



MTN Group Limited

Transparency Report
for the year ended 31 December 2025

Accelerating Impact

Empowering Africa



Welcome to our 2025 Transparency Report

Our purpose is leading digital solutions for Africa's progress

Inside this report:

01	Our reporting suite	04	Message from our Group President and CEO	13	Our governance structure
02	Navigating this report	05	Our sustainability context	13	Our approach to law enforcement assistance
03	About this report	06	Our material sustainability-related information	13	Governance instruments guiding responsible decision making
		08	Our digital human rights journey		
		09	Our operating context		
		10	Salient digital human rights matters		
		11	Trade-offs		
15	Our strategy	34	Risk management	40	Markets report
16	Our digital human rights due diligence framework	35	Digital human rights impact assessment and toolkit	58	Looking forward
17	UN Guiding Principles on Business and Human Rights	36	Digital human rights impact assessments	59	Glossary
17	MTN's digital human rights framework	37	Collaborating with partners and stakeholders	60	Administration
17	MTN's Digital Human Rights Policy	38	Transparency and ranking digital rights		
19	Our digital human rights approach				
20	Data privacy and protection				
21	Case study: Strengthening cybersecurity resilience following a legacy-environment breach				
22	Case study: Strengthening digital human rights through data-privacy awareness in Uganda				
23	Responsible AI				
24	Case study: Human rights risk assessment on Zigi Chatbot in Nigeria				
25	Child online protection				
26	Case study: Empowering educators to protect and inspire Uganda's next generation of digital citizens				
27	Case study: Room of Safety youth online safety campaign				
28	Case study: Bona Bana Programme – Web Rangers and Article 12 policy working group				
29	Case study: Ghana Deep dives AI-generated podcast				
30	Case study: Election readiness and human rights risk mitigation				
31	Human rights-related position statements				

Throughout this report we use the * symbol:

* Constant currency after taking into account *pro forma* adjustments. These are the responsibility of the directors and have been reviewed by our external auditors.

The forward looking financial information disclosed in this report is the responsibility of the directors and has not been reviewed, audited or otherwise reported on by our external auditors.

Our reporting suite

This report is part of a comprehensive reporting suite that provides stakeholders with an integrated view of MTN's financial, operational and sustainability performance. The suite follows a double-materiality approach and demonstrates MTN's commitment to transparent governance, strategy, performance and risk disclosures.

Integrated Report



The Integrated Report enables investors and other stakeholders to make well-informed evaluations of our performance and prospects, strategic direction and the value we create, preserve or erode through our activities. It provides a forward looking view of MTN's financial and non-financial performance, including strategy, risks and opportunities, targets and governance.

Materiality lens: Financial and impact

Information for shareholders



Notice of AGM
The Notice of AGM and form of proxy give information to shareholders who want to participate in the Group's Annual General Meeting (AGM).



King IV and King V Assessment Report

This document provides a summary of MTN's application of the King IV™ and King V™ principles.

Materiality lens: Financial

Sustainability reporting



Sustainability Report



Climate Report



Transparency Report



ESG Data Booklet

These reports provide a comprehensive view of MTN's strategy and performance in relation to sustainability matters that are potentially material both to MTN's business and to MTN's impacts on society and the environment. They present performance across a wide range of metrics and targets.

Materiality lens: Impact

Financial reporting



Annual Financial Results



Annual Financial Statements



Five-year Review



Tax Transparency Report

Our comprehensive financial reports provide detailed insight into MTN's performance, including an analysis of the Group's financial results, a five-year review and our tax approach. These reports not only highlight our financial health and operational efficiency, but also offer a clear view of our strategic direction and prospects.

Materiality lens: Financial

People reporting



People Report

This tells the story of the individuals and teams who bring our purpose to life, enable us to keep pace with a rapidly evolving environment and to serve our customers.



Remuneration Report

Our Remuneration Report outlines the Group's approach to fair, responsible and transparent remuneration. It explains the policies, governance structures and decision-making processes that guide how we reward our executives, senior leaders and employees.

Materiality lens: Financial and impact

Regulatory and reporting frameworks used¹:

Mandatory reporting considerations

Companies Act

JSE



IFRS

Amended Financial Sector Code (IFSC)

B-BBEE Act

Voluntary reporting frameworks and standards



SASB STANDARDS
New part of IFRS Foundation



IABS



Our **IR** and the supplementary reports are available online for review. This report is also available in a web version for an additional interactive experience.

¹ For more details see page 97 in the **IR**

Navigating this report

The following icons serve as reference points to illustrate interconnected themes throughout our reporting suite.

Our sustainable development goals

MTN supports the achievement of the **United Nations Sustainable Development Goals (SDGs)**, which target a sustainable society with a plan to end poverty, protect the planet and ensure equality for all by 2030. While all the SDGs are important, and MTN supports most of them by providing other sectors with digital and financial services, MTN contributes directly and primarily to the following SDGs.



Our primary SDG contribution areas for shared value creation:



MTN's material sustainability information matters are prioritised with the overarching MTN Group material matters in mind, with a special focus on environmental, social and governance (ESG) impacts.



Our material sustainability-related information



Digital and financial inclusion



Digital integrity



Unemployment and skilling



Climate action



Responsible and inclusive supply chain



Diversity and inclusion



Anti-bribery, compliance and whistle-blowing



Circularity



AI and emerging technologies



Human rights

Other icons



Limited assurance obtained



International Sustainability Standards Board



www.mtn.com



Our material sustainability information is expanded on pages 06 and 07.

About this report

This Transparency Report provides insight into MTN Group's approach to managing digital human rights risks and opportunities and how these factors influence the Group's ability to operate responsibly and sustainably. It offers clear and relevant disclosures that enable readers to assess our performance, understand the governance and processes guiding our decisions and evaluate how we safeguard the rights, safety and dignity of the people who use our networks and digital services.

Reporting entity

In line with MTN's Integrated Report, this report adopts the financial reporting entity model of control and significant influence. It provides commentary, performance insights and prospects for our major subsidiaries – **MTN South Africa**, **MTN Nigeria** and **MTN Ghana** – and for our two operating regions:

- **SEA** – Southern and East Africa.
- **Francophone Africa**.

This scope includes information on our operating markets.

In addition, report data excludes quantitative data from Sudan, owing to the ongoing conflict and instability within the country that makes it challenging for us to obtain complete and accurate data. However, MTN makes reasonable efforts to assess and monitor the situation as circumstances allow. Irancell is excluded from this disclosure scope due to the MTN Group's indirect minority shareholdings, which do not provide the ability to influence management decisions or operational practices.

In alignment with the standards of the International Sustainability Standards Board (ISSB), the following core content pillars guide our disclosures.

Timeframe

This report encompasses the reporting period from 1 January to 31 December 2025.

We consider the outlook over **three time horizons**:

- **ST** The short term (less than three years).
- **MT** The medium term (three to five years).
- **LT** The long term (beyond five years).

Reporting standards and guidelines

The following standards and guidelines have been applied to this report:

The Global System for Mobile Communications Association (GSMA) Human Rights Guidance for the Mobile Industry



Ranking Digital Rights (RDR) Index disclosure criteria



United Nations Global Compact (UNGC) transparency standard



The Global Network Initiative (GNI)



United Nations Guiding Principles on Business and Human Rights



Governance

Our governance structure ensures that climate-related considerations are embedded into enterprise decision making, risk oversight and capital allocation, with clear accountability from management through to the Board.

This section outlines the integrated oversight of climate-related risks and opportunities by management, the Executive Committee (Exco) and the Board.



Strategy

Our climate approach is shaped by Africa-specific operating realities and focuses on strengthening network resilience, managing transition risks and enabling long-term value creation through disciplined, implementable actions.

This section outlines the key programmes and approaches that guide our efforts to mitigate greenhouse gas (GHG) emissions, strengthen climate resilience and support the transition to a low-carbon, sustainable future.



Risk management

By integrating climate risks into our enterprise risk management (ERM) framework, we proactively manage potential impacts on operations, supply chains and financial performance, supporting business continuity and long-term resilience.

This section outlines how effective climate risk management is integral to our environmental strategy, as it enables us to identify, assess and mitigate the potential physical and transition risks associated with climate change that could impact our operations, value chain and long-term resilience.



Metrics and targets

Our metrics and targets are designed to track progress in a decision-useful manner, enabling performance management, informing strategic choices and strengthening accountability as our climate maturity continues to evolve.

This section outlines our progress in achieving our short- to long-term strategic objectives, while recognising successes and barriers that need to be addressed.

Materiality

Material matters are those that could substantially affect our strategy, profitability and sustainability and therefore influence our ability to create and sustain value for our stakeholders. In line with global disclosure standards and frameworks, we take a double materiality approach across our suite of annual reports. We therefore considered both impact materiality, or MTN's positive and negative impacts on people and planet and financial materiality for those matters that substantially affect or may affect the Group's financial performance.

This Transparency Report reflects the subset of material sustainability information matters most relevant to digital human rights, data privacy, information security and responsible technology governance.

Feedback

We welcome feedback on this report and remain committed to engaging with our stakeholders about our performance and sustainability efforts. Please address all feedback to Group Sustainability at: sustainability@mtn.com

Message from our Group President and CEO

As digital infrastructure becomes ever more central to economic participation, democratic life and social cohesion, the role of telecommunications providers is no longer neutral. Connectivity shapes power, access and opportunity. Our responsibility is to ensure this power is exercised with integrity and respect for digital human rights.

Ralph Mupita
Group President and CEO



Our purpose is leading digital solutions for Africa's progress. In 2025, MTN grew to nearly 300 million subscribers, a milestone that reflected the accelerating digitalisation of African society rather than a purely commercial achievement. More people than ever relied on our networks to communicate, learn, work, trade and participate in public life. This illustrates how deeply embedded connectivity has become in economic opportunity, social cohesion and democratic participation.

As Africa's largest telecommunications provider by number of subscribers, MTN plays a uniquely important role in shaping the continent's digital future. Our infrastructure supports livelihoods, enterprises, public services and innovation across our footprint. With that role comes responsibility. Guided by the UN Guiding Principles on Business and Human Rights, we continue to embed respect for human rights into our strategy, governance and relationships across the Information and Communication Technology (ICT) ecosystem, recognising that Africa's progress and our long-term value creation are fundamentally interconnected.

Operating context

In 2025, our operating environment was shaped by political transitions, economic pressure and rapid technological change. Electoral cycles, social contestation and geopolitical fragmentation sharpened expectations of telecommunications providers as custodians of digital access. At the same time, advances in artificial intelligence and rising cyber risks intensified global debates about privacy, safety and accountability in the digital economy.

These dynamics reinforced a central reality: trust is now a strategic asset. In this environment, respect for digital human rights is not peripheral to our business but foundational to legitimacy, resilience and sustainable value creation. Our approach therefore prioritises principled decision making that balances legal obligations with global norms and the expectations of the communities we serve.

Digital human rights and risk

Digital risks increasingly sit at the intersection of technology, regulation, politics and society rather than being purely technical or legal matters. Accordingly, we view digital human rights as an integral part of our broader enterprise risk outlook, recognising that questions of privacy, expression, safety and fairness are inseparable from commercial and operational risk in a highly connected world. This perspective has shaped how we think about strategy, resilience and long-term value creation across the Group.

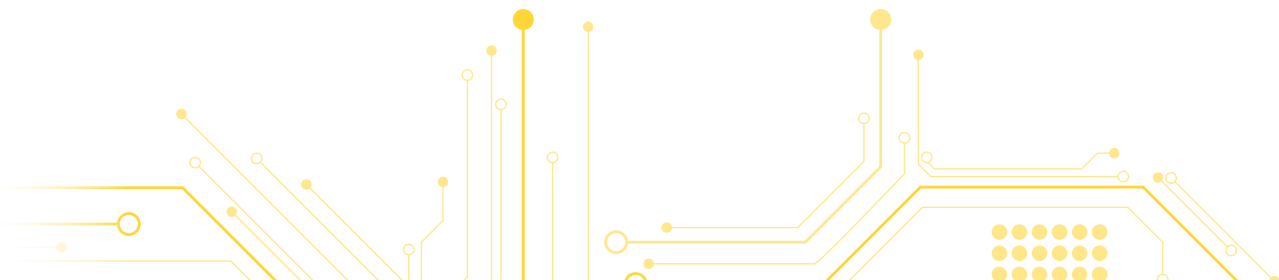
Collaboration beyond MTN

In the year under review, we continued to engage with regulators, civil society, industry peers and global experts to shape shared approaches to privacy, lawful access, online safety and responsible innovation. These engagements reflect a growing recognition that the governance of digital spaces is a collective endeavour requiring co-ordination across borders and sectors.

A significant step in 2025 was our participation in the Africa Taskforce on Child Online Protection, a continental initiative bringing together mobile operators, global technology companies, academia and civil society to co-ordinate responses to emerging online risks affecting children. This platform aligns with our conviction that safeguarding digital rights requires regional co-operation and shared responsibility.

Outlook

As we look ahead to 2026, MTN remains guided by the conviction that connectivity must enable dignity, opportunity and inclusion for every person we serve. Technology will continue to advance rapidly, reshaping economies in a context of heightened geopolitical uncertainty. At the same time, systemic pressures driven by climate change, poverty and inequality will increasingly influence how digital infrastructure is governed and experienced. Against this backdrop, we will remain focused on our long-term strategy across connectivity, fintech and digital infrastructure, making disciplined, principled decisions while staying agile in a volatile world. This approach will help ensure the next hundreds of millions of Africans who come online do so in a way that expands opportunity, strengthens trust and supports the continent's progress.



Our sustainability context

The 2025 financial year was marked by continued geopolitical and economic uncertainty, with global volatility affecting the operating environments of many African markets. In this context, businesses must remain agile and responsive while upholding strong governance and ethical practices. Despite persistent structural challenges such as poverty and unemployment, Africa's resilient and youthful population continues to drive innovation and is well positioned to benefit from rapid technological advancement across the continent.



Shifts in the ESG landscape

Global momentum behind sustainability has continued to strengthen, driven by rising expectations from investors, consumers and employees for companies to demonstrate responsible environmental, social and governance (ESG) practices. While climate transition and social inclusion remain central to ESG agendas, digital human rights have become increasingly prominent as technology reshapes economic, political and social life.

Across MTN's markets, regulatory frameworks continue to evolve in response to these shifts. Environmental and social regulations are being strengthened and disclosure expectations are rising through the adoption of global reporting standards such as the ISSB. At the same time, greater scrutiny is being placed on how companies manage digital risks, protect privacy, safeguard freedom of expression and respond to lawful access requests. These considerations are now widely recognised as material sustainability issues for the telecommunications sector.

Rapid advances in digital technologies, including artificial intelligence (AI) and cloud computing, have accelerated innovation and expanded access to services, while also introducing new ethical, security and societal risks. The World Economic Forum Global Risks Report 2026 mentions misinformation, data misuse and cyber threats as significant near-term challenges, reinforcing the expectation that companies embed human rights considerations into the design, deployment and governance of technology.

Consumer expectations continue to evolve in parallel. Stakeholders increasingly assess brands not only on environmental and social performance, but on how responsibly they handle data, protect personal information and respect digital rights. Younger consumers in particular are more aware of privacy, online safety and data governance, shaping expectations of ethical digital behaviour and accountability.

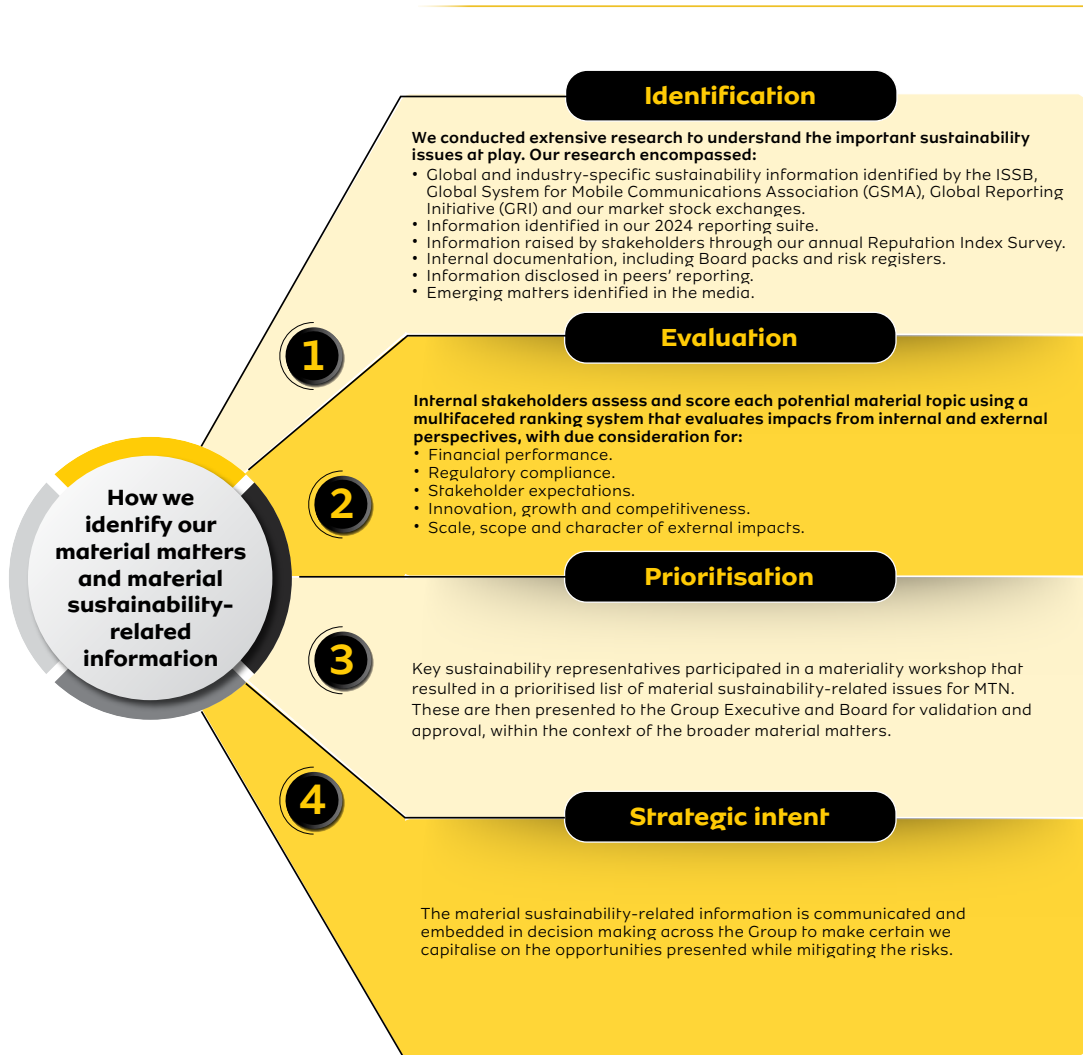
The ESG landscape has also become more fragmented. Shifts in political leadership and policy priorities in major global economies have introduced uncertainty and, in some cases, a retrenchment from sustainability commitments. In this context, consistency of approach and adherence to internationally recognised human rights principles have become critical to maintaining trust and credibility across diverse operating environments.

Against this backdrop, MTN's sustainability strategy recognises digital human rights, cybersecurity and responsible technology governance as interconnected strategic priorities. Respect for digital human rights underpins how we approach risk management, governance and long-term value creation in an increasingly digital and interconnected world.

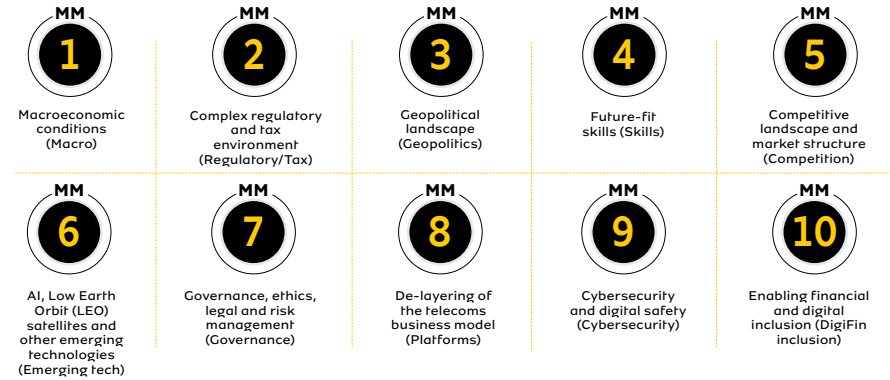
Refer to our sustainability strategy on page 20 of the Sustainability Report.

Our material sustainability-related information

MTN conducts a robust double materiality determination process to identify and prioritise the key matters that impact both the business and our stakeholders. In 2025, we expanded this exercise to explore material sustainability-related information that impacts financial performance. These help to inform our sustainability strategy beyond **Ambition 2025** while allowing the Group to adapt to new risks and opportunities.

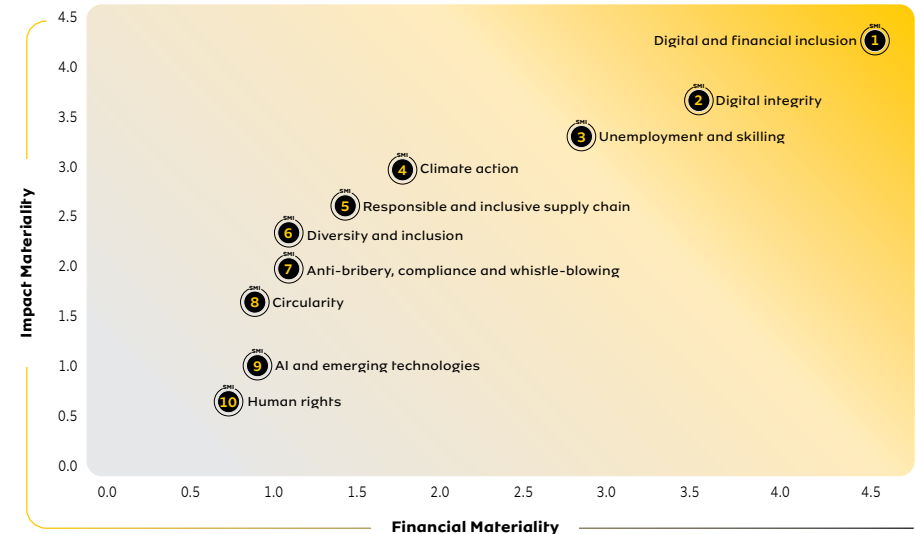


MTN Group material matters



Our material sustainability-related information

In 2025, our sustainability materiality matrix, composed of the most material sustainability-related information, is prioritised as follows.



Our material sustainability-related information continued

MTN's material sustainability-related information aligns closely with the overarching Group material matters, supporting our business strategy and priorities.

Material sustainability-related matters	Description	SR page reference	Link to 2025 MTN Group material matters
Digital and financial inclusion	Digital and financial inclusion is a critical pillar as it underpins participation in the digital economy and enables socioeconomic development. Barriers such as rural and remote connectivity, device and data affordability, digital skills gaps, coupled with limited meaningful-use offerings, constrain equitable access and mobile internet adoption, impacting MTN's long-term business growth and our ability to deliver meaningful impact to societies.	30 – 39	Enabling financial and digital inclusion
Digital integrity	Data protection remains one of our biggest responsibilities, with cybersecurity a major risk globally and across our markets. In addition, as more people, specifically youth, access digital services in the age of AI, it is important to safeguard them from online fraud, bullying and other threats.	49 – 51	Cybersecurity and digital safety
Unemployment and skilling	High rates of unemployment hinder socioeconomic development across our markets. MTN's Skills Academy is a growing resource for consumer skills development, especially as the platform matures to include specialised nano-degrees and job placement guidance.	44 – 47	Future-fit skills
Climate action	Climate change presents material risks to vulnerable communities, economic activity and MTN's operational resilience, with potential impacts on lives, infrastructure and network continuity. Through Project Zero, MTN is reducing its carbon footprint, contributing to the mitigation of long-term climate risks.	23 – 25	Environmental stewardship
Responsible and inclusive supply chain	Small and medium enterprises are major sources of employment and economic growth in low-income communities. MTN actively looks to empower local small businesses in our markets while ensuring all our suppliers adhere to our environmental, social and governance standards.	53	Supply-chain management
Diversity and inclusion	Gender equality and pay parity remain under pressure in our markets. MTN responds by embedding fair labour practices and equal pay in our operations, simultaneously providing marginalised communities with access to digital and financial products and services.	41 – 42	Employee engagement and culture
Anti-bribery, compliance and whistle-blowing	MTN commits to adhering to the highest standards of governance and ethics. Our third-party whistle-blower hotline provides a safe avenue for stakeholders to report any malfeasance.	52	Governance, ethics, legal and risk management
Circularity	E-waste is of material concern in the telecommunications sector, with several markets introducing e-waste legislation in response. MTN pursues circularity through our Project Infinity, extending the life of our equipment and allowing consumers to recycle their electronic devices responsibly.	26	Environmental stewardship
AI and emerging technologies	AI and other emerging technologies present a risk of exacerbating socioeconomic gaps and poses risks to society thus must be inclusive and safe by design. At the same time, these technologies offer significant opportunities to support socioeconomic development, climate stewardship and environmental resilience.	49	AI, LEOs and other emerging technologies
Human rights	MTN upholds the digital human rights of its users and customers by promoting safe, inclusive and meaningful participation in the online environment. Our approach is guided by the UN Guiding Principles on Business and Human Rights.	50	Cybersecurity and digital safety

Our digital human rights journey

MTN's approach to digital human rights has evolved alongside the rapid expansion of digital connectivity and the growing societal expectations placed on technology companies. Over time, the Group has strengthened its governance, transparency and due diligence practices to ensure that digital services are delivered in a manner that respects privacy, freedom of expression and the safety of users.

