Doing for tomorrow, today

MTN Group Limited

Transparency Report for the year ended 31 December 2022

Inside this report

Welcome
to our Transparency Report 2022

About this report

Introduction

04

Technology and human rights

Technology has evolved into a vital enabler of human rights

Treating customers fairly

MTN seeks to take every necessary measure to ensure customer satisfaction

Governance: Rights and incident management

Impact management

Responsible advocacy

Disclosure and performance management

20

Managing impact on children

We at MTN believe we have a critical role in ensuring every African child is kept safe online

Markets report

Our purpose is to enable the benefits of a modern connected life for everyone

Navigating this report: The following icons are used throughout our Integrated Report to show the connectivity between our ***Ambition 2025*** strategic priorities, our capitals, material matters and value creation for our stakeholders.

2025 strategic priorities:

- Build the **largest and most valuable platforms**
- Drive **industry-leading** connectivity operations
- Create **shared value**
- Accelerate portfolio **transformation**

Environmental, social and governance (ESG) remains **at the core** of our strategy. This aligns with our work to advance the United Nations **Sustainable Development Goals** (SDG) through our business activities and our support of governments, communities and customers. The SDGs target a sustainable society with a plan to end poverty, protect the planet and ensure equality for all by 2030. We are committed to bridging the digital divide and furthering financial inclusion to advance the attainment of the goals. **For details on how we determine the SDGs on which we have the greatest impact, see page 64**.

MTN focus SDGs

SDGs on which we have an indirect impact

Our material stakeholders:

- Government and regulators
- Civil society
- Investment community
- Subscribers/ customers
- MTNers

Our capitals:

- Natural
- Financial
- Intellectual
- Human
- Manufactured
- Social

Other icons:

- LA — Limited assurance obtained
- www.mtn.com

Material matters:

- MM1 Geopolitical and macroeconomic conditions
- MM2 Regulatory environment
- MM3 Network and platform performance
- MM4 Greater focus on ESG
- MM5 Cybersecurity and digital safety
- MM6 Financial resilience
- MM7 Future-fit skills and culture
- MM8 De-layering of the telecoms business model

Our reporting suite

These reports are available online at www.mtn.com or on request from investor.relations@mtn.com, where we also welcome feedback from readers on our reports.

IR — Integrated Report
Our primary communication to stakeholders, aiming to enable them to make an informed assessment of our performance and prospects, and the value we create through our activities.

AFS — Annual Financial Statements
Detailed statements, analysis of the Group's financial results and the full Audit Committee report.

5Y — Five-Year Review
Comprehensive view over five years of the income statement; statements of financial position and cash flows; performance per share; as well as key non-financial information.

TAX — Tax Report
MTN's approach to tax and dealing with uncertain tax positions; views on specific tax risks; and our total tax contribution.

KIV — King IV™ Report
MTN's application of the King IV™ principles.

SR — Sustainability Report
Detailed reporting on how MTN is creating value for stakeholders and driving responsible environmental, social and governance practices.

TR — Transparency Report
Insight on how the policies and actions of governments and corporations affect privacy, security and access to information.

GRI — GRI Report
Structured disclosure on the impacts of the Group's activities using the GRI standards.

CDP — CDP Report
Global environmental disclosure, reporting on risks and opportunities in climate change, water security and broader environmental management.

About this report

The purpose of this report is to provide insight into MTN's approach to digital human rights strategy and practice.

MTN is committed to protecting and respecting human rights, especially those that pertain to digital rights. Through its networks, products and services, MTN facilitates digital communications and enhances the lives of the society in which it operates. As a company, we believe all people should be able to communicate freely, access and exchange information responsibly, and enjoy privacy and security when using digital communication and data. The publication of this report represents our commitment to uphold digital human rights and promote transparency and accountability.

Basis for preparation

Our geographical footprint spans across 18 markets on two continents; therefore, robust operational oversight is critical. Data collected for this report is derived from two overarching methods. The first is a questionnaire in which the operating markets were requested to provide information about the countries in which they operate. The participating operational markets used internal records, regulatory documents and government regulatory sources to complete the questionnaires for the report. The MTN markets provided comprehensive information on market-specific laws, regulators and requests made by competent authorities and private parties. This information was verified by Group legal and external legal counsel in each country and lastly by external legal counsel in South Africa. The second process is qualitative and involves interviews with senior staff members, transcribing the interviews and conducting a thematic analysis of the data and policies related to digital human rights.

Feedback

We welcome feedback on this report and are committed to listening to our stakeholders about our sustainability and human rights efforts. Please address all feedback to Group Sustainability: humanrights@mtn.com.

Scope and boundaries

Timeframe

This report covers the reporting period commencing 1 January and ending 31 December 2022. Where possible, data for the previous two financial years has been included.

Markets covered

This report covers our 'operating markets' in 16 countries:

- Benin, Cameroon, Congo-Brazzaville, Côte d'Ivoire, eSwatini, Ghana, Guinea-Bissau, Guinea-Conakry, Liberia, Nigeria, Rwanda, South Africa, South Sudan, Sudan, Uganda and Zambia.
- MTN Afghanistan was excluded from this report owing to MTN's ongoing, phased exit from the country and Middle East. As part of our mindful approach to exiting Afghanistan, we conducted an exit impact assessment and provided recommendations, which we then handed to the purchasing company. To upskill them, we conducted training on human rights and provided our human rights strategy, policy, digital human rights playbook and impact assessment tools. We offered our support to their human rights team for the first six months, during which the purchasing company could seek our advice on strategic and technical issues related to human rights.
- Irancell and Mascom are excluded as MTN Group has indirect minority shareholding and no management control.

Owing to legislative constraints in certain countries, some markets are prohibited from providing specific information to the public. This material has not been included in this report in compliance with the local laws. In addition, there are situations and markets that experienced technical difficulties with retrieving some of the data.

Who we are and where we are going

Our purpose is to enable the benefits of a modern connected life for everyone

MTN is a pan-African mobile operator. Our purpose is embodied in our belief statement that *everyone deserves the benefits of a modern connected life*. Our strategic intent is leading digital solutions for Africa's progress. We provide a diverse range of voice, data, fintech, digital, enterprise, wholesale, and API services to more than 289 million customers in 19 markets.

We were established in South Africa at the dawn of democracy in 1994 as a leader in transformation. Since then, we have grown by investing in sophisticated communication infrastructure, developing new technologies and by harnessing the talent of our diverse people to now offer services to communities across Africa and in the Middle East.

MTN Group Limited is a publicly owned entity whose shares are traded on the JSE. At the end of 2022 our market capitalisation was approximately R240 billion (US$14 billion).

How we define value: For us, value is progress in achieving our strategic intent and delivering on our belief that everyone deserves the benefits of a modern connected life in our footprint.

Guided by our

Strategic intent

Ambition 2025

'Leading digital solutions for Africa's progress'

And delivering on our

2025
Strategic priorities

- Build the largest and most valuable platforms
- Drive industry-leading connectivity operations
- Create shared value
- Accelerate portfolio transformation

We are creating the MTN of tomorrow

enabled by our values:

Lead with Care
Can-do with Integrity
Collaborate with Agility
Serve with Respect
Act with Inclusion

With ESG at the core

Creating value for all

289m subscribers	**137m** active data users	Africa's largest fixed and mobile network: invested capex of **R38.2bn**	
69m active MoMo users	**22m** active ayoba users	Economic value of **~R149bn** added across our markets	Broadband coverage **~88%** (targeting 95% by 2025)
R196bn in service revenue	**17 462** skilled MTNers	Reduction of **~13.9%^** in GHG emissions (targeting 50% reduction by 2030 and Net Zero emissions by 2040)	Women are **40%** of our workforce (targeting 50% by 2030)

Doing for tomorrow, *today.*

^Excluding South Africa which was impacted by loadshedding.

Our operating context

We operate in a rapidly changing environment; we strive to understand everything, from our customer profiles and stakeholder concerns of how people use and interact with communications technology, to the regulatory frameworks that govern the use of communications infrastructure in each of our multiple operating countries.

According to Statista, the number of mobile internet users globally amounts to an estimated 4.7 million and is projected to reach 5.5 billion users by 2025. This translates to 58% of the world's population. According to Global System for Mobile Communications Association (GSMA), 40% of the adult population in sub-Saharan Africa are currently connected to mobile internet services. Nonetheless, an additional 44% of residents in areas served by mobile broadband networks do not use mobile internet services (the usage gap).

MTN is Africa's largest mobile network operator. MTN provides voice, data, Fintech, digital, enterprise, wholesale and API services to more than 289 million customers in 18 markets.

Despite this, there are still large numbers of people who do not have access to the internet. It is this digital divide that MTN aims to address. To fulfil the promise of mobile connectivity to drive economic growth and development in a post-pandemic world, MTN collaborates with its stakeholders to prioritise addressing the primary barriers to mobile internet adoption for these individuals, including affordability and digital skills.

We operate in different countries in Africa, which have differing regulatory frameworks, which present opportunities and challenges. Our operating markets are unique and require unique approaches and solutions.

Technology has evolved into a vital enabler of human rights at individual, national and global levels. MTN is committed to leveraging this power of technology to promote and protect human rights. As communications technology has become more enmeshed with daily life, we have witnessed the significant disruptions when communications are interrupted. For this reason, it is essential that MTN remains a market leader in Africa and continues to provide its customers with sustainable mobile services. In this manner, MTN continues to contribute to the United Nations Sustainable Development Goals (UNSDG).

Digital human rights in our operating environments

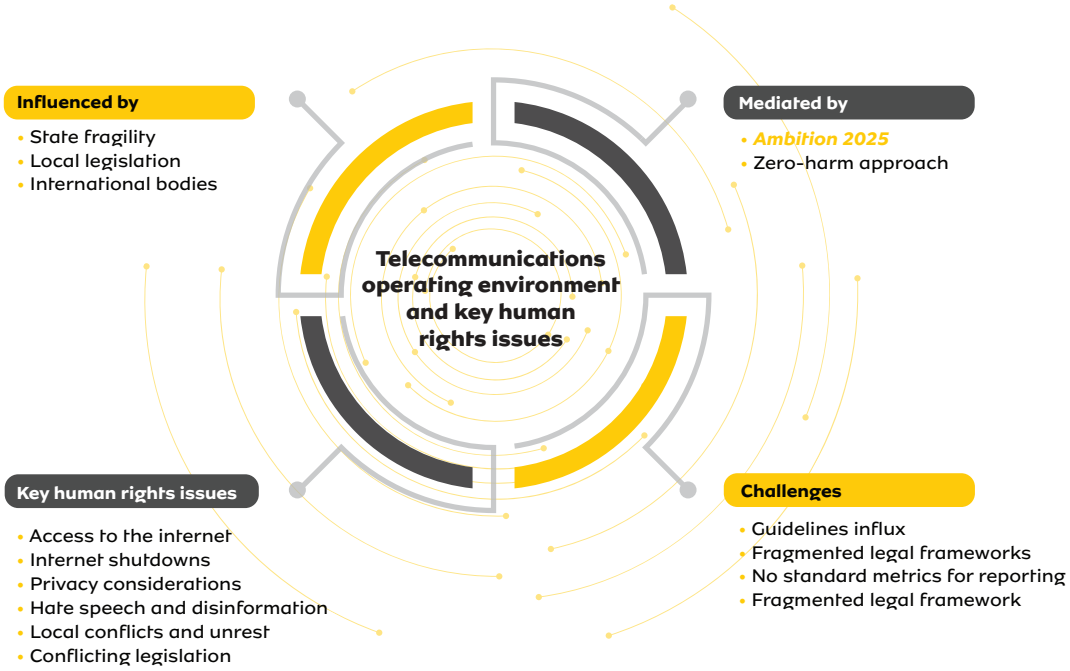
MTN's *Ambition 2025* strategy is 'Leading digital solutions for Africa's progress.' As one of the leading telecommunications companies in Africa, we have unique opportunities to operate in the continent thanks to our extensive experience and infrastructure in the region. With a presence in 18 countries across Africa and the Middle East, we have built a strong brand and reputation in the region, which provides a platform for growth and expansion. Africa's vast and largely untapped market presents significant opportunities for MTN to provide essential communication services to millions of people, including those in rural and remote areas. Additionally, with the increasing adoption of smartphones and digital services in Africa, we are well-positioned to offer innovative solutions and products that can drive economic growth and improve people's lives. With a focus on investing in local communities and working closely with governments, we can continue to be a positive force for development and progress in the region.

However, there are risks associated with doing business in these markets which are not unique to MTN. The way we do business and the framework we use are constantly evolving and being innovated to address these risks. Our teams also share lessons between markets continuously.

The challenge of restricting internet access in countries with many internet service providers is much greater than in countries with fewer providers. MTN is the only communication platform available in a number of countries. Therefore, withdrawing from such countries would violate the human rights of our users because they would be denied their right to communicate digitally.

To ensure they have access to digital solutions and are not digitally excluded, we are willing to navigate these complex situations with them.

Recognising the connection between internet connectivity and country development as a pan-African company, we are committed to playing a role in reducing the digital divide and contributing to the realisation of the goals of digital access for all. We always aim for zero harm in our approach.



Source: GSMA: An introduction to human rights for the mobile sector and MTN's DHRIA 2022.

Digital human rights in our operating environments continued

Salient human rights issues

The most salient human rights issues are those that are at risk of severe negative impact through business activities or business relationships. MTN focuses on these crucial human rights issues in its operations. We prioritise addressing the most severe risks, based on how they could affect people rather than just the risk to our business. This ensures we operate responsibly with respect to human rights.

Government requests for customer data, including direct access

According to the GNI, governments' strategies and capabilities for gaining access to data – including voice and data communications – have evolved over time. Regulatory and technical arrangements that enable government authorities to access data streams directly– without requesting access from or even notifying the service providers that collect and/or transmit the data as part of their services – are a particularly prevalent trend.

Government service restriction orders (SRO), including blocking, filtering and throttling

Blocking or geo-blocking is utilised by online media companies, streaming services and subscription plans to comply with licensing agreements between media properties, certain countries' regulatory systems, or other agreements and regulations. Geo-blocking is also used to restrict access to websites that promote activities deemed illegal in certain nations (like online gambling). Some internet service providers may use geo-blocking to throttle your internet connection. Filtering is also a technology used to stop users from viewing certain URLs or websites by preventing their browsers from loading pages from these sites.

Access to the internet

The internet is a catalyst for the enjoyment of human rights. It is essential for gaining access to educational and economic opportunities and achieving other development objectives. This is why the UN Human Rights Council, passed a resolution in 2016 declaring access to the internet, a human right, and imploring states to refrain from infringing on this right.

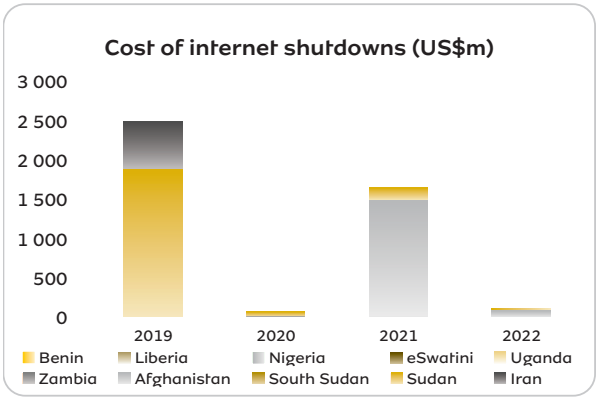
Access to the internet directly bolsters the right to free speech and expression. Indirectly, it supports several additional human rights, including political rights associated with freedom of assembly, the right to non-discrimination and the right to participate in political processes. Internet access can positively affect human development-related rights such as the right to education and health.

Internet shutdowns

Increasing internet shutdowns have been widely condemned as a violation of human rights. While a variety of justifications are provided for the need to restrict internet access, the timing of these restrictions, which frequently coincide with periods of social unrest and elections, has created suspicion regarding the offered justifications and the role of service providers in such restrictions.

In addition, an increasing number of societal actors are speaking out about human rights issues, including digital human rights, resulting in a rise in demonstrations led primarily by Africa's large youth population. State security forces frequently struggle to contain these protests, particularly as they become more widespread. They resort to social media and internet shutdowns regularly to prevent potential violence and public disorder.

Shutdowns in locations where MTN operates account for just under 20% of the costs related to internet shutdowns on average according to *Top 10 VPN The Global Cost of Internet Shutdowns (top10vpn.com)*. It is largely owing to shutdowns in Sudan in 2019 and Nigeria in 2021. These shutdowns are also associated with human rights violations, restrictions on freedom of assembly, election interference and freedom of the press.



Source: Top 10 VPN The Global Cost of Internet Shutdowns (top10vpn.com).

Digital human rights in our operating environments continued

Salient human rights issues continued

Product and business model development, which may include bias in data analytics, monetising data or facilitating hate speech and disinformation.

In recent years, we have noted that as the internet and social media platforms gain prominence as sources of information, so increases the dangers of misinformation and disinformation. We have seen the impact of this in terms of misleading information about COVID-19 vaccines and election results. Therefore, digital literacy and understanding of algorithms become critical in protecting individuals and communities. In the process of expanding our business model and our reach in Africa, we are critically aware of our impact on society and we remain steadfast in our aim of creating zero harm.

Data governance

According to TechTarget, data governance is the process of managing the availability, usability, integrity and security of data in enterprise systems in accordance with internal data standards and policies that govern data usage. Effective data governance ensures data is consistent, dependable and not misappropriated. MTN faces new data privacy regulations and relies more and more on data analytics to optimise operations and drive business decisions and this is becoming increasingly important.

In response to business and individual concerns about data privacy, governments and regulators in several regions have issued new data privacy regulations with which companies must comply. Transparency regarding how companies collect, utilise and share personal data is now a crucial aspect of any customer-business relationship.

Child online protection

Children are vulnerable and need responsible adults and organisations to help keep them safe. According to the Organisation for Economic Co-operation and Development, children today spend an increasing part of their lives online. Since 2011, the number of 12- to 15-year olds who own smartphones has increased by more than 50%.

The digital environment offers tremendous benefits to children, opening new channels for education, creativity and social interaction. But it also presents serious risks, including cyberbullying, sextortion and risks to privacy. These risks have become particularly acute amid the COVID-19 crisis and the surge in screen time has precipitated.

