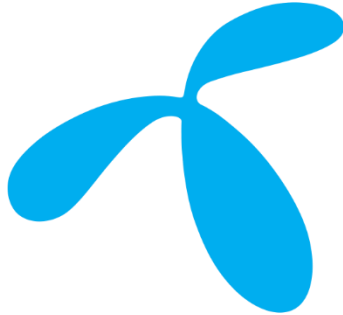


SASB Report

2023



telenor group

Topic	CODE	METRIC	Telenor's response
Environmental Footprint of Operations	TC-TL-130a.1	1) Total energy consumed	6 904 800 GJ. Equal to 1 918 GWh of energy.
		2) Percentage grid electricity	80%. A total of 1 527 GWh has been sourced through the grid.
		3) Percentage renewable	36%. Telenor Group has sourced 655 GWh of renewable electricity through national electricity grids. Renewable grid electricity has been purchased in our Nordic operations via Guarantee of Origin Certificates and in Pakistan and Bangladesh via IRECs. A remaining 24 GWh of renewable electricity has been generated mostly via solar off-grid sites.
Data Privacy	TC-TL-220a.1	Description of policies and practices relating to behavioural advertising and customer privacy	Telenor Group Privacy governance is part of our commitment to Responsible Business. A description can be found on our corporate website at https://www.telenor.com/sustainability/responsible-business/privacy-governance/ Telenor is a diverse group of companies, operating in different markets across Europe and Asia. Each Telenor company is its own data controller and disclose their privacy practices on the respective company's website as part of their privacy statement.
	TC-TL-220a.2	Number of customers whose information is used for secondary purposes	Telenor Group companies may only use customer data for defined and lawful purposes in accordance with current legislation and our internal Group Privacy Policy. Any further use of customer data for secondary purposes may happen in anonymised form, only. A description of our privacy governance structure and the role of our Group Privacy Policy can be found on our corporate website at Privacy governance in Telenor - Telenor Group .
	TC-TL-220a.3	Total amount of monetary losses as a result of legal proceedings associated with customer privacy	We have not registered any losses as a result of legal proceedings associated with customer privacy.
	TC-TL-220a.4	<ol style="list-style-type: none"> 1) Number of law enforcement requests for customer information 2) Number of customers whose information was requested 3) Percentage resulting in disclosure 	Telenor Annual Authority Requests Disclosure report is available here: Telenor Annual Authority Request Disclosure Report 2023

Data Security	TC-TL-230a.1	<ol style="list-style-type: none"> 1) Number of data breaches 2) Percentage involving personally identifiable information (PII), 3) Number of customers affected 	<p>Telenor Group do not report this indicator as details around data breaches are confidential. Global companies, such as Telenor Group, are at constant risk of cyber-attacks. While we are constantly increasing our efforts to actively protect our networks, products and customer data, advanced threat actors are increasingly aiming to steal information, modify customer data or make our services unavailable. Specific details associated with security incidents are subject to national laws and regulation and confidential, as to not compromise the integrity of ongoing and future investigations. For more information on Telenor’s commitment to cyber security, refer to Telenor's Cyber Security page.</p>
	TC-TL-230a.2	<p>Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards</p>	<p>The Telenor Group approach to managing security risk encompasses the utilization of various security standards, notably ISO/IEC 27001. We engage in continuous monitoring the threat landscape through predictive analysis to adaptively establish proactive security measures. These measures include preventative controls, stringent access management, comprehensive vulnerability management, and detective controls. Our monitoring is executed through Security Operation Centers, ensuring vigilant oversight. Additionally, we have reactive controls in place designed for prompt response to challenges through our well-defined incident management procedures. Our strategy extends to recovery processes, guided by robust disaster recovery and crisis management frameworks. Consequently, this comprehensive approach significantly mitigates the impact of security incidents. Read more on how we work with cyber security on Telenor.com and our public position on cyber security. We also refer to our Annual Report for further description in the chapters: ‘Cyber security’ and ‘Risk management’.</p>