A global shift towards respect for digital human rights

Over the past decade, respect for human rights has become one of the most important markers of responsible technology practice. As digital platforms expanded and governments increased their requests for information, shutdowns and content restrictions, global expectations for openness and accountability grew sharply. Companies were expected not only to comply with the law, but also to explain how they balance national security, privacy, freedom of expression and the safety of their users.

This period marked a significant evolution in how organisations approached digital human rights. Early efforts focused on policy commitments and high-level principles. Over time, the emphasis shifted to clearer governance structures, consistent application of the company's human rights due diligence and independent assessments. Transparency reporting has emerged as a global tool for demonstrating accountability, guiding decision making and building public trust across diverse markets.

Globally, telecommunications and technology operators now operate within complex political, legal and social contexts where connectivity plays a central role in democratic participation, economic activity and access to information. In this environment, transparent decision making – particularly in relation to lawful access requests, content-related interventions and network integrity – has been essential to maintaining stakeholder confidence and supporting the protection of digital human rights.

As expectations for transparency and responsible digital practice have evolved, MTN has steadily shaped its own approach to digital human rights, which is informed by the UN Guiding Principles on Business and Human Rights.

What began as a commitment to global principles has grown into a more mature framework that prioritises sound governance, meaningful transparency and practical safeguards across all markets in which we operate.



Timeframe

2012

2015

2016

2019

2020

2021

2022

2022

2023

2024

2025

Our strategy

MTN illustrates its commitment to the UN Guiding Principles on Business and Human Rights and UN SDGs by joining the UNGC.

MTN strengthens governance and due diligence processes to better identify and mitigate human rights risks.

MTN drafts a comprehensive Group digital human rights toolkit to guide markets on privacy, lawful access and content-related requests.

MTN develops the digital human rights framework, creating a unified approach to managing digital human rights impacts across all operating companies.

MTN publishes its first Transparency Report, providing disclosures on government requests and digital human rights risks.

MTN conducts its first digital human rights impact assessment.

MTN adopts a revised digital human rights strategy that reflects evolving risks related to emerging technologies and regulatory changes.

MTN concludes an independent digital human rights impact assessment, further strengthening accountability and ethical practice.

MTN integrates human rights considerations into emerging technology governance, including AI, data ethics and platform development.

MTN completed its first Global Network Initiative assessment.

MTN joins the Africa Taskforce on Child Online Protection, becoming an early contributor to a continent-wide collaboration that unites operators, regulators, global tech firms and civil society.

Our operating context

MTN operates across two regions, namely Southern and East Africa and Francophone Africa. These regions are characterised by diverse regulatory landscapes, political dynamics and socioeconomic realities that influence how digital technologies are governed and experienced. Understanding this context is essential to how we manage our responsibilities as a provider of vital digital infrastructure.

In this environment, connectivity plays a defining role in shaping how people learn, work and participate in society. It is now inseparable from the protection of human rights, as digital networks increasingly influence how people engage with institutions, information and each other. Our operations therefore intersect with critical digital human rights themes such as privacy, data protection, access to information, freedom of expression and online safety. These intersections have direct implications for the communities we support and the decisions we take across our markets.

Several themes shaped our operating environment in 2025, as outlined in the diagram.



Overview of digital human rights issues

Key digital human rights issues

- ⌚ Access to affordable and reliable connectivity.
- ⌚ Children's rights and online protection.
- ⌚ Data privacy, data protection and responsible AI.
- ⌚ Network integrity, cybersecurity and service continuity.
- ⌚ Lawful access requests and content-related pressures.
- ⌚ Elections and other geopolitical factors that may heighten digital risks.
- ⌚ Online safety, including risks of misinformation and harmful content.

Influenced by

- ⌚ Customer needs and societal expectations.
- ⌚ Political stability and election cycles.
- ⌚ Evolving data protection laws and regulatory enforcement.
- ⌚ Rapid digitalisation and emerging technologies.
- ⌚ Global standards, benchmarking frameworks and best practice.

Mitigated by

- ⌚ Global human rights frameworks, such as the UN Guiding Principles on Business and Human Rights.
- ⌚ MTN Group digital human rights framework.
- ⌚ MTN Group human rights due diligence and impact assessments.
- ⌚ Election readiness planning in all markets including high-risk markets.
- ⌚ Responsible AI Policy and data privacy safeguards.
- ⌚ Training and capacity building across MTN markets.
- ⌚ Stakeholder engagement and contribution to policy development.
- ⌚ Strong governance practices and internal escalation processes.

Challenges

- ⌚ Conflicting legal requirements and regulatory uncertainty.
- ⌚ Asymmetry of information during political events, including elections.
- ⌚ Fragmented or newly introduced data protection regimes.
- ⌚ Rising cybersecurity threats and data-sovereignty demands.
- ⌚ Limited child online safety frameworks in some markets.
- ⌚ Pressure to balance lawful compliance with protection of user rights.

Our operating context continued

Salient digital human rights issues

MTN's salient digital human rights issues reflect the areas where our operations, services and operating environments have the greatest potential to affect people's rights. These issues arise from the intersection of connectivity, regulation, technology and the social contexts in which we operate. As digital ecosystems evolve, we continue to apply our human rights due diligence framework to identify, assess and manage risks linked to privacy, freedom of expression, online safety, data protection and responsible technology use. The following salient matters represent the most material human rights considerations across our markets in 2025.

Each of the salient digital human rights issues is outlined below, with its relevance to MTN and the actions we are taking to manage associated risks.



1

Digital human rights

Digital human rights remain a core focus for MTN as connectivity becomes increasingly central to how people access information, communicate and participate in society. Our services intersect directly with rights such as access, privacy, data protection, freedom of expression, online safety and digital inclusion. We recognise that certain groups, including refugees, internally displaced persons, persons with disabilities, women and girls, youth, rural communities, low-income households and linguistic minorities, may experience additional barriers to safe and meaningful connectivity. As digital ecosystems evolve, we work to make sure our networks, products and governance processes support inclusive, safe and rights-respecting digital participation across all our markets. This includes ongoing human rights due diligence, responsible technology development and principled decision making in environments where regulatory, political or security pressures may affect how people exercise their digital human rights.



2

Data privacy, security and protection

Data privacy, security and protection remain critical priorities as emerging technologies reshape the way information is collected, processed and used. The growing adoption of artificial intelligence and advanced analytics increases expectations for strong cybersecurity measures, transparent data governance and responsible data-handling practices. We continue to strengthen our privacy management approach, conduct human rights impact assessments on products and apply responsible AI principles to products that we source and use, and guide design and deployment where we develop.

As part of this work, Project Guardian was initiated in 2024 to strengthen MTN's privacy posture across the Group. The project is built around 12 core components, including accountability, transparency, data minimisation, integrity, security and the protection of data-subject rights. Project Guardian provides a structured approach to identifying privacy risks, enhancing internal controls and overseeing that new technologies, including AI systems, are implemented in a way that respects user rights and aligns with international data-protection standards.



3

Freedom of expression

Freedom of expression is a salient issue in several of our markets where regulatory, political and security pressures intersect with digital communication services. As an operator, we receive lawful requests from authorities, some of which may carry implications for user rights. Our governance processes ensure all such requests are assessed carefully and that any compliance is lawful, necessary and proportionate.



4

Vulnerable and marginalised groups

Children and other vulnerable groups face increasing risks as digital platforms become embedded in everyday life. These include exposure to harmful content, cyberbullying, exploitation and privacy violations. The establishment of the UNICEF and GSMA Africa Taskforce on Child Online Protection in 2025 highlights the urgency of strengthening safeguards in mobile-first regions.

We continue to promote digital literacy, raise awareness among caregivers and embed safety-by-design principles into our products and services. Our efforts include measures to make our platforms less conducive to harmful behaviour, supporting safer digital experiences for children while enabling them to benefit from the opportunities of connectivity.



5

Responsible AI

The rapid integration of artificial intelligence into networks, products and decision-making processes has made responsible AI a salient digital human rights issue for MTN. While AI offers significant potential to improve service quality, efficiency and digital inclusion, it also introduces risks related to bias, transparency, accountability, privacy and data protection. In response to this, MTN is embedding responsible AI principles across its operations, including clear governance, human oversight, impact assessments and safeguards to prevent discriminatory or harmful outcomes.

This approach is guided by international standards and aligned with MTN's broader digital human rights and privacy frameworks, making certain that AI is developed and deployed in a manner that is ethical, trustworthy and respectful of user rights.

Industry bodies recognise a wide range of potential human rights risks associated with the mobile sector. The salience of these issues varies by operator, supply chain involvement, service portfolio and operating environment. For MTN, our salient digital human rights matters reflect the issues most directly linked to our business model and the contexts in which we operate.

Our operating context continued

Trade-offs

Managing digital human rights involves balancing privacy, security, safety and regulatory obligations across varied markets. The table below sets out the key trade-offs MTN navigated during 2025, together with the gains, challenges and mitigation measures informing our approach to responsible digital human rights practice.

Gains

Trade-offs

Mitigation

Balancing privacy and security

Strengthening privacy protections while maintaining network resilience and service reliability.

Navigating tensions between user privacy, national security expectations and lawful requirements, especially during politically sensitive periods.

Enhancing encryption, privacy-by-design processes and transparent communication. Project Guardian strengthened privacy controls and accountability.

AI and digital human rights

Using AI to enhance safety, improve services and support responsible digital participation.

AI may increase risks linked to data use, algorithmic bias or misuse by malicious actors.

In line with MTN's Responsible AI Policy, we ensure all AI-related products and solutions are sourced from partners who meet our policy and framework requirements. This includes undertaking human rights impact assessments and applying a risk-based governance approach across the lifecycle. MTN further facilitates regular training across the business to promote the responsible use of AI, including ethical principles, responsible-by-design practices, appropriate usage, and governance standards. AI usage is monitored on an ongoing basis to ensure compliance with the policy and to support effective oversight and risk management.

Data retention and user rights

Retaining data for operational, safety and service purposes.

Balancing operational needs with privacy, minimisation expectations and compliance requirements.

Enforcing MTN's Data Privacy and Protection Policy, applying lawful/time-bound retention, anonymising or deleting data when no longer required.

Access to user information for lawful requests

Supporting lawful investigations and public-safety efforts.

Fulfilling lawful requests while safeguarding user privacy and avoiding perceptions of political influence.

Using defined governance pathways for lawful requests, applying human rights due diligence and activating election readiness procedures.

Network neutrality versus traffic management

Ensuring fair access to essential communication services.

Maintaining service quality during peak periods may require temporary prioritisation of essential traffic.

Transparent traffic-management processes, protecting emergencies and essential services and avoiding discriminatory practices.

User consent and data collection

Improving user experience with relevant, personalised services.

Ensuring informed, voluntary consent while minimising unnecessary data collection.

Clear opt-in/opt-out processes, simplified consent language and strengthened data-subject rights through Project Guardian.

Localisation versus global standards

Building constructive regulatory relationships and aligning with local laws.

Global standards may conflict with local requirements, creating real-world implementation complexity.

Developing policies that respect local legislation while aligning with human rights principles; engaging consistently in policy dialogue.

Collaboration with governments versus user advocacy

Contributing expertise to shape safer, more rights-respecting digital environments.

Balancing constructive government engagement – especially during elections – with advocating for user rights and proportionate regulations.

Transparent engagement protocols, cross-functional reviews, election readiness packs and continued advocacy for rights-aligned policies.

Governance



Our digital human rights governance

-  **Board oversight**
Board-led governance aligned with MTN's sustainability and digital human rights commitments.
-  **Executive Committee function**
Executive accountability ensuring consistent implementation across regions.

Our governance structure

Sound governance underpins our ability to deliver on MTN's sustainability commitments, manage sustainability-related risks and opportunities, and create sustainable long-term value for our stakeholders. The Board retains ultimate responsibility for overseeing sustainability matters across the Group. Through a clearly defined multi-tier governance framework, we ensure sustainability considerations are embedded into strategy, risk management, performance oversight and decision making at every level of the organisation.

MTN's digital human rights governance is built on clear oversight, structured decision making and a co-ordinated approach across the Group. Responsibilities are embedded at every level, from Board committees through to Opco working groups, ensuring policies are implemented consistently and risks are managed proactively. This integrated system enables us to respond effectively to complex regulatory environments, safeguard user rights and maintain accountability in how we handle digital human rights, security and lawful requests.

Our governance structure

Oversight of sustainability matters, including digital human rights, rests with the Group Social, Ethics and Sustainability Committee (SESCO), acting on behalf of the MTN Group Board. The Group Executive Committee, led by the MTN Group President and CEO, actively oversees implementation and progress. Regional vice presidents and country CEOs ensure effective governance and accountability within their operations, supported by functional and operational working groups that co-ordinate and monitor sustainability and human rights activities across the footprint.

Our approach to law enforcement requests

MTN applies clear and robust procedures to ensure lawful requests from authorities are met while upholding international human rights standards. Our law enforcement assistance activities follow defined governance pathways and are overseen through the relevant Executive Committee structures, with regular reporting to SESCO. In this way, decisions are principled, transparent and consistent across all markets in which we operate.

Governance instruments guiding responsible decision making

Our governance instruments, including the Group Digital Human Rights Policy, the Data Privacy Framework and the Law Enforcement Assistance Policy, provide clear guidance for responsible decision making in diverse and often challenging environments. Alignment with the UN Guiding Principles on Business and Human Rights, together with the integration of digital human rights considerations into our ESG framework, reinforces our aim of ensuring digital connectivity serves as a tool for empowerment rather than exclusion.

Our governance structure

Key responsibilities

- Reviews and approves digital human rights and sustainability strategy and targets.
- Oversees progress on digital human rights matters.
- Aligns operations with the SDGs and stakeholder expectations.
- Manages sustainability risks and opportunities.
- Provides quarterly oversight of management's performance.

- Directs digital human rights and sustainability priorities across the Group.
- Recommends actions for approval by the Board committees.
- Ensures alignment on digital human rights and sustainability commitments across functions.

- Integrates sustainability into Group strategy and planning.
- Escalates strategic sustainability and human rights matters.
- Co-ordinates initiatives that support long-term sustainability objectives.

- Reviews and approves sustainability strategy and targets.
- Oversees progress on digital human rights matters.
- Aligns operations with the SDGs and stakeholder expectations.
- Manages digital human rights and sustainability risks and opportunities.
- Provides quarterly oversight of management's performance.

- Reviews and approves digital human rights and sustainability strategy and targets.
- Oversees progress on digital human rights matters.
- Aligns operations with the SDGs and stakeholder expectations.
- Manages digital human rights and sustainability risks and opportunities.
- Provides quarterly oversight of management's performance.

Board Ultimate accountability

Reviews and approves

Mtn Group Social, Ethics and Sustainability Committee (SESCO) (meets biannually)

Directs and recommends

Exco

Executive Committee (meets monthly)

Integrates and escalates

Sustainability Steering Committee (Exco subcommittee) (meets biannually)

Advises and informs

Management Committee

Functional Sustainability Working Group

Executes and reports



Opco/platform

Opco Sustainability Working Group (meets monthly)

Strategy

MTN monitors the actual and potential impacts of digital human rights risks and opportunities on our business and strategy. This ongoing assessment enables us to refine and strengthen our approach, ensuring it remains relevant, responsive and aligned with our strategic objectives.

Our approach to risks and opportunities related to digital human rights

-  **Digital human rights due diligence framework and policy**
We continually strengthen our due diligence framework to guide us to identify, assess and address digital human rights impacts across all operations.
-  **Data privacy and protection**
We reinforce data-protection measures that prioritise security, transparency and user choice, supporting responsible handling of personal information.
-  **Responsible AI**
We apply our Responsible AI Policy to ensure AI is used safely, fairly and accountably across MTN, supporting transparent and responsible technology adoption.
-  **Child Online Protection**
MTN applies a human rights-based approach to child online protection, combining prevention, accountability and empowerment to safeguard children in digital environments.
-  **Election readiness and human rights mitigation**
MTN implements election readiness plans and human rights risk assessments to help ensure network resilience, service continuity and the safety of people and infrastructure, and respect for human rights during electoral periods.

Our strategy

As one of the leading telecommunications operators in Africa, MTN operates within a unique and dynamic environment shaped by a range of socioeconomic and environmental factors. Our industry's diverse nature requires us to ensure our strategy remains resilient, robust and agile, enabling us to adapt to current and emerging ESG-related trends.

Our strategy is underpinned by four pillars: doing for planet, doing for people, doing it right, and doing for growth. This framework drives our business and fosters sustainable growth. These pillars are tailored to our operating context and business model to enable us to respond to current and emerging risks. Our strategic pillars steer our organisation through clear action plans and focus areas, which are engrained throughout our Group and Opcos. Our extensive experience in the ICT industry, coupled with our proactive stakeholder engagement, allows us to drive our strategy efficiently and effectively. Each sustainability pillar contains clearly defined focus areas informed by local and global ambitions. Our sustainability efforts are supported by comprehensive policies and procedures that guide our markets, with frequent benchmarking against international best practice to ensure we are aligned with evolving regulatory landscapes, geopolitical changes, and stakeholder expectations.

Strategic intent: Ambition 2030: Leading digital solutions for Africa's progress



Commitments

We are committed to protecting our planet and achieving Net Zero emissions by 2040.

We are committed to driving digital financial inclusion toward a diverse society.

We are committed to creating and protecting value for our partners and stakeholders.

We are committed to boosting inclusive economic growth on the continent.

Metrics and actions

- Project Zero: Reduce GHG emissions.
- Energy footprint: Improve energy efficiency within our networks and deploy renewables.
- Waste management: Develop a circular economy and manage our waste.
- Water management: Reduce our impact through water conservation measures.

- Increase access and reduce the cost of communication.
- Increase financial inclusion.
- Generational equality: Increase women representation.
- Contribution through ICT: Digital education, skills and jobs.

- Responsible policies and practices: Business ethics and enterprise-wide risk management.
- Enhance reputation and trust with stakeholders.
- Promote digital human rights.
- Responsible procurement and supply chain practices.

- Tax contributions across markets.
- Invest in network infrastructure.
- Empower local governments and enterprises.

SDGs



Our digital human rights due diligence framework

Our Group strategy takes digital human rights into account. These considerations underpin our licence to operate, shape regulatory expectations, influence stakeholder trust and support long-term commercial growth across our markets.

Overview of the digital human rights strategy

Vision As we drive inclusion, we remain committed to protecting and promoting the rights of our customers and stakeholders across our footprint



Governance

- Standard operating procedures
- Scenarios playbook
- Decision matrix



Strategy

- Digital Human Rights Policy
- Responsible AI Policy
- Data Privacy and Protection Policy



Risk management

- Impact assessments
- Advocacy opportunities
- Capacity building of stakeholders
- Strategic memberships



Targets and metrics

- Transparency reporting
- Independent external assessments

MTN's digital human rights strategy is grounded in clear policies, practical tools and structured processes that guide consistent decision making across the Group. Through this strategy, we integrate human rights considerations into product design, network operations, data practices and commercial activities. Our approach includes risk-based assessments, responsible technology governance, active engagement with regulators and industry bodies as well as targeted capacity building for employees and external stakeholders.

Strategic partnerships and memberships support alignment with global standards, while transparent reporting and independent evaluations enable accountability and continuous improvement. Together, these elements ensure that we protect users, respect their rights and provide appropriate remedies where impacts occur.

Protect, Respect and Remedy through effective and meaningful human rights due diligence

Our digital human rights due diligence framework continued

UN Guiding Principles on Business and Human Rights

MTN aligns with the UN Guiding Principles on Business and Human Rights. These global guidelines set out the roles and responsibilities of both states and companies in relation to human rights. Endorsed by the United Nations in 2011, they provide a framework for preventing and addressing negative human rights impacts linked to business activities.

Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.

The UN Guiding Principles on Business and Human Rights.

Principle

Protect

The state has a duty to protect against human rights abuses by third parties, including businesses.

Respect

Businesses have a responsibility to respect human rights throughout their operations.

Remedy

Access to effective remedies for those affected by business-related human rights abuses

Enforcement measure

To fulfil this commitment, the business must have a human rights policy that is:

- Approved at the most senior level.
- Informed by relevant internal and external expertise.
- Explicit in its expectations regarding human rights.
- Communicated throughout the business and publicly available.
- Reflected in operational practices and procedures.

The human rights due diligence process includes:

- Assessing actual and potential human rights impacts.
- Integrating and acting upon the findings.
- Tracking the effectiveness of responses.
- Communicating how impacts are identified and addressed.

Lessons learning and understanding:

- An understanding of the incident and lessons learnt, to be better prepared for or mitigate the impact of future incidents.

MTN's digital human rights framework

MTN's digital human rights due diligence framework provides a structured approach for managing human rights across our business and digital platforms. It is aligned with our strategic priorities and anchored in the "Protect, Respect and Remedy" Framework. The framework guides how we identify, prevent and address digital human rights impacts through rights and incident management, impact management, responsible advocacy, and disclosure and performance oversight.

The framework is closely aligned with the Group strategy and supported by the governance mechanisms that translate policy into practice. These include standard operating procedures, scenario playbooks, decision matrices, risk-assessment tools, impact assessments, responsible advocacy opportunities, capacity-building initiatives, strategic memberships and transparent reporting processes. Together, these components facilitate consistent, principled decision making and make sure digital human rights considerations are integrated into product development, data-handling practices, commercial activities and operations across our markets.

Regular reporting and oversight through the Group SESCO, the Group Exco and the Group President and CEO reinforce accountability. Our digital human rights approach is strengthened through active engagement with external stakeholders, including regulators, industry bodies, civil society organisations and independent assessors.

MTN's Digital Human Rights Policy

MTN's Digital Human Rights Policy aligns with international human rights standards and sets out our responsibility to respect human rights as part of responsible business conduct. It applies to MTN directors, officers, employees and representatives, as well as to suppliers, agents, business partners and intermediaries. Although the policy is implemented consistently across the Group, its application is tailored at operating company level to reflect country-specific legal and regulatory contexts.

The policy provides the central framework for how MTN identifies, prevents and mitigates digital human rights risks across its operations, products and partnerships. It supports coherent decision making in areas where connectivity, regulation and technology intersect, strengthening trust and enabling safer, more inclusive digital participation.

MTN continuously evolves the policy in response to emerging risks and global standards. It is supported by targeted instruments, including the Responsible AI Policy and the Data Privacy and Protection Policy, and reinforced through ongoing training and governance processes.

Together, these elements embed digital human rights considerations into core business practices and ensure MTN's approach remains relevant, responsive and aligned with its purpose.

Our digital human rights due diligence framework continued

Complying with legislative requirements

MTN operates within the legal and regulatory frameworks of all its markets. We recognise that regulatory compliance is essential for maintaining trust, sustaining our licence to operate and ensuring the continuity of our services. Non-compliance may result in fines, sanctions or the loss of operating authorisation. For these reasons, our business conduct is guided by the following principles.

- Protecting our customers' rights to access information and express themselves online.
- Practising and advocating for good data governance among our stakeholders.
- Providing secure communication services in the jurisdictions of our operating markets.

The Group evaluates each lawful request from authorities relating to access, information or network services with great care. We assess legal validity in accordance with local legislation and international human rights law. Where legislation is ambiguous or appears inconsistent with international standards, we seek additional legal counsel so that decisions are well supported and we protect the rights of our users while meeting our legal obligations.

Reasons MTN would comply:

- 1 The request is issued lawfully by an authorised public body in line with governing legislation.
- 2 The request is required to support regulatory proceedings conducted by a competent authority.
- 3 The request relates to legitimate licence or lawful obligations.