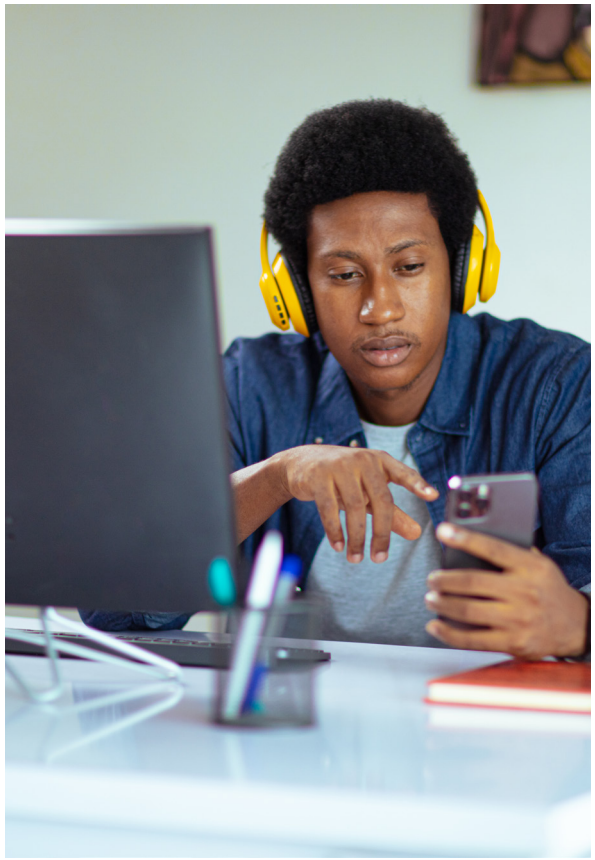
Digital human rights in our operating environments continued

TRADE-OFFS TO BE MANAGED IN PROTECTING DIGITAL HUMAN RIGHTS

The protection of human rights often requires balancing competing rights. Our commitment to protecting the most salient of these rights often requires us to make trade-offs. Below are some of the trade-offs we have to consider.

	Gains	Trade-offs	Mitigations
Operating in challenging markets	Inherently more potential. Fewer providers mean less competition thus more growth potential. Digital access has higher relative impact on people.	Heightened scrutiny of potential interference from host nations and other stakeholders.	We operate in various markets and, as such, have access to a broad array of experiences and management strategies to mitigate risks in this regard.
The need for data versus the cost of protecting data	Access to customer data enhances service provision and segmentation. Data is becoming an increasingly valuable asset.	Data safety becomes a big responsibility. Valuable data increases unlawful access attempts. Securing user data becoming expensive. Legislation can hinder moving data to safer locations.	Our policy for data protection, in line with best practices, sets a minimum standard with which all our operations must comply to provide our customers with the most effective products and services. We do collect personal information which is utilised as; explained in our human rights-related policies and processes.
Protection of the individual privacy versus protection of everybody's safety	Legitimate reasons for government to be able to access data relating to citizens. Mostly related to national security considerations. Enhanced corporate citizenship if managed correctly.	People view government requests for information as an invasion of privacy. Reasons for access often motivated by national security reasons.	Striking a balance between security and privacy is extremely difficult, and the country and context of a request are significant. MTN does as much due diligence as is possible in these cases.
Protection of freedom of expression versus preventing harm caused by online abuse, and discrimination	Freedom of expression is a fundamental right that is a hallmark of democratic countries.	Individuals' rights may be considered to be infringed such as privacy, dignity and non-discrimination.	Our principles and values as a company guide us in where to draw lines of principle in limiting individuals' rights as we seek to ensure everyone remains protected from genuine threats from abuse of internet platforms.

Modified view from MTN Transparency Report 2021



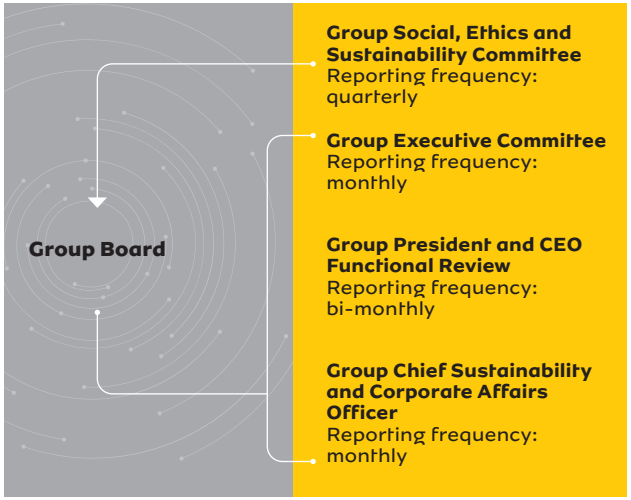
Governance: rights and incident management

Governance and decision framework

Governance at MTN is structured in line with best practices. In 2021, we revised the operational governance framework and structure to better align with *Ambition 2025*.

The Group Social, Ethics and Sustainability Committee, oversees the governance of sustainability including digital human rights on behalf of the MTN Group Board. It is also tracked on an ongoing basis by the Group Executive Committee led by the MTN Group President and Chief Executive Officer (CEO) (see our sustainability governance structure below). Regional vice-presidents and country CEOs play a vital role at regional and country levels.

Our sustainability governance and reporting structure

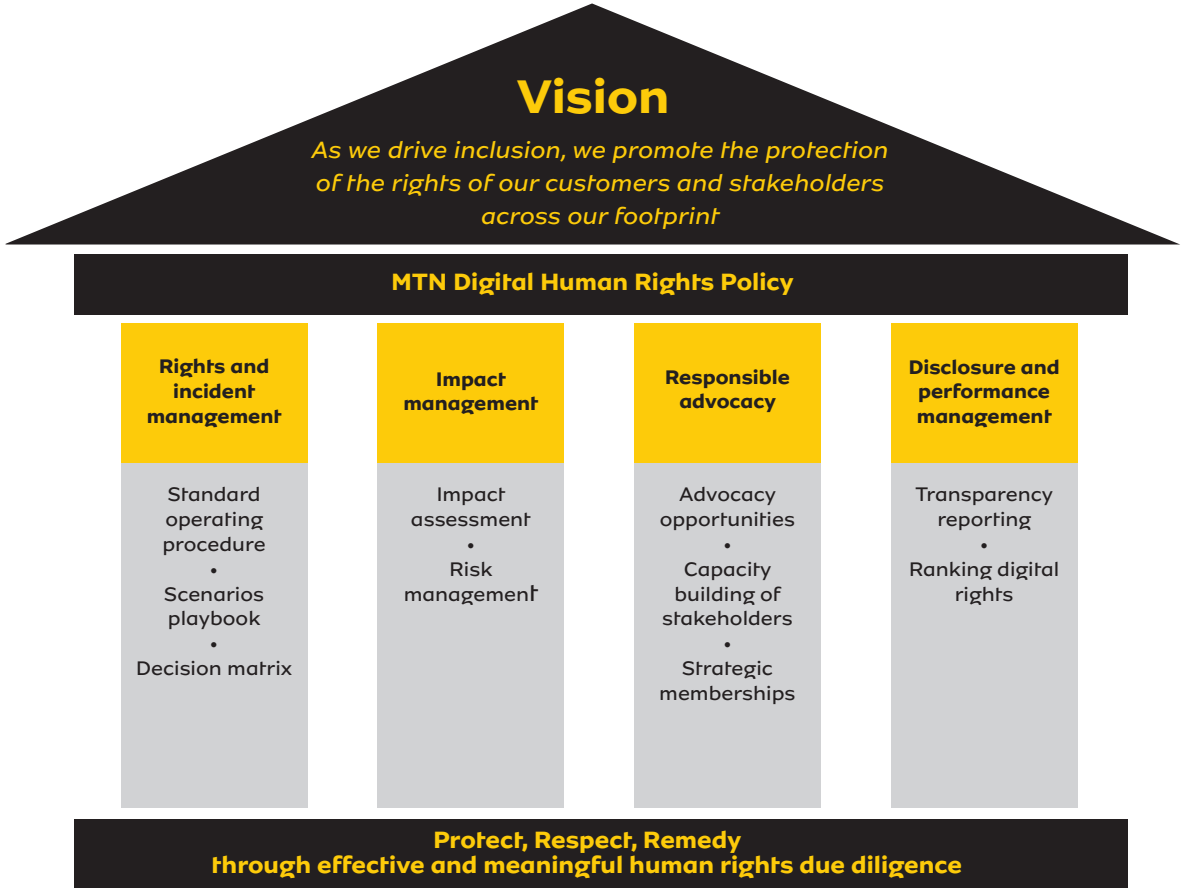


MTN digital human rights strategic framework

Digital human rights issues extend beyond requests by the government for user data. They affect us in a myriad of ways throughout our value chain. Our main objective is to manage these human rights issues in a consolidated manner across our business and platforms.

Our programmatic approach to human rights, revised in 2021, enables a Group-wide approach and responsibility for human rights while improving opportunities for building and leveraging strengths across the Group.

Overview of the digital human rights strategy

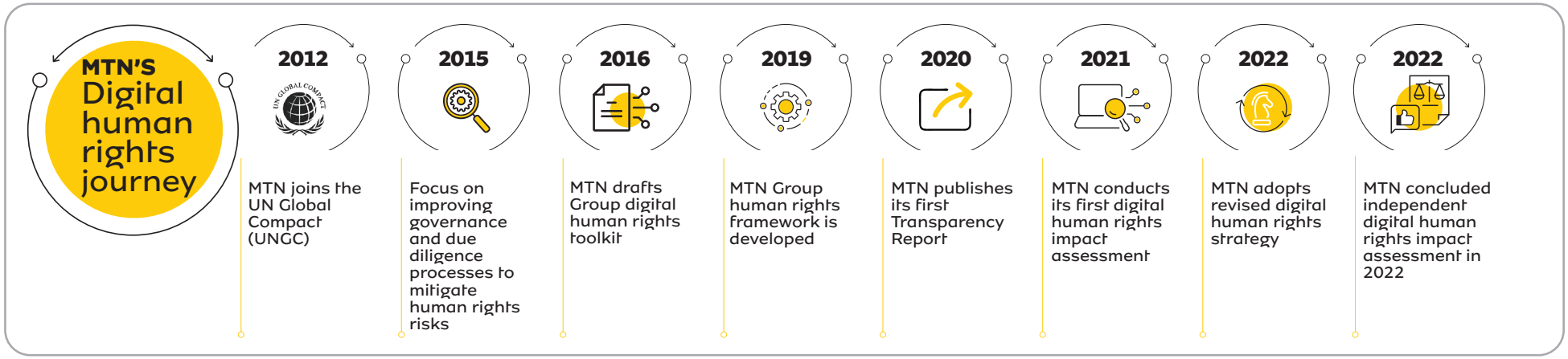


The report is structured around the four pillars of the MTN Digital Human Rights Policy. These pillars are:

- **Rights and incident management**
- **Impact management**
- **Defining our human rights advocacy approach** – Responsible advocacy
- **Disclosure and performance management**
- **Markets reports**

Governance: rights and incident management continued

MTN digital human rights strategic framework
continued



MTN is a member of these key bodies:
- Signatory of the UNGC
- Global Network Initiative
- Global Systems of Mobile Communications (GSMA)
- Sustainability Network
- Data Protection and Privacy Working Group
- Centre for Internet Security
- Information Security Forum

We increased our focus on digital human rights when we signed the UNGC. Since then, MTN has made significant strides in advancing our understanding of human rights impacts and enhancing human rights governance by adopting and implementing policies, procedures and systems aimed at protecting and promoting human rights.

MTN Digital Human Rights Policy

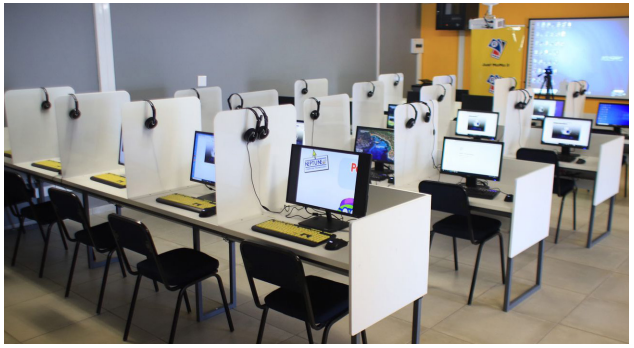
MTN embarked on a journey to protect digital human rights more than a decade ago. As we started on this journey, we focused on putting good governance structures in place to ensure we achieve our objectives of protecting these rights. We developed strategies, policies and due diligence processes. We also developed capacity by employing experts who could assist us in this journey. Now that we have laid the right foundation to protect digital human rights, we continue to go beyond embedding our policies and processes into our business model on every level and in all our operating markets.

MTN is guided by the following globally defined standards:
- The United Nations Universal Declaration on Human Rights.
- The United Nations 'Protect, Respect and Remedy' Framework and Guiding Principles.
- Africa Union Convention on Cybersecurity and Personal Data Protection.
- ECOWAS Supplementary Act on Personal Data Protection (2010).
- SADC Model Law on Data Protection.

Application of our Digital Human Rights Policy

Our Digital Human Rights Policy applies to all our directors, officers, employees and representatives of the Company, whether permanent, temporary or on contract.

We expect our intermediaries, agents, contractors, suppliers and business partners to uphold the same standards. Our Supplier Code of Conduct outlines the minimum requirements,



including human rights, that each supplier of products or services must comply with.

We ensure we remain abreast of new developments, review lessons learnt and update our processes and policies to align with evolving international standards. In addition, we provide detailed training to staff and partners based on the extent of their roles and ability to impact and or influence these rights.

The policy is applied Group-wide and is customised at Company level to meet country-specific requirements.

Governance: rights and incident management continued

MTN digital human rights strategic framework
continued

Key principles of MTN's Digital Human Rights Policy

- Right to **non-discrimination:** MTN opposes any actions that discriminate against people.
- Right to **freedom of opinion and expression:** MTN believes in the rights of all people using digital communications to freely communicate, share and receive information as well as share opinions and thoughts without interference.
- Right to **privacy:** MTN endeavours to uphold the right to privacy and information security without arbitrary interference.
- Right to **data protection:** MTN stipulates the personal customer data we capture, retain, process, use and provide to third parties. We inform customers of the purpose of our data collection and usage processes, why we may share data and how people can control their data.
- Right to **information:** Where appropriate and in accordance with the law, we take steps to inform users in cases where their rights may be infringed.
- MTN **seeks to limit the scope, extent or duration** of human rights impacts. MTN **may restrict access to services,** where MTN owns, operates or has technical control over online platforms, in instances where potential exists to harm the rights of people.
- Restrictions would be applied if the content is illegal or harmful as defined in terms of prevailing national laws in the jurisdictions in which we operate or the UN Universal Declaration of Human Rights.
- Right to **access remedy:** MTN strives to investigate incidents of alleged digital human rights violations and, in appropriate cases, engage with affected stakeholders.
- **MTN seeks solutions to avoid, prevent or mitigate digital human rights risks** and adverse impacts through effective stakeholder collaboration and engagement.
- MTN **strives to enhance transparency by reporting** annually about its efforts to mitigate digital human rights risks. MTN **communicates within disclosure parameters permitted by legislation or licence conditions,** without harming persons at risk.

Governance: rights and incident management continued

Digital Human Rights Due Diligence Framework

The UN Guiding Principles on business and human rights states that:
"In order to gauge human rights risks, business enterprises should identify and assess any actual or potential adverse human rights impacts with which they may be involved, either through their own activities or as a result of their business relationships. This process should: (a) draw on internal and/or independent external human rights expertise; and (b) involve meaningful consultation with potentially affected groups and other relevant stakeholders, as appropriate to the size of the business enterprise and the nature and context of the operation."

MTN tries to avoid adverse human rights impacts where it identifies a risk of violating these rights. Before, during and after a digital human rights incident, the framework outlines the steps that all MTN operations need to take. This framework enables our teams to respond to incidents through a clearly defined process, which includes identifying remedies for affected customers.

MTN has a due diligence framework that assists us in managing human rights incidents. The framework outlines the steps that all MTN operations need to take before, during and after an incident.

States have a duty to PROTECT human rights

Companies have a responsibility to RESPECT human rights

Individuals whose rights are harmed by business must have access to REMEDY

Policy commitment must be:
- Approved by the most senior level.
- Informed by relevant internal and external expertise.
- Explicit in stipulating human rights expectations of the business.
- Communicated throughout the business and be publicly available.
- Reflected in operational practices and procedures.

Human rights due diligence consists of:
- 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.

To be effective, grievance mechanisms must be:
- Legitimate.
- Accessible.
- Predictable.
- Equitable and transparent.
- Rights-compatible.
- A source of continuous learning.
- Based on engagement and dialogue.

Governance: rights and incident management continued

Our digital human rights due diligence process approach

1. Before

Proactive management

- **Conducting risk and impact assessments:** Digital human rights risk and mitigation plans are reviewed bi-monthly. Impact assessments are done on an annual basis.
- **Engaging stakeholders:** Ongoing engagements with stakeholder on digital human rights and related matters.

2. During

Incident management

- **Managing requests or incidents:** In determining MTN's response to requests received from authorities and non-governmental entities, the following key steps are undertaken:
  - All requests that may limit freedom of expression, access to information or privacy or harm the information security of MTN's customers are evaluated. It follows a due diligence approach to determine if the authorities and non-governmental entities are regulatorily authorised to make the request and have followed the prevailing regulatory processes.
  - MTN engages with relevant stakeholders for guidance before responding to requests to clarify, seek an amendment to the request or ask that the request be set aside where possible.
  - Review requests in accordance with the laws and applicable regulatory requirements of the countries in which we operate. The various applicable laws, including international laws, will also be assessed in all instances.
  - MTN assesses whether engaging with authorities to reject the request or partially comply with it will increase the risk to the safety of employees or compromise MTN's ability to continue operations.
  - Following the due diligence and evaluation in terms of good governance, regulatory and risk management processes, we would respond in any of the following ways:
    - Reject the request where possible.
    - Partially comply with the request.
    - Fully comply with the request.
- **Mitigating the impact of disruptions:** MTN ensures it communicates with impacted parties based on applicable law. We work to safeguard employees, customers and partners for whom we are responsible and ensure the integrity of our infrastructure is maintained.
- **Situational stakeholder engagement:** MTN engages with various stakeholders to ensure their perspectives are obtained; to identify potential mitigations; and manage the situation as effectively as possible. Grievances can be logged through our in-country customer complaints lines and via email to humanrights@mtn.com.

