects in accordance with the **EU General Data Protection Regulation (GDPR – Regulation EU 2016/679)** and applicable national legislation. The company has implemented a structured **Privacy Governance Framework** designed to ensure the correct management of personal data throughout its entire lifecycle.

Privacy Governance and Organizational Structure

FiberCop acts as **Data Controller** for the personal data it processes. In line with GDPR requirements, the **Board of Directors appointed a Data Protection Officer (DPO) on 1 July 2024**, responsible for overseeing the company's compliance with data protection regulations and providing guidance to management and employees.

The DPO operates with the support of the **Privacy Supervisory Unit within the Legal Governance, Processes & Analysis function** and works closely with the Chief Compliance Officer and other corporate functions to ensure consistent implementation of privacy policies across the organization.

FiberCop's Privacy model includes the designation of **Internal Privacy Delegates (Delegati Interni Privacy – DIP)** across relevant business units. These delegates are responsible for the operational implementation of GDPR requirements within their respective departments and ensure alignment with the company's privacy policies and procedures.

This governance structure ensures the monitoring of regulatory developments, internal compliance assessments, and the integration of data protection principles into operational processes.

Privacy Compliance Processes

The FiberCop privacy framework includes a series of processes designed to ensure compliance with applicable data protection laws and the effective management of personal data. These include:

- Maintenance and regular updating of the **Register of Processing Activities** in accordance with Article 30 of the GDPR.
- Continuous monitoring of applicable legislation and regulatory developments.
- Implementation of procedures for the **management and notification of personal data breaches**.
- Legal and operational support to business functions on privacy matters, including **privacy risk assessments and impact evaluations**.
- Integration of **Privacy Impact Assessments (PIA)** and risk analysis activities in cases where new processing operations may present risks to data subjects.

The DPO and the Privacy governance structure also support contractual activities with third parties and ensure the appropriate integration of privacy clauses and requirements in supplier and partner agreements.

Data Subject Rights

FiberCop ensures that individuals can exercise their rights under the GDPR, including the rights of **access, rectification, deletion, restriction of processing, and objection**.

To facilitate these rights, FiberCop provides a **dedicated communication channel with the Data Protection Officer** through the following contact point:
dpo.fibercop@fibercop.com
This channel provides a direct and traceable mechanism through which data subjects may submit requests, obtain information, or raise privacy-related concerns. An additional internal mailbox supports privacy-related communications within the company.
Further information regarding the processing of personal data is available in FiberCop's **public Web Privacy Policy**, which describes the purposes of data collection, the categories of data processed, the legal bases for processing, and the potential involvement of third-party service providers:
https://www.fibercop.com/en/informations/web-privacy-policy-cookies/

Data Security and Information Protection

FiberCop integrates data protection with its broader **information security and risk management framework**.
The company has obtained **ISO/IEC 27001 certification** for the management of all technological assets and ICT risk management processes and it covers 100% of sites (2 key sites where Security function is located). This certification confirms the presence of structured controls for the protection of information assets and the management of cybersecurity risks associated with data processing activities.
In addition, FiberCop's privacy governance is integrated with its cybersecurity and compliance functions in order to ensure the continuous monitoring of risks and the implementation of appropriate safeguards for the protection of personal data.

Training and Awareness

Training and awareness activities represent a key element of FiberCop's privacy and information security governance model. The company provides **mandatory training both on cybersecurity awareness and privacy legislation and data protection principles** to all employees.
These programs are designed to ensure that employees understand their responsibilities under GDPR and are able to apply the company's privacy policies and procedures in their daily activities. Additional training initiatives are provided to Internal Privacy Delegates and other personnel involved in the operational management of personal data.

Data Breach Monitoring and Compliance Oversight

FiberCop maintains internal procedures for the identification, management, and notification of personal data breaches in line with GDPR requirements.

Integration with Corporate Governance

The privacy framework is integrated into FiberCop's broader corporate governance and compliance system. The DPO works closely with corporate functions responsible for compliance, cybersecurity, internal audit, and risk management in order to ensure that data protection considerations are incorporated into operational processes and decision-making structures.