Alignment with digital human rights best practice

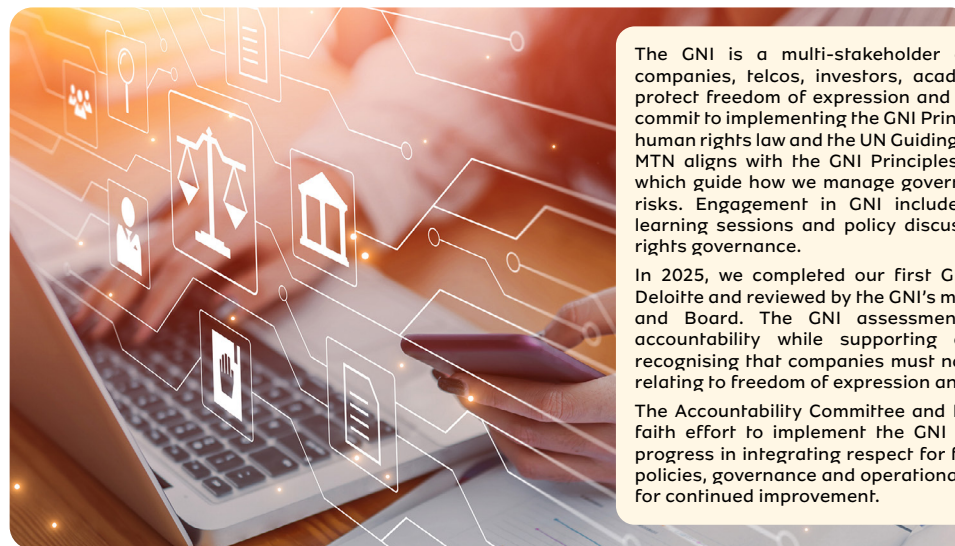
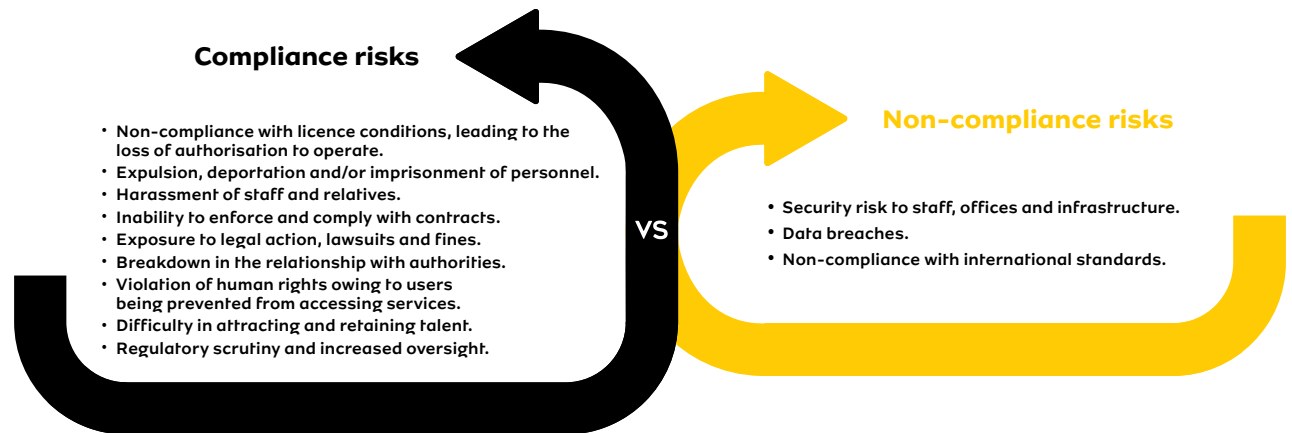
MTN aligns its approach to digital human rights with leading international, continental and regional frameworks to ensure credibility, consistency and collective action. Membership of platforms such as the UNGC, the GNI and the GSMA supports ongoing learning, peer collaboration and alignment with evolving best practice in sustainability, data protection and internet governance.

At regional level, MTN's engagement with instruments such as the African Union Convention on Cybersecurity and Personal Data Protection, the ECOWAS Supplementary Act on Personal Data Protection and the SADC Model Law on Data Protection informs our understanding of regulatory trends and shared responsibilities across our footprint. In 2025, participation in the Africa Taskforce on Child Online Protection further strengthened MTN's contribution to collective efforts to advance safer digital ecosystems for children and young people.

Compliance considerations

MTN is a member of the GSMA, the global organisation representing mobile network operators and the broader mobile ecosystem. Through this membership, MTN participates in industry dialogue and monitors evolving regulatory developments, global standards and sector guidance relevant to the mobile industry. This engagement supports alignment with recognised industry practices and informs ongoing governance and compliance oversight.

MTN recognises that operating in complex and evolving environments presents compliance risks and remains vigilant in managing these proactively. Compliance failures, where they occur, may have serious consequences, including adverse human rights impacts, risks to the safety of staff, offices and infrastructure, litigation exposure, reputational harm, business disruption, data breaches and non-compliance with international standards. Non-compliance with applicable laws and licence conditions may also result in regulatory action, financial penalties or restrictions on operations. These compliance and non-compliance risks are informed by applicable legal and regulatory standards.



The GNI is a multi-stakeholder organisation that brings together tech companies, telcos, investors, academics and civil society to promote and protect freedom of expression and privacy rights in the ICT sector. Members commit to implementing the GNI Principles, which are grounded in international human rights law and the UN Guiding Principles on Business and Human Rights. MTN aligns with the GNI Principles on Freedom of Expression and Privacy, which guide how we manage government requests and broader digital rights risks. Engagement in GNI includes monthly company constituency calls, learning sessions and policy discussions that strengthen our digital human rights governance.

In 2025, we completed our first GNI assessment, which was conducted by Deloitte and reviewed by the GNI's multi-stakeholder Accountability Committee and Board. The GNI assessment is designed to promote meaningful accountability while supporting continuous learning and improvement, recognising that companies must navigate emerging and complex challenges relating to freedom of expression and privacy in a rapidly digitalising context.

The Accountability Committee and Board concluded that MTN made a good-faith effort to implement the GNI Principles and demonstrated meaningful progress in integrating respect for freedom of expression and privacy into its policies, governance and operational practices, while identifying priority areas for continued improvement.

Our digital human rights due diligence framework continued

Our digital human rights approach

Management process	Description	Mitigating actions
<p>1</p> <p>Before</p> <p>Proactive management</p>	<ul style="list-style-type: none"> • Evaluating risks and impact: Quarterly reviews are conducted on digital human rights risks and mitigation plans. • Annual assessments: Detailed digital human rights assessments are conducted annually. 	<ul style="list-style-type: none"> • Engaging stakeholders: Ongoing engagements with stakeholders on digital human rights and related matters. • Implementing assessments: Implementing mitigation actions to minimise the risks and impacts identified in the assessments.
<p>2</p> <p>During</p> <p>Management</p>	<p>Managing requests or incidents: MTN adopts a considered approach in determining its response to requests from authorities and non-governmental entities. This includes:</p> <ul style="list-style-type: none"> • Evaluating requests that may impact freedom of expression, access to information or customer privacy, assessing the regulatory authorisation of the requesting entities and ensuring compliance with prevailing regulatory processes. • Engaging relevant stakeholders for guidance before responding to requests, seeking clarification or requesting amendments where possible. • Reviewing all requests in accordance with the laws and regulatory requirements of the relevant jurisdictions, alongside international human rights standards. • Assessing potential risks to employee safety and operational continuity before deciding to reject, partially comply with, or fully comply with a request. The decision is based on due diligence, regulatory and risk management principles and applicable country laws. 	<ul style="list-style-type: none"> • Mitigating the impact of disruptions: MTN communicates with affected parties based on applicable law to safeguard employees, customers and partners. We also ensure the integrity of our infrastructure is maintained during disruptions. • Situational stakeholder engagement: MTN actively engages with various stakeholders to gather perspectives, identify potential mitigations and manage situations effectively. Grievances can be reported through in-country customer complaints lines or via email to humanrights@mtn.com.
<p>3</p> <p>After</p> <p>Post-incident management</p>	<ul style="list-style-type: none"> • Reflections: Reviewing incidents and lessons learnt to strengthen future preparedness and reduce risk. 	

Data privacy and protection

Our targeted approach Data privacy and protection

Our strengthened approach began with Project Guardian, a Group-wide initiative designed to overhaul and elevate MTN's data privacy capabilities. The project introduced a comprehensive data privacy and protection programme built on 12 key components aligned with international best practice. These components span accountability, transparency, data minimisation, integrity, security and data-subject rights. The revised policy applies across all markets and sets a consistently high standard, including in jurisdictions where local legislation is still developing. Dedicated tools, templates and controls were introduced to support compliance and ensure that partners uphold MTN's requirements.

Data privacy and protection are fundamental to MTN's operations. Data privacy is not treated as a compliance exercise but as an essential part of how we conduct business. Safeguarding the personal data of our customers, employees and partners protects a core human right and reinforces the trust that underpins our relationships. This trust is a competitive advantage, positioning MTN as a responsible service provider with strong, reliable data governance and protection practices.

Complementing this, MTN's information security approach focuses on the resilience, integrity and protection of the systems, networks and processes that store, transmit and process personal data. Strong information security controls are essential to prevent unauthorised access, mitigate cyber threats and maintain service continuity, thereby enabling effective privacy protection in practice. Together, robust privacy governance and advanced information security form an integrated defence that protects both data and the digital environments in which it operates.

The MTN Group Privacy Office has successfully transitioned its data privacy programme from 'project mode' (i.e. Project Guardian) into 'business-as-usual mode', under the name Privacy Guardian.

With the foundational capabilities established through Project Guardian, accountability for data privacy is now embedded within day-to-day operations. Business units are responsible for consistently applying established privacy controls as part of their normal processes, including how personal data is collected, used, shared, stored, and disposed of.

The Group Privacy Office has successfully conducted various data privacy training interventions ensuring ongoing awareness, capability building and cross-functional collaboration. Over the past year, the Group Privacy Office has successfully rolled out data privacy awareness campaigns across all markets, reinforcing core data privacy principles, regulatory obligations and employees' day-to-day responsibilities when handling personal data. In addition, 'Privacy Pulse' sessions are regularly hosted by the various markets, focusing on key data privacy topics, emerging regulatory developments and practical lessons learnt, thereby embedding a culture of continuous learning and accountability.

To support and sustain these efforts, the Group Privacy Office drives ongoing collaboration with key stakeholders such as Information Security and AI teams. This includes integrating privacy-by-design and security-by-design concepts and addressing the specific risks associated with advanced technologies and AI-enabled solutions. Through these joint initiatives, MTN ensures data privacy is not addressed in isolation, but is embedded into broader risk management, technology and innovation practices across the Group.



Data privacy and protection continued

Case study

Strengthening cybersecurity resilience following a breach in a legacy environment



In 2025, MTN experienced a cybersecurity incident involving a legacy environment that had been scheduled for migration into the Group's fully managed domain. Before the migration was completed, the environment was compromised, exposing a logging server receiving data from several operating companies. Although the number of affected customers was small, relative to MTN's base of 300 million subscribers, the incident underscored the importance of accelerating the modernisation of legacy systems and maintaining stringent cybersecurity measures across our environment.

MTN acted swiftly and transparently. Within 48 hours the compromised server had been identified, isolated and permanently removed from the network, eliminating immediate risk. MTN promptly notified all relevant regulators and directly informed every affected customer.

In addition, MTN initiated a detailed review across all our markets. The assessment examined potential vulnerabilities, accelerated the migration of unmanaged environments and strengthened interim controls where full integration was not yet possible. This Group-wide review informed a two-year cybersecurity enhancement programme that will be completed in 2026.

Lessons learnt

The incident reinforced the importance of early detection, rapid containment and clear engagement with regulators and customers. It also highlighted the need to eliminate legacy vulnerabilities and ensure all systems are brought into the Group's managed security environment. The experience strengthened MTN's overall cyber maturity and sharpened its focus on continuous improvement.

Outlook

MTN will continue to strengthen its security posture through a Group-wide enhancement programme and ongoing monitoring of global threat developments. The Group will also track the evolving role of AI in both cyber defence and cybercrime, guided by our Responsible AI Policy approved by the Ethics subcommittee of the Board. Furthermore, we are reviewing security capabilities across all markets so they remain fit for purpose and aligned with international standards.



Data privacy and protection continued



Case study

Strengthening digital human rights through data-privacy awareness in Uganda



MTN Uganda sought to deepen practical understanding of data protection responsibilities under Project Guardian. While policies were in place, the business recognised the need to strengthen behavioural awareness and ensure consistent application across employees and third parties. Rising data privacy risks and evolving regulatory expectations made it important to position privacy as an everyday practice rather than a compliance exercise. Data Privacy Week provided an opportunity to strengthen a shared culture of accountability and reinforce legal and ethical responsibilities.

What we did

MTN Uganda delivered an interactive programme for employees and third-party partners. The week opened with leadership messages from the Managing Director and the CEO of MTN MoMo Uganda, reinforcing privacy as a core organisational value. An on-floor Privacy Pledge Wall invited employees from Technology and Mobile Money to share personal reflections on why privacy matters in their work. Staff wrote their experiences and commitments, creating a visible reminder of shared responsibility.

A digital quiz tested knowledge on core concepts such as data breaches, lawful handling of personal information and internal response processes. The quiz attracted 217 employees, providing a practical way to assess understanding and highlight areas needing further support.

To extend awareness across the supply chain, MTN Uganda hosted a virtual training session for more than 110 third-party providers,

facilitated by the Personal Data Protection Office of Uganda. The session clarified roles, common compliance failures and lessons from regulatory cases.

The week concluded with an interactive 'Two Truths and a Lie: Data Privacy Edition' activity to encourage discussion and critical thinking.

Outcomes and impact

The programme strengthened MTN Uganda's privacy culture through leadership engagement, practical learning and active participation. Employees showed improved familiarity with data protection principles, while strong participation in the quiz and pledge wall demonstrated internal commitment. Third-party providers gained clearer understanding of their legal responsibilities, supporting more consistent privacy practices across the ecosystem and bringing Project Guardian principles to life locally.

Lessons learnt

Participatory formats proved most effective in driving reflection and learning. Collaboration with the national Data Protection Office enhanced credibility and relevance. MTN Uganda will extend thematic activities throughout the year to sustain momentum and embed privacy as a continuous practice.

Responsible AI

Our targeted approach: Responsible use of artificial intelligence



MTN is committed to the responsible and ethical use of artificial intelligence (AI), ensuring that innovation is deployed in a manner that protects digital human rights, promotes fairness and builds stakeholder trust. Our Responsible AI approach is anchored in the Balance, Responsibility, Awareness, Integrity and Nurturing (BRAIN) principles, which guide the design, deployment and oversight of AI across the Group.

These principles are embedded within a robust governance framework aligned with leading global standards, including the NIST AI Risk Management Framework (Govern, Map, Measure, Manage) and ISO/IEC 23894 on AI risk management. As part of our continuous improvement journey, we are advancing alignment with ISO/IEC 42001, establishing a formal Artificial Intelligence Management System to strengthen accountability, risk management and regulatory readiness.

Through this integrated framework, MTN ensures that AI systems are developed and deployed responsibly across their lifecycle, from design to monitoring, with a focus on transparency, fairness, privacy and security. This enables us to harness the benefits of AI to drive inclusive digital growth, while proactively managing risks and upholding our commitments to customers, employees and broader society.

During 2025, we strengthened the practical application of this approach across the business. We introduced an internal Responsible AI Toolkit to support teams with consistent decision making, risk screening and documentation when developing or procuring AI-enabled solutions. Responsible AI playbooks were also rolled out across markets to operationalise the policy and guide teams on governance processes, risk management and responsible development practices.

We also embedded AI considerations into our human rights impact assessment methodology and AI products used across the Group, ensuring that potential impacts related to bias, transparency, privacy and accountability are systematically assessed.

To inform this work, we piloted and assessed two AI-enabled products. Early insights highlighted the importance of robust data governance and model explainability to build trust, as well as the need for clear guardrails to prevent unintended consequences in customer-facing applications. These learnings are being used to refine controls, training and procurement criteria across markets.

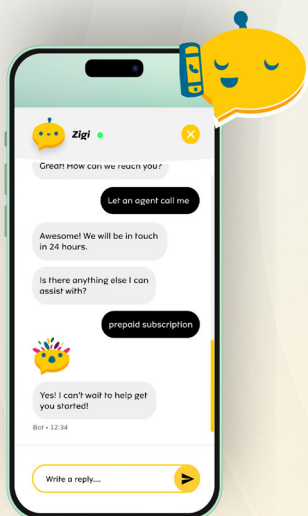
In parallel, MTN continued to monitor emerging risks linked to AI, including the global rise of AI generated child sexual abuse material. We deepened our partnership with the Internet Watch Foundation (IWF) to strengthen network level safeguards, while cross-functional governance structures across Digital, Legal, Risk, Sustainability and Corporate Affairs co-ordinated principled, consistent responses to AI-related risks and opportunities.



Responsible AI continued

y'ello! I'm Zigi.

A quick query or a deep dive into MTN products, I'm your go-to for instant self-service.

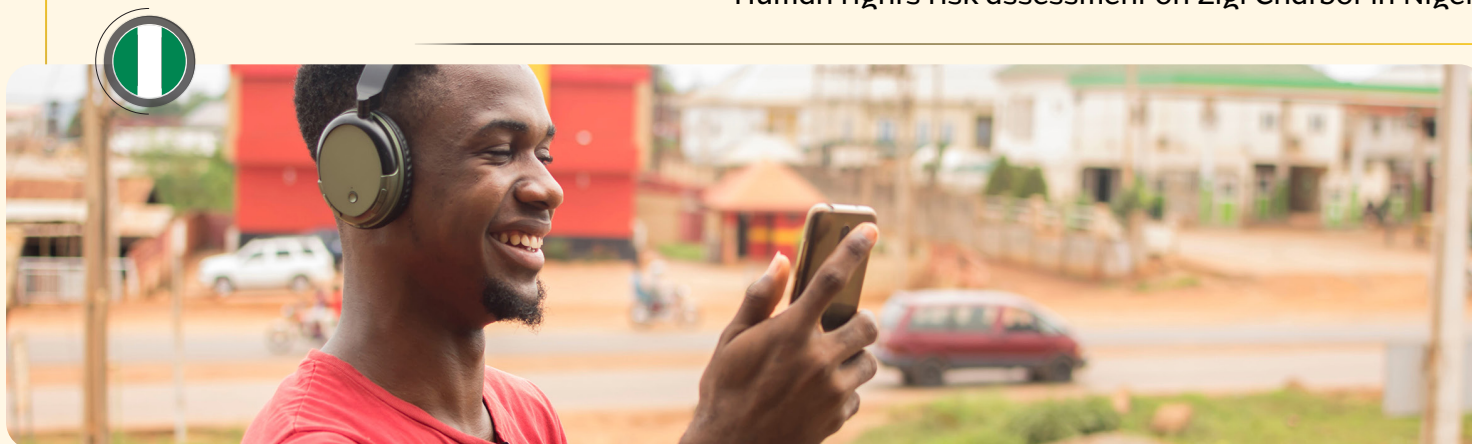


Scan the QR code to begin.

#ZigiThat

Case study

Human rights risk assessment on Zigi Chatbot in Nigeria



MTN conducted a human rights risk assessment on Zigi, MTN Nigeria's AI-enabled customer service chatbot, as part of its broader Responsible AI and digital human rights governance approach, guided at a high level by MTN's BRAIN principles. The assessment was grounded in the UN Guiding Principles on Business and Human Rights and formed part of MTN's standard AI risk management processes.

Zigi supports customers with everyday interactions such as checking available offers, viewing balances, purchasing bundles and airtime, and connecting with a human agent when required. It is used for both transactional and non-transactional purposes and provides a convenient, remote alternative to in-store or call centre engagement, helping to reduce congestion in physical channels while improving service efficiency.

The assessment focused on how Zigi could affect the rights to freedom of expression, access to information, privacy, consumer protection, and language and cultural identity.

What we did

MTN assessed both the potential benefits and risks of Zigi from a human rights perspective. The review recognised that digital chat solutions can expand access to information, reduce language barriers and enable more convenient access to services. It also considered risks such as the potential spread of incorrect information, biased or unfair outcomes in automated interactions, privacy and data protection concerns, and exposure to inappropriate content if safeguards were insufficient.

To manage these risks, MTN strengthened controls around Zigi's operation. The chatbot is being progressively enhanced to better reflect local languages, expressions

and communication styles to ensure more natural and culturally appropriate engagement for Nigerian customers. Human teams daily review all content prompts and responses to ensure accuracy, reliability and alignment with MTN standards. Customer data processed through Zigi is anonymised and pseudonymised, with identification occurring only when customers log in through an authorised channel and limited to that session. Where Zigi cannot resolve a query, it is transferred to a human agent for appropriate support.

Outcomes and impact

The assessment improved MTN's understanding of how AI-enabled customer service tools can affect people's rights and informed the design of stronger safeguards. Zigi now operates as a complementary service channel alongside email and call centre support, enabling more efficient customer service while maintaining strong protections for customer rights, privacy and trust. The process also reinforced cross-functional co-ordination between Digital, Legal, Risk, Sustainability and Corporate Affairs teams on AI-related decision making.

Lessons learnt

Human rights considerations need to be integrated early in the design and deployment of AI-enabled customer tools. Regular human oversight is essential to maintaining accuracy, trust and accountability. Localisation and cultural relevance are critical for inclusive digital services in linguistically diverse markets, and ongoing monitoring and iterative improvement are necessary to ensure AI-powered solutions remain aligned with MTN's values and digital human rights commitments.

Child online protection

MTN's approach to child online protection

Children are connecting to the digital world at younger ages, increasing both their opportunities for learning and their exposure to online risks. As digital engagement accelerates, so does the likelihood of encountering harmful content, manipulation, exploitation or algorithm-driven risks, such as AI-generated grooming or deepfake abuse. These risks are intensifying across our markets and require sustained, multi-layered intervention rather than awareness alone. In this context, protecting children online is both a human rights priority and a core operational responsibility for MTN. Our child online protection programme operates across all levels of the business and reflects a shift towards proactive, safety-by-design principles informed by human rights impact assessments, stakeholder insight and emerging digital trends. The programme is guided by five core objectives.

Empowerment

Supporting young people to become online safety champions who promote responsible digital behaviour among their peers.

Awareness

Raising awareness about online risks and strengthening understanding of available reporting mechanisms to encourage the use of national and MTN-supported reporting portals.

Knowledge

Building evidence-based insight to inform online safety interventions and contribute to the broader development of digital safety practices across the continent.

Capacity

Equipping caregivers, educators and law enforcement with the skills and knowledge needed to protect children online, while contributing to policy development through advocacy forums.

Blocking child sexual abuse material (CSAM)

Promoting the MTN-IWF portal, which enables the identification and blocking of CSAM to prevent its circulation across our networks.

Strengthening child protection through our partnership with the Internet Watch Foundation

MTN recognises that protecting children online requires a collective approach involving telecommunications providers, regulators, law enforcement and civil society organisations. This understanding informs our long-standing partnership with the IWF, where MTN has held a top-tier membership position since 2019. Through this partnership, MTN benefits from access to the IWF's CSAM URL blocking list, which is applied across all operating companies to prevent the transmission and re-sharing of harmful content.

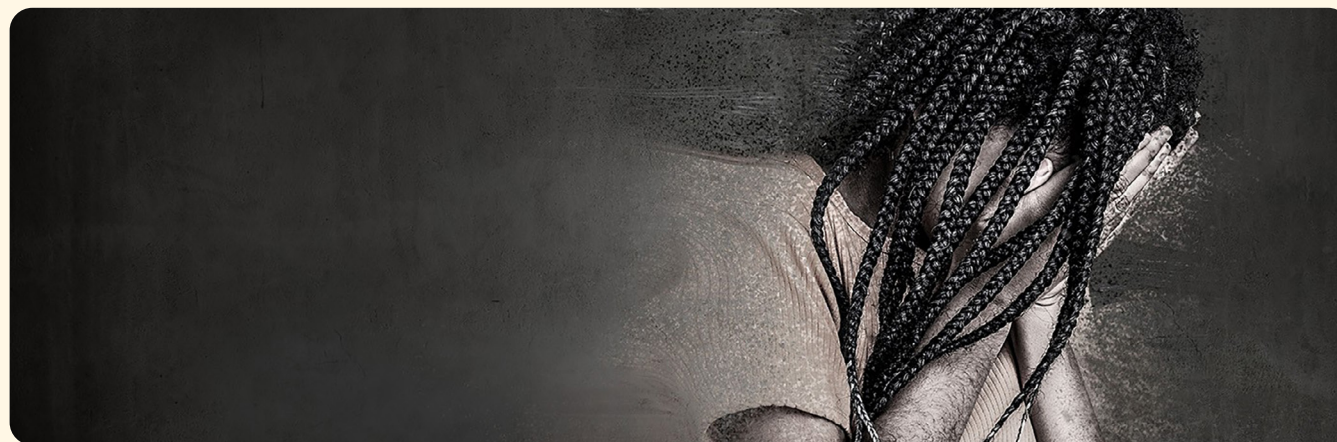
MTN's adaptive mobile blocking activities

MTN uses an adaptive system designed to identify and block URLs deemed inappropriate or potentially harmful to its users. This system is flexible and considers each market's unique characteristics, providing a dependable and efficient method for filtering out harmful content. The filtering process is anchored in a daily list of URLs supplied by the IWF feed, which catalogues information about websites known to host CSAM or other illicit content. Through our partnership with Adaptive Mobile, this list is received and used to block access to flagged URLs. This proactive measure protects MTN's users from potential exposure to harmful content.