3. After

Post-incident management

- **Record-keeping:** To facilitate corporate learning and obtain information required for stakeholder engagement and reporting, MTN strives to maintain a documented trail of evidence relating to relevant events, decisions and actions.
- **Remedies for affected customers and stakeholders:** MTN works to offer remedies to customers negatively impacted on a case-by-case basis.

Governance: rights and incident management continued

Digital Human Rights Due Diligence framework continued

Grounds for complying with legislative requirements

We are committed to operating within the legal and regulatory frameworks of all our operating markets. Following applicable legislative, regulatory and licence requirements, we conduct business with the following objectives in mind:

- Protecting our customers' rights to access information and express themselves online.
- Good data governance.
- Providing secure communication services in the jurisdictions of our operating markets.

MTN is dedicated to conducting business with honesty and aims to always act with skill, care and diligence. Recognising that non-compliance with regulatory frameworks may result in fines, sanctions and even licence revocation. We have zero tolerance for non-compliance.

All potential human rights risks associated with granting or denying requests are carefully evaluated. In line with international and local human rights law, we consider legal validity, necessity and proportionality of each request. We seek additional legal counsel in most cases and especially if laws and/or licence conditions are ambiguous or in conflict with international standards.

Reasons why MTN would comply:

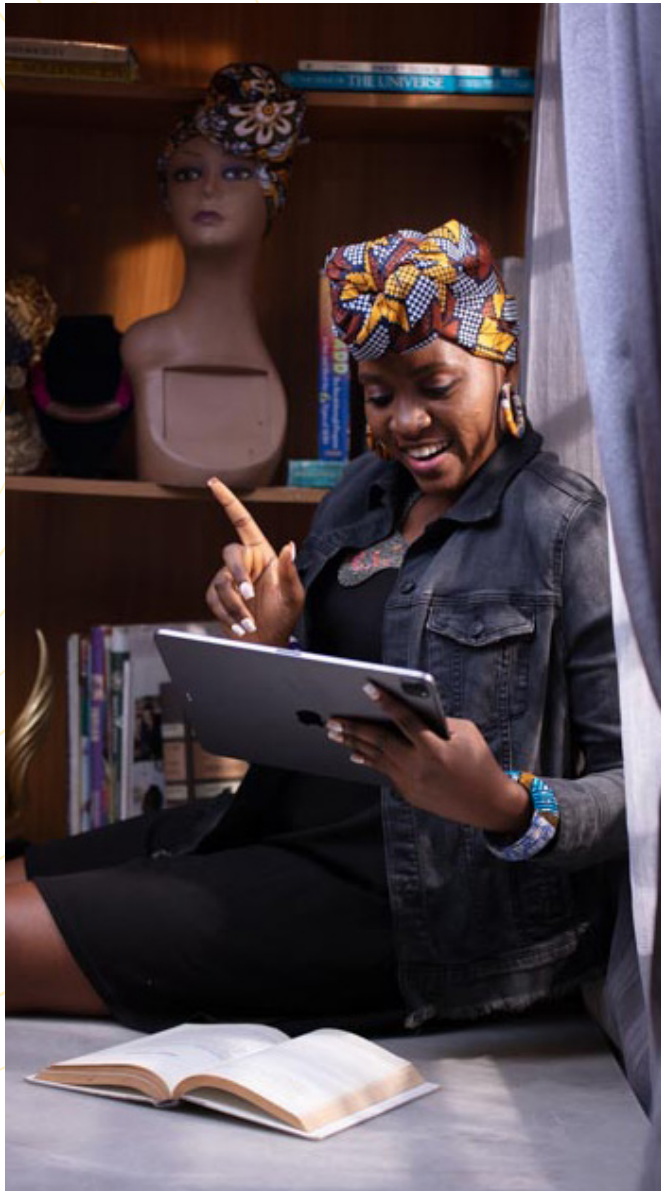
- Lawful request by an authorised public body as outlined in the governing legislation.
- Support the conducting of regulatory proceedings undertaken by a competent authority.
- Lawful purposes concerning licence and/or regulatory obligations.

Compliance risks:

- Violation of human rights
- Loss of life
- Security risk to staff, offices and infrastructure
- Possible litigation risk
- Reputational risk
- Backlash from civil society

Non-compliance risks:

- Non-compliance with licence conditions, leading to loss of authorisation to operate
- Expulsion, deportation, and/or imprisonment of personnel
- Harassment of staff and relatives
- Inability to enforce and comply with contracts
- Exposure to fines
- Breakdown in relationship with authorities
- Violation of human rights due to users being prevented from accessing services



Governance: rights and incident management continued

Digital Human Rights Due Diligence framework continued

Human rights-related policies, processes and position statements

Our Digital Human Rights Policy is complemented by a number of our policies. Below, we highlight the most important internal policies and processes concerning human rights adapted as a result of our commitment to embedding human rights across our value chain.

All our position statements, which are summary of our policies referred to in the sections below are publicly available at: Our positions - MTN Group.

Data privacy and protection

The Data Privacy and Protection Policy clearly articulates our commitment to data privacy and protection of our stakeholders.

We endeavour to comply with applicable data protection laws when collecting, processing , storing and disclosing personal information.

We are currently implementing a comprehensive privacy and data protection initiative at MTN to ensure that we maintain the desired level of compliance and have also appointed an information officer and deputy information officer to assist with monitoring internal compliance, providing guidance on data privacy and protection, and establishing clear procedures for reporting personal information breaches.

Enhancing information security

MTN continues to enhance its information security posture across the MTN footprint through the deployment of the MTN Group Information Security Policy, which sets out the requirements for securing MTN's information, systems and people. MTN's approach is guided by leading good practice such as National Institute of Standards and Security (NIST) Cyber Security Framework and ISO/IEC 27001:2013.

We thrive to comply with the information security regulatory requirements, such as having Fintech specific security strategies where required by legislation, within our operating markets.

Treating customers fairly

MTN is committed to ensuring the best customer experience by focusing on customer needs and expectations and meeting them. We protect customers and ensure fairness for those interacting with our products and services.

We have developed a policy and framework that ensures our customers are treated fairly to promote transparency and customer control. The framework mandates the implementation of key customer service processes across all MTN operations.

Responsible marketing

MTN is committed to preserving our brand's credibility and reputation. Our interactions with the public, including our marketing initiatives, are distinguished by courtesy and responsibility. Our customers are at the centre of everything we do, and we strive to cultivate strong, mutually beneficial relationships with them.

Reputation and goodwill are indispensable assets that contribute to the long-term viability of MTN. MTN has built its reputation by emphasising social responsibility, transparency and the creation of value for all its stakeholders. We acknowledge not only the need to state our belief – that everyone deserves the benefits of a modern connected life – but also to be evaluated against it and continuously demonstrate that our activities are consistent with our mission.

We strive to ensure our marketing activities are ethical, non-offensive, accurate, consistent and appropriate across all our geographic markets. Our approach to responsible marketing encompasses all types of advertising and marketing materials, including written, digital, social media-based, audio, verbal, electronic or distributed via any other media platform.

Whistle-blowing

MTN is committed to a Company-wide culture of zero tolerance for fraud, bribery, corruption, theft and illegal activity. We acknowledge the importance of having procedures and mechanisms in place through which employees and other stakeholders can safely and anonymously report fraud, misconduct, illegal activities and other irregularities (i.e. incidents that interfere with judicially protected freedoms of expression, information security and privacy).

MTN views whistle-blowing as a positive practice that aids the Company in detecting early instances of fraud, misconduct and illegal activity. It allows us to limit or prevent financial and reputational harm to the Company, prevent future occurrences and take corrective action against those who have committed illegal acts.

Through relevant policies, we encourage employees to report any fraud, misconduct, bribery, corruption, misappropriation or illegal activity committed by an internal or external party against MTN and by MTN. This is achieved by utilising available reporting procedures and resources. Additionally, employees or individuals who have reported such incidents to MTN in good faith and without malice are not subject to retaliation.

MTN provides the whistle-blower and household members with reasonable personal protection, if necessary.

Governance: rights and incident management continued

Protecting children online

MTN has a zero-harm policy with regard to the abuse and exploitation of children. We strive to respect and protect the rights of children online and create responsible digital citizens. MTN has been a member of the Internet Watch Foundation (IWF) since 2019 and forms part of the top-level band of members of the IWF. MTN benefits from the protection of IWF's services, especially the child sexual abuse material (CSAM) URL blocking list, available to our operating companies Opcos throughout Africa. (Please also see pages 19-22 to understand the impact).

MTN's support in the mutual fight against online child sexual abuse has often gone above and beyond membership. For example, MTN launched the Help Children Be Children campaign, which aims for Africa-wide awareness and capacity building. (Please also see pages 19-22 of this report to see how we specifically manage our impact on child online protection).

1

Zero-tolerance approach to the abuse and exploitation of children

To ensure responsible use of digital communications, our efforts are guided by the global organisations and law enforcement authorities managing this complex matter.

- We strive to comply with relevant national laws and regulations of host countries. We are a signatory of the UNGC, principles related human rights, including those of children.
- We support the United Nations Convention on the Rights of the Child (UN CRC), which placed a legal obligation on states to protect the rights of children.
- We are a signatory of the GSMA Mobile Alliance Against Child Sexual Abuse, which works to create significant barriers to the misuse of mobile networks and services for hosting, accessing or profiting from child sexual abuse imagery.

2

Strive to protect, respect and ensure the rights of children online

We apply our best endeavours to ensure CSAM is not made available to our customers by our third-party content providers.

- Using neutral third-party software, we will block CSAM that is identified by IWF, whose remit is to minimise the availability of online sexual abuse content.
- Regulatory and legal assessments and risks posed to MTN regarding CSAM at each Opco level.
- Guided by out toolkit to raise public awareness and report CSAM.

Case study: South Africa

DATA REQUEST TYPE: NON-GOVERNMENTAL ENTITIES

MTN SA has seen an increase in requests for personal information from subscribers themselves. This is a growing trend given the requirements of the Promotion of Access to Information Act 2 of 2000, which requires that we grant users access to their information upon request.

Fortunately, the act also specifies requirements that have to be fulfilled before any information is released to the subscriber, and these include verification that the subscriber is the registered owner of the cellular number in respect of which information has been requested, accompanied by a signed affidavit detailing the information requested.

These requirements assist us in safeguarding our customers' personal information, while at the same time, respecting their right to have access to the information. The identification process becomes a crucial safeguarding mechanism. The affidavit ensures the customer's right to accessing their personal information is protected and we have a record of the request.

Impact management

The UN Guiding Principles on Business and Human Rights states that:

"In order to gauge human rights risks, business enterprises should identify and assess any actual or potential adverse human rights impacts with which they may be involved, either through their own activities or as a result of their business relationships. This process should: (a) draw on internal and/or independent external human rights expertise; (b) involve meaningful consultation with potentially affected groups and other relevant stakeholders, as appropriate to the size of the business enterprise and the nature and context of the operation."

States have a duty to *Protect* human rights

Companies have a responsibility to *Respect* human rights

Policy commitment must be:
- Approved by the most senior level.
- Informed by relevant internal and external expertise.
- Explicit in stipulating human rights expectations of the business.
- Communicated throughout the business and be publicly available.
- Reflected in operational practices and procedures.

Human rights due diligence consists of:
- 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.

Individuals whose rights are harmed by business must have access to *Remedy*

To be effective, grievance mechanisms must be:
- Legitimate.
- Accessible.
- Predictable.
- Equitable and transparent.
- Rights-compatible.
- A source of continues learning.
- Based on engagement and dialogue.

Risk management and impact assessments

Impact and risk assessments are a crucial component of MTN's digital human rights strategy, allowing us to identify areas where the risks of adverse human rights impacts could be significant. We conduct impact assessments on an annual basis, using either internal or external resources as necessary. Owing to the dynamic nature of digital communication risks, we update our digital human rights risk identification and mitigation strategies quarterly.

MTN partnered with BSR (a sustainable business network and consultancy) in late 2021 to conduct digital human rights impact assessments (DHRIA) for MTN, in seven operating markets and develop a DHRIA toolkit for MTN's ongoing human rights due diligence across all markets. DHRIAs in seven of its operating markets were conducted and focused on the human rights risks associated with the use of MTN's products and services. The DHRIAs did not focus on MTN's supply chains.

BSR also conducted a DHRIA on MTN's free instant messaging application, Ayoba. Recommendations were provided for the following:
- Product functionality and features (e.g. user reporting channels).
- Product policy (e.g. prohibited content and conduct on Ayoba).
- Product policy enforcement (e.g. trust and safety capacity).
- Government/law enforcement relationships (e.g. advocating in favour of end-to-end encryption).

Impact management continued

Risk management and impact assessments continued

In addition, BSR provided MTN with a human rights due diligence toolkit for all operating markets and products. This included DHRIA tools for product evaluation; operating markets evaluation; responsible entry and exit; and mergers and acquisitions. MTN has implemented the due diligence toolkit in all of its operating markets and continues to analyse this information on an ongoing basis.

The DHRIAs were informed by a literature review, interviews with MTN Group and operating markets employees, and interviews with external stakeholders and market-specific experts.

The purpose of the DHRIAs was to identify the most pressing human rights issues for MTN by answering the following questions.

1. *How many individuals could be affected by the risk?*
2. *How severe would the risk be for those impacted?*
3. *Remediability: Will the remedy restore affected parties to the same or equivalent position as before the damage?*
4. *How likely is it that the impact will occur within the next five years?*

Common findings from BSR's digital human rights impact assessment

	Government requests for customer data, including direct access – In most cases, law enforcement agencies are demanding access to user data collected and stored by MTN through a court order, informal (immediate) request or direct access to the network. MTN needs to continue to strengthen its mechanisms on how data is being used.
	Government (SRO), including blocking, filtering and throttling – There are instances where government agencies are demanding that MTN disrupts the network through a court order or formal or informal requests. The request may consist of instructions to undertake a full or partial network shutdown or request specific sites or IP addresses to be blocked or filtered. The government may also request that the network is slowed down (known as throttling) to make it difficult to access particular sites. It is critical for MTN to ensure that its digital human rights policies and procedures are consistently applied and provide the necessary training to ensure that the appropriate process is followed in every instance.
	Access to the internet – Access to the internet has been recognised by the UN as a human right and offers the opportunity to reduce inequalities within countries as well as enable people to fully participate online in activities that have broader economic and social impact such as education, learning, health, government services and business. MTN needs to continue to evolve its approach to cater for the varying needs of its customers and stakeholders.
	Product and business model development – New product development and business models bring new risks that could impact the fundamental rights of users and customers. Examples include replicating or catalysing existing bias, resulting in unequal and discriminatory impacts; or facilitating, incentivising or motivating online speech and behaviour, which results in offline harm. MTN needs to ensure it applies its products and services digital human rights impact assessment to make certain risks associated to new and existing products and services are mitigated.
	Data governance – Failing to adequately address how data is governed may violate the privacy rights of customers and employees. It may also put them at enhanced risk that data either directly attributable to them, or insight inferred by the combining of datasets related to them, will have discriminatory outcomes or restrict their freedom of movement or political participation. MTN needs to continue to strengthen its data protection and privacy practices to ensure it remains abreast of changing customer needs.
	Child online protection – Children have a right to fully participate online and access to the internet can play an important role in the provision of education. However, children may face particular risks given their vulnerability, including privacy, discrimination, harassment and the risk of sexual abuse. New product and business model development and data collection must continue to cater to risks associated with having more children online.

Impact management continued

"In recent years, MTN has made significant strides in establishing digital human rights frameworks, policies and escalation processes, as noted by the DHRIAs. The DHRIAs emphasised that the Company is shifting in the right direction in advancing the implementation and monitoring of these frameworks, policies and processes." – BSR

The DHRIAs have identified human rights issues for MTN	
Capacity building	Provide operating companies with human rights training, guidance and resources, such as rehearsals, scenario planning and opportunities to participate in GNI events and dialogue.
Stakeholder engagement	Take a strategic approach to establishing stakeholder relationships that facilitate the early identification of human rights risk and a proactive approach to addressing these.
Product and business model development	Work to continuously ensure product and business model development remove bias in data analytics, monetising data or facilitating hate speech and disinformation.
Business model due diligence	Anticipate, prevent and mitigate potential human rights risks posed by the ***Ambition 2025*** strategy.
Transparency	Provide additional insight into the regulatory and licensing context (where legally permissible) and continuously publish deeper insight into MTN's actual experience with SRO, such as through case studies.

Managing our impact on children: child online protection

We believe all our users deserve to benefit from the free and open nature of information and communication technologies. However, this comes with grave risks to the most vulnerable in society. It is critical to educate children, parents, teachers and caregivers about how to responsibly use digital technology to ensure children stay safe online. Our Group-wide Child Online Protection programme complements local operating company initiatives.

Impact management continued

Managing our impact on children: child online protection continued

UNICEF's research on child online sexual abuse and exploitation conducted in 13 African countries highlighted the need to focus on child online safety. The study found that one in three children did not disclose their abuse, with nearly half citing a lack of knowledge on where to go or who to tell. Additionally, formal reporting channels are underutilised, with only 3% of victims calling a helpline or contacting the police. There is a great need, specifically in Africa, to help children report these incidents in an easily accessible and anonymous platform.

For this reason, when it comes to protecting children, we would like to answer the call for **Doing for tomorrow**, **today**, literally. The question to be answered is therefore: what is MTN doing today, to protect children? The global population is aware of the threats the internet poses to children. On the one hand, it opens vast opportunities for exploration and learning and, on the other hand, perpetrators can use the internet for abuse. We take our responsibility to protect children from these perpetrators very seriously and subsequently launched the campaign entitled Help Children Be Children in 2022. MTN also supported the development of an Africa-wide child safety online portal. It is the first of its kind as a reporting mechanism for child sexual abuse imagery online. MTN has been working with the IWF to develop this and it is available at: Campaign - MTN Group.