Product End-of-Life Management

TC-TL-440a.1

- | | |
|---|--|
| 1) Materials recovered through take back programmes | 466 185 devices. |
| | Telenor Group reports the number of devices returned through take back programmes in the Nordic business units. These consist of mobile devices such as smartphones and fixed CPE devices such as TV boxes and broadband routers. A total of 107 519 mobile devices were returned through take-back programmes of which 93% were reused and 7% were recycled. A total of 358 666 fixed devices were returned through take-back programmes of which 70% were re-used and 30% were recycled. |
| 2) Percentage recovered materials reused | 75% of returned devices (93% of returned mobile devices and 70% of returned fixed devices). |
| 3) Percentage recovered materials recycled | 25% of returned devices (7% of returned mobile devices and 30% of returned fixed devices). |
| 4) Percentage recovered materials landfilled | 0% |

Competitive Behaviour and Open Internet	TC-TL-520a.1	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behaviour regulations	We are not aware of any monetary losses related to legal proceedings associated with anti-competitive behavior in 2023.
	TC-TL-520a.2	Average sustained download speed of 1) owned and commercially-associated content and 2) non-associated content	<p>Mobile network 4G: 19 Mbps Group average DL throughput per user (Mbps).</p> <p>Mobile network 5G: Nordic only: 150 Mbps Nordic average DL throughput per user (Mbps).</p> <p>Telenor does not differentiate between owned, commercial and non-associated content. The source of the average download speed is based on measurement directly from the radio end/equipment and is the average download speed per user for the whole reporting period. The reported 4G download speed is the average of the business units in both Nordic and Asia, while the 5G download speed is average of the Nordic business units.</p>
	TC-TL-520a.3	Description of risks and opportunities associated with net neutrality, paid peering, zero rating and related practices	Legislation on net neutrality, paid peering, zero rating and related practices vary according to the markets where we operate. Telenor Group complies with the applicable legislations in each and every one of them. The company's approach to IP-Interconnection (Peering, IP-Transit and CDN) reflects limited materiality and is focused on optimization in terms of costs and quality. The ruling of the European Court of Justice in September 2021 and the subsequent guidelines from The Body of European Regulators for Electronic Communications (BEREC) in June 2022 eliminated the possibility for Telenor Group's European business units to provide zero rated tariffs. The implementation of this ruling has been completed in all Telenor Group's European business units. The company considers opportunities to be limited within these topics.

Managing Systemic Risks from Technology Disruptions

- TC-TL-550a.1
- 1) System average interruption frequency
 - 2) Customer average interruption duration

Telenor Group is not reporting this indicator as there is no Group wide definition of how to measure this. Our approach to managing systemic risks includes both preventive and corrective actions to avoid major service interruptions and to limit impact to our customers.

The Telenor Risk management policy ensures that risks in Telenor are identified, assessed, and treated in a way that supports Telenor in achieving our ambitions and goals. The Telenor policy framework ensures that Telenor Group is compliant to regulations including security and privacy, enabled through technology design and solutions.

- TC-TL-550a.2
- Discussion of systems to provide unimpeded service during service interruptions

The main business continuity risks associated with technology are technical failures, cyber-attacks, or weather events. The main measures applied to mitigate Business continuity risks from the three main areas include:

- Regular assessment and measurement on service operations according to international standard (e.g. ITIL, TMForum)
- Implementing security capabilities to prevent and reduce the effect of a range of threats to protect the confidentiality, integrity of customer data and internal business information and the availability of services.
- Yearly benchmarking process level against international best practices and capabilities for monitoring and detection. To support incident management and response is measured and developed through Security Operations Center – Capability Maturity Model (SOC-CMM) across Telenor business units to mitigate threats.
- Focus on continuous improvement process to increase automation, operating quality and to better support business and improve customer experience.

In the event of major incidents crisis management plan (CMP) & processes is followed. The CMP is updated on a yearly basis. We also refer to our [Annual Report](#) for supplementary information in the ‘Risk management’ chapter.

Activity Metrics	TC-TL-000.A	Number of wireless subscribers	136 million.
	TC-TL-000.B	Number of wireline subscribers	0.2 million. Nordic only.
	TC-TL-000.C	Number of broadband subscribers	2.2 million. Nordic only.
	TC-TL-000.D	Network traffic (Petabyte)	10 804 PB. Mobile network only.

The SASB report and figures have been in scope for limited assurance. The independent auditor's assurance report is published [here](#).

Reporting Boundaries

The scope of the SASB report follows the Group reporting structure for year-end 2023.