The following table presents data highlighting our efforts in collaboration with the IWF and Adaptive Mobile to remove content deemed harmful to children. The data indicates increases in the number of blocked URLs since 2022.

MTN's adaptive mobile blocking activities	2025	2024	2023	2022
Number of URLs inspected	62m	129	656	145
Number of URLs blocked (million)	48.62	0.87	1.00	0.70
Blocking rate (%)	1.28	67	17	46
Number of URLs blocked per day	154 296	9 600	3 000	1 800

Data reported in FY2024 was for Q1 only. Excluding – Uganda, South Sudan and eSwatini.



About the Internet Watch Foundation (IWF)

The IWF is a non-profit organisation dedicated to protecting children online. With a history spanning more than 27 years, the organisation provides a secure way for people to report child sexual abuse imagery anonymously – available in more than 50 countries. The community includes more than 190 global technology companies committed to this cause. Highly trained analysts within the organisation assess public reports and take proactive steps to make the internet safer for everyone.

Child online protection continued

Case study

Empowering educators to protect and inspire Uganda's next generation of digital citizens



Uganda's rapidly digitising education landscape continues to widen the gap between children's growing online exposure and teachers' ability to protect them in digital spaces. Many primary school educators lack the confidence and practical skills to address risks such as cyberbullying, harmful content, data misuse and unsafe digital behaviour. MTN Uganda recognised this need and developed a programme to equip frontline educators with the practical competencies to uphold digital human rights and foster responsible digital citizenship from an early age, in line with MTN's Ambition 2025 strategy and SDGs 4, 9, 10 and 16.

What we did

MTN Uganda partnered with Faces Up Uganda to integrate a digital human rights module into the Art for Educators Programme. A one-day, skills-based workshop was delivered to 30 primary school teachers in Rubaga Division, Kampala, focusing on recognising online risks, protecting children's privacy, embedding online safety into lessons and supporting learners who experience harm. MTN provided funding, digital safety materials and technical guidance, while Faces Up Uganda contributed its arts-based pedagogy and facilitation expertise.

Outcomes and impact

Thirty teachers were trained, with each expected to reach approximately 2 000 learners annually with improved guidance on safe and responsible internet use. They reported greater confidence in identifying cyber risks and integrating digital safety into routine lessons. Schools showed early shifts towards more responsible device use and stronger engagement with parents on online safety, strengthening community awareness and rights-respecting practices.

Lessons learnt

Teachers need continuous support to keep pace with evolving online risks. Integrating digital safety into an existing, trusted programme proved more effective than standalone training. Lasting impact depends on engaging the wider ecosystem around the child, including parents and school leadership, while partnerships between business and civil society enable scalable, practical models for child online protection.



Child online protection continued

Case study

Room of Safety youth online safety campaign



Young people across our markets increasingly rely on digital platforms for learning, social connection and entertainment, while facing rising risks such as cyberbullying, exposure to harmful content, coercive peer dynamics and misuse of AI-generated companions. Educators, caregivers and youth reported feeling overwhelmed and uncertain about how to navigate these risks.

In response, MTN created the **Room of Safety** campaign, designed as a youth-led, culturally relevant intervention that moved beyond awareness messaging to promote safer behaviours, clearer reporting pathways and stronger protection for vulnerable users.

What we did

MTN partnered with **MTV Base** to co-create a 10-part short-form series that premiered on 20 July 2025 on DStv 322 and digital platforms. Youth creators, influencers and experts shaped the scripts and storylines to maintain authenticity, with relatable language and realistic online dilemmas.

Each episode addressed themes like online harms, digital peer pressure, AI companions, positive digital behaviours and available reporting mechanisms. Audiences were directed to national reporting portals, child helplines and MTN's **Help Children Be Children** platform. MTN Group and all Opcos collaborated on amplification, supported by Ipsos research to refine messaging and understand youth behaviour.

Outcomes and impact

The campaign reached millions of young people across the continent through television and digital channels. Young participants involved in the filming process described feeling “seen”, empowered and proud to use their voices to help others stay safe online.

In addition, the series equipped young people with practical tools to recognise risks, report harmful behaviour and make safer choices online. Educators and caregivers also noted that the campaign opened conversations about online safety at home and in schools. The initiative enhanced awareness of child-protection portals and reinforced MTN's leadership role in advancing online safety and digital human rights.

Lessons learnt

Effective youth engagement requires genuine agency rather than top-down messaging. Youth-led storytelling proved more relatable and impactful. The campaign underscored that connectivity without protection can increase vulnerability, reinforcing the need to embed safety features, clear reporting pathways and cross-sector partnerships in all future youth initiatives.



Child online protection continued



Case study

Bona Bana Programme – Web Rangers and Article 12 policy working group



In 2025, MTN advanced its Help Children Be Children campaign through the Bona Bana Programme, MTN South Africa's flagship child participation initiative. The programme strengthened children's digital human rights through youth-led learning, advocacy and institutional capacity building.

South African children continue to face serious online risks. UNICEF's Disrupting Harm study found that 7–9% of internet-using children had experienced online sexual exploitation or abuse, while many schools lacked the skills and resources to respond. Bona Bana addressed this gap by embedding practical digital literacy in schools, strengthening safeguarding approaches and enabling meaningful youth participation.

What we did

The programme was delivered through two core initiatives, facilitated by Moxii Africa (formerly Media Monitoring Africa).

First, 246 members of the Representative Council of Learners (RCL), aged 12–17, completed two-day workshops across five provinces, covering AI and algorithms, cyberbullying, CSAM, responsible communication and harmful content.

Second, trained Web Rangers worked with teachers to reach a further 1 217 learners through peer-led sessions, with teachers noting stronger learner engagement when messages came from peers. Web Rangers also supported awareness campaigns during key national moments, reaching an additional 1 626 learners and engaging parents.

In parallel, the Article 12 policy working group produced youth-led research and advocacy outputs, including work on climate disinformation, contributions to an M20* policy brief, a comic on AI and disinformation, and a podcast series for 16 Days of Activism. Media Development and Diversity (MDDA), South African Police Services (SAPS) and the Films and Publication Board (FPB) supported delivery through expertise, resources and policy linkages.

Outcomes and impact

Bona Bana strengthened digital literacy, improved school safeguarding practices and supported more confident parent engagement. Building on results from the 2024 model that informed 2025 delivery, 2 424 learners were reached across seven provinces, along with 35 teachers and five school governing body members. Feedback indicated 95% of teachers felt better equipped to address online harms and schools began strengthening online safety content in safeguarding policies. The Article 12 policy working group also deepened collaboration with policymakers and digital platforms.

Lessons learnt

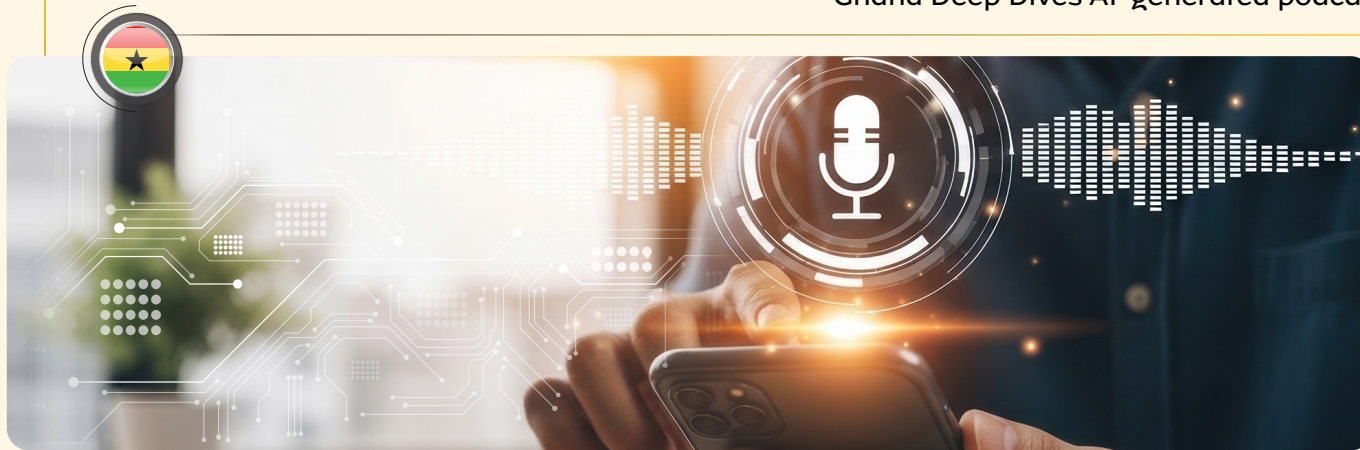
The programme revealed the importance of multilingual materials, deeper engagement with school governance structures and diversified funding for policy work. Overall, Bona Bana demonstrated a scalable, child-centred approach to digital inclusion and will inform future efforts to protect children online while advancing their digital human rights.

* Media 20 (M20) is the official G20 youth engagement initiative focused on media, journalism and information integrity.

Child online protection continued

Case study

Ghana Deep Dives AI-generated podcast



In 2025, MTN Ghana conducted digital human rights roadshows across all business divisions, focusing on teams whose decisions most directly affect human rights outcomes. The sessions strengthened understanding of MTN's Digital Human Rights Policy and employees' responsibilities as custodians of safe, responsible connectivity. However, we recognised that long policy documents are not always accessible or engaging in a fast-paced work environment. This created an opportunity to reinforce learning through a scalable, easy-to-consume format that employees could revisit at their convenience. The initiative sought to deepen understanding of MTN's digital human rights commitments, strengthen risk awareness and support SDG 16 (Peace, Justice and Strong Institutions), SDG 4 (Quality Education) and SDG 10 (Reduced Inequalities).

What we did

A concise script was developed, drawing on the Digital Human Rights Policy and key issues such as child online safety, child sexual abuse material, responsible data use and the challenges encountered in addressing these risks. This formed the basis of a five-minute AI-generated shortcast, which underwent several rounds of refinement to ensure clarity, accuracy and engagement.

The Regulatory and Compliance team, Corporate Services and the Digital Production team collaborated on content and design, while HR Internal Communications distributed the shortcast via email. Executive assistants amplified it across divisional and departmental WhatsApp groups to maximise reach.

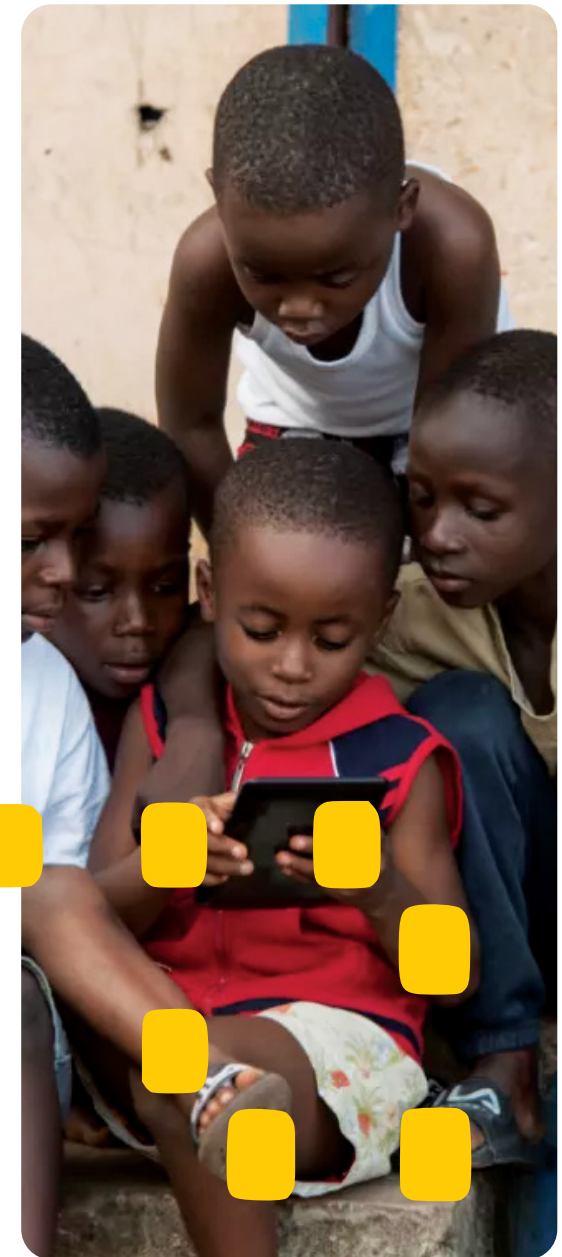
Outcomes and impact

The roadshows and shortcast collectively strengthened employee understanding of MTN's digital human rights commitments. In 2024 and 2025, more than 500 employees were reached through in-person roadshows and the first Deep Dives episode reached over 1 000 staff and contract employees via email and WhatsApp.

The shortcast provided an accessible summary of MTN's Digital Human Rights Policy and highlighted ongoing initiatives, including MTN's partnership with the Internet Watch Foundation to filter child sexual abuse material at network level. Early feedback indicated greater interest in digital safety issues and a more proactive approach to identifying and escalating risks.

Lessons learnt

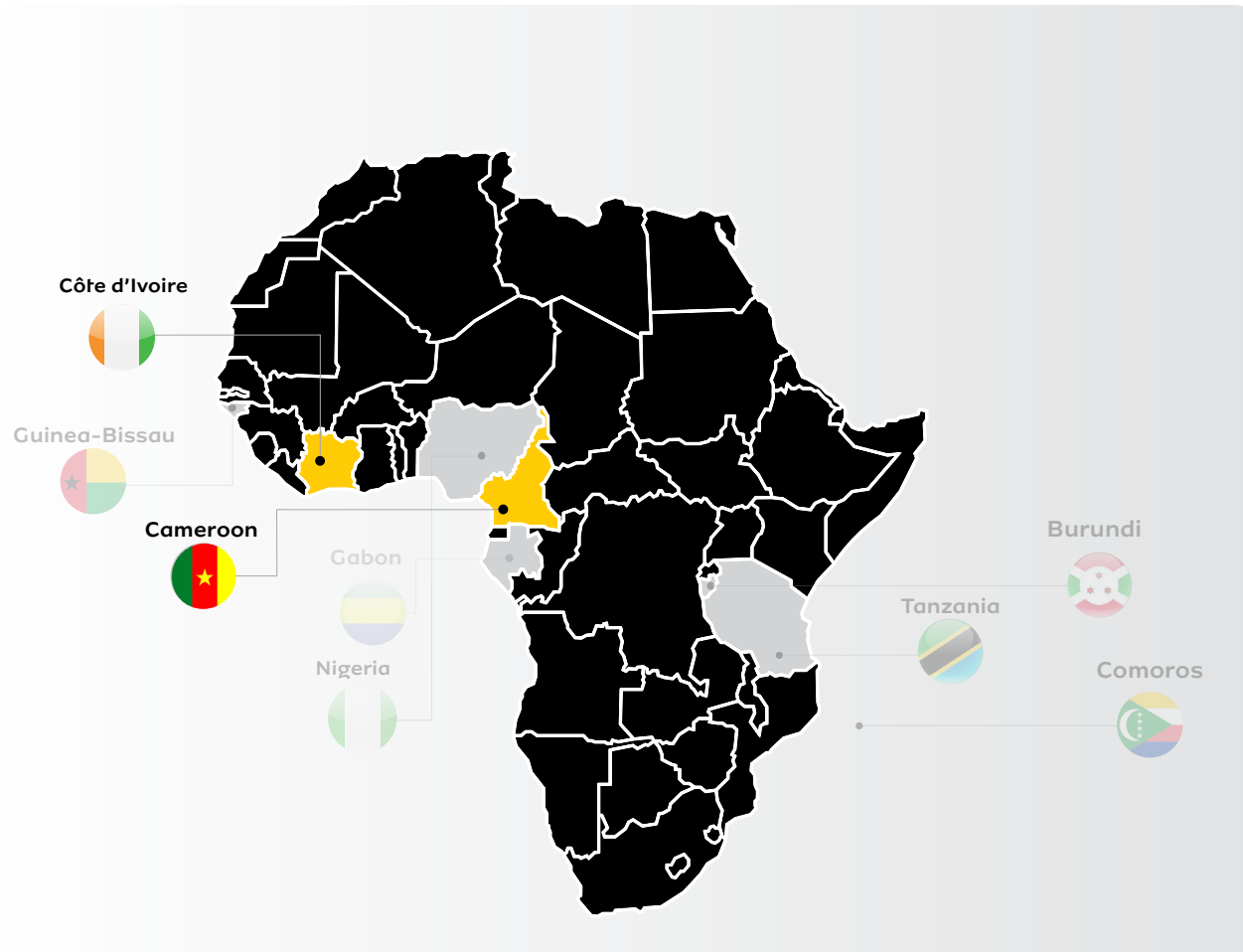
Employee engagement improves when digital human rights messaging aligns with broader thematic observances. October's Cybersecurity Month proved an effective launch window. Future editions will be timed to coincide with Safer Internet Day (February 2026) and Privacy Week (January–February 2026) to reinforce key messages during periods of heightened awareness.



Election readiness and human rights risk mitigation

Access Now election 2025 watchlist

In 2025, several African countries held elections, including Côte d'Ivoire and Cameroon, both MTN markets. These countries are highlighted on the map to reflect where MTN monitored electoral developments during the year.



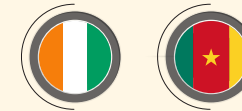
Source:

[2025 elections and internet shutdowns watch](#)



Case study

Managing election-related risks in our markets



Election periods are widely recognised as times of heightened sensitivity for digital communications. Independent monitors – such as the Access Now #KeepItOn coalition – have reported that temporary internet restrictions or service disruptions may occur in some countries during elections, particularly where political tensions are high. These events, when they occur, affect all operators equally and can limit people's ability to access information or communicate during important national moments.

In 2025, two of our markets, Cameroon and Côte d'Ivoire, held national elections. Ahead of both elections, we applied our human rights due diligence framework, which included comprehensive human rights impact assessments, social and political context monitoring and the development of election readiness approaches. These processes enabled us to identify potential risks, support our teams in affected markets and put in place measures to safeguard network integrity, staff security and user rights.

In Cameroon, external observers noted reduced internet availability in certain parts of the country around the election period. While we do not influence decisions relating to national network restrictions, we maintained strong internal co-ordination, monitored service performance closely and ensured our engagements with authorities followed established lawful processes. Elections in Côte d'Ivoire were largely peaceful and we followed the same readiness and due-diligence procedures to support responsible and proportionate decision making. Across both markets, our actions were aligned with international human rights standards.

Human rights-related position statements

Our human rights policies, processes and position statements reflect our commitment to ethical conduct and transparency. Each policy is thoughtfully developed, informed by both internal and external expertise and formally endorsed by our leadership. These policy statements are publicly available at <https://www.mtn.com/our-positions-certifications/?tablink=sound-governance>, reinforcing our commitment to openness and accountability.

Policies and positions

Data privacy and protection

MTN recognises data privacy and protection as a fundamental human right and a central component of responsible business conduct. Personal information is processed lawfully, transparently and only for defined, legitimate purposes, with collection limited to what is necessary. The Group safeguards data through appropriate technical and organisational controls, applies a risk-based approach to managing privacy and security risks, and extends these requirements to third parties acting on its behalf. Accountability is embedded across governance structures, supported by policies, oversight and ongoing awareness and training. MTN remains committed to protecting stakeholder rights and maintaining compliance with applicable laws and standards.

Zero rating

MTN recognises zero rating as an important mechanism to promote digital inclusion and equitable access to essential online services. The Group supports the responsible implementation of zero-rated offerings that enable access to qualifying educational, health and public interest content without data charges, subject to regulatory frameworks and commercial sustainability. MTN applies transparent eligibility criteria, governance oversight and risk management to ensure fairness, prevent misuse and maintain network integrity. These initiatives align with MTN's broader strategy to expand connectivity, reduce barriers to access and contribute to social and economic development across its markets.

Information security

MTN regards information as a critical business asset and prioritises its protection to preserve confidentiality, integrity and availability. The Group applies a risk-based approach to information security, guided by globally accepted standards and supported by an organisation-wide Information Security Management System. Information security is embedded within governance frameworks, operational controls, technology lifecycles and business continuity processes to strengthen resilience, safeguard resources and enable trusted operations. These requirements apply to employees, users and third parties, underpinned by clear accountability, oversight, compliance obligations and ongoing awareness and training. MTN remains committed to continuously reviewing and enhancing its information security practices in response to evolving threats, technologies and regulatory expectations.

Responsible AI

MTN regards AI as a strategic enabler that must be developed and deployed responsibly, ethically and transparently. The Group applies governance principles that promote fairness, accountability, privacy, security and respect for human rights, ensuring AI systems align with MTN's values, ESG priorities and digital transformation objectives. Responsible AI practices are guided by internationally recognised standards, implemented through the BRAIN framework and supported by a risk-based approach across the AI lifecycle. These commitments extend across MTN Group, its operating companies and third parties, underpinned by clear oversight, accountability, compliance obligations and ongoing awareness and training. MTN remains committed to continuously strengthening its Responsible AI approach in response to evolving technologies, risks and regulatory expectations.

Treating customers fairly

MTN delivers an exceptional customer experience by prioritising and meeting customer needs and expectations. This extends to ensuring fairness in all interactions with our products and services. A comprehensive policy and framework guide how we protect customers, promote transparency and empower users.

Responsible marketing and advertising

MTN's Responsible Marketing Policy provides a framework to ensure our marketing efforts are accurate, appropriate and inclusive. We comply with global standards and local legal requirements, guaranteeing ethical and transparent communication across all media platforms. This includes avoiding content that may incite violence, discrimination or harmful stereotypes. The policy also governs interactions with third parties and the responsible handling of personal data. Where AI used to optimise advertising delivery, we do not profile minors; prohibit targeting sensitive attributes; and apply informed-consent and easy opt-out mechanisms.

Responsible mobile advertising and sales

Our Responsible Advertising Sales Policy protects MTN users and customers while safeguarding the MTN brand. It prevents unsolicited targeted advertising that may offend minorities or be considered defamatory or obscene. We comply with local and international laws, including responsible access and use of first-party customer data.

Customers

Employees

Procurement

Government/ Regulators



Human rights-related position statements continued

Policies and positions

Responsible supply chain

The Supplier Code of Conduct outlines our approach to driving sustainable business practices and achieving high ethical standards. It reinforces our commitment to respecting and promoting human rights, fair labour practices, environmental sustainability and zero tolerance for bribery and corruption. Compliance with our Supplier Code of Conduct is a prerequisite for doing business with MTN. All our suppliers are required to adhere to standards established in the MTN Supplier Code of Conduct.

Whistle-blowing Policy

MTN has a zero-tolerance approach to fraud, bribery, corruption, theft and illegal activities. The Group's whistle-blowing mechanisms offer safe, anonymous channels for reporting. MTN protects individuals who report concerns in good faith and treats whistle-blowing as a positive mechanism for early detection of misconduct and the mitigation of financial and reputational risks.

Code of Conduct

MTN's Code of Conduct establishes the standards of ethical behaviour expected from employees and business partners. It reflects the values that underpin our operations and the trust placed in us by employees, customers, shareholders, communities and society. Compliance with our Supplier Code of Conduct is a prerequisite for doing business with MTN. All our suppliers are required to adhere to standards established in the MTN Supplier Code of Conduct.

Fair labour practices

MTN is committed to responsible labour practices across all markets. Our approach aligns with internationally recognised labour principles while ensuring compliance with local legal obligations and licence conditions.

Occupational health and safety

MTN adheres to world-class occupational health and safety standards. Our Occupational Health and Safety (OHS) Framework, aligned with ISO 45001, International Labour Organization (ILO) standards and national legislation, supports safe working environments for employees, customers and stakeholders across our value chain.

Political contributions

The Political Contributions Policy ensures transparent and responsible engagement in political party funding. It prioritises accountability, ethical conduct and compliance with legal requirements. The policy also mitigates risks such as reputational harm, legal exposure and erosion of stakeholder trust. This aligns with our broader commitment to stable democracies and digital human rights.