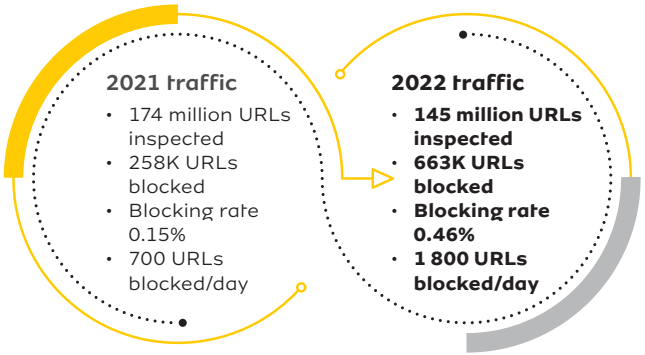
The Help Children Be Children campaign aims to raise awareness of CSAM and how it can be reported in target countries among the public. Additionally, the campaign helped train law enforcement and child helplines in the continent, positively impacting policy through roundtables and encouraging critical actors, including the industry, to join the global fight against CSAM.

As we lead digital solutions for Africa's progress, MTN believes we have a critical role to play to ensure every African child in our markets is kept safe online. The Online Child Safety Africa Portal is one way we can create a safe online village for our children.

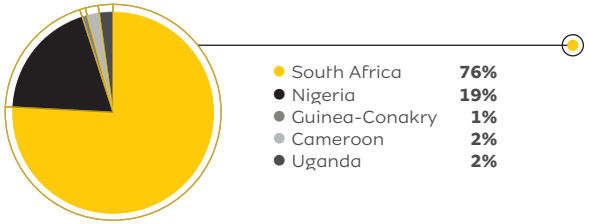
Illustrating impact through our IWF membership and blocking activities

As opposed to section 3 of this report, MTN forms part of the top-level band of members of the IWF. MTN benefits from the protection of IWF's services, especially the CSAM URL blocking list, available to MTN's Opcos throughout Africa. The graphs below provide some data on how we have been able to remove content that might be harmful to children through the work of the IWF. There have been significant increases since 2021 in the amount of URLs that were blocked. This is a concerning development but might indicate we are becoming more effective in protecting children.

MTN's adaptive mobile blocking activities



Top five Opcos – 80% of blocked traffic



MTN uses an adaptive system to detect and block URLs deemed inappropriate or harmful to its users. This system takes into account the specific characteristics of each market and is designed to provide a reliable and effective means of filtering out harmful content. The filtering process is based on a daily list of URLs provided by the IWF feed, which contains information about websites known to contain CSAM or other illegal content. MTN's partnership with Adaptive Mobile receives this list and uses it to block access to these URLs, thereby helping to protect its users from exposure to harmful content. This approach is a key component in our commitment to promoting a safe and responsible online environment for our customers, and we continue to refine and improve our adaptive system to ensure it remains effective and up to date.

Impact management continued

MTN's blocking software rollout status

MTN has been working on an adaptive mobile rollout strategy, which involves the deployment of mobile networks in a way that is tailored to the specific needs and characteristics of each market. This approach takes into account factors such as population density, terrain and existing infrastructure, and aims to provide reliable and affordable mobile services to as many people as possible. We have made significant progress in this rollout and the Company continues to expand its coverage and improve its network quality in many of the markets where it operates.

The MTN Group has been members of the IWF since 2019 and forms part of the top-level band of members of the IWF. MTN benefits from the protection of IWF's services, especially the CAM URL blocking list, available to MTN's Opcos throughout Africa.

MTN's support in the mutual fight against online child sexual abuse has often gone above and beyond membership. For example, MTN has helped to drive our Help Children Be Children Campaign for Zambia and Uganda, and is now funding phase 2 of this campaign for an Africa-wide awareness and capacity building for 2022.

Live
Côte d'Ivoire
Ghana
Nigeria
South Sudan
Uganda
Zambia
South Africa

In progress
Benin
Sudan

Future development
Guinea-Bissau
Guinea-Conakry
Cameroon
Congo-Brazzaville
Rwanda

Impact management continued

Illustrating impact through survivor stories

According to the UNICEF Child Online Protection Update Report from 2022, the commemorations of the first UN World Day for the Prevention of and Healing from Child Sexual Exploitation, Abuse and Violence on 18 November was a significant international event. A long overdue moment of global recognition to show survivors the entire world supports them and that they have a right to justice and healing. In response, the UN General Assembly created this new UN World Day in November. It is important to acknowledge some of the survivor stories in this report to better understand how MTN assists in this protection and healing process.

MTN is therefore relieved to report we have had some impact on Helping Children Be Children. These survivor stories are based on true stories provided by the IWF. The names have been changed to protect the identity of children involved.

Pierre

10 months

The innocence of 10-month-old Pierre was snatched when his body was sexually violated by an adult relative, leaving him with an indelible scar on his young soul and body.

Pascal

Six years

Pascal was six when an adult forced him to engage in sexual sadism, capturing every gruesome moment on camera. The images made their way onto a website, each click delivering a blow to the young child's formative years.

Imani

Three years

Imani was only three when the sexual torture started. As it continued, unabated, each episode was filmed and shared online, eroding the life that each child deserves to have.

Case study: Zambia

In April 2022, MTN Zambia in partnership with the Meta, the International Centre for Missing and Exploited Children, Child Helpline International and United Nations Office on Drugs and Crime, and the IWF launched the Help Children Be Children Campaign and the Child Safety Online Africa Portal to help prevent the spread of CSAM online and raise awareness of where to report such material.

Following its launch, MTN Zambia ran internal and external campaigns as a way to raise public awareness on the prevalence of child sexual abuse and help counter the distribution of such material online on the African continent.

MTN Zambia's internal campaign focused on encouraging staff to post awareness materials on various social media platforms and the staff that had the most views and likes were given prizes ranging from branded T-shirts, caps and hoodies printed with the Help Children Be Children messages. The main winner received a Samsung 22 phone during the monthly townhall sessions.

The external campaign involved working with the Zambian national football team known as the Chipolopolo who graciously agreed to participate to raise awareness through a video recording. It was exciting to see all the internationally based footballers participate in the campaign led by the team captain Enock Mwepu. MTN Zambia leveraged on its partnership with the Football Association of Zambia (FAZ) and made a presentation on the campaign during the 2022 annual football awards ceremony broadcast live on DStv and watched in 47 countries.

In addition, representatives from Zambia Information and Communication Technology Authority (ZICTA) made a presentation at the FAZ Awards ceremony on the provisions of the Zambia law to protect children. They highlighted the activities being undertaken by ZICTA to protect children and announced local civil society organisations providing protection to children.

The final part of the campaign focused on public awareness and encouraged Zambians to post awareness messages on media platforms. Weekly prizes were given to members of the public and the grand prize was a Samsung 22 phone with campaign-branded materials.

Thanks to these social media campaigns, 2.5 million people were reached. In addition, in 2021, MTN Zambia engaged with law enforcement authorities to investigate potential sexual abuse crimes committed against children on MTN's platforms, which saw various stakeholders come together to support children.

Responsible advocacy

Strategic memberships

We are members and active participants in key industry organisations to stay informed and in line with best practices, to share our expertise and experience, and to provide input on industry policies. Our membership in these organisations provides an additional training mechanism, as the Board receives feedback from these groups' activities and thought leadership.

MTN is a member of the following key bodies:
- Signatory of the United Nations Global Compact.
- Global Systems of Mobile Communications (GSMA).
- GNI.
- Sustainability Network.
- Data Protection and Privacy Working Group.
- Centre for Internet Security.
- Information Security Forum.
- Joint Audit Co-operation (JAC) Human Rights Workstream.

MTN became an active member of the GNI and participated in other initiatives, such as the JAC, embedding human rights ethos in the supply chain. Similarly, we participated in GSMA's ESG metrics pilot and digital integrity pilot.

MTN uses JAC for:
- Sharing best practices, case studies and lessons learnt.
- Sharing approaches on mapping of supply chains and Human Rights Index used.
- Establishing collaboration with civil societies within JAC.
- Broadening human rights workstream to risks in supply chain, including human rights, logistics, wars and energy disruption.

The GNI has set up global principles on freedom of expression and privacy (GNI Principles). These principles and Implementation Guidelines have been set by numerous organisations to advance and protect freedom of expression and privacy in the global information and communications (ICT) industry in the face of government demands to restrict content or hand over user information.

MTN joined GNI to get assistance in respecting freedom of expression and privacy rights when faced with government pressure to hand over user data, remove content or restrict communications. GNI provides MTN with opportunities to engage with multiple stakeholders. These international exchanges enrich MTN's digital human rights approach and allows for peer learning. It provides MTN with an opportunity to influence emerging policies.

Responsible advocacy continued

Stakeholder engagements

MTN has shown significant progress in terms of engaging with its stakeholders on a regular basis about digital human rights specifically.

Key relationships

MTN participated in panel discussions at the UNBHR Forum in Accra and Geneva, where MTN was able to share its experiences, not only from a business perspective, but also as a company operating in the Global South. These were great opportunities for peer learning and information sharing.

The UNBHR Forum in Accra MTN had a panellist representative on a session titled: 'Understanding and mitigating the impacts of the use and development of technologies by businesses in Africa'. The UNBHR Forum in Geneva MTN welcomed a panellist representative on a session titled: 'Mandating responsible business conduct in the tech sector – Advancing the UNGPs in regulatory debates'.

These engagements allow MTN to build and leverage new relationships across multiple sectors. They enable MTN to draw lessons from these various stakeholders on how to better protect and promote human rights.

Other civil society organisations

- MTN engaged several civil society organisations that work on child protection such as the Department of Social Development in South Africa; the South African Human Rights Commission; Teddy Bear Clinic and Save the Children Foundation.
- MTN engaged with a few research institutions to explore possibilities of collaborating to build knowledge around child online safety in Africa. MTN met with Unisa's Youth Research Unit to explore possible research opportunities.
- MTN also took part in regional and international discussions of UNGPs corporate accountability.
- In June 2022, MTN attended Access Now's #rightscon, the world's leading summit for human rights in the digital age.
- MTN attended Trialogue's webinar on Business and Human Rights on 24 March 2022 and was able to share some of MTN's lessons learnt.

Membership and meeting frequency

		Meeting frequency
Memberships	GNI	Once a month
	IWF	Once a month
	Business for Social Responsibility	Quarterly
	UN Global Compact	Once a month
	GSMA (Mobile Alliance Against Child Sexual Abuse)	Once a month

		Meeting frequency
Working Groups/committees	JAC Human Rights Stream	Once a month
	GNI Policy Committee	Once a month
	GNI Armed Conflict Working Group	Once a month
	GSMA Sustainability Network Meeting	Once a month
	GSMA ESG Metrics for Mobile pilot session	Monthly

		Meeting date
Ad hoc events or meetings	GNI Content Regulation event with UK and EU policymakers	6 – 10 June 2022
	Launch of GSMA SDG Impact Report 2022 – promotional toolkit	21 September 2022
	Launch of the Department of Social Developments	4 November 2022
	Disrupting Harm South Africa report	
	UNICEF met with the partnership specialists in Eastern and Southern Africa's regional offices	19 October 2022

Human rights awareness, training and recognition

MTN continues with ongoing internal awareness campaigns on the understanding and education on digital human rights, freedom of expression and privacy. As is evident from the information provided on pages 20 to 22 of this report, we have made great strides in terms of creating awareness about child online protection.

On 21 February 2022, a business and digital human rights seminar was held to train and educate many MTNer, employees across employees from across our markets, including members of management and the Board. BSR also presented to Board, the findings of the impact assessments to the Board. Additionally, MTN employees attended the GSMA 2021–2022 human rights webinars; the implementation series. These interventions have assisted us in capacitating our staff members and improving their human rights knowledge. This, in turn, has made it easier for us to create a human rights culture in the organisations.

Case study: Sudan

25 October 2022 marked Sudan's first anniversary of military takeover. The anniversary was accompanied by violent protest and civil unrest. In an attempt to restore order, a request was made to all operators to restrict access to the internet.

MTN received an order to shut down internet access for stipulated periods of time. Given the potential human right impact, we instituted our escalation procedure. We took steps to verify the authenticity of the request. We conducted numerous stakeholder engagements with our ICT and other related stakeholders to obtain a multi-stakeholder perspective on the issue. We determined we had no choice but to comply with this request.

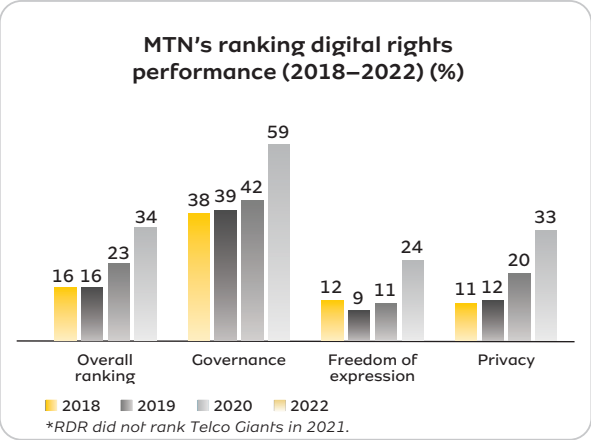
Before going ahead with this, we sent bulk SMSes to all our customers informing them of the pending shutdown. We also informed customers they would be compensated for lost subscription quota. We took our customers into confidence by providing details and reasons for the shutdown. We informed them and the order was issued against all operators as it affected all users, except banking and electronic points of sale.

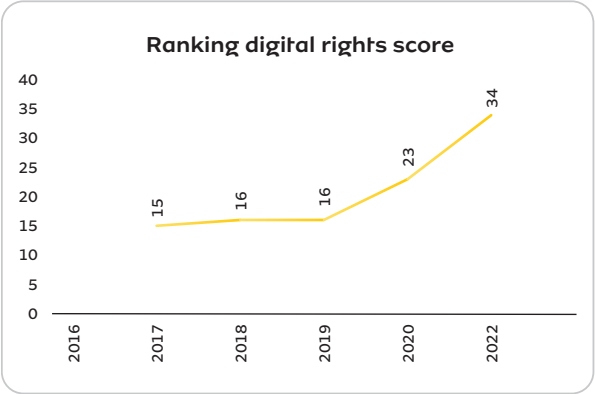
Disclosure and performance management

Transparency reporting

It is important to note that in 2017 MTN was the first pan-African telecommunications company to embark on a transparency reporting journey. We have improved our reporting every year since 2017 and are receiving recognition for this from authoritative organisations in this space. We acknowledge this process is a journey we are committed to, but is by no means complete.

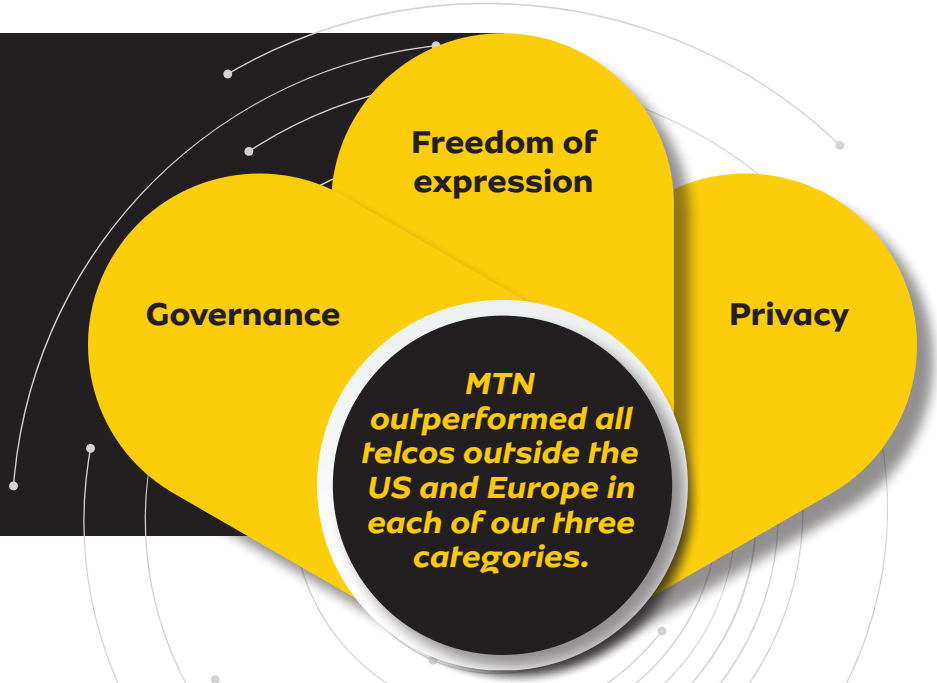
MTN disclosed annual human rights impact assessments, which considered digital human rights such as freedom of expression and opinion, information security and data privacy.





Progress in ranking digital rights

"In terms of ranking digital rights, MTN's score on privacy never surpassed that of any European telecommunications company, but in 2022, it surpassed both Telenor and Orange. This improvement was mainly due to our commitment to stronger internal security measures and by disclosing government demands for user information in the transparency reporting programme." – RDR



Markets report

MTN operates in various markets with different socioeconomic and political contexts. The situation presents both challenges and opportunities. It is, however, imperative to understand the nuances of each country to properly serve them. In the following markets report, we provide a brief overview of the human rights context in all our operating markets to help our stakeholders better understand that operating in the exact same way may not be possible. MTN believes and respects the rule of law in every country in which we operate.

Our portfolio at 31 December 2022	(MTN Group effective shareholding)
MTN South Africa	**100.0%**
MTN Nigeria ▲	**75.7%**
SEA	
MTN Uganda ▲	**83.1%**
MTN Rwanda ▲	**80.0%**
MTN Zambia ▲	**89.8%**
MTN South Sudan	**100.0%**
Mascom Botswana$^{\Delta}$	**53.1%**
MTN eSwatini$^{\Delta}$	**30.0%**
WECA	
MTN Ghana ▲$^{\#}$	**84.3%**
MTN Cameroon	**80.0%**
MTN Côte d'Ivoire	**66.8%**
MTN Benin	**75.0%**
MTN Guinea-Conakry	**75.0%**
MTN Congo-Brazzaville	**100.0%**
LonestarCell (MTN Liberia)	**60.0%**
MTN Guinea-Bissau	**100.0%**
MENA	
MTN Sudan	**85.0%**
MTN Afghanistan ■	**100.0%**
MTN Irancell$^{\Delta}$	**49.0%**
Associates, JVs and other investments	
aYo	**50.0%**
IHS Group	**25.7%**
Iran Internet Group$^{\Delta}$	**29.5%**
Middle East Internet Holding$^{\Delta}$	**50.0%**

▲ *Localisations.*
■ *Exiting in an orderly manner over the medium term .*
Δ Equity accounted.
 # Legal ownership is 79.3%.