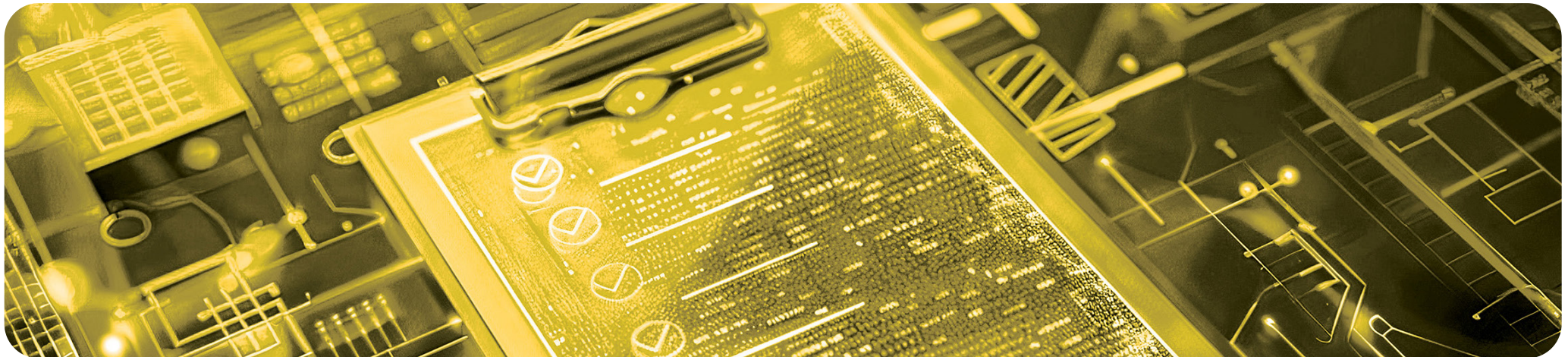
Customers

Employees

Procurement

Government/ Regulators

	✓	✓	
✓	✓		
	✓	✓	
	✓	✓	
✓	✓		
	✓		✓



Risk management

Integrating risks related to human rights into our risk management framework ensures a comprehensive and market-specific approach to risk management and is part of our overall enterprise risk management (ERM) system.

Our Markets report section covers the following categories.

Our management approach

-  **Digital human rights impact assessments**
We conduct continuous assessments of our human rights impacts using our digital human rights impact assessment and toolkit to ensure we keep an eye on emerging developments and report on these in a transparent manner.
-  **Collaborating with partners and stakeholders**
MTN is a member of various bodies that allow us to gain insight to further our efforts to uphold our focus on digital human rights. Our engagements with stakeholders showcase our commitment to strengthening our relationships and learning from our peers.
-  **Transparency and ranking digital rights**
MTN is a member of the Global Network Initiative, which enables us to gain insights and recommendations for protecting the freedom of expression and privacy rights of our customers

Risk management

Enterprise risk management

Risk management at MTN is a structured process that involves both management and the Board. It supports our strategic objectives by identifying risks that may affect our operations and applying appropriate mitigation measures. Our Group risk management framework is applied through a human rights lens to identify, prioritise and manage risks with potential human rights impacts.

Human rights risks are assessed in terms of the likelihood that our activities may infringe on the rights of individuals or communities. This includes risks linked to our digital human rights strategy, the way our systems and decisions may affect users and the emergence of new and evolving risks. We follow a three-part approach of Protect, Respect and Remedy, which commits us to preventing harm, respecting rights and addressing any adverse impacts that may arise.

Identified risks are recorded in the digital human rights risk register. The register sets out mitigation and remedy actions and assigns accountability to the relevant responsible owner within the business. This approach promotes consistency and discipline in how human rights risks are understood and managed across the Group.

MTN integrates digital human rights considerations into its ERM process. Human rights risks are identified, assessed and prioritised within our Group risk framework, supported by clear responsibilities at both Group and operating company levels. These risks are tracked in the digital human rights risk register, supported by mitigation actions and escalation pathways that enable consistent oversight and timely response.

MTN applies a structured enterprise risk management process that strengthens governance, supports decision making and enables consistent oversight of risks across all our markets.

1

ERM at MTN is centrally co-ordinated, supported by structured inputs from all operating companies.

2

The objective is to give management the tools and methods needed to identify threats and opportunities that influence strategic and operational performance.

3

Dedicated ERM resources support both Group-led activities and market-level risk processes.

4

Management and Exco teams engage risk management as a standing priority on their agendas.

5

Risk committees and forums at Group and market levels advance the effectiveness of ERM and internal control.

6

The ERM framework spans all MTN activities and reflects the full principal risk universe.

ERM system

Establish context

Risk assessment

Risk identification

Risk analysis

Risk evaluation

Risk treatment

Monitoring and review

Communicate and consult



Digital human rights impact assessment and toolkit

Our digital human rights impact assessments (DHRIA) form the foundation of this process. These assessments evaluate how our activities, business relationships and services affect all human rights and enable us to identify salient human rights issues relevant to our operating environments. Building on the DHRIA, we conduct risk assessments across all operating Opcos to deepen our understanding of local and thematic risk factors.

Our approach to human rights impact management

As a responsible business, aware of our direct and indirect influence on the human rights of our users, we follow a comprehensive impact management process to identify, prevent, mitigate and address potential and actual human rights risks. Our digital human rights impact assessments are supported by expert insight to determine how our activities, business relationships and services may affect people. This process enables us to identify salient human rights issues that materially affect our operations. To strengthen this approach, MTN conducts further risk assessments across all operating markets to understand jurisdiction-specific risk factors.

Strategic objectives of our digital human rights framework

- Provide MTN with a common vision for how it will respect and promote human rights, guided by our core beliefs.
- Enable continuous improvement of our digital human rights approach, policies and systems.
- Support the integration of MTN's digital human rights strategic responses.
- Ensure consistent operationalisation of digital human rights across the business.
- Embed digital human rights into the organisation through a structured programme.

Building awareness and strengthening accountability

MTN offers comprehensive training programmes to deepen understanding of human rights principles among employees, business partners, suppliers and agents. We conduct ongoing assessments of digital human rights impacts to remain informed about emerging developments and disclose these findings transparently. To support accountability, we maintain a secure and confidential whistle-blowing hotline that enables individuals to report human rights concerns safely and without fear of retaliation.

Digital human rights impact assessment and toolkit

MTN's DHRIA toolkit supports continuous digital human rights due diligence across all markets. It provides specialised tools for product evaluation, operating market assessments, responsible entry and exit, and mergers and acquisitions. These tools help Opcos identify, prevent and address potential human rights risks in a consistent and structured manner.

Digital human rights training

MTN completed digital human rights training for all Opcos in 2025. The training equipped employees with a clear understanding of MTN's obligations under the United Nations Guiding Principles on Business and Human Rights. It focused on how to assess, mitigate and prevent digital human rights violations, especially when responding to government-ordered requests involving service suspension, website throttling or disclosure of user information. Employees were also trained in how to complete their digital human rights impact assessments, ensuring they apply MTN's principles confidently and consistently across their operations.

Identifying the actions required for the business to mitigate negative impacts

Scope

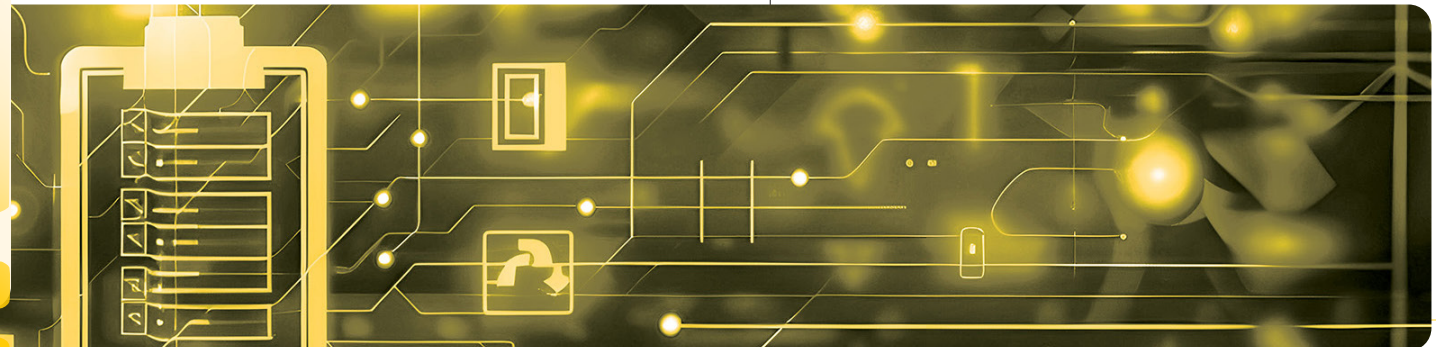
How many individuals could be impacted by the adverse effect?

Scale

How significant would the adverse effects on the rights-holder be?

Remediability

Will the remedy restore the rights-holder to a similar or comparable position as they were before the harm occurred?



Digital human rights impact assessment and toolkit continued

Digital human rights impact assessments

Issue

Capacity building

Stakeholder engagement

Product and business model development

Business model due diligence

Transparency

Description

Provide Opcos with human rights training, guidance and resources, such as rehearsals, scenario planning and opportunities to participate in GNI events and dialogue.

Take a strategic approach to establishing stakeholder relationships that facilitate the early identification of human rights risks and a proactive approach to addressing these.

Work continuously to ensure product and business model development removes bias in data analytics, the monetisation of data and the facilitation of hate speech and disinformation.

Anticipate, prevent and mitigate potential human rights risks posed by the Group strategy.

Provide additional insight into the regulatory and licensing context (where legally permissible) and continuously publish deeper insight into MTN's experience with state-required outcomes relating to lawful government requests.

2025 achievement

In 2025, we provided our employees and stakeholders with human rights training, practical guidance and scenario-based rehearsals that improved preparedness for complex lawful access and content-related requests. We shared insight from the digital human rights impact assessment. We also continued our participation in GNI learning sessions and participated in the UNGC Human Rights Accelerator programme.

We take a strategic approach to establishing stakeholder relationships that facilitate the early identification of human rights risks and a proactive approach to addressing these. In 2025, we deepened this work through expanded engagements with civil society and participation in the Internet Governance Forum in Norway, as well as in industry platforms such as the Ministerial Roundtable on Child Online Safety in Africa at the Mobile World Congress Barcelona. In addition, we contributed research insight to the Africa Taskforce on Child Online Protection.

We design products and business models that uphold human rights and minimise the risk of harm. In 2025, we strengthened our approach by applying clearer human rights considerations to digital and financial solutions. This is seen in the human rights assessments of our AI products (Zigi). These steps supported more ethical product development and reinforced our commitment to responsible innovation.

We aim to anticipate, prevent and mitigate potential human rights risks associated with our strategy and business model. In 2025, we strengthened due diligence by integrating human rights considerations into strategic reviews, expanding digital human rights impact assessments to include AI products and services, and improving how emerging risks are identified and escalated. These efforts supported more responsible decision making across markets and reinforced our commitment to safeguard people as we evolve our products and services.

We aim to enhance transparency by providing meaningful insight into the regulatory and licensing context, where legally permissible, and by sharing deeper reflections on our experience with state requests for online and network services. We have advanced this commitment through expanded disclosures, clearer explanations of our governance processes and richer case studies that illustrate how we apply human rights principles in practice.



Collaborating with partners and stakeholders

MTN continues to strengthen engagement with key stakeholders to advance digital human rights across our markets.

In 2025, we deepened our role in regional and global collaboration by joining the Africa Taskforce on Child Online Protection and sustaining our participation in platforms such as the Global Network Initiative and the Internet Watch Foundation. These engagements support responsible practices on privacy, freedom of expression and the blocking of harmful content, while informing the evolution of our transparency commitments through independent bodies such as Ranking Digital Rights. Across our footprint, we work with regulators, policymakers and civil society partners, including the Department of Social Development, the South African Human Rights Commission, the Teddy Bear Clinic and Save the Children Foundation.

This collective engagement strengthens accountability, broadens insight into emerging risks and enhances our ability to protect children and uphold digital human rights across diverse operating contexts.



MTN is guided by the following international standards and guidelines

- Africa Union Convention on Cybersecurity and Personal Data Protection
- ECOWAS Supplementary Act on Personal Data Protection (2010)
- International Bill of Human Rights
- International Covenant on Civil and Political Rights
- International Covenant on Economic, Social and Cultural Rights
- SADC Model Law on Data Protection
- United Nations Guiding Principles on Business and Human Rights
- United Nations Universal Declaration on Human Rights



MTN is a member of the following bodies:

- Africa Taskforce on Child Online Protection
- Global Network Initiative
- Global System for Mobile Communications Association (GSMA) mobile alliance to combat Digital Child Sexual Exploitation
- Internet Watch Foundation
- Signatory of the UNGC

Africa Taskforce on Child Online Protection

In 2025, MTN strengthened its commitment to child online safety by joining the Africa Taskforce on Child Online Protection, launched at Mobile World Congress Africa in Kigali, Rwanda. The Taskforce brings together mobile operators, global technology companies, regulators, academia and civil society to co-ordinate a unified, Africa-wide response to emerging online risks affecting children.

Africa continues to experience one of the world's fastest increases in the number of children coming online, driven by widespread mobile access and a rapidly growing youth population. As a result, young users face heightened exposure to cyberbullying, online exploitation, harmful content and misinformation. The Taskforce addresses these challenges by convening stakeholders from the mobile industry, technology companies, regulators, law enforcement agencies, civil society and youth representatives to develop a co-ordinated, Africa-led framework for child online safety. MTN's participation ensures the company contributes actively to shaping the policies, standards and best practices that underpin a safer digital ecosystem for children across its footprint.

The Taskforce's work is structured around shared objectives to strengthen prevention, protection and response mechanisms across the continent. These priorities include promoting safety-by-design in digital products and services, improving the accessibility and effectiveness of reporting and referral mechanisms, enhancing digital literacy and resilience among children and caregivers, and supporting greater policy coherence and regulatory alignment with child online protection. The initiative also aims to advance cross-sector data-sharing and collaboration to address rapidly evolving risks, including those associated with AI-generated harmful content.

As an early participant, MTN contributes operational insights and digital human rights expertise across multiple workstreams, including advocacy, policy alignment and technical safeguards. Our involvement helps elevate child online protection as a regional priority, supports alignment of safety practices across markets, and contributes to the development of safer and more resilient digital environments for children throughout Africa.

Transparency and ranking digital rights



Progress in ranking digital rights

Transparency reporting continues to evolve as global expectations shift towards greater corporate accountability on digital human rights. Companies are now expected to disclose their policies and processes, as well as the reasoning behind decisions that affect privacy, security and freedom of expression. This trend is shaping how we assess our own reporting and how we prepare for external evaluations.

Ranking Digital Rights (RDR), which now sits under the World Benchmarking Alliance (WBA) – a global organisation that benchmarks corporate performance on sustainability and human rights – has played an influential role in setting global norms for transparency and digital human rights disclosure. These standards guide how companies communicate their human rights performance, with particular emphasis on algorithmic transparency, due diligence processes, remedy mechanisms and the governance of emerging technologies.

Against this backdrop, in 2025 we undertook an internal benchmarking exercise to assess how far we have progressed against these standards. Key enhancements resulting from the assessment included strengthened transparency reporting, clearer governance arrangements, more rigorous data-privacy and protection measures, expanded child online safety initiatives and deeper integration of responsible AI principles across the business.

In the WBA assessments published in January 2026, MTN achieved an overall score of 42/100, ranking 8th out of 26 companies and performing above the industry average of 36.1/100. The Group performed strongest in governance, scoring 67/100, which compares favourably with several global peers and reflects relatively mature governance structures and oversight disclosures. However, scores in freedom of expression (35/100) and privacy (37/100) indicate room for improvement, particularly when benchmarked against higher scoring companies in these categories. While MTN's overall positioning places it in the upper tier of assessed operators, strengthening transparency and disclosure in rights-related areas would further enhance the Group's performance and stakeholder confidence.

Metrics and targets

In this section, we present data from our operating markets reflecting requests received from authorities and non-governmental organisations. We also outline key regulatory developments and provide context on the legislative frameworks shaping our operations.

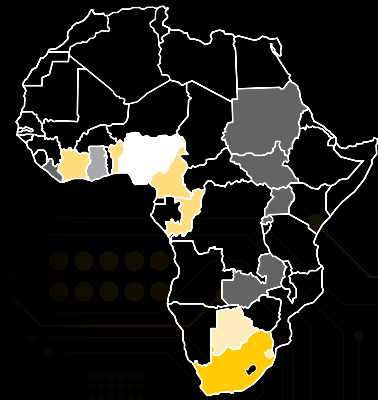
Our performance

Our Markets report section covers the following categories.

-  **Regulatory trends**
Insight into evolving regulatory developments across our markets and their implications for our business.
-  **Legislative requirements**
An overview of the legislative obligations and reporting requirements applicable to our operations.
-  **Requests received from authorities**
Data on the categories, volume and nature of requests received from authorised bodies.
-  **Looking forward**
An overview of emerging priorities and technological developments.

Markets report

MTN Group is a Pan-African digital operator, serving 307.2 million customers across 16 markets. Robust operational and governance oversight structures underpin our growth strategy. In November 2025, we streamlined our operating model for greater efficiency and growth. As a result, our operations are organised as follows: South Africa; Nigeria; Ghana; SEA; and Francophone Africa.



307.2
million
Stronger

	MTN Group effective shareholding	Subscribers
MTN South Africa	100.0%	40.6m
MTN Nigeria	76.3%	87.3m
MTN Ghana	72.9%	31.2m
SEA		
MTN Uganda	76.0%	24.2m
MTN Rwanda	80.0%	8.2m
MTN Zambia	89.8%	7.0m
MTN South Sudan	100.0%	4.2m
MTN Sudan	85.0%	3.2m
LonestarCell (MTN Liberia)	60.0%	2.2m
Francophone Africa		
MTN Cameroon	80.0%	13.1m
MTN Côte d'Ivoire	66.8%	15.3m
MTN Benin	75.0%	6.4m
MTN Congo-Brazzaville	100.0%	3.9m
Associates, JVs and other investments^Δ		
IranCell Group ^Δ	49.0%	57.6m
Mascom Botswana ^Δ	53.1%	1.9m
MTN Eswatini ^Δ	30.0%	1.1m

^Δ Equity accounted, not under MTN operation.

The Group also has investments in aYo (50%); IHS Group (24.7%); Snapp Group (29.5%); Middle East Tech Ventures Holding (50.0%) and others.

Our financial performance

+22.7%* to R218.5bn
service revenue

+36.4%* to R101.5bn
data revenue

+23.2%* to R30.3bn
fintech revenue

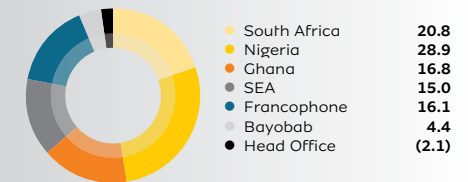
+36.8%* to R98.5bn
EBITDA

17.0%*
capex intensity

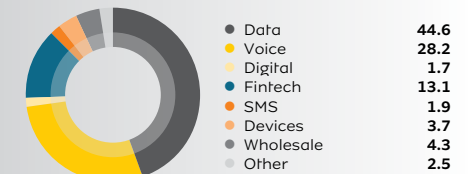
R38.5bn
capex (ex-leases)

Service revenue contribution

by geography %

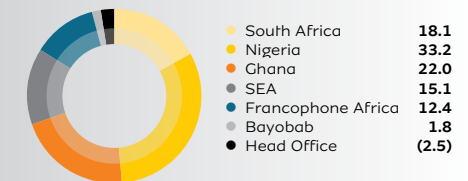


by services %



EBITDA contribution

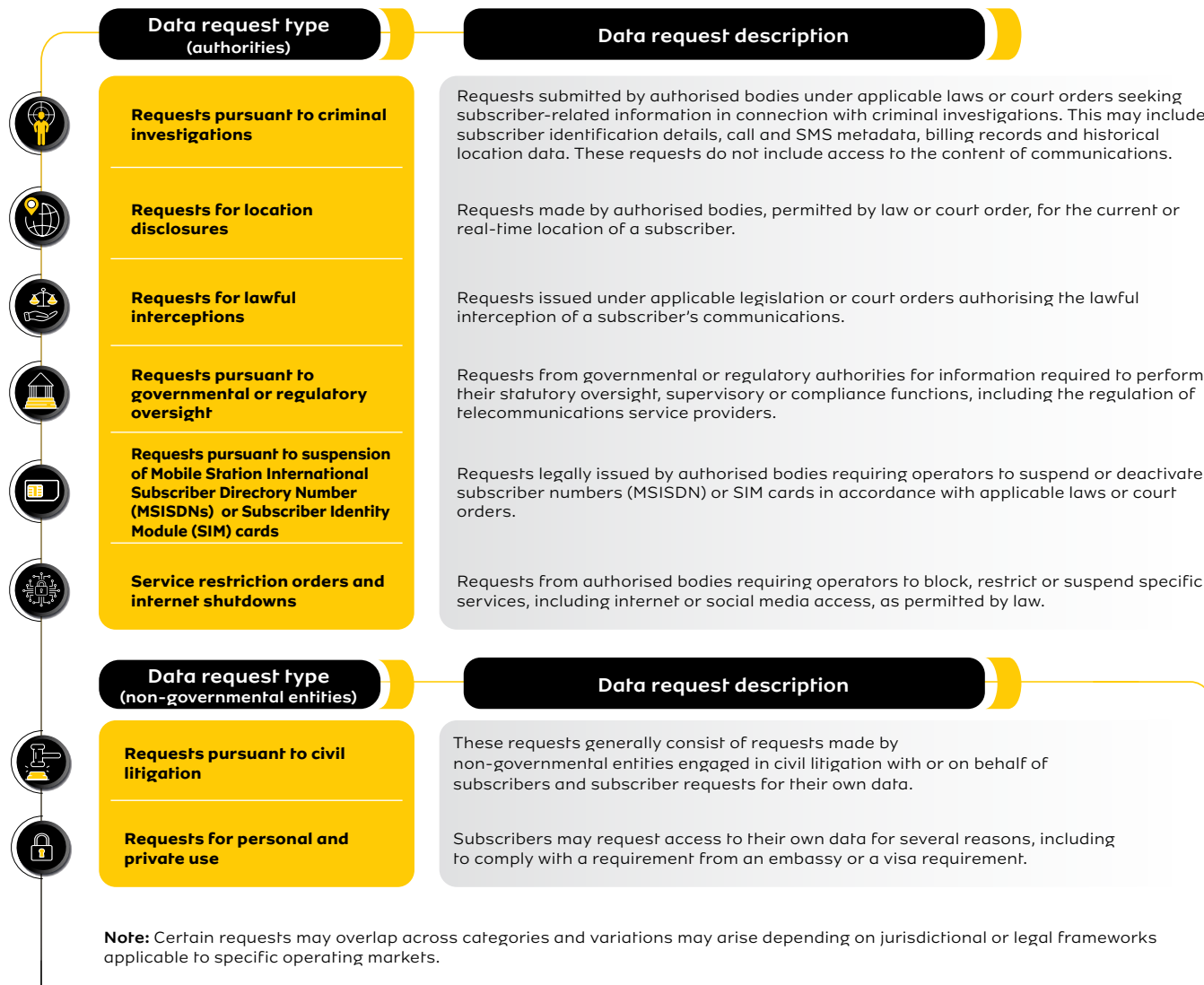
by geography %



Markets report continued

Categories of requests from authorities

Operating markets have supplied data relating to requests received from both authorities and non-governmental entities. Given the diverse array of laws and regulations applicable across our markets, requests from authorised bodies have been classified into relevant categories based on their legal basis and purpose. While each category reflects a distinct regulatory or legal framework, certain requests may overlap depending on jurisdictional requirements.



Regulatory trends in our markets

In 2025, jurisdictions across Africa continued to refine legal and regulatory frameworks shaping the digital operating environment. Developments across cybersecurity, data protection, artificial intelligence, platform oversight and digital identity systems signal a progressively maturing digital governance landscape. While regulatory approaches vary, the overall direction reflects expanding compliance expectations, heightened enforcement visibility and growing scrutiny of data and technology practices.

Several countries strengthened **cybersecurity and cybercrime legislation**, introducing new regulatory authorities, incident response structures and expanded protections for critical information infrastructure. These reforms increase organisational accountability for cyber resilience, breach management and system security. Firms operating across multiple jurisdictions face rising complexity in aligning controls, reporting obligations and regulatory engagement.

Artificial intelligence governance emerged as a key regulatory frontier. New strategies and legislative proposals introduced ethical principles, assessment frameworks and oversight mechanisms governing AI development and deployment. These shifts elevate expectations regarding transparency, algorithmic accountability, bias management and responsible technology use.