Markets report continued

Categories of requests from authorities and NGOs

The markets have provided information relating to the requests received from the authorities and non-governmental entities. Given the broad range of laws and requirements applicable to the markets, we have categorised the types of requests received from authorities as follows:

Data request type (authorities)	Data request description
Requests pursuant to criminal investigations	Requests by authorities submitted pursuant of the terms of applicable laws or by virtue of a court order for information of subscribers in the context of criminal investigations, such as subscriber identification, call and SMS information, billing statement and historical location data. These requests do not include requests by authorities for the content of the underlying communications.
Requests for location disclosure	Requests by authorities that are regulatorily permitted by applicable laws or by virtue of a court order for the current location of a subscriber.
Requests for lawful interception	Requests by authorities that are regulatorily permitted by applicable laws or by virtue of a court order for the lawful interception of a subscriber's communication.
Requests pursuant to governmental or regulatory oversight	Requests by authorities for information required by the authorities to perform their designated governmental or regulatory functions, including their oversight of telecommunication service providers.
Requests pursuant to suspension of MSISDNs, and subscriber identification module (SIM) cards	Requests by authorities that are legally permitted by applicable laws or by virtue of a court order obliging mobile network operators to suspend/ deactivate SIM cards or mobile subscriber integrated services digital network (MSISDN) numbers of subscribers.
Service restriction orders and/or internet shutdown	Requests by authorities that are legally permitted by applicable laws or by virtue of a court order obliging mobile network operators to block or restrict a service or shutdown the internet / social media services.

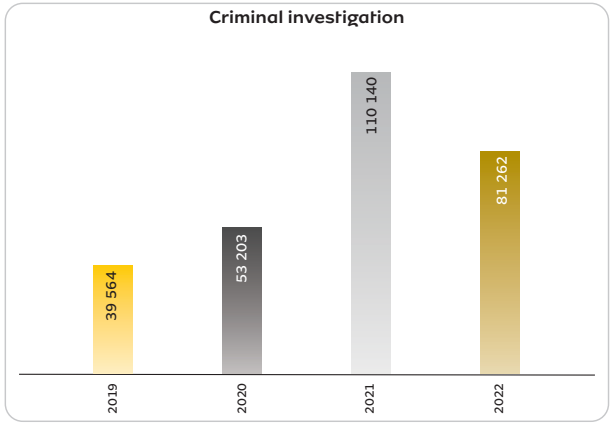
Data request type (non-governmental entities)	Data request description
Requests pursuant to civil litigation	These requests generally consist of requests made by non-governmental entities engaged in civil litigation with or on behalf of subscribers and subscriber requests for their own data.
Requests for personal and private use	Subscribers may request access to their own data for several reasons, including to comply with a requirement from an embassy or a visa requirement.

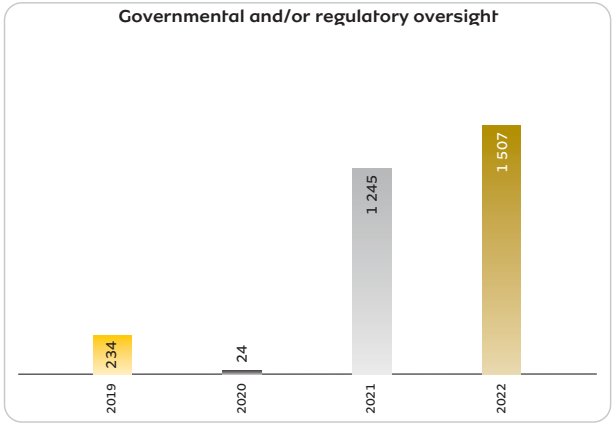
There may be, to some extent, an overlap between the above-mentioned categories of requests as certain requests received by a market may be broader than others.

Markets report continued

Overview of total requests received

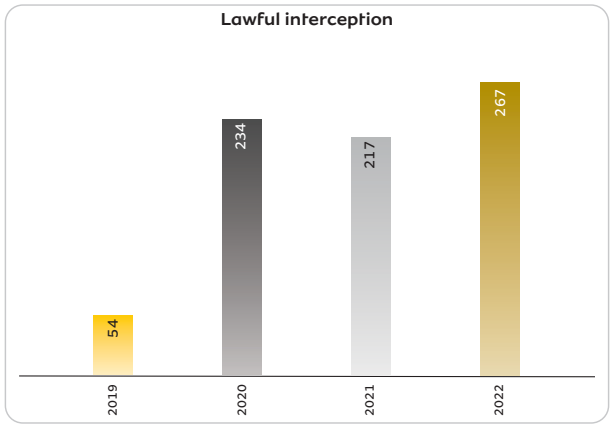
- Criminal investigations and requests pursuant to suspension of Mobile Station International Subscriber Directory Numbers (MSISDN) and subscriber identification module (SIM) cards have remained the largest category of government requests received.
- The increase in requests for location disclosures is linked to the increase in requests for criminal investigations as some criminal investigation requests are accompanied by a location disclosure request. This can be attributed to increased legislation that seeks to curb crime on the continent and more specifically organised crime and cybercrime. An Industrial Development Corporation (IDC) report titled 'The Impact of Cyber Extortion in Africa' stated that Africa is losing US$4 billion annually to cybercrime, but this is slowly changing as countries like Kenya and Zambia implement new cybersecurity laws.
- It is worth noting there has been a steady increase in requests pursuant to the suspension of MSISDNs and SIM cards are consistently owing to mandatory SIM registration laws where mobile network operators are obliged to deactivate unregistered SIM cards.
- While MTN received more SRO and internet shutdowns in this financial year than it did in 2021, from a regional perspective, SROs decreased. AccessNow states, "In Africa, seven countries imposed shutdowns nine times, a significant decrease from 2021 where 12 countries disrupted the internet 19 times."
- Non-government requests declined by 60%. Non-government requests in the year under review totalled 2 250 compared to last year's figure of 5 622.

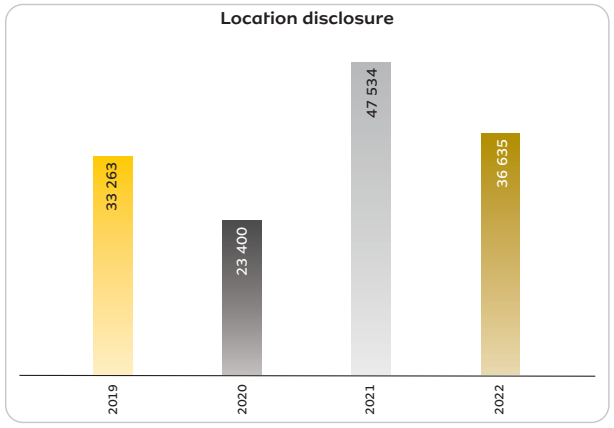


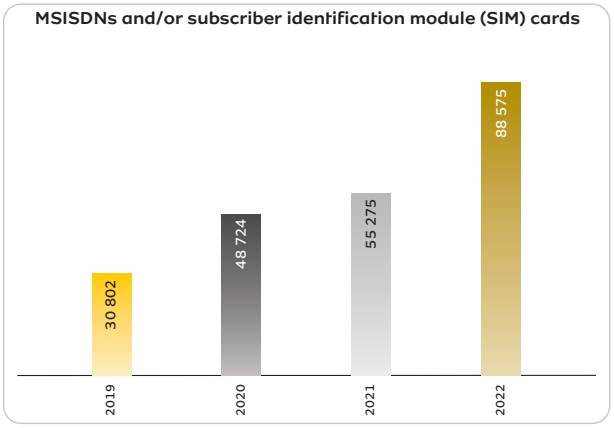


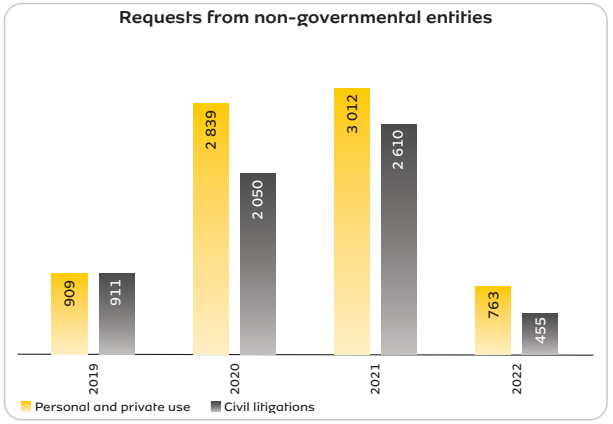
[1] https://techcabal.com/2022/12/16/digital-cyber-threats-in-africas-e-commerce-and-payment-sectors/

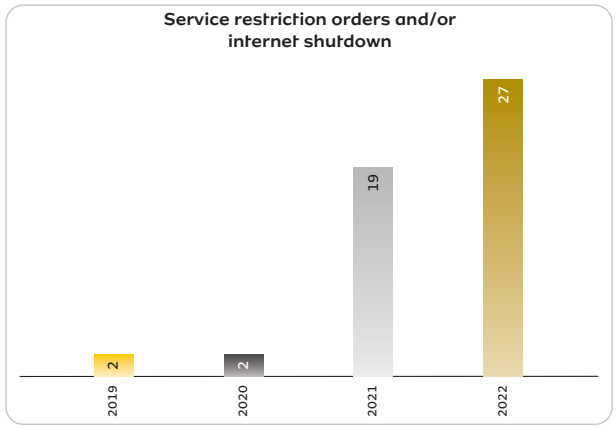
Markets report continued











Markets report continued

Mapping trends in African digital human rights:

- Digital rights in Africa has been a topical issue in the past years with several countries continually adopting agile regulation principles to address various digital human rights issues[1]. This has assisted in providing legal certainty for businesses operating in the region. However, legal fragmentation remains a challenge.
- Data protection and privacy are becoming essential topics for internet governance in Africa. We are witnessing an increased attempt at the development of legal frameworks that seek to protect user data. Notably, in the year under review, countries such as eSwatini and Nigeria passed new data protection and privacy laws. Nigeria went further to establish an independent Data Protection Commission for the regulation of the processing of personal data.
- We have also seen a few countries passing laws relating to online safety and child protection. Uganda passed the Anti-Pornography Act, which we hope will assist in reducing CSAM. Similarly, South Africa amended its Film and Publication Amendment Act that includes a regulation on online content, which requires internet service providers to ensure children are protected from harmful content such as CSAM.
- The African Union has consulted perspectives from businesses, civil society and academia to develop policy frameworks on data and digital identities. This inclusive multi-stakeholder approach resulted in workable frameworks that encourage innovation through data sharing and cross-border data flows for African e-commerce while protecting the rights of individuals. These African Union frameworks on data and digital identities are important cornerstones to build an African digital single market, the vision of the Smart Africa Alliance that is endorsed by all members of the African Union[2] .
- States are struggling to deal with misinformation, disinformation, hate speech and fake news. This struggle has adversely impacted digital human rights. Countries have implemented mandates to curtail these issues. While some of these mandates are necessary, others are a response to the absence of effective forms of controls for harmful or illegal online content[3].
- A growing number of countries on the continent are collecting biometric data digitally. However, these programmes pose new risks to the realisation and enjoyment of human rights and freedoms. These digital programmes enable the capture of biometric information of their citizens for various purposes such as issuance of national identity cards, biometric voter registration, national e-passport initiatives, refugee registration and mandatory biometric SIM card registration. In order to accomplish these programmes, sensitive personal data of millions of citizens must be collected and processed, and that data must be protected from a technical, legal, regulatory and procedural perspective[4]. This includes programmes such as biometric registration of SIM cards. Regulators require telecommunication operators to register the SIM cards of subscribers in a bid to curb insecurity and crimes. While this is understandable, it has negative unintended consequences for undocumented users as it inevitably denies them access to telephone services. There is also a risk that some of the data can be used for nefarious purposes such as surveillance.

[1] https://blogs.worldbank.org/africacan/equipping-leaders-tools-digital-transformation
[2] Ibid.
[3] https://www.ahrlj.up.ac.za/simiyu-ma
[4] https://cipesa.org/2022/09/state-of-internet-freedom-in-africa-2022-the-rise-of-biometric-surveillance/

Benin

MTN has been present in Benin since 2006 and has approximately 7.6 million subscribers. In 2022, MTN's revenue in Benin was R6.7 billion.

Lawful interceptions
Regulatory framework:

- Law No. 2012-15 of 18 March 2013 on the Code of Criminal Procedure in the Republic of Benin amended by Law 2018-14 of 14 February 2018 and Law No. 2020-23 of 29 September 2020.
- Law No. 2015-07 of 20 March 2015 – Carrying information and communication code in the Republic of Benin.
- Law No. 2015-08 of 8 December 2015 – Bearing the child code in the Republic of Benin.
- Law No. 2017-08 of 19 June 2017 – Identifying individuals in the Republic of Benin.
- Law No. 2017-20 – Digital Code in the Republic of Benin.
- Law No. 2016-36 of 23 January 2017 – Regulation of credit information bureaus in the Republic of Benin.
- Law No. 2017-44 of 5 February 2018 – Collection of intelligence in the Republic of Benin.
- Law No. 2018-17 of 25 July 2018 – The fight against money laundering and the financing of terrorism in the Republic of Benin, amended by Law No. 2020-25 of 2 September 2020.
- Law No. 2020-08 of 23 April 2020 – The modernisation of justice.
- Law No. 2020-34 of 10 December 2020 – The simplification and dematerialised management of civil status.
- Decree No. 2006-752 of 31 December 2006 – Establishing, attributions, organisation and functioning of the National Unit for the Processing of Financial Information.

Benin continued

Lawful interceptions continued
Regulatory framework:

- Instruction No. 002-01-2015 of 13 January 2015 – Procedures for obtaining the customer's consent by data providers to the Credit Information Offices within the framework of the credit information sharing system in the WAMU member states.
- Instruction No. 005-05-2015 of 8 May 2015 – Methods of transmission of information on Credit-to-credit Information Offices.
- Instruction No. 007-05-2015 of 8 May 2015 – Methods of receiving and processing customer complaints by the Credit Information Offices.
- Instruction No. 009-06-2015 of 15 June 2015 – Security systems of the information systems of the Credit Information Offices.
- Decree No. 2016- 465 of 3 August 2016 – The obligation to identify subscribers to electronic communications networks and services in the Republic of Benin.
- Decree No. 2018-206 of 6 June 2018 – The attributions, organisation and functioning of the National Agency for the Identification of Persons.
- Decree No. 2018-471 of 4 July 2018 – Defining the modalities and operation of the administrative framework for carrying out registration by way of exception to the civil status and setting the rules relating to the dematerialisation of documents.
- Decree No. 2019-216 of 31 July 2019 – Setting the terms of granting licences, authorisations and conditions for making the declaration relating to the exercise of communications activities.
- Decree No. 2020-187 of 11 March 2020 – Authorising the collection and processing by the Republican Police of personal data of travellers at the borders of Benin.
- Decree No. 2020-249 of 22 April 2020 – Conditions for identifying users of electronic communications services.
- Decree No. 2020-281 of 13 May 2020 – Fixing the conditions for establishing and operating Internet of Things networks and services in the Republic of Benin.
- Decree No. 2014-418 of 4 August 2014 – Establishing the National Unit for Analysis and Intelligence on Terrorism.
- Decree 2021-051 of 3 February 2021 – Fixing the limit values of exposure to electric, magnetic and electromagnetic fields and the modalities of control and inspection of radioelectric equipment and installations.
- Decision No. 2021-360 of 20 December 2021 – Establishing the procedure for approval of equipment, national and international laboratories, and the conditions for recognition of standards and technical specifications in Benin.
- The African Charter on Human and People's Rights.
- Decree No. 2021-375 of 14 July 2021 approving the National Radio Frequency Plan in the Republic of Benin.
- Decree No. 2021-550 of 27 October 2021 approving the security policy rules for state information systems in the Republic of Benin.
- Decision No. 2022-0248 laying down the perimeters and security measures and the camouflage rules of radio sites in the Republic of Benin.
- Decision No. 2022-082 laying down 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 on 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 '.bi' 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.

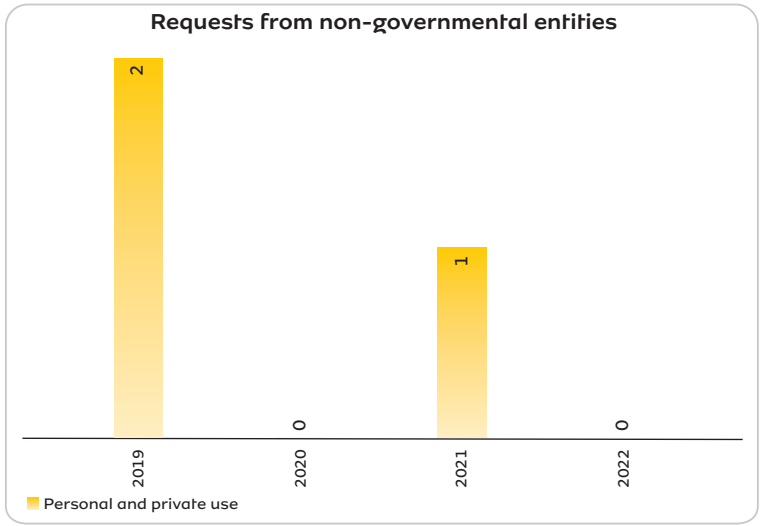
Authorities:

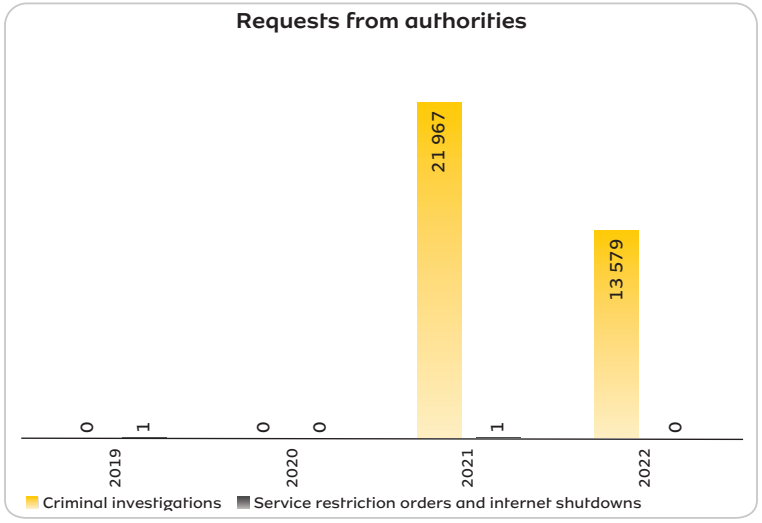
- Ministry of Justice.
- Human Rights Commission of Benin.
- Constitutional Court.
- Courts and tribunals of the country.
- Digital and Communication Ministries.
- Economic Crimes and Terrorism Court.
- Information Systems and Digital Agency (ASIN).
- Authority of Post and Electronics Communication.
- Regulatory Authority.
- Personal Data Protection Authority.
- National Financial Information Processing Units.
- General Directorate of The Republican Police.
- National Personal Identification Agency.
- Ministry Of Economy and Finance.
- Ministry in Charge of The Interior and Public Security and Cultures.
- Ministry in Charge of National Defence.

Impact assessment:

- Progress has been made to socialise the MTN Digital Human Rights Policy among key staff. MTN Benin is developing a localised toolkit to promote greater adherence to the policy and increase capacity of relevant teams.
- Information security is a high priority for MTN Benin and it has been heavily invested in this, including measures to limit risk of potential data breaches. There is a priority on Fintech and digitisation.
- SRO are infrequent.
- Civil society support MTN's efforts and progress, but would welcome greater transparency on requests that MTN receives, and more collaboration. It encourages MTN to use its position to help shape public policy debate.

Benin continued





Cameroon

MTN has been present in Cameroon since 2000 and has approximately 10.7 million subscribers. In 2022, MTN's revenue in Cameroon was R7.8 billion.

Lawful interceptions
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 Cyber Criminality.
- Law No. 2010/021 of 21 December 2010 relating to electronic commerce in Cameroon.
- Decree No. 2013/0399/PM of 27 February 2013 Laying down 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.
- Decree No. 2017/2580/PM of 6 April 2017 laying down conditions for the establishment and exploitation of electronic communication networks that are subject to the regime of authorisation.
- Law No. 2015/007 of 20 April 2015 governing audiovisual activities in Cameroon.

Cameroon continued

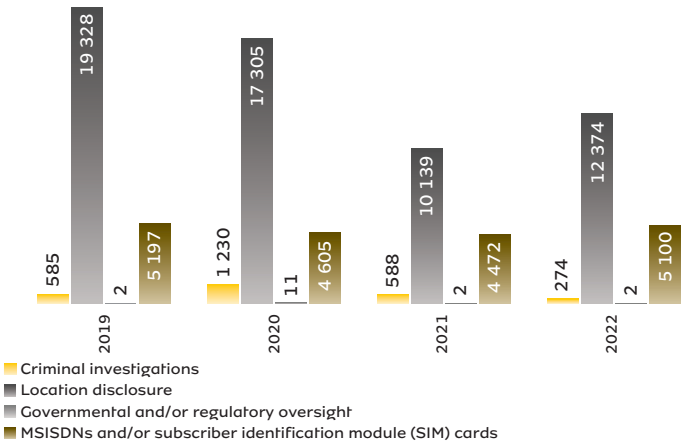
Authorities:

- Minister of Posts and Telecommunications.
- Telecommunications Regulatory Board.
- National Agency of Information and Communications Technology.

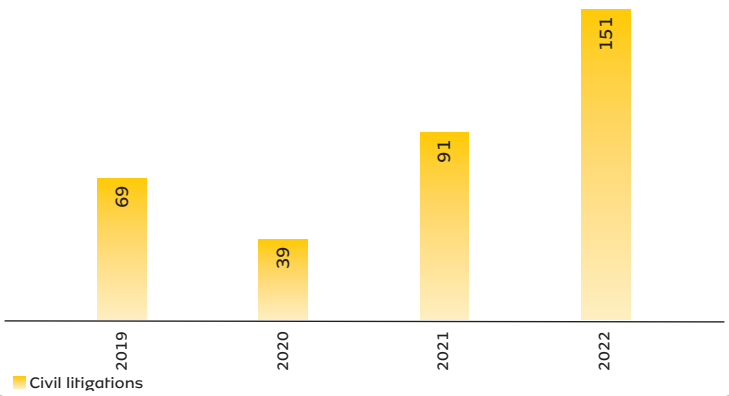
Impact assessment:

- Cameroon needs to prioritise localisation of the Digital Human Rights Policy and ensure greater understanding of the policy among staff.
- Information security is a high priority for the business and it has heavily invested in this, including measures to limit risk of potential data breaches. Child protection online is another priority.
- Civil society is increasingly targeted online and SROs are limited but becoming more frequent.
- Digital literacy skills among the population remain low, exacerbating the threat of end-user security vulnerabilities.
- There is government action to increase access to the internet, which remains mainly urban. Affordability is a limiting factor.
- Civil society support MTN's efforts and progress, but would welcome greater transparency on requests that MTN receives, and more collaboration. It encourages MTN to use its position to help shape public policy debates, and to push back more on SRO requests.
- There has been good progress made on collaborative efforts between MTN and civil society on children and women's rights.

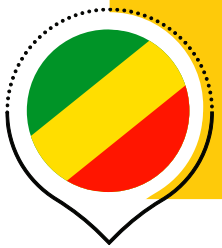
Requests from authorities



Requests from non-governmental entities



Congo-Brazzaville



MTN has been present in Congo-Brazzaville since 2005 and has approximately 3.3 million subscribers. In 2022, MTN's revenue in Congo-Brazzaville was R3.4 billion.

Lawful interceptions
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 of information system security.
- Law No. 26-2020 of 5 June 2020 on cybersecurity.
- Law No. 27-2020 of 5 June 2020 on fighting cybercrime.
- Law 43-2020 of 20 August 2020 authorising the ratification of the convention of the African Union on cybersecurity and the protection of personal data.
- Article 18-20 of Law No. 073/84 of 17 October 1984 on Family Code.

Congo-Brazzaville continued

Lawful interceptions continued

Regulatory framework:

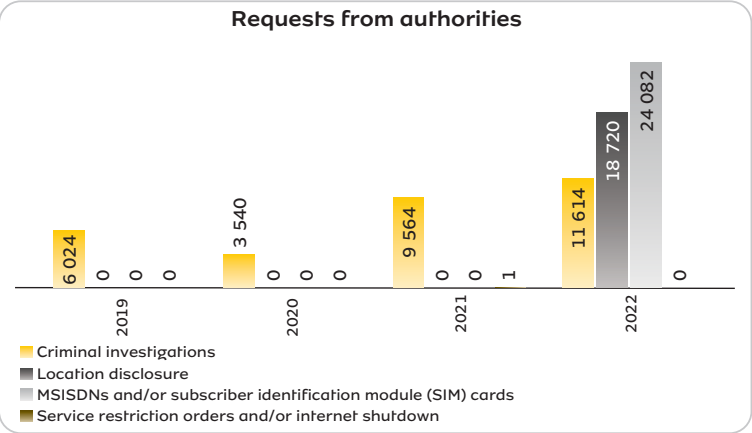
- Article 26 of the Constitution of the Republic of the Congo of 6 November 2015.

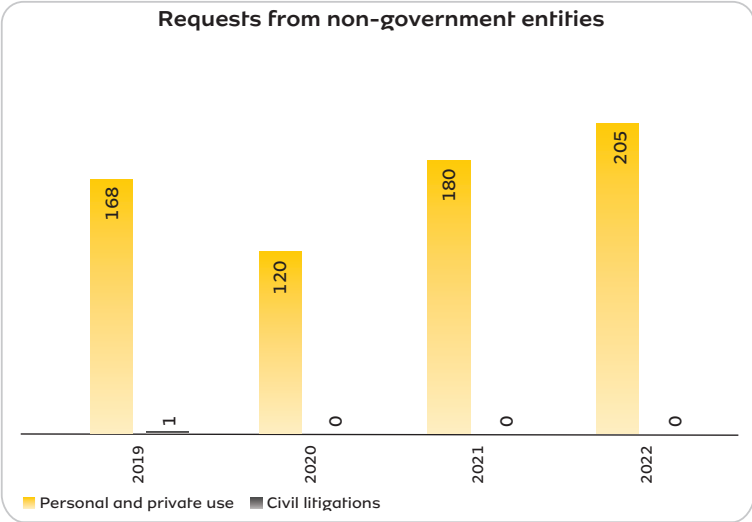
The Republic of Congo is one of six member countries of the Central African Economic and Monetary Community (CEMAC). As such, at a regional level, digital human rights are regulated by the CEMAC through:

- Directive No. 06/08-UEAC-133-CM-18 defining the regime of universal service in the electronic communications sector among CEMAC state members.
- Directive No. 07/08-UEAC-133-CM-18 defining the regulatory 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 state members.
- Directive No. 09/08-UEAC-133-CM-18 harmonising the regulatory framework of electronic communication activities in CEMAC state members.
- Directive No. 10/08-UEAC-133-CM-18 harmonising the rules of establishing and controlling tariffs for electronic communication services in the CEMAC.
- Directive No. 21/08-UEAC-133-CM-18 harmonising the rules and regulations of electronical communication in the CEMAC.

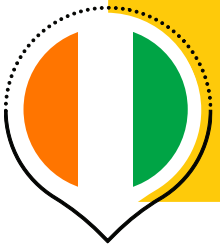
Authorities:

- l'Agence de Régulation des Postes et des Communications. Electroniques du Congo-Brazzaville (ARPCE).
- National Agency of Information System Security (ANSSI).
- Directions Générale des Postes et Télécommunications, (DGPT).
- Central Bank.





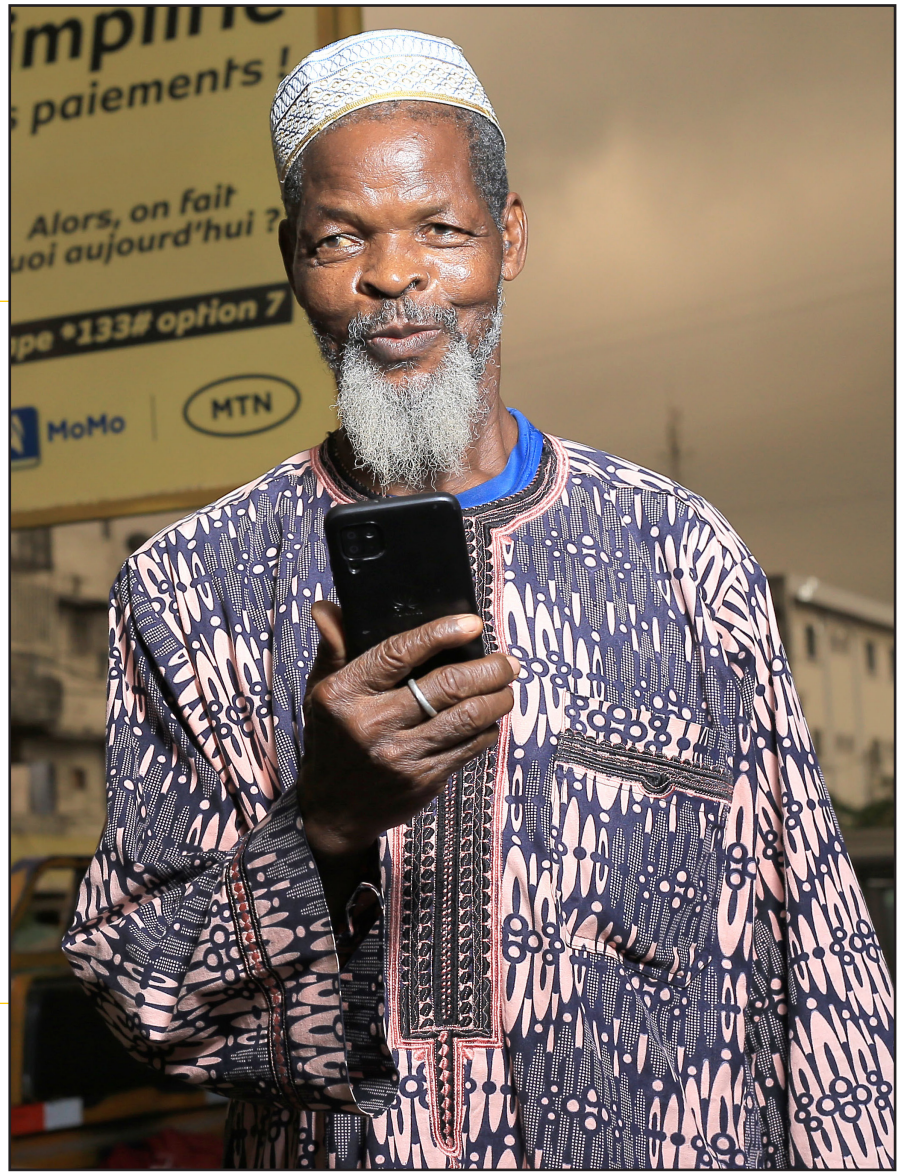
Côte d'Ivoire



MTN has been present in Côte d'Ivoire since 2005 and has approximately 16.3 million subscribers. In 2022, MTN's revenue in Côte d'Ivoire was an estimated R8.9 billion.

Lawful interceptions
Regulatory framework (at the national level):

- Order No. 2012-293 of 21 March 2012 relating to Telecommunications and Information and Communication Technologies.
- Law No. 2013-450 of 19 June 2013 on the protection of personal data.
- Law No. 2013-451 of 19 June 2013 on the fight against cybercrime.
- Law No. 2013-546 of 30 July 2013 on electronic transactions.
- Law No. 2017-802 of 7 December 2017 on the orientation of the information society in Côte d'Ivoire.
- 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 C 1 A, 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 (CNDSI).
- 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.



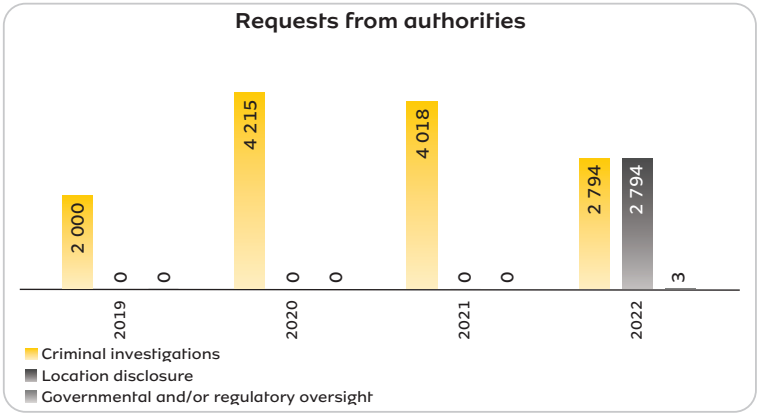
Côte d'Ivoire continued

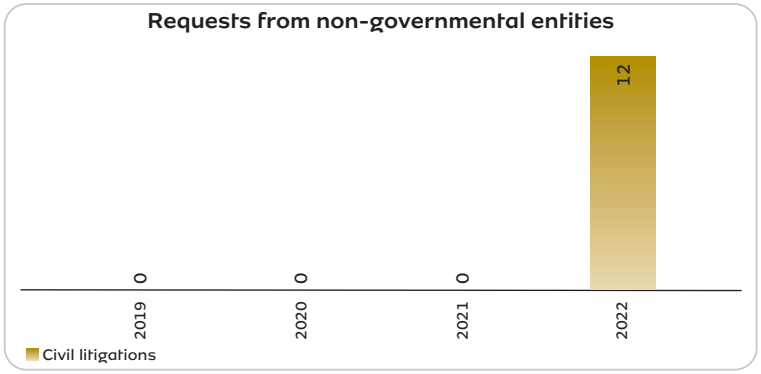
Lawful interceptions continued
Regulatory framework (at the community level):

- Directive No. 02/2006/CM/UEMOA on the harmonisation of regulatory regimes applicable to telecommunication network operators and service providers.
- Additional Act A/SA. 3/01/07 ECOWAS of 19 January 2007 on the regulatory regime applicable to operators and service providers.

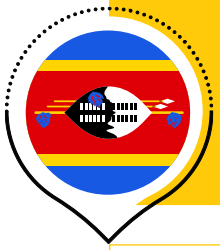
Authorities:

- Autorité de Régulation des Télécommunications/ICT de Côte d'Ivoire (ARTCI).
- Agence Ivoirienne de Gestion des Fréquences radioélectriques (AIGF).
- Agence Nationale du Service Universel des Télécommunications (ANSUT).
- Platform for Combating Cybercrime (PLCC).
- Ministry of Justice and Human Rights.
- Ministry of Security.
- Ministry of Defence.
- Police administrations.





eSwatini



MTN has been present in eSwatini since 1998. The joint venture has approximately 1.0 million subscribers. In 2022, MTN's revenue in eSwatini was R0.5 billion.