Data protection and privacy regimes also evolved, supported by regulatory amendments, implementation directives and the operationalisation of enforcement authorities. These developments heighten regulatory, financial and reputational exposure associated with data-handling practices while reinforcing the strategic importance of robust data governance and security frameworks.

Platform regulation, online content oversight and digital identity reforms continued to develop, influencing obligations related to digital services, subscriber registration and customer data verification. In select jurisdictions, temporary network restrictions highlighted the intersection of digital governance, political risk and business continuity considerations.

Digital financial services regulation advanced in response to rapid fintech and mobile money expansion. New rules addressing consumer protection, ethical conduct, privacy safeguards and localisation requirements reflect increasing regulatory attention to digital conduct and data stewardship risks.

Regional harmonisation initiatives and data localisation trends further shaped the regulatory landscape, affecting infrastructure decisions, cross-border data management and compliance strategies. Collectively, these developments underscore the need for continuous regulatory monitoring, adaptive compliance capability and strengthened governance oversight of digital, data and technology-related risks.

Markets report continued

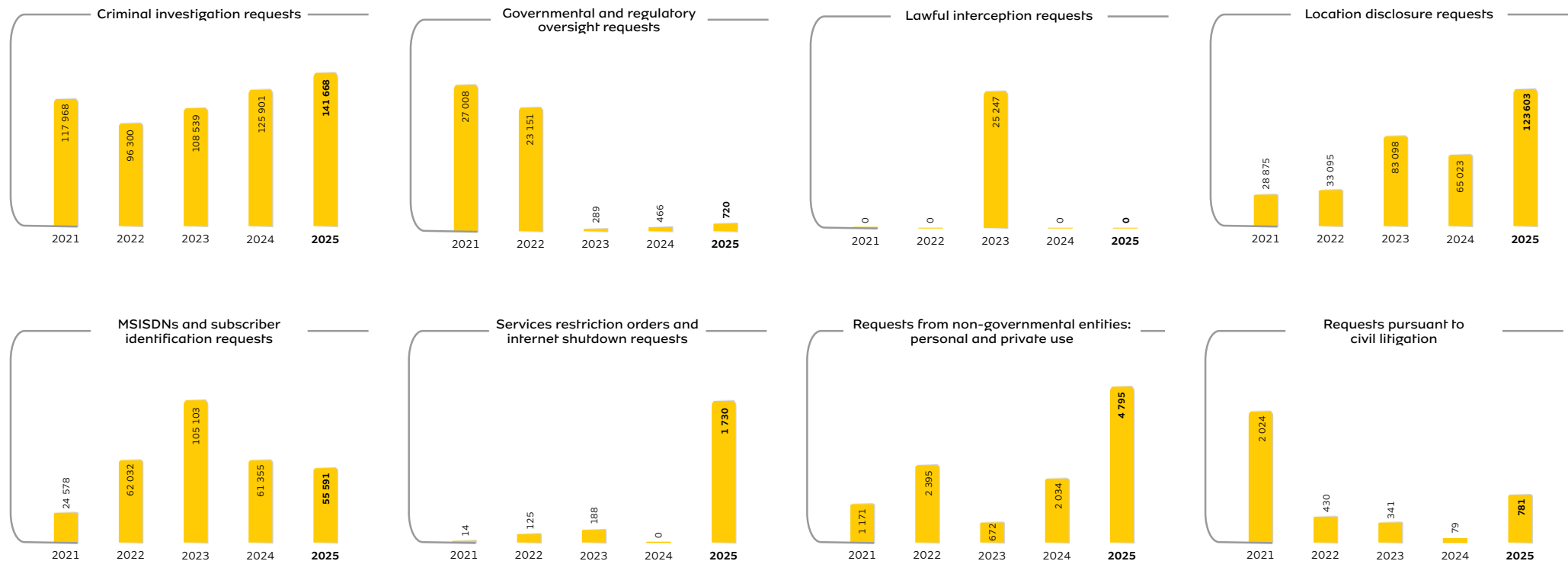
Overview of total requests received

The digital human rights landscape in our markets remained dynamic in 2025, as reflected by the quantitative data. These shifts indicate the impact of technology, regulatory amendments and growing concerns in the digital human rights space.

It is not possible to definitively determine the exact reasons behind individual requests at this time, and therefore an analysis of the increase or decrease in the data would be speculative. However, we have observed certain trends across the markets that may provide insight into the potential factors influencing these changes. Please note that this is not a conclusive assessment but rather an informed observation based on current patterns. In our estimation, these shifts may have occurred as a result of: (i) shifts in law enforcement strategies; (ii) increased social conflict and protests in various regions; (iii) geopolitical shifts; and (iv) legislative changes (including those pertaining to national identity systems and SIM card registration processes).

- Criminal investigation requests increased from 125 901 in 2024 to 141 668 in 2025. This increase can be attributed to robust action taken within our markets to address fraudulent criminal activities, following the introduction of new consumer protection rules and regulations in the financial sector across many of our markets.
- Government regulatory oversight increased from 466 in 2024 to 720 in 2025.
- Lawful interception requests in 2024 and 2025 are now being captured and classified by Opcos under criminal investigation data as a result of many lawful interception requests being required during criminal investigations by law enforcement authorities.
- Location disclosure requests increased from 65 023 in 2024 to 123 603 in 2025 owing to compliance with law enforcement requests.

- MSISDNs and subscriber identification requests decreased from 61 355 in 2024 to 55 591 in 2025.
- Service restriction orders increased to 1 730 in 2025. This rise is primarily attributable to a higher volume of government-issued directives during periods of heightened national activity across several markets, as well as improved internal processes for capturing and reporting data from markets. MTN continues to comply with all lawful requests while maintaining a strong focus on safeguarding human rights through enhanced governance, oversight and transparency mechanisms.
- Requests for personal and private use increased from 2 034 in 2024 to 4 795 in 2025.
- Civil litigation requests increased from 79 in 2024 to 781 in 2025.



In 2025, we enhanced our data capture and reporting processes across all markets, reflecting our growing organisational maturity and commitment to data accuracy. These improvements included a comprehensive review of historical data and the implementation of stronger controls to ensure that all information is consistently captured and accurately reflected.

Markets report continued



Benin



MTN has operated in Benin since 2006 and serves approximately 6.4 million subscribers. In 2025, the Group generated revenue of R6.2 billion from its operations in the country.

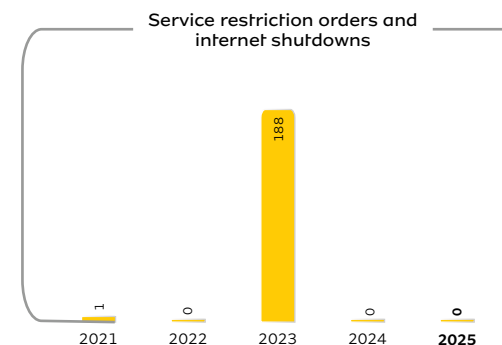
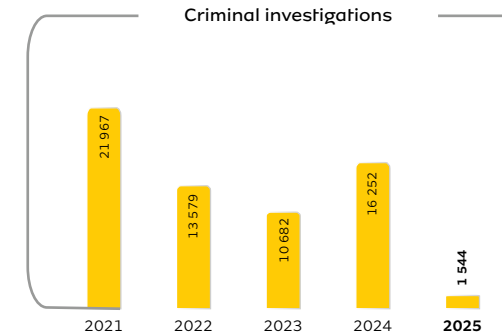
Regulatory framework

- Decision No. 2022-0248 laying down the parameters and security measures and the camouflage rules of radio sites in the Republic of Benin.
- Decision No. 2022-082 laying down the conditions for the termination of SIM cards by operators of electronic communications networks and services in the Republic of Benin.
- Decision No. 2022-049 on the framework of the rates for electronic communications services provided by mobile operators in the Republic of Benin.
- Decision No. 2022-025 on guidelines for national roaming on mobile electronic communications networks in the Republic of Benin.
- Decision No. 2021-197 on rules for managing the top-level Internet domain name '.bj' in the Republic of Benin.
- Decision No. 2021-237 approving the standard specifications laying down the conditions for the establishment and operation of an Internet access supply network in the Republic of Benin.
- Decision No. 2021-075 approving the standard specifications laying down the conditions for the establishment and operation of virtual mobile networks (MVNOs and MVNEs) in the Republic of Benin.
- Bilateral memorandum of understanding signed on 18 October 2023 between ARCEP BENIN and ARCEP Togo to implement the ECOWAS regulation on community roaming and communications facilities.
- Bilateral memorandum of understanding concluded on 9 December 2023 between ARCEP BENIN and AMRTP Mali to implement the ECOWAS regulation on community roaming and communications facilities.

- Decision No. 2023-113/ARCEP/PT/SE/GU of May 2023 on guidelines for national roaming on mobile electronic communications networks in the Republic of Benin.
- Article 23 of the Constitution of Benin (Law No. 2019-40 of 7 November 2019 amending the Constitution of 11 December 1990).
- Decree No. 2023-060 of 22 February 2023 approving the Protection Policy Rules of the Critical Information Infrastructures in the Republic of Benin.
- Bilateral memorandum of understanding signed on 27 March 2024 between ARCEP BENIN and National Communication Authority of Ghana to implement the ECOWAS regulation on community roaming and communications facilities.
- ARCEP Decision No. 2024-150/ARCEP/PT/SE/DJPC/GU on the organisation of the process for identifying users of electronic communication services in the Republic of Benin.
- Law No. 2024-22 of 26 July 2024 on the Beninese Commission for Human Rights.
- Law No. 2024-12 of 29 March 2024 authorising the ratification of the African Union Constitution and the Convention on Telecommunications adopted in Cape Town (South Africa) on 7 December 1999 and in Harare (Zimbabwe) on 10 July 2014.
- Decree No. 2024-861 of 29 March 2024 ratifying the African Union Constitution and the Convention on Telecommunications adopted in Cape Town (South Africa) on 7 December 1999 and in Harare (Zimbabwe) on 10 July 2014.
- Law No. 2024-05 of 1 February 2024 authorising the ratification of the African Union Convention on Cybersecurity and Personal Data Protection adopted in Malabo (Equatorial Guinea) on 27 June 2024.
- Decree No. 2024-772 of 1 February 2024 ratifying the African Union Convention on Cybersecurity and Personal Data Protection adopted in Malabo (Equatorial Guinea) on 27 June 2014.
- Law No. 2024-06 of 1 February 2024 authorising accession to the Convention on Cybercrime adopted in Budapest (Hungary) on 23 November 2001, to the Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems adopted in Strasbourg (France) on 28 January 2003, and the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence adopted in Strasbourg (France) on 12 May 2022.
- Law No. 2025-12 of 2 July 2025 amending the law No. 2017-08 relating to the identification of individuals.
- Decree No. 2025-363 of 2 July 2025 establishing the conditions for carrying on the activity of electronic archiving service providers.
- Decree No. 2025-368 of 2 July 2025 establishing the rules on interception and access to data, defining the authorised authorities and establishing the procedures for implementing operations and specific provisions on cryptology.

Authorities

- Authority of Post and Electronic Communications (ARCEP Benin).
- Central Office for the Repression of Cybercrime.
- Constitutional Court.
- Courts and Tribunals in Benin.
- Economic Crimes and Terrorism Court.
- Information Systems and Digital Agency (ASIN).
- Ministry of Digital and Digitalisation.
- Ministry of Economy and Finance.
- Ministry of Foreign Affairs.
- Ministry of the Interior and Public Security.
- Ministry of Justice.
- Ministry of National Defence.
- National Centre for Digital Investigation.
- National Financial Information Processing Units.
- National Personal Identification Agency.
- Personal Data Protection Authority (APDP).
- Republican Police: General Directorate of the Republican Police.



Markets report continued



Cameroon



MTN has operated in Cameroon since 2000 and serves approximately 13.1 million subscribers. In 2025, the Group generated revenue of R13.5 billion from its operations in the country.

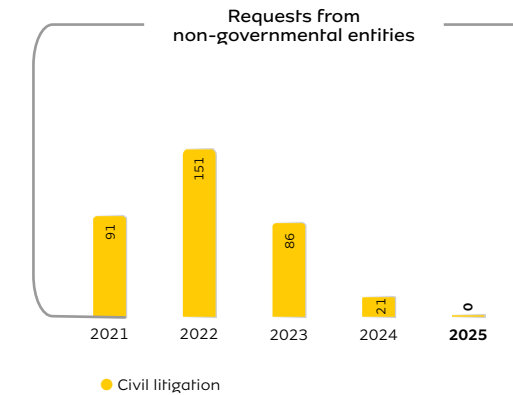
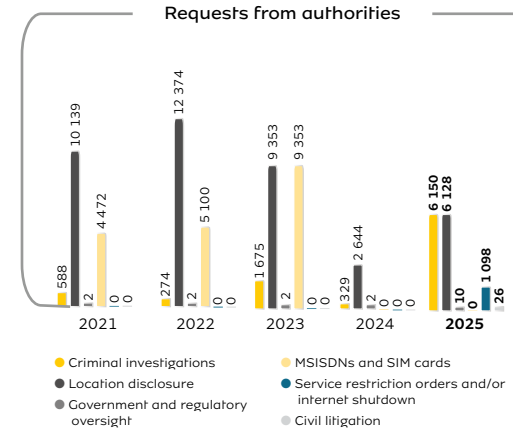


Regulatory framework

- The Preamble of Cameroon's Constitution.
- Law No. 2010/013 of 21 December 2010 regulating electronic communications in Cameroon, as modified and completed by Law No. 2015/006 of 20 April 2015.
- Law No. 2010/012 of 21 December 2010 relating to cybersecurity and cybercrime.
- Law No. 2010/021 of 21 December 2010 relating to electronic commerce in Cameroon.
- Decree No. 2013/0399/PM of 27 February 2013 establishing the modalities for the protection of consumers of electronic communications services.
- Decree No. 2015/3759 of 3 September 2015 laying down conditions for the identification of subscribers and terminal equipment of electronic communications networks.
- Law No. 2016/007 of 12 July 2016 establishing the Penal Code in Cameroon.
- Decree No. 2017/2580/PM of 6 April 2017 establishing the conditions for the establishment and exploitation of electronic communications networks subject to the authorisation regime in Cameroon.
- Law No. 2015/007 of 20 April 2015 governing audiovisual activities in Cameroon.
- Law No. 2023/009 of 25 July 2023 instituting the Charter on Child Online Protection in Cameroon.
- Law No. 2024/017 of 23 December 2024 relating to personal data protection in Cameroon.

Authorities

- Civil Courts.
- General Delegation for National Security.
- Ministry of Finance.
- Ministry of Justice.
- Ministry of Labour and Social Security.
- Ministry of Posts and Telecommunications.
- Ministry of Territorial Administration.
- National Agency for Information and Communication Technologies (ANTIC).
- Public Prosecutor's Office.
- Telecommunications Regulatory Board.



Markets report continued



Congo-Brazzaville



MTN has operated in Congo-Brazzaville since 2006 and serves approximately 3.9 million subscribers. In 2025, the Group generated revenue of R4.8 billion from its operations in the country.

Regulatory framework

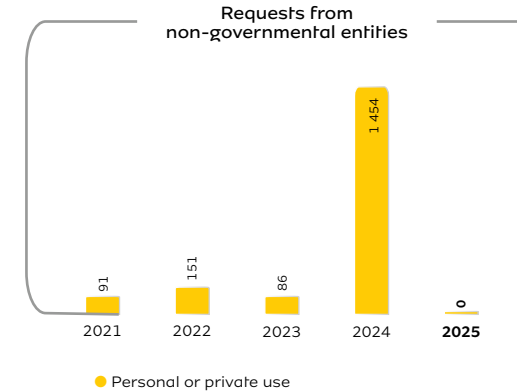
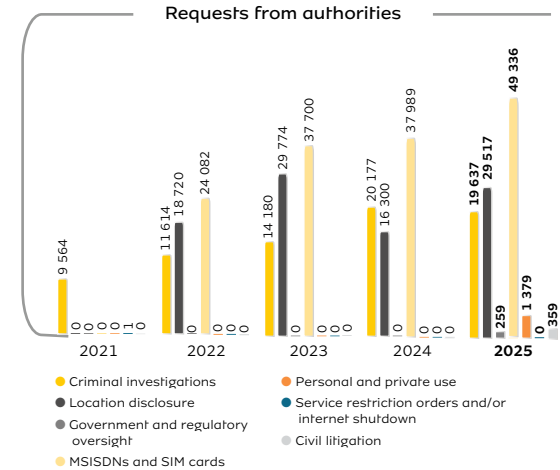
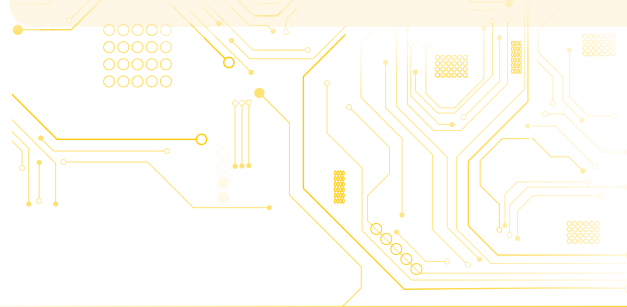
- Law No. 8-2001 of 12 November 2001 on freedom of information and communication.
- Law No. 9-2009 of 25 November 2009 on the regulation of electronic communications.
- Law No. 11-2019 of 25 November 2009 on the creation of the regulatory agency for posts and electronic communications.
- Law No. 29-2019 of 10 October 2019 on the protection of personal data.
- Law No. 30-2019 of October 2019 on the creation of the National Agency for Information Systems Security.
- Law No. 26-2020 of 5 June 2020 on cybersecurity.
- Law No. 27-2020 of 5 June 2020 on combating cybercrime.
- Law No. 43-2020 of 20 August 2020 authorising the ratification of the Convention of the African Union on Cybersecurity and the Protection of Personal Data.
- Articles 18 to 20 of Law No. 073/84 of 17 October 1984 on the Family Code.
- Article 26 of the Constitution of the Republic of the Congo of 6 November 2015.
- Law No. 36-2024 of 11 October 2024 on consumer protection.

The Republic of Congo is one of six member countries of the Central African Economic and Monetary Community (CEMAC). As such, at a regional level, digital human rights are regulated by CEMAC through:

- Directive No. 06/08-UEAC-133-CM-18 defining the regime of universal service in the electronic communications sector among CEMAC member states.
- Directive No. 07/08-UEAC-133-CM-18 defining the legal framework of network and electronic communication services' users rights and protection in the CEMAC.
- Directive No. 08/08-UEAC-133-CM-18 on interconnection and access to network and electronic communications services in CEMAC member states.
- Directive No. 09/08-UEAC-133-CM-18 harmonising the legal framework of electronic communications activities in CEMAC member states.
- Directive No. 10/08-UEAC-133-CM-18 harmonising the rules of establishing and controlling tariffs for electronic communications services in the CEMAC.
- Directive No. 21/08-UEAC-133-CM-18 harmonising the rules and regulations of electronic communications in the CEMAC.
- Law No. 19-2024 of 16 August 2024 establishing the Competition Authority.
- Law No. 5-2025 of 29 March 2025 on the creation of the National Commission for the Protection of Personal Data.
- Decree No. 2025-538 of 31 December 2025 nominating the members of the Commission for the Protection of Personal Data.

Authorities

- ARPCE, the Congolese Authority for the control, monitoring and regulation of the postal and electronic communications sectors.
- Charter on Child Online Protection.
- Ministers.
- National Agency for Information Systems Security (ANSSI).
- President of the Republic.
- Regulators.



Markets report continued



Côte d'Ivoire



MTN has operated in Côte d'Ivoire since 2005 and serves approximately 15.3 million subscribers. In 2025, the Group generated revenue of R10 billion from its operations in the country.

Regulatory framework (at national level)

- Law No. 2024-352 of 6 June 2024 relating to electronic communications (repeals Order No. 2012-293 of 21 March 2012 on Telecommunications and Information and Communication Technologies, except for Articles 51, 71 and 157, respectively creating the Agence ivoirienne de Gestion des Fréquences, the Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire and the Agence nationale du Service universel des Télécommunications/TIC).
- Law No. 2017-802 of 7 December 2017 on the orientation of the information society in Côte d'Ivoire (sets the general legal and institutional principles of the information society in Côte d'Ivoire).
- Law No. 2016-886 of 8 November 2016, establishing the Constitution of the Republic of Côte d'Ivoire, as amended by constitutional Law No. 2020-348 of 19 March 2020.
- Law No. 2013-450 of 19 June 2013 on the protection of personal data.
- Law No. 2013-451 of 19 June 2013 combating cybercrime.
- Law No. 2013-546 of 30 July 2013 on electronic transactions.
- Ordinance No. 2024-368 of 12 June 2024, on the Organization of Civil Society.
- Penal Code.
- Decree No. 2012-934 of 19 September 2012 on the organisation and operation of the Autorité de Régulation des Télécommunications/ICT de Côte d'Ivoire (ARTCI).
- Decree No. 2013-301 of 2 May 2013 on the approval of terminal and radio equipment and the approval of installers.
- Decree No. 2013-439 of 13 June 2013 setting the conditions and procedures for reserving, allocating and withdrawing numbering resources, as well as the amounts and procedures for payment of fees for the use of numbering resources.

- Decree No. 2015-812 of 18 December 2015 approving the specifications attached to each individual licence in category C1A, for the establishment of networks and the provision of telecommunications/ICT services.
- Decree No. 2017-193 of 22 March 2017 on the identification of subscribers to telecommunications/ICT services open to the public and users of cybercafés.
- Decree No. 2018-875 of 22 November 2018 establishing the powers, composition, organisation and functioning of the National Commission for the Development of the Information Society (CNSI).
- Article 19 of the Constitution of the Republic of Côte d'Ivoire dated 8 November 2016.
- Article 15 of Law No. 2015-493 dated 7 July 2015 combating terrorism.
- Decree No. 2021-245 of 26 May 2021 fixing the fees for the use of radio frequencies.
- Decree No. 2021-917 of 22 December 2021 defining the audit, control and certification procedures for information systems.
- Decree No. 2021-916 of 22 December 2021 adopting the general information systems security framework and the critical infrastructure protection plan.
- Decree No. 2021-915 of 22 December 2021 adopting the information systems security policy of the public administration.
- Law No. 2017-867 of 27 December 2017 on the press regime.
- Law No. 2022-978 of 20 December 2022 amending Law No. 2017-867 of 27 December 2017 on the legal regime of the press.
- Decree No. 2024-958 of 30 October 2024 on the creation, powers, organisation and operation of the National Agency for the Security of Information Systems (ANSSI-CI).
- Law No. 2022-979 of 20 December 2022 amending Law No. 2017-868 of 27 December 2017 on the legal regime for audiovisual communication and the High Authority for Audiovisual Communication (HACA).

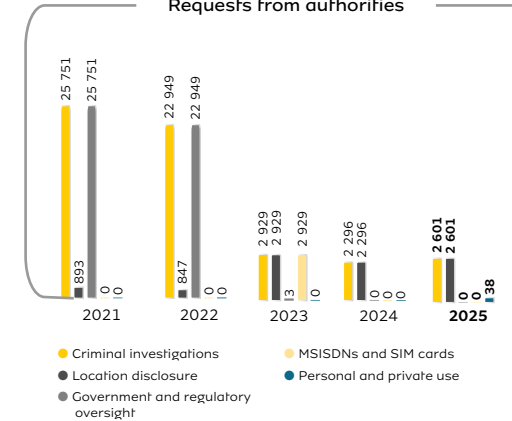
Regulatory framework (at community level)

- Directive No. 02/2006/CM/UEMOA on the harmonisation of legal regimes applicable to telecommunications network operators and service providers. It is specified that the transposition of this Directive into national law does not affect the specific regulations adopted by the member states, particularly those on the basis of compliance with essential requirements and other requirements in the public interest.
- Additional Act A/SA. 3/01/07 ECOWAS of 19 January 2007 on the legal regime applicable to operators and service providers: aims to harmonise the ECOWAS legal regimes applicable to the activity of telecommunications network operators and service providers and to specify the procedures for granting licences, authorisations and declarations and the conditions applicable to these different regimes. Its transposition into domestic law does not affect the specific regulations adopted at national level.

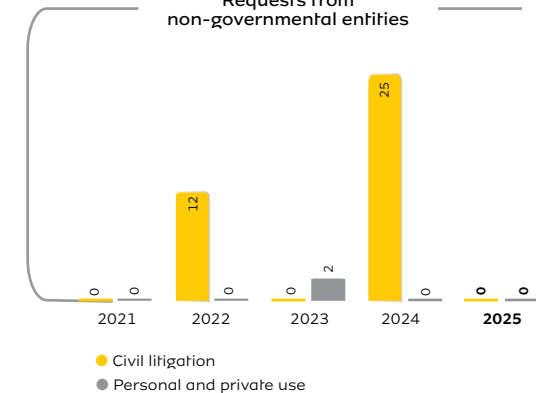
Authorities

- Agence Ivoirienne de Gestion des Fréquences Radioélectriques.
- Agence Nationale du Service Universel des Télécommunications.
- Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI).
- High Authority for Audiovisual Communication (HACA).
- Ministry of Defence.