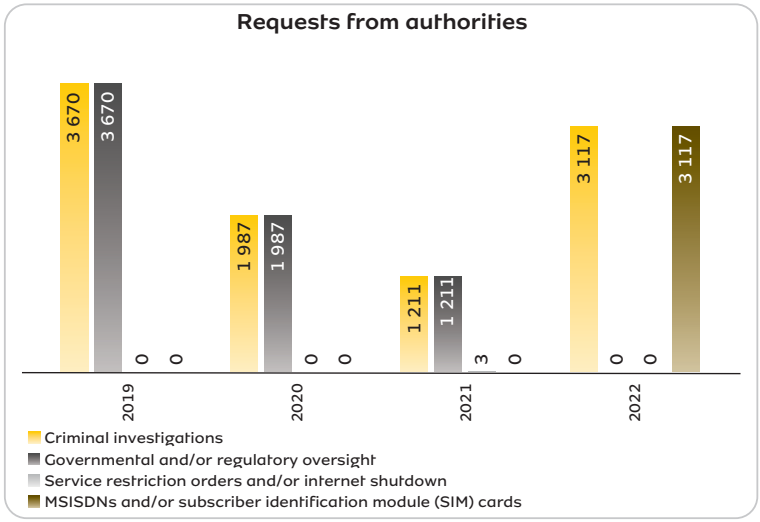
Lawful interceptions
Regulatory framework:

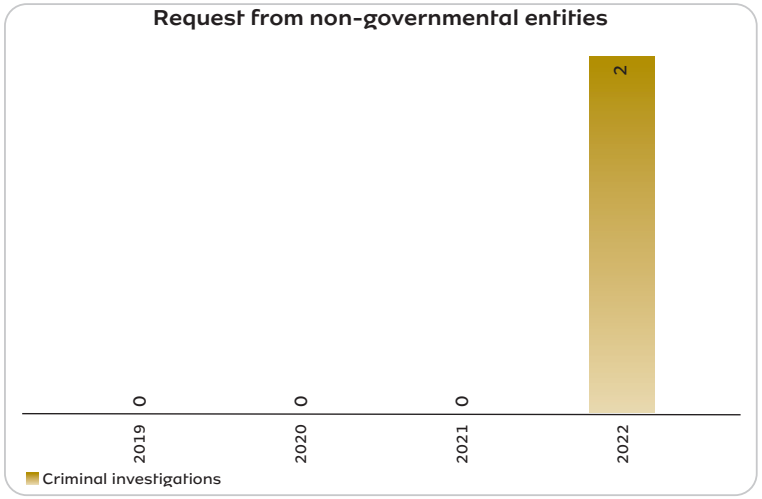
- Swaziland Communications Commission Act 10/2013.
- Electronic Communications Act 09/2013.
- Swaziland Communications Commission (Consumer Protection) Regulations, 2016.
- Swaziland Communications Commission (Subscriber Registration) Regulations, 2016.
- Television Guidelines, 2017.
- Data Protection Bill, 2020.
- Computer Crime and Cybercrime Bill, 2017.
- Section 18 of the Constitution (Protection from Inhumane Treatments) of the Kingdom of eSwatini Act 001/2005.
- Section 24(1) and 24(2) of the Constitution of the Kingdom of Swaziland Act 1, 2005.
- Section 49(1) of the Criminal Procedure and Evidence Act, 1938.
- Data Protection Act, 2022.
- Computer Crime and Cybercrime Act, 2022.
- Electronic Communications Transactions Act, 2022.

Authorities:

- Ministry of Information, Communication and Technology (ICT).
- Swaziland Communications Commission.
- Courts.

eSwatini continued





Ghana

MTN has been present in Ghana since 2006 and has approximately 28.6 million subscribers. In 2022, MTN's revenue in Ghana was R18 billion.

Lawful interceptions Regulatory framework:

- 1992 Constitution.
- Cybersecurity Act 2020 ((Act 1038).
- Electronic Communications Act 2008, (Act 775).
- Electronic Transactions Act 2008, Act 778.
- Data Protection Act 2012 (Act 843).
- Electronic Communications Regulations, 2011.
- Establishment of Emergency Communications System Instrument, 2020 (EI 63).
- Directive for the Protection of Critical Information Infrastructure (CII).
- Revenue Administration Act 2016, (Act 915).
- Electronic Transfer Levy (E-Levy) Act, 2022, Act 1075.
- Electronic Transfer Levy (E-Levy) (Amendment) Act 2022 (Act 1089).
- Right to Information Act 2019 (Act 989).
- Anti-Terrorism Act, 2008 (Act 672).
- SIM Registration Regulations LI 2006.
- Criminal Offences Act 1960 (Act 29).
- Communication Service Tax Act, 2008 (Act 758).

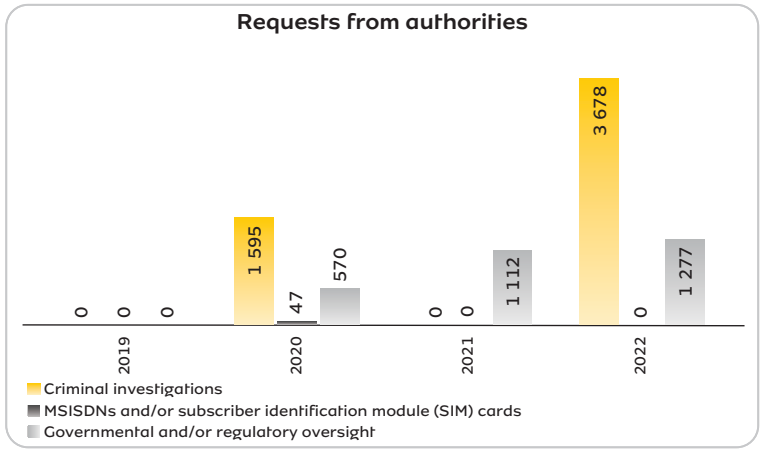
Authorities:

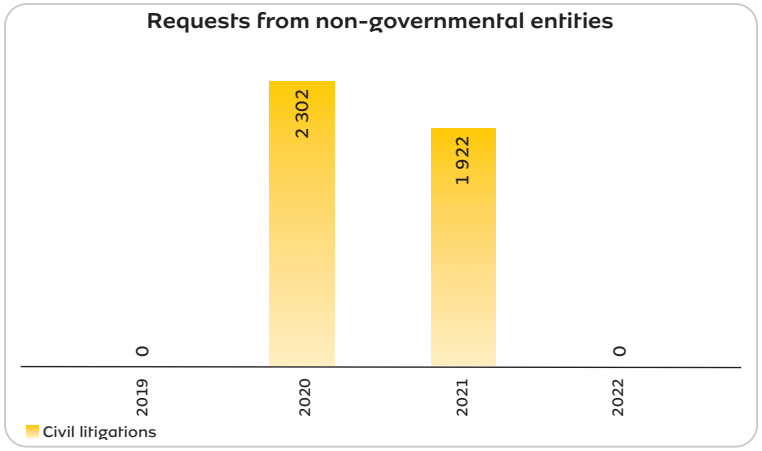
- National Communications Authority.
- Cybersecurity Authority.
- National Information Technology Agency.
- Data Protection Commission.
- Financial Intelligence Centre.
- Economic and Organised Crime Office.
- The Bank of Ghana.
- The Courts.
- Security, Law Enforcement, and Intelligence Agencies.
- Ghana Police Service.
- National Intelligence Bureau (formerly Bureau of National Investigations).
- National Signals Bureau.
- Ghana Prisons Service.
- Ghana Immigration Service.
- Ghana Armed Forces.

Impact assessment:

- The MTN Digital Human Rights Policy was adopted by MTN Ghana in 2021 and implementation, including localisation and awareness creation, is ongoing.
- Information security is a high priority for the business and it has been heavily investing in this. Child protection online is another priority.
- Traditional human rights are emphasised by civil society, but awareness of digital human rights is growing.
- The Cybersecurity Act 2020 (Act 1038) introduced lawful interception, but it is not yet operational. MTN Ghana receives increasing requests for subscriber data and complies with lawful requests. MTN Ghana demonstrated good practice by pushing back against overly broad and unlawful requests for customer data.
- There may be privacy challenges associated to the storage of SIM registration data in the Central Subscriber Identity Module Register. Governance to regulate government, law enforcement and third-party access to this data is not within the control of MTN or other operators.
- There is collaboration between government and MTN to increase access to the internet, which remains mainly urban. Affordability is a limiting factor, compounded by the introduction of a new tax.
- Relationships between MTN, civil society and the government are good, with civil society an effective ally to hold the government and industry accountable.
- Civil society support MTN's efforts and progress, while encouraging MTN Ghana to engage more directly with the regulator on data requests.

Ghana continued





Requests from the Courts, previously reported under non-governmental entities have been reclassified in the 2022 report.

Guinea-Bissau

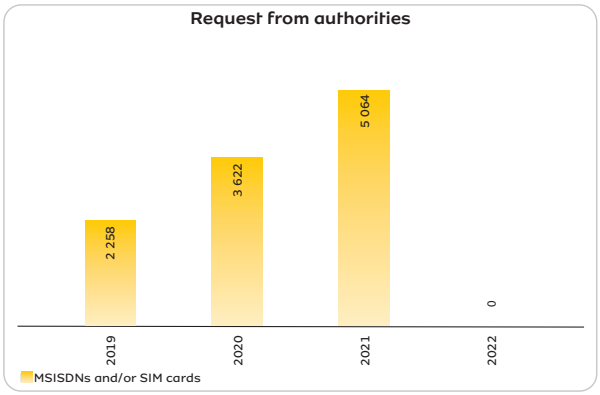
MTN has been present in Guinea-Bissau since 2005 and has approximately 0.8 million subscribers. In 2022, MTN's revenue in Guinea-Bissau was R0.3 billion.

Lawful interceptions Regulatory framework:

- Constitution of the Republic of Guinea-Bissau.
- Resolution 2/2018, of 25 June 2018 – Approval of government programme and initiatives.
- Law 5/2010, of 27 May 2010 – Information Technology and Communications Framework Law.

Authorities:

- Autoridade Reguladora Nacional.
- Conselho Nacional Da Comunicação Social.
- Criminal courts.
- Government of the Republic of Guinea-Bissau.



Unable to retrieve data due to technical difficulties.

Guinea-Conakry

MTN has been present in Guinea-Conakry since 2005 and has approximately 3.1 million subscribers. In 2022, MTN's revenue in Guinea-Conakry was R1.7 billion.

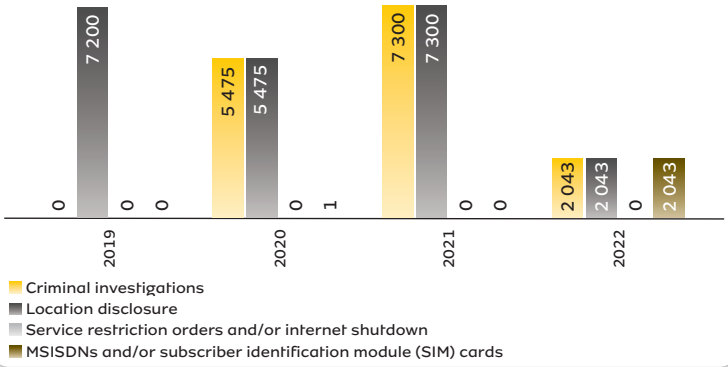
Authorities:

- L'Autorité de Régulation des Postes et Télécommunications (Regulatory body).

Lawful interceptions
Regulatory framework:

- 2020 Guinean Constitution under its Title II- Rights – Freedom and Duties.
- Law L/2016/059/AN dated 26 October 2016, carrying on Criminal Code of the Republic of Guinea under Title III – Cybercriminality (Act 856 to Art. 879).
- Law 2015/018/AN related to telecommunication and technologies of information in Republic of Guinea under Article 116 dated 13 August 2015.
- African Union Convention on Cybersecurity and the Protection of Personal Data dated 14 June 2014.
- Additional Act A/SA.1/01/10 related to protection of personal data in ECOWAS area dated 16 February 2010.
- Law L/2016/037/AN related to cybersecurity and the protection of personal data in Republic of Guinea dated 16 July 2016.

Requests from authorities



Liberia

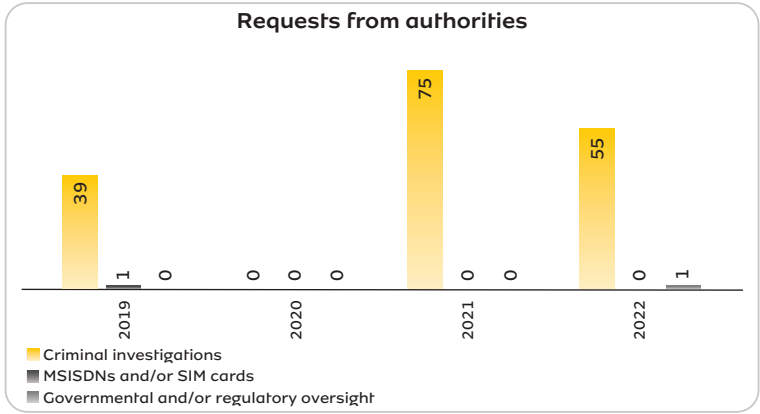
MTN has been present in Liberia since 2005 and has approximately 2 million subscribers. In 2022, MTN's revenue in Liberia was R1.5 billion.

Lawful interceptions
Regulatory framework:

- Article 15 of the Liberian Constitution (1986).
- Telecommunications Act, 2007.
- Supplementary Act A/As. 1/01/10 on Personal Data Protection within ECOWAS.
- Amended SIM cards/removable user identity module registration regulations.
- Liberia's country code Top Level Domain (ccTLD). Regulation for its Re-delegation, Management and Operations, 2020.
- Regulations for the Treatment of Confidentiality, Dispute Resolution, Compliance and Enforcement 2009 LTA-Reg-0002.
- Regulation C/Reg. 21/12/17 on Roaming on Public Mobile Communications Network in the ECOWAS region.
- Interconnection Regulations 2009 LTA-Reg-0003.
- LTA Order: 0018-01-15-20 on the 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.
- Regulations on International Traffic LTA-Reg-0005.
- B. Draft Laws/regulations.
- Draft Summary Regulation on National Numbering Plan LTA-Reg-007.

Authorities:

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



Nigeria

MTN has been present in Nigeria since 2001 and has approximately 76 million subscribers. In 2022, MTN's revenue in Nigeria was an estimated R77.3 billion.

Lawful interceptions Regulatory framework:

- Section 37 of the Constitution of the Federal Republic of Nigeria, 1999.
- NDPR Implementation Framework, 2020.
- Cybercrime (Prohibition, Prevention, etc.) Act 2015.
- Consumer Code of Practice Regulations, 2007.
- Section 39 of the Constitution of the Federal Republic of Nigeria, 1999.
- Criminal Code Act.
- Defamation Law of the various states.
- Penal code and penal laws of the various states.
- National Identity Management Commission Act.
- Nigerian Communications Regulations, 2019.
- Part 3 1-16 of the Nigerian Data Protection Regulation 2019.
- Article 38-45 of the ECOWAS Data Protection Act 2010.
- Article 13-23 of the African Union Convention on Cybersecurity and Data Protection.
- Section 47(1)(e) of the Mutual Assistance in Criminal Matters Act 2019.
- Section 38(5) of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
- Section 8 of the Nigerian Communications (Enforcement Process, etc.) Regulations, 2019.
- Section 20, 26 and 28 of the National Identity Management Commission Act, 2007.
- Child's Right Act, 2003.
- Child's Right Law (of Lagos State) 2007.
- Freedom of Information Act, 2011.
- Lagos State Data Protection Bill, 2021 (LDPB).
- National Information Technology Development Agency Act (Amendment) Bill, 2022.
- Draft Data Protection Bill – There is a new draft Data Protection Bill with executive backing that has been approved by the Federal Executive Council of Ministers for transmission to the legislature. The draft Nigeria Data Protection Bill 2022 seeks to provide the legal framework for the protection of personal data and establish the Nigeria Data Protection Commission for the regulation of the processing of personal data.

Nigeria continued

Regulations, policies and guidelines

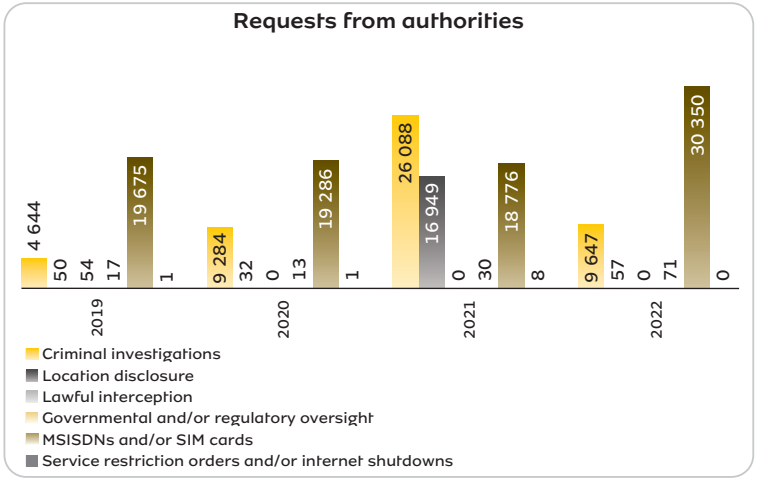
- National Information Technology.
- Development Agency (NITDA): Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries.
- Central Bank of Nigeria: Consumer Protection Regulations 2019.
- Nigerian Communications Commission: Child Online Protection Policy.
- Nigerian Communications Commission: Lawful Interception of Communications Regulations 2019.
- Nigerian Communications Commission: Value-added Services and Aggregator Framework 2018 (amended).
- Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011.

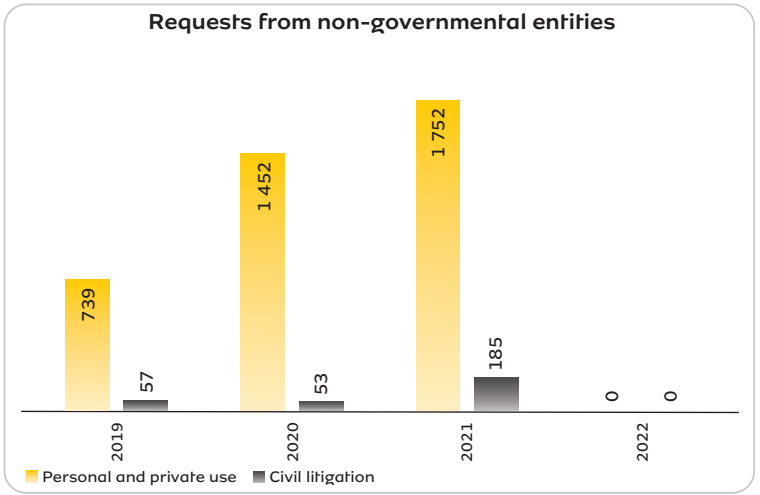
Authorities:

- NITDA.
- Nigerian Police Force.
- Various law enforcement agencies are responsible for the implementation and enforcement of the provisions of the Cybercrime (Prohibition, Prevention, etc.) Act, 2015; however, the office of the National Security Adviser is the coordinating body for all security and enforcement agencies under the Act.
- Nigerian Communications Commission.
- Nigerian courts.
- Relevant authorities defined under section 20 of the Nigerian Communications Regulations, 2019.
- National Identity Management Commission.
- Nigeria Police Force (NFF) and other Law Enforcement Agencies (Nigerian Armed Forces and other Paramilitary establishments).
- Minister of Communications and Digital Economy.
- Federal Competition and Consumer Protection Commission.
- Nigeria Data Protection Bureau (NDPB).