Requests from authorities



Requests from non-governmental entities



- Ministry of Digital Transition and Digitalisation.
- Ministry of the Interior.
- Ministry of Justice and Human Rights.
- Ministry of Security.
- National Agency for the Security of Information Systems.
- National Human Rights Council (CNDH).
- Platform for Combating Cybercrime.
- Police Administrations.

Markets report continued



Eswatini



MTN has operated in Eswatini since 1998 and serves approximately 1.1 million subscribers. In 2025, the Group generated revenue of R441 million from its operations in the country.



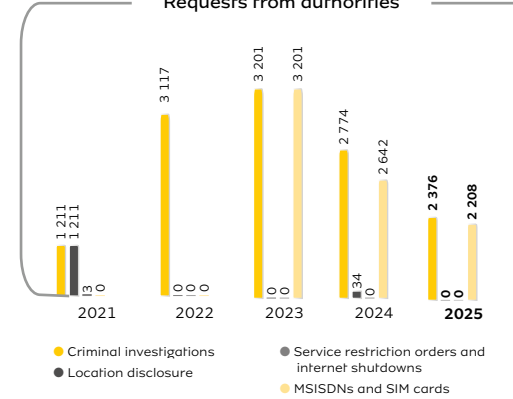
Regulatory framework

- Swaziland Communications Commission Act No. 10/2013.
- Electronic Communications Act No. 09/2013.
- Swaziland Communications Commission (Consumer Protection) Regulations, 2016.
- Swaziland Communications Commission (Subscriber Registration) Regulations, 2016.
- Television Guidelines, 2017.
- Section 18 of the Constitution (Protection from Inhuman Treatment, which, when interpreted by the courts, includes the right to privacy) of the Kingdom of Eswatini Act No. 001/2005.
- Section 24(1) and 24(2) of the Constitution of the Kingdom of Swaziland Act No. 1 of 2005.
- Data Protection Act 2022.
- Eswatini Data Protection Authority Advisory Guidelines on the Appointment of Data Protection Officers of 2023.
- Computer Crime and Cybercrime Act 2022.
- Electronic Communications and Transactions Act 2022.
- Clause 15 of the Services and Network Licence Conditions.
- Section 212 and 331 of the Companies Bill 2024.
- Children's Protection and Welfare Act, 2012 (Act No. 3 of 2022).
- Child Online Protection Strategy (proposed, 2025).
- Section 14 of the Constitution (protects the right to privacy, including communications) of the Kingdom of Eswatini Act No. 1 of 2005.
- National Cybersecurity Strategy (NCS 2025).

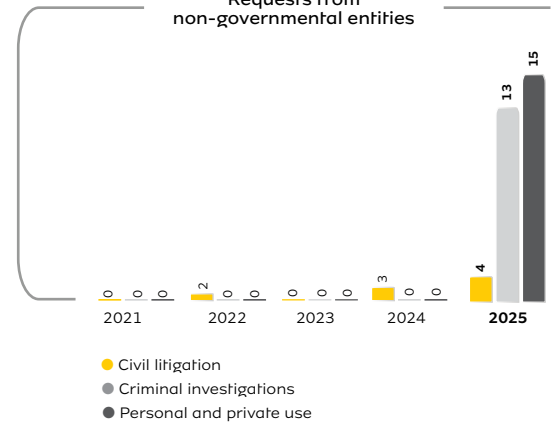
Authorities

- Anti-Corruption Commission.
- Courts.
- eSwatini Communications Commission.
- eSwatini Data Protection Authority (EDPA).
- eSwatini Revenue Authority.
- Judiciary of Eswatini.
- Ministry of Information Communication and Technology.
- Ministry of Justice and Constitutional Affairs.
- Royal eSwatini Police.

Requests from authorities



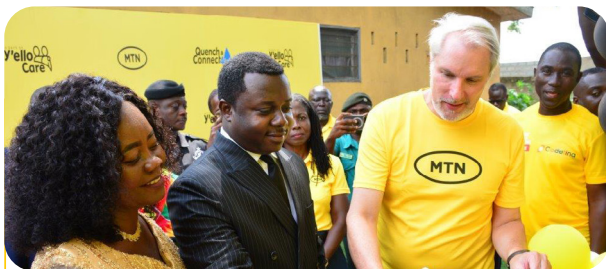
Requests from non-governmental entities



Markets report continued



Ghana



MTN has been present in Ghana since 2006 and has approximately 31.2 million subscribers. In 2025, MTN's revenue in Ghana was R35.8 billion.



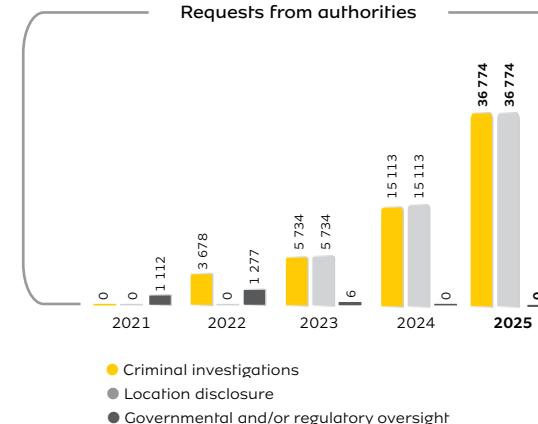
Regulatory framework

- 1992 Constitution of Ghana.
- Cybersecurity Act, 2020 (Act 1038).
- Electronic Communications Act, 2008 (Act 775) as amended.
- Electronic Transactions Act, 2008 (Act 772) as amended.
- Data Protection Act, 2012 (Act 843).
- Electronic Communications Regulations, 2011 (L.I. 1991).
- Directive for the Protection of Critical Information Infrastructure (CII).
- Revenue Administration Act, 2016 (Act 915) as amended.
- Right to Information Act, 2019 (Act 989).
- Anti-Terrorism Act, 2008 (Act 762) as amended.
- Subscriber Identity Module (SIM) Registration Regulations, 2011 (LI 2006).
- Criminal Offences Act, 1960 (Act 29) – addresses defamation, obscene publications and related offences applicable to digital platforms.
- Establishment of Emergency Communications System Instrument, 2020 (E.I. 63).
- Communication Service Tax Act, 2008 (Act 754) as amended.
- Payment Systems and Services Act, 2019 (Act 987).
- Office of the Special Prosecutor Act, 2017 (Act 959).
- Office of the Special Prosecutor (Operations) Regulations, 2018 (L.I. 2374).
- Mobile Number Portability Regulations, 2011 (LI 1994).
- National Child Online Protection Framework – addresses child online safety and child sexual abuse material.
- Anti-Money Laundering Act, 2020 (Act 1044).
- Electronic Transfer Levy (E-Levy) (Repeal) Act, 2025 (Act 1128).
- National Information Technology Agency Act, 2008 (Act 771)
- National Communications Authority Act, 2008 (Act 769)
- National Identification Authority Act, 2006 (Act 707)
- Ghana Investment Promotion Centre Act, 2013 (Act 865)
- Securities Industry Act, 2016 (Act 929)
- Labour Act, 2003 (Act 651)
- Companies Act, 2019 (Act 992)

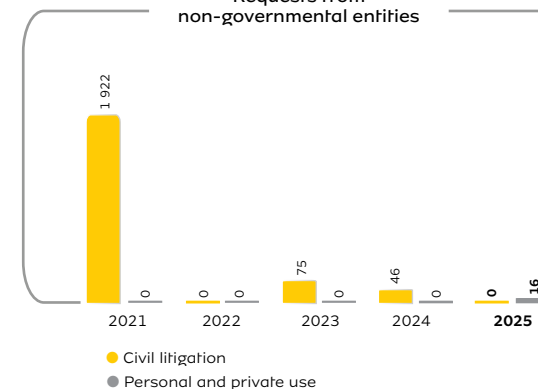
Authorities

- Bank of Ghana (BoG).
- Courts.
- Commission on Human Rights and Administrative Justice (CHRAJ).
- Cybersecurity Authority (CSA).
- Data Protection Commission (DPC).
- Ghana Investment Promotion Centre.
- Ghana Revenue Authority (GRA).
- Ghana Stock Exchange.
- Judiciary – Constitutional interpretation and enforcement of laws.
- Labour Commission.
- National Communications Authority (NCA).
- National Information Technology Authority (NITA).
- Office of the Registrar of Companies.
- Office of the Special Prosecutor.
- Securities and Exchange Commission.
- Security and intelligence agencies: Ghana Police Service, National Intelligence Bureau, National Signals Bureau and Research Department.

Requests from authorities



Requests from non-governmental entities



Markets report continued



Liberia



MTN has operated in Liberia since 2005 and serves approximately 4.7 million subscribers. In 2025, the Group generated revenue of R2 billion from its operations in the country.

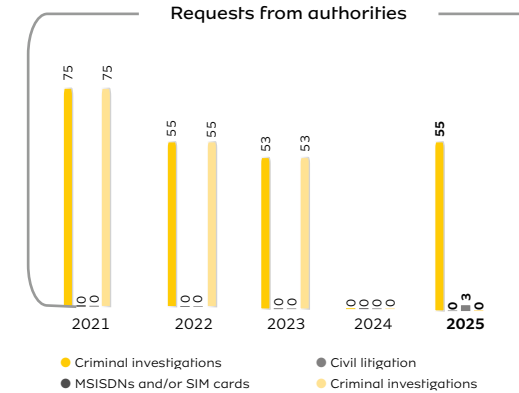
Regulatory framework

- Articles 15 and 16 of the Liberian Constitution (1986).
- Telecommunications Act of 2007.
- Supplemental Act to the Liberia Telecommunications Authority Act of 2007.
- Electronic Transactions Law (c.2002).
- Freedom of Information Act (2010).
- Personal Data Protection and Privacy Act (Draft 2024–2025).
- National ICT Policy (2019, Section 5.15.1).
- Cybercrime Act (Senate passed in November 2025).
- Penal Law of Liberia (1978, amended).
- Kamara Abdullai Kamara Press Freedom Act (2019).
- Children's Law.
- Act to Amend Sections 14, 16, 17 and 18 of the Penal Law, Title 26, Liberian Code of Laws Revised and to add thereto a new section 20.
- Central Bank of Liberia Consumer Protection Regulations (2020).
- Competition Law.
- Ministry of Commerce Regulations.
- LTA Class and Individual Licences and Regulations.
- Ministry of Posts and Telecommunications Policy Documents.
- International Covenant on Civil and Political Rights (ICCPR) – ratified by Liberia; establishes rights to privacy (Article 17) and freedom of expression (Article 19).

- Convention on the Rights of the Child (CRC) – ratified by Liberia; establishes child protection standards.
- ECOWAS Supplementary Act on Personal Data Protection.
- African Union Convention on Cybersecurity and Personal Data Protection.
- African Charter on the Rights and Welfare of the Child.
- Optional protocol to the convention on the rights of the child, on the sale of children, child prostitution and child pornography.
- African Charter on Humans and People's Rights.
- Mobile Money Regulations, 2014.
- Supplementary Act A/As. 1/01/10 on Personal Data Protection Within ECOWAS.
- Amended Subscriber Identity Module (SIM) cards/removable user identity module (RUIM) registration regulations.
- Regulations for the Treatment of Confidentiality, Dispute Resolution, Compliance and Enforcement, 2009 (LTA-REG-0002).
- Regulation C/Reg. 21/12/17 – roaming on public mobile communications network in the ECOWAS region.
- Interconnection Regulations, 2009 (LTA-REG-0003).
- LTA Order: 0018-01-15-20 – implementation of free roaming on public mobile communications networks in the ECOWAS region.
- LTA Order: 0018-03-12-20 – implementing the SIM card registration regulations.
- LTA-REG-008 – amended SIM card registration regulations.
- LTA-REG-0005 – regulations on international traffic.
- Regulation No. LTA-REG-LTA-011 – regulation on consumer protection.
- Regulation No. LTA-REG-0011 – regulation on wholesale access and value-added services.
- LTA-REG-0010 – regulation on national numbering resources

Authorities

- Courts of Liberia.
- Liberia Telecommunications Authority.
- Ministry of Justice.



Markets report continued



Nigeria



MTN has been present in Nigeria since 2001 and has approximately 87.3 million subscribers. In 2025, MTN's revenue in Nigeria was an estimated R61.7 billion.

Regulatory framework

- Section 37 of the Constitution of the Federal Republic of Nigeria, 1999.
- Section 39 of the Constitution of the Federal Republic of Nigeria, 1999.
- Nigeria Data Protection Act (NDPA), 2023.
- Nigerian Communications Act, 2003.
- Criminal Code Act.
- Defamation laws of the various states.
- Penal Code and other state penal laws.
- National Identity Management Commission Act, 2008.
- Child Rights Act, 2003.
- Child Rights Law of Lagos State, 2007.
- Federal Competition and Consumer Protection Act, 2018.
- State consumer protection laws, e.g. Lagos State Consumer Protection Law, 2024, Ogun State Consumer Protection Law
- Freedom of Information Act, 2011.
- Cybercrime (prohibition, prevention, etc.) Act, 2015 and Cybercrime (prohibition, prevention, etc.) (Amendment) Act, 2024.
- Advertising Regulatory Council of Nigeria Act, 2022.
- Terrorism (Prevention and Prohibition) Act, 2022.
- Copyrights Act, 2022.
- Violence Against Persons Act, 2015 and Violence Against Persons Laws of various states in Nigeria.
- Violence Against Persons Laws of various states in Nigeria, e.g. Lagos State Protection Against Domestic Violence Law, 2007.
- Investment and Securities Act (ISA), 2025.
- National Human Rights Commission (Amendment) Act, 2010.

Subsidiary regulations

- Nigerian Communications Commission Consumer Code of Practice Regulations, 2024.
- Nigerian Communications Commission Registration of Communications Subscribers Regulations, 2022.
- Nigerian Communications Commission (Enforcement Process, etc.) Regulations, 2019.
- Nigerian Communications Commission Lawful Interception of Communications Regulations, 2019.
- Nigerian Communications Commission Internet Code of Practice, 2026.
- Nigerian Communication Commission: Licence Framework for Value Added Services.
- Nigerian Communications Commission: Value-Added Services and Aggregator Framework, 2018 (amended).
- Nigerian Communications Commission: Guidelines on Short Code Operations in Nigeria, 2023.
- Nigerian Communications Commission: Business Rules for the Registration of Communications Subscribers Regulations, 2025.
- Federal Competition and Consumer Protection Commission: Restrictive Agreements and Trade Practices Regulations, 2022.
- Federal Competition and Consumer Protection Commission: The Abuse of Dominance Regulations, 2022.
- Federal Competition and Consumer Protection Commission: Digital, Electronic, Online, or Non-Traditional Consumer Lending Regulations.
- Advertising Regulatory Council of Nigeria: Nigerian Code of Advertising, 2023.
- Nigeria Data Protection Act General Application and Implementation Directive (GAID), 2025.
- NITDA: Code of Practice for Interactive Computer Service Platforms and Internet Intermediaries, 2022.
- Central Bank of Nigeria: Consumer Protection Regulations, 2019.
- Central Bank of Nigeria Foreign Exchange Code, 2025.
- Nigerian Communications Commission Licence Framework for International Application to Person (A2P) Messaging in Nigeria, 2025.

Policies

- Nigerian Communications Commission: Child Online Protection Policy.
- Lagos State Safeguarding and Child Protection Policy, 2016.
- National Artificial Intelligence Strategy, 2025.

Licence terms

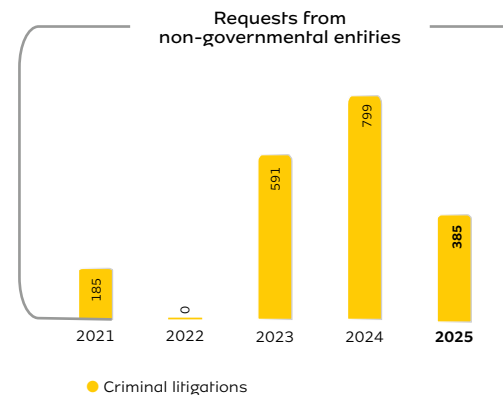
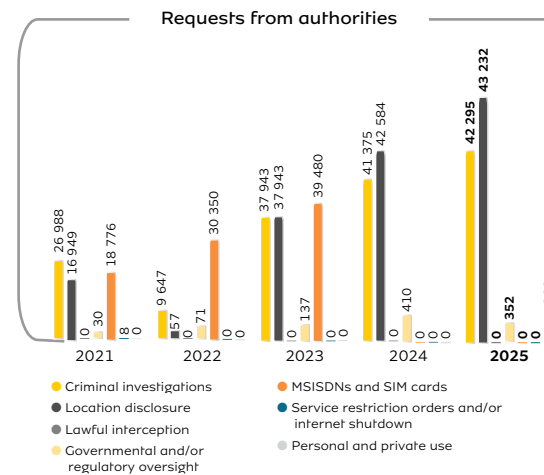
- Code 2 of the Unified Access Service Line.

Authorities

- Advertising Regulatory Council of Nigeria (ARCON).
- Attorney-General of the Federation.
- Authorised government agencies.
- Central Bank of Nigeria.
- Courts.
- Cybercrime Advisory Council: Multi-stakeholder body responsible for implementation of the Act.
- Family Courts.
- Federal Ministry of Communications, Innovation and Digital Economy (FMCIDE).
- Federal Ministry of Women Affairs.
- Federal Competition and Consumer Protection Commission (FCCPC).
- Local Government Child Rights Implementation Committees.
- Lagos State Child Rights Law Implementation Committee.
- Lagos State Domestic and Sexual Violence Response Team.
- National Identity Management Commission.
- National Information Technology Development Agency (NITDA).
- National Human Rights Commission.
- Nigerian Communications Commission (NCC).
- Nigerian Computer Emergency Response Team (ng-CERT).
- Nigerian Copyright Commission.
- Nigeria Data Protection Commission (NDPC).
- Nigeria Police Force.
- Office of the National Security Adviser (ONSA).
- Securities and Exchange Commission.
- State competition and consumer protection regulators.
- State governments.

Markets report continued

Nigeria continued



Markets report continued



Rwanda



MTN has operated in Rwanda since 1998 and serves approximately 8.2 million subscribers. In 2025, the Group generated revenue of R3.8 billion from its operations in the country.

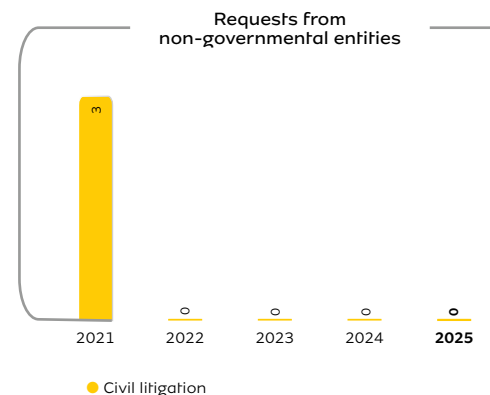
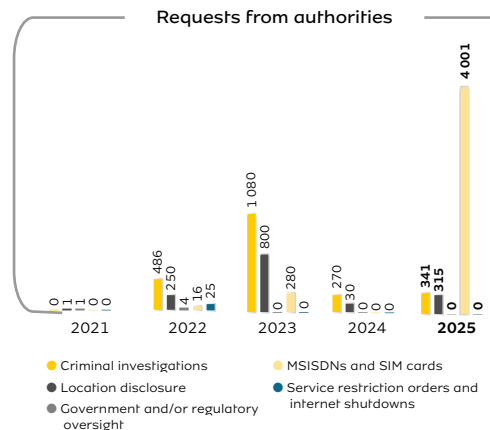
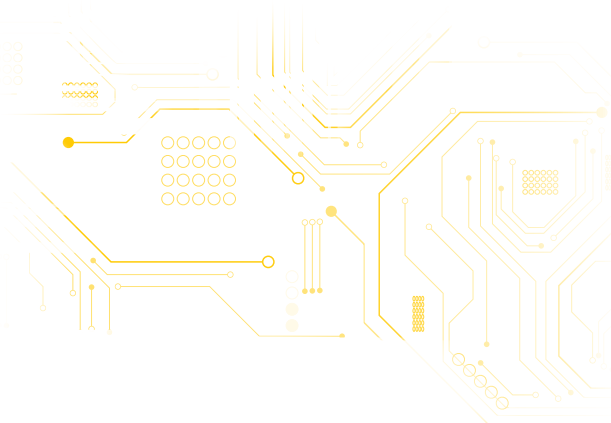
Regulatory framework

- Constitution of the Republic of Rwanda of 2003 as revised in 2015.
- Law No. 68/2018 of 30 August 2018 determining offences and penalties in general.
- Law No. 22/2009 of 12 August 2009 on media.
- Law No. 60/2018 of 22 August 2018 on prevention and punishment of cybercrimes.
- Law No. 71/2018 of 31 August 2018 relating to the protection of the child.
- Law No. 24/2016 of 18 June 2016 Governing Information and Communications Technologies (ICT Law).
- Law No. 055/2024 of 20 June 2024 on the protection of intellectual property.
- Law No. 058/2021 of 13 October 2021 relating to the protection of personal data and privacy.
- Regulation No. 010/R/CR-CSI/RURA/020 of 29 May 2020 on cybersecurity.
- Law No. 04/2013 of 8 February 2013 relating to access to information.
- Prime Minister's Order No. 028/03 of 28 June 2024 determining the regulatory authority for gaming activities.
- Law No. 66/2018 of 30 August 2018 regulating labour in Rwanda.
- Ministerial Order 03/19.19 of 27 July 2009 determining the modalities of facilitating persons with disabilities to easily access employment.

- Ministerial Instructions No. 001/MINICT/2024 of 22 March 2024 on child online protection.
- Regulation No. 18/R/SM-ICT/RURA/2024 of 9 August 2024 governing SIM card registration in Rwanda.
- Law No. 017/2021 of 3 March 2021 relating to financial services consumer protection.
- Regulation No. 50 /2022 of 2 June 2022 of National Bank of Rwanda on Cybersecurity in Regulated Institutions.
- Regulation No. 019/r/ict/rura/2024 governing mobile number portability in Rwanda.
- Regulation No. 54/2022 of 1 September 2022 governing the electronic money issuers.

Authorities

- Ministry of Culture and Sports.
- Ministry of Information Communication Technology and Innovation (MINICT).
- Ministry of Public Service and Labour.
- National Bank of Rwanda and Capital Market Authority.
- National Cyber Security Authority (NCSA).
- National Public Prosecution Authority (NPPA).
- Office of the Ombudsman.
- Rwanda Development Board (RDB).
- Rwanda Inspectorate, Competition and Consumer Protection Authority (RICA).
- Rwanda Investigation Bureau (RIB).
- Rwanda Media Council (RMC).
- Rwanda Utilities Regulatory Authority (RURA).
- The Judiciary – The Supreme Court.



Markets report continued

South Africa

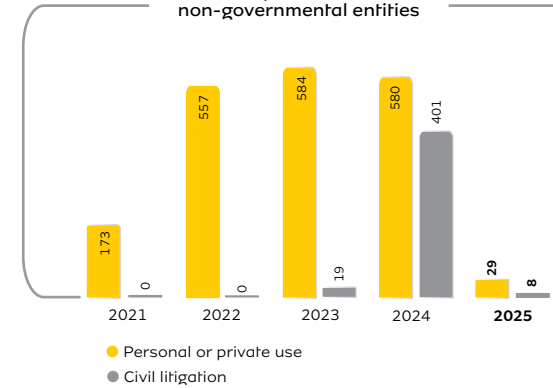


MTN has operated in South Africa since 1994 and serves approximately 40.6 million subscribers. In 2025, the Group generated revenue of R51.1 billion from its operations in the country.

Authorities

- Defence Force (the South African Defence Force).
- Department of Communications and Digital Technologies.
- Department of Justice and Constitutional Development.
- Department of Trade, Industry and Competition.
- Equality Courts (established under the Promotion of Equality and Prevention of Unfair Discrimination Act, 2000).
- Film and Publications Board.
- Independent Communications Authority of South Africa (ICASA).
- National Consumer Commission.
- Information Regulator (South Africa).
- National Consumer Tribunal.
- National Prosecuting Authority of South Africa.
- South African Human Rights Commission.
- South African Police Services.
- State Security Agency.

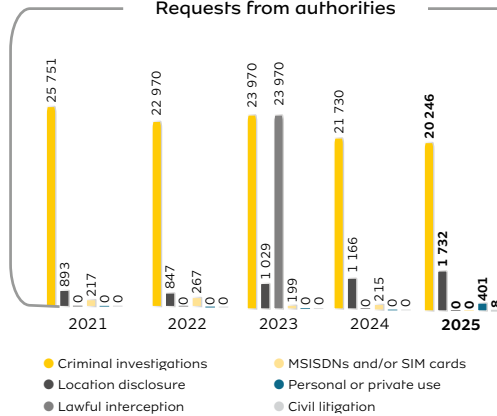
Requests from non-governmental entities



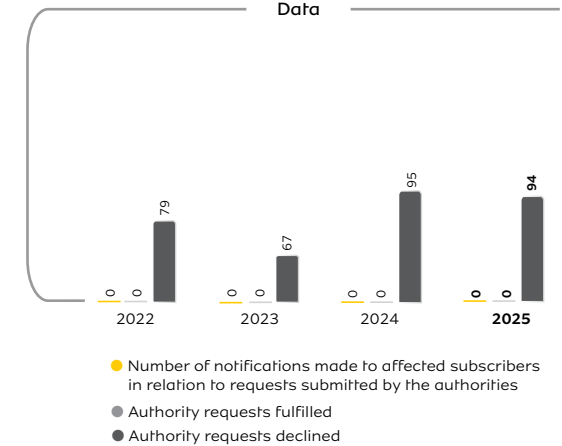
Regulatory framework

- Constitution of the Republic of South Africa, 1996.
- Promotion of Access to Information Act, 2 of 2000.
- Regulation of Interception of Communications and Provision of Communication-related Information Act, 70 of 2002.
- Certificate of Exemption in terms of section 46(3) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002.
- Electronic Communications and Transactions Act, 25 of 2002.
- Electronic Communications Act, 36 of 2005.
- Consumer Protection Act, 68 of 2008.
- Cybercrimes Act, 19 of 2020.
- Protection of Personal Information Act, 4 of 2013 (POPIA).
- Guidance Note on Direct Marketing in terms of the Protection of Personal Information Act, 2024.
- Film and Publication Amendment Act, 65 of 1996 as amended by the Films and Publications Amendment Act, 11 of 2019.

Requests from authorities



Data



Markets report continued



Sudan



MTN has operated in Sudan since 2005 and serves approximately 3.2 million subscribers. In 2025, the Group generated revenue of R2.2 billion from its operations in the country.



Regulatory framework

- Constitutional Charter for the Transitional Period 2019 (Constitutional Charter).
- Telecommunications and Post Regulation Act, 2018 (Telecommunications Act).
- General Telecommunications Regulation 2012 (General Telecommunication Regulation).
- Electronic Transactions Act, 2007.
- Combating Information Crimes Act, 2018 as amended in 2020 (Cyber Crimes Act).
- Access to Information Act, 2015 (Information Act).
- Licence Agreement between telecommunications companies and the Telecommunications and Post Regulatory Authority (Licence Agreement).
- Press and Press Printed Materials Act, 2009 (Press Act).
- Criminal Code, 1991 (Criminal Code).
- National Security Act, 2010, as amended in 2020 (National Security Act).
- Child Protection Act, 2010 (Child Act).

Authorities

- Constitutional Court.
- General Court.
- Information Crimes Court.
- Information Prosecution – Public Prosecution.
- Information Police.
- Minister of Communications and Information Technology.
- National Intelligence and Security Services (the Agency).
- Press and Press Printed Materials National Council.
- Right of Access to Information Commission.
- Telecommunications and Post Regulatory Authority.



Markets report continued



South Sudan



MTN has operated in South Sudan since 2011 and serves approximately 4.3 million subscribers. In 2025, the Group generated revenue of R2.8 billion from its operations in the country.

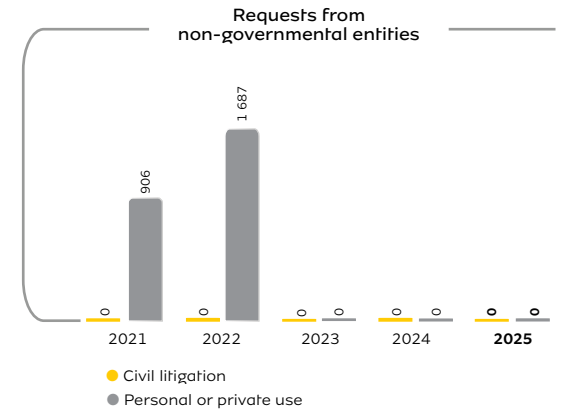
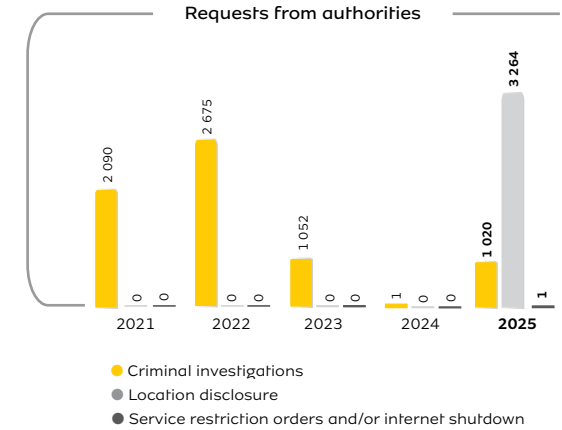


Regulatory framework

- Transitional Constitution of the Republic of South Sudan, 2011.
- Right of Access to Information Act, 2013.
- National Communication Act, 2012.
- Penal Code, 2008.
- National Communications Frequency Regulation, 2016.
- National Communications Tariffs Regulation, 2016.
- National Communications Dispute Resolution Regulation, 2016.
- National Communications Standards, Specifications and Type Approval Regulation, 2016.
- National Communications Inspection, Monitoring and Enforcement Regulation, 2016.
- National Communications Numbering Regulation, 2016.
- National Communications Competition Regulation, 2016.
- National Communications Licensing Regulation, 2016.
- National Security Service Act, 2014.
- Electronic Money Regulations of South Sudan, 2017.
- Anti-Money Laundering and Counter-Terrorist Financing Act, 2012.
- Cybercrimes and Computer Misuse Provisional Order, 2021 (passed on 25 November 2025).
- Child Act, 2008.

Authorities

- Bank of South Sudan.
- Financial Intelligence Unit.
- High Court.
- Independent Child Commission.
- Ministry of Information, Communication Technology and Postal Services.
- National Communications Authority (NCA) of South Sudan.
- Republic of South Sudan Information Commission.
- Specialised Prosecution Unit (Ministry of Justice).
- Supreme Court.



Markets report continued



Uganda



MTN has operated in Uganda since 1998 and serves approximately 24.2 million subscribers. In 2025, the Group generated revenue of R17.9 billion from its operations in the country.

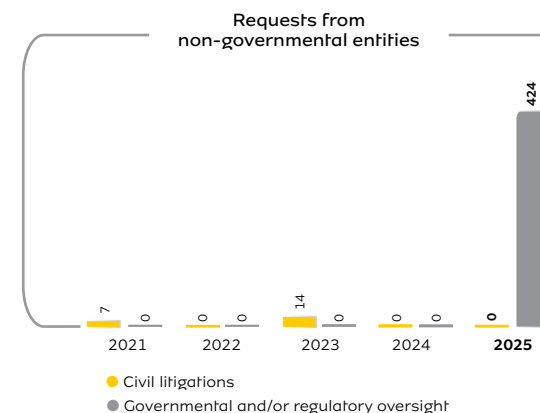
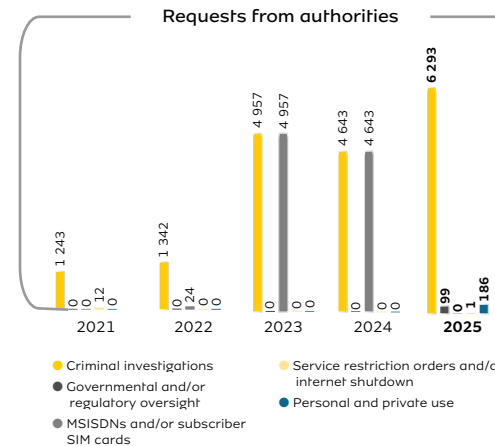


Regulatory framework

- Articles 27(2) and 29 of the Constitution of the Republic of Uganda, 1995.
- Uganda Communications Act, Cap. 103.
- National Payment Systems Act, Cap. 59.
- Anti-Money Laundering Act, Cap. 118.
- Regulation of Interception of Communications Act, Cap. 101.
- Data Protection and Privacy Act, Cap. 97.
- Computer Misuse Act, Cap. 96.
- Electronic Transactions Act, Cap. 99.
- Anti-Pornography Act, Cap. 119.
- Anti-Terrorism Act, Cap. 120.
- Electronic Signatures Act, Cap. 98.
- Anti-Homosexuality Act, Cap. 117.
- Data Protection and Privacy Regulations, 2021.
- Uganda Communications (Intelligent Network Monitoring System) Regulations, 2019.
- Uganda Communications (Centralised Equipment Identification Register) Regulations, 2019.
- Uganda Communications (Text and Multimedia Messaging) Regulations, 2019.
- Uganda Communications (Consumer Protection) Regulations, 2019.
- Uganda Communications (Content) Regulations, 2019.
- Uganda Communications (Emergency Response) Regulations, 2019.
- Uganda Communications (Computer Emergency Response Team) Regulations, 2019.
- Regulation of Interception of Communications Regulations, 2023.
- National Environment (Audit) Regulations, 2020.

Authorities

- Bank of Uganda.
- Courts of law.
- Directorate of Public Prosecutions.
- External Security Organisation.
- Financial Intelligence Authority.
- Internal Security Organisation.
- Ministry of Internal Affairs.
- Ministry of Information and Communications Technology and National Guidance.
- Ministry of Justice and Constitutional Affairs.
- National Environment Management Authority.
- National Information Technology Authority.
- Personal Data Protection Office.
- Uganda Communications Commission.
- Uganda People's Defence Force.
- Uganda Police Force.



Markets report continued



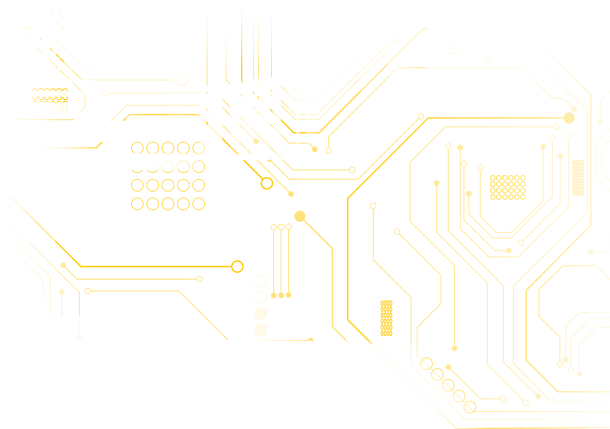
Zambia



MTN has operated in Zambia since 1995 and serves approximately 7.1 million subscribers. In 2025, the Group generated revenue of R3.6 billion from its operations in the country.

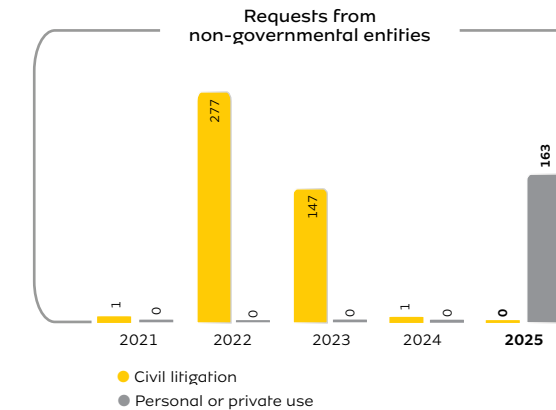
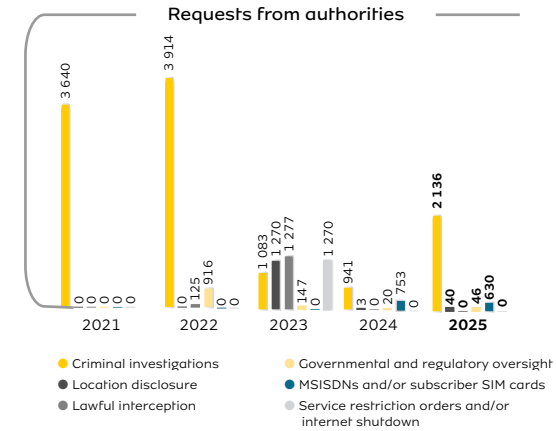
Authorities

- Anti-Corruption Commission established under the Anti Corruption Act No. 3, 2012.
- Anti-Money Laundering Investigations Unit, established under the Prohibition and Prevention of Money Laundering Act No. 14, 2001.
- Child Development Department, which operates under the provisions of the Children's Code.
- Drug Enforcement Commission.
- Financial Intelligence Centre, established under the Financial Intelligence Centre Act.
- Human Rights Commission.
- Office of the Data Protection Commissioner, established under the Data Protection Act.
- Public Protector established under the Constitution.
- Zambia Cyber Security Agency, established under the Cyber Security No. 3, 2025. Zambia Information and Communication Technology Agency established under the Information and Communication technologies Act No. 15, 2009.
- Zambia Police Service established under the Constitution.
- Zambia Revenue Authority, established under the Zambia Revenue Authority Act, Chapter 321 of the Laws of Zambia.
- Zambia Security Intelligence Service established under the Zambia Security Intelligence Service Act, Chapter 109 of the Laws of Zambia.



Regulatory framework

- Constitution of Zambia (Amendment) Act No. 2, 2016.
- Electronic Communications and Transactions Act No. 4, 2021.
- Data Protection Act No. 3, 2021.
- Financial Intelligence Centre Act No. 46, 2010, as amended by Act No. 4 of 2016 and Act No. 16, 2020 (Financial Intelligence Centre Act).
- Zambia Information and Communication Technology Authority Network Licence Standard Terms and Conditions.
- Children's Code Act No. 12, 2022 (Children's Code).
- Electronic Communications and Transactions (General) Regulations, Statutory Instrument No. 71, 2011 issued pursuant to the Electronic Communications and Transactions Act No. 21, 2009.
- Access to Information Act No. 24, 2023 (Access to Information Act) Statutory Instrument No. 80, 2015.
- Information and Communication Technologies (Telecommunication Traffic Monitoring) Regulations issued pursuant to the Electronic Communications and Transactions Act No. 21, 2009.
- Cyber Security Act No. 3, 2025.
- Cyber Crimes Act No. 4, 2025.
- Penal Code, Chapter 87 of the Laws of Zambia.



Looking forward

As we look ahead to 2026, MTN is guided by our purpose in leading digital solutions for Africa's progress.

Connectivity across Africa continues to expand rapidly, with more people relying on digital networks to communicate, learn, work, trade and participate in public life. As digital infrastructure becomes increasingly embedded in economic and social systems, the responsibility of telecommunications providers to respect and protect digital human rights becomes ever more important.

Operating across diverse markets requires navigating an environment shaped by geopolitical shifts, economic pressures and rapid technological change. In this context, trust in digital infrastructure has become a strategic asset. Guided by the United Nations Guiding Principles on Business and Human Rights, MTN will continue embedding respect for human rights into our governance, policies and operational decision making. Our digital human rights due diligence processes will remain central to identifying and mitigating risks associated with connectivity, privacy, data protection and online safety.

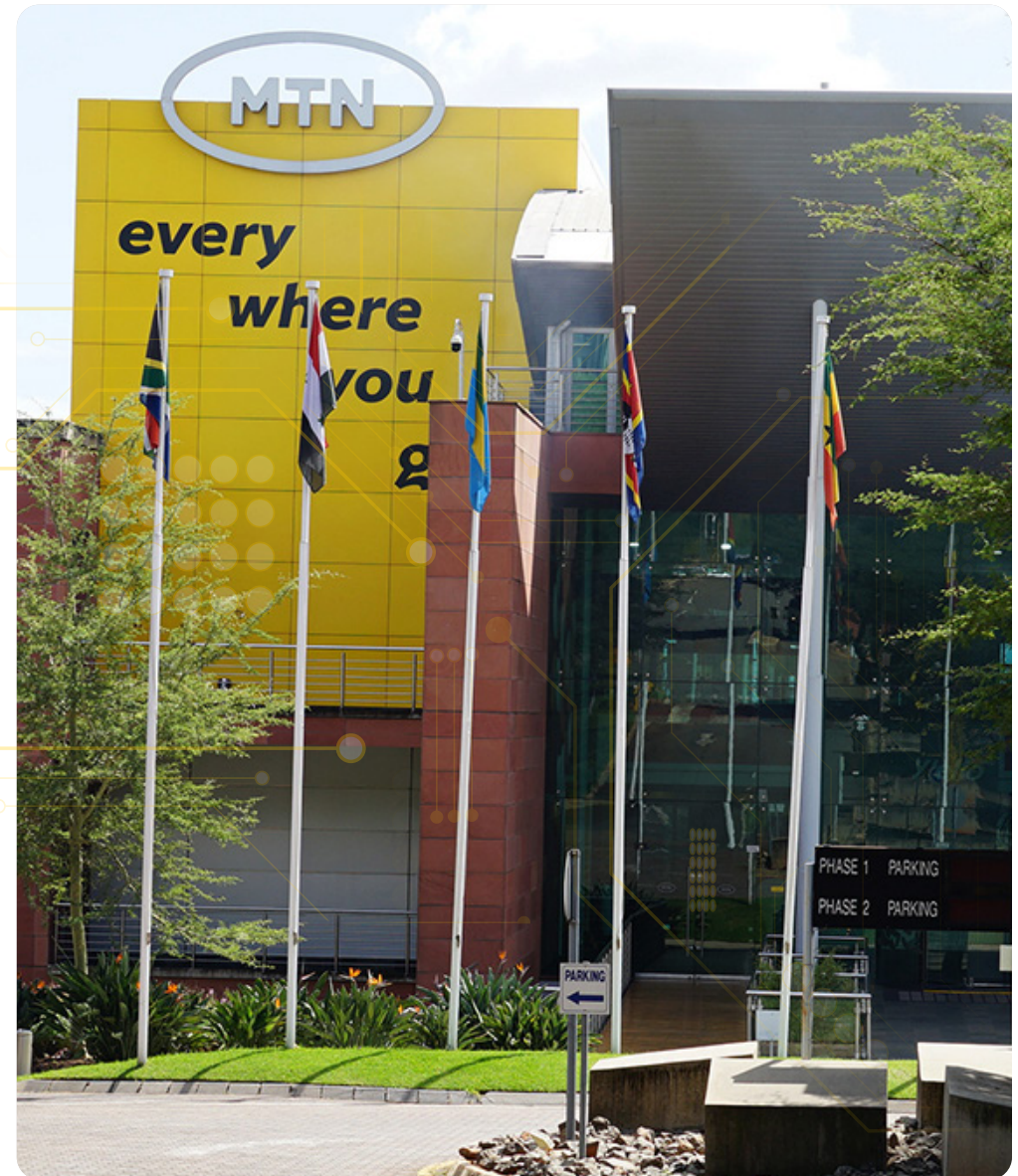
Technological innovation, particularly in areas such as AI and data-driven systems, is transforming the digital landscape. While these developments present significant opportunities for innovation and economic participation, they also raise important questions relating to privacy, surveillance and the responsible use of personal data. MTN will continue strengthening governance frameworks to ensure that emerging technologies are adopted responsibly and with appropriate safeguards for human rights.

At the same time, political transitions, regulatory developments and social tensions in many markets continue to shape the operating environment for telecommunications providers. These dynamics may increase the likelihood of government requests to restrict or suspend services, which can have implications for rights such as freedom of expression and access to information. MTN will continue approaching such requests with careful scrutiny, guided by our Digital Human Rights Policy and our commitment to transparency and accountability.



Glossary

Acronym	Definition
AI	Artificial intelligence
CEO	Chief Executive Officer
CSAM	Child sexual abuse material
ERM	Enterprise risk management
ESG	Environmental, social and governance
GHG	Greenhouse gas
GNI	Global Network Initiative
GSMA	Global System for Mobile Communications Association
ICT	Information and Communication Technology
ISSB	International Sustainability Standards Board
IWF	Internet Watch Foundation
MENA	Middle East and North Africa
MSISDN	Mobile Station International Subscriber Directory Number
SDGs	Sustainable Development Goals
SEA	Southern and East Africa
SESCO	Social, Ethics and Sustainability Committee
SIM	Subscriber Identification Module
UN	United Nations
UNGC	United Nations Global Compact
WECA	West and Central Africa



Administration

MTN Group Limited

Incorporated in the Republic of South Africa

Company registration number:

1994/009584/06
ISIN: ZAE000042164
Share code: MTN

Board of Directors

MH Jonas
 KDK Mokhele
 HL Bosman
 NP Gosa
 SAX Gwala
 SN Mabaso-Koyana
 SP Miller¹
 CWN Molope
 N Newton-King
 T Pennington²
 VM Rague³
 GJ Rasehamba
 SLA Sanusi⁴
 IS Sehoole
 NL Sowazi
 S Richard⁵
 S Yeboah-Amankwah⁶
 RT Mupita⁷
 TBL Molefe⁷

¹ Belgian
² British
³ Kenyan
⁴ Nigerian
⁵ French
⁶ Ghanaian
⁷ Executive director

Acting Group Company Secretary

MML Mokoka
 Private Bag X9955, Cresta, 2118

Registered office

216 – 14th Avenue
 Fairland
 Gauteng, 2195

American depository receipt (ADR) programme

A sponsored ADR facility is in place
 Cusip No. 62474M108
 ADR to ordinary share 1:1

Depository:

The Bank of New York Mellon
 101 Barclay Street, New York NY, 10286, USA

MTN Group sharecare line

Toll free: 0800 202 360 or +27 11 870 8206
 if phoning from outside South Africa

Transfer secretaries

Computershare Investor Services
 Proprietary Limited
 Registration number 2004/003647/07
 Rosebank Towers, 15 Biermann Avenue
 Rosebank, 2196
 PO Box 61051, Marshalltown, 2107

Auditor

Ernst & Young Inc.
 102 Rivonia Road, Sandton, Johannesburg,
 South Africa, 2196

Lead sponsor

Tamela Holdings Proprietary Limited
 First Floor, Golden Oak House,
 35 Ballyclare Drive, Bryanston, 2021

Joint sponsor

J.P. Morgan Equities (SA) Proprietary Limited
 1 Fricker Road, cnr Hurlingham Road,
 Illovo, 2196

Attorneys

Webber Wentzel
 90 Rivonia Road, Sandton, 2196
 PO Box 61771, Marshalltown, 2107

Contact details

Telephone: International +27 11 912 3000
 Facsimile: National 011 912 4093
 International +27 11 912 4093

Email: sustainability@mtn.com

Website: <http://www.mtn.com>

Date of release: 29 April 2026

Forward looking information

Any forward looking financial information disclosed in this report is the responsibility of the directors and has not been reviewed or audited or otherwise reported on by our external auditor. Opinions and forward looking statements expressed in this report represent those of the company at the time. Undue reliance should not be placed on such statements and opinions because by nature, they are subjective to known and unknown risk and uncertainties and can be affected by other factors that could cause actual results and company plans and objectives to differ materially from those expressed or implied in the forward looking statements.

Neither the company nor any of its respective affiliates, advisers or representatives shall have any liability whatsoever (based on negligence or otherwise) for any loss howsoever arising from any use of this report or its contents or otherwise arising in connection with this presentation and do not undertake to publicly update or revise any of its opinions or forward looking statements whether to reflect new information or future events or circumstances otherwise.

Our reporting suite reports with reference to the following standards and frameworks

The Integrated Reporting Framework	IR	AFS
Companies Act, No 71 of 2008 (as amended)	IR	AFS SR KIV
JSE Listings Requirements	IR	AFS SR KIV
FTSE/JSE Responsible Investment Index	IR	SR KIV TR CDP
King IV™^ Principles	IR	AFS SR KIV TR
International Financial Reporting Standards (IFRS)	IR	AFS
UN GRI	IR	SR
JSE Sustainability Disclosure Guidance	IR	SR
Global System for Mobile Communications Association (GSMA) ESG Metrics	SR	TR
Sustainability Accounting Standards Board (SASB) Telecommunication Services industry	IR	SR
SDGs	IR	SR
UN Global Compact (UNGC)	SR	TR
UN Guiding Principles on Business and Human Rights	SR	TR
CDP	SR	CDP
IFRS Sustainability Disclosure Standards (IFRS S1 and S2)	IR	SR
IFRS S2 Climate-related Disclosures	SR	CDP CR

^ Copyright and trademarks are owned by the Institute of Directors South Africa NPC and all of its rights are reserved.





www.mfn.com

Tel: +27 11 912 3000
Innovation Centre
216 14th Avenue
Fairland, 2195
South Africa