Impact assessment:

- Progress has been made by MTN Nigeria on privacy and data protection, and Digital Human Rights Policy.
- Information security is a high priority for the business and it has been heavily invested in this, including measures to limit risk of potential data breaches. Child protection online is another priority.
- Digital human rights are becoming a priority focus within Nigeria.
- The frequency and length of SROs in the country leads to concern.
- There is government action to increase access to the internet, which remains mainly urban. Affordability is a limiting factor.
- The relationship between MTN and civil society is complex and needs to be continuously improved.





Rwanda

MTN has been present in Rwanda since 1998 and has approximately 6.8 million subscribers. In 2022, MTN's revenue in Rwanda was R3.5 billion.

Lawful interceptions
Regulatory framework:

- The Constitution of Rwanda 2003 with Amendments through 2015.
- Law No. 04/2013 of 8 December 2013 relating to access to information.
- Law No. 24/2016 of 18 June 2016 governing Information and Communication Technologies.
- Law No. 02/2017 of 18 February 2017 establishing Rwanda Information Society Authority and determining its mission, organisation and functioning.
- Law No. 26/2017 of 31 May 2017 establishing the National Cybersecurity Authority and determining its mission, organisation and functioning.
- Law No. 09/2013 of 1 March 2013 establishing Rwanda Utilities Regulatory Authority and determining its mission, organisation and functioning.
- Law No. 60/2018 of 22 August 2018 on Prevention and Punishment of Cybercrimes.
- Law No. 60/2013 of 22 August 2013 regulating the Interception of communications.
- Law No. 02/2013 of 8 February 2013 regulating Media.
- Law No. 73/2018 of 31 August 2018 governing Credit Reporting System.
- Draft Regulation Governing use of Personal data in Rwanda 2019 (this remains in draft form).
- Regulations Governing Cybersecurity of 2020.
- Article 14 of the Regulation governing the Electronic Money Issuers No. 08/2016 of 1 December 2016.
- Regulations on Protection of Payment Service Users (2020) – Article 47.
- Law No. 75/2019 of 29 January 2020 on Prevention and Punishment of Money Laundering, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction (Articles 9–13).

Rwanda continued

Lawful interceptions continued

Regulatory framework:

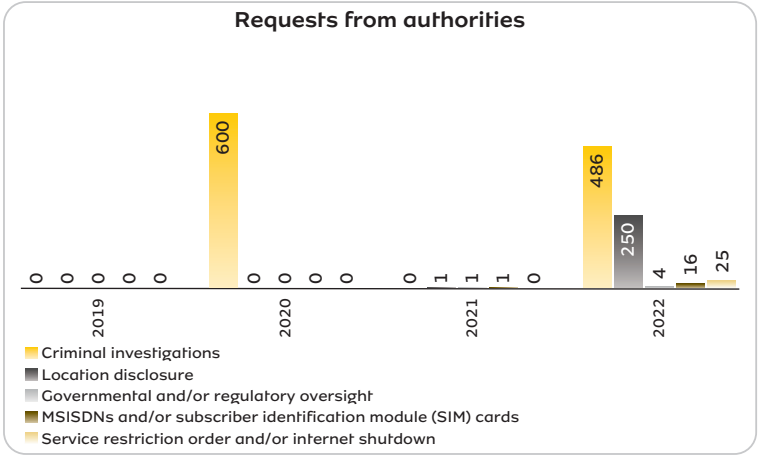
- Law Relating to the Protection of Personal Data and Privacy No. 058/2021 of 13 October 2021.
- Law No 061/2021 of 14 October 2021 governing the payment system.
- Law No 017/2021 of 3 March 2021 relating to financial service consumer protection.
- Article 3.6 of MTN Rwandacell's Individual Licence (July 2021 – under new licensing framework, the former cellular mobile licences are now called individual licences).
- New SIM registration and SIM swap process (July 2021) the amended Regulations that will encompass this process are in draft form, shared this week for consultation.

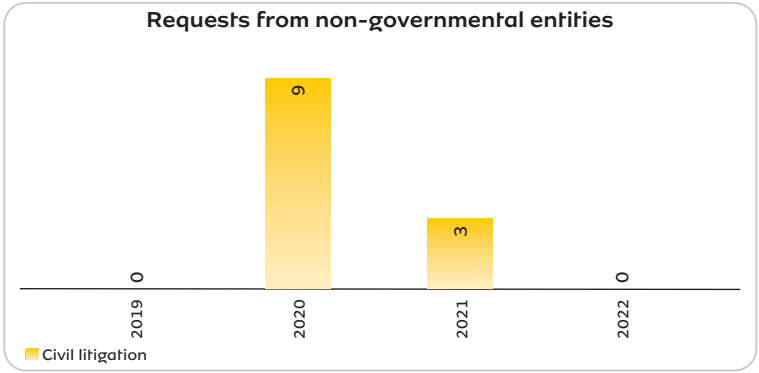
Authorities:

- Rwanda Information Society Authority (RISA) is established by Law No. 02/2017 of 18 February 2017.
- National Cybersecurity Authority (NCSA) is established by Law No. 26/2017 of 31 May 2017.

Impact assessment:

- MTN Rwanda has adopted the Digital Human Rights Policy and is planning its implementation and socialisation.
- Information security is a high priority for the business and it has heavily invested in this, including measures to limit risk of potential data breaches. Child protection online is another priority.
- Digital human rights are not a priority focus as civil society focus on more traditional human rights. However, digitalisation is a priority both for MTN Rwanda and for the government.
- Civil society is increasingly targeted online, and surveillance is increasing.
- Civil society support MTN's efforts and progress but would welcome greater transparency on requests that MTN receives, and more collaboration. It encourages MTN to use its position to help shape public policy debate.





South Africa

MTN has been present in South Africa since 1994 and has approximately 36.5 million subscribers. In 2022, MTN's revenue in South Africa was R50.6 billion.

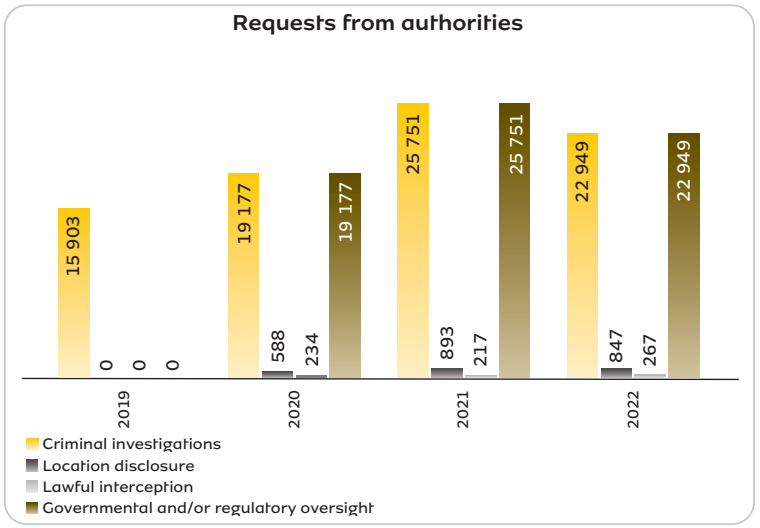
Lawful interceptions
Regulatory framework:

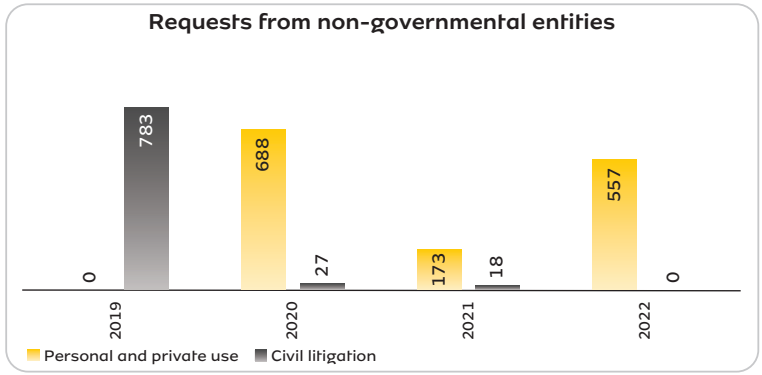
- Constitution of the Republic of South Africa, 1996.
- Promotion of Access to Information Act 2, 2000.
- Regulation of Interception of Communications and Provision of Communication-related Information Act 70, 2002.
- Electronic Communications and Transactions Act 25, 2002.
- Electronic Communications Act 36, 2005.
- Consumer Protection Act 68, 2008.
- Protection of Personal Information Act 4, 2013.
- Cybercrime Act 19, 2020.
- Film and Publication Amendment Act 65, 1996 as amended by the Films and Publications Amendment Act 11, 2019 – Government Notice 1292 in Government Gazette 42743 dated 3 October 2019. Commencement date: 1 March 2022 (Proc. 52 in Gazette 45959 dated 25 February 2022).

Authorities:

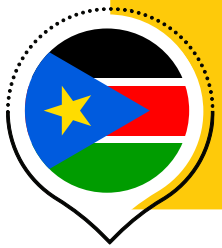
- Department of Justice and Constitutional Development.
- The South African Human Rights Commission.
- National Prosecuting Authority of South Africa.
- South African Police Services.
- South African Defence Force.
- State Security Agency.
- Information Regulator (South Africa).
- Film and Publications Board.
- In addition, the above laws, acts, regulations, the terms of any licence or other regulatory instruments referred to above are interpreted and ruled upon by the South African judiciary, which is a separate organ of State from the executive branch (which operates the above-mentioned state authorities).

South Africa continued





South Sudan



MTN has been present in South Sudan since 2011 and has approximately 2.5 million subscribers. In 2022, MTN's revenue in South Sudan was R2.3 billion.

Lawful interceptions
Regulatory framework:

- Transitional Constitution of the Republic of South Sudan.
- Right of Access to Information Act, 2013.
- National Communication Act, 2012.
- Penal Code, 2008.
- National Communications Licensing Regulations, 2016.
- Media Authority Act 64, 2013.
- Broadcasting Corporation Act 63, 2013.
- National Security Services, 2014.
- Electronic Money Regulations of South Sudan, 2017.
- Anti-money Laundering and Counter Terrorist Financing Act, 2012.

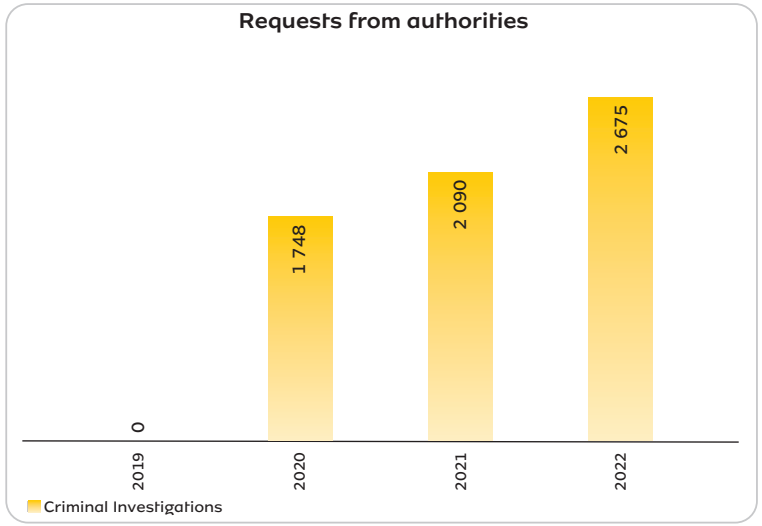
Authorities:

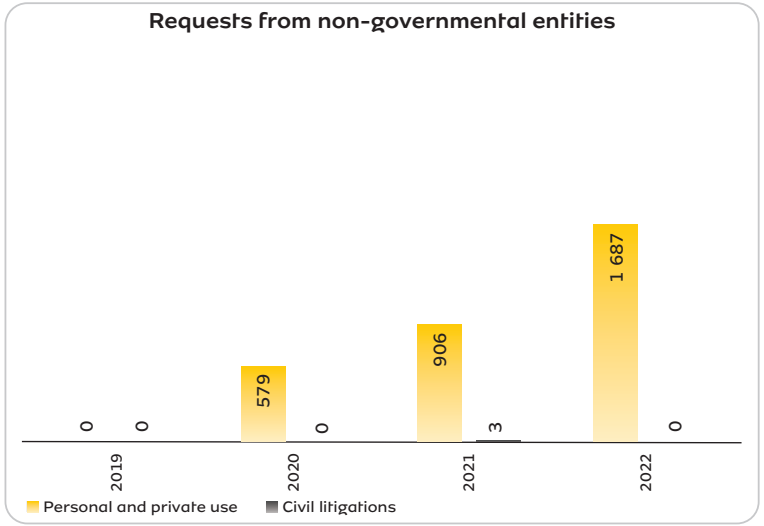
- Ministry of Information Communication Technology and Postal Services.
- Information Commission.
- National Communication Authority.
- High Court.
- Supreme Court.
- Bank of South Sudan.
- Financial Intelligence Unit.

South Sudan continued

Impact assessment:

- MTN South Sudan has approved the Digital Human Rights Policy and is in planning stages of its implementation and socialisation.
- Information security is a high priority for the business and it has heavily invested in this, including measures to limit risk of potential data breaches. Child protection online is another priority.
- Digital human rights are not a priority focus as civil society focuses more on traditional human rights.
- Civil society is increasingly targeted online and SROs are limited but becoming more frequent.
- Fraudulent behaviour online by external actors poses a threat to safeguarding users' data.
- Access to the internet remains mainly urban. Affordability is a limiting factor, as well as lack of infrastructure.
- Civil society supports MTN's efforts and progress but would welcome greater transparency to better understand the requests that MTN receives. It would welcome more collaboration with MTN and encourages MTN to use its brand and market position to help shape public policy debates. The public does not understand pressures that can be applied to MTN.





Sudan

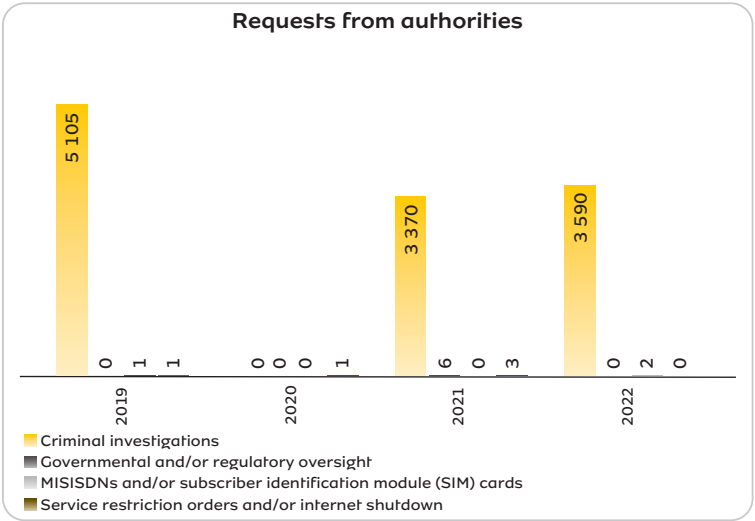
MTN has been present in Sudan since 2005 and has approximately 9.0 million subscribers. In 2022, MTN's revenue in Sudan was R4 billion.

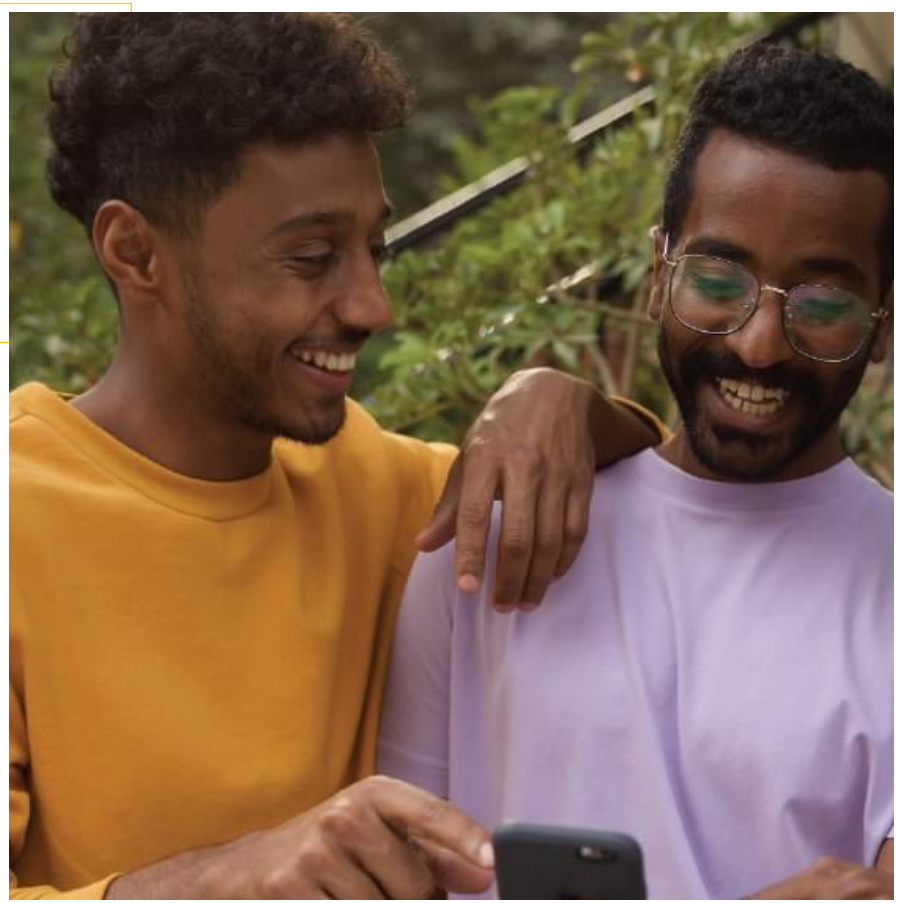
Authorities:

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

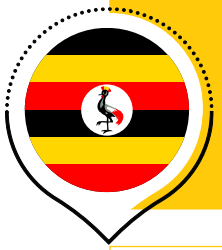
Lawful interceptions
Regulatory framework:

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





Uganda



MTN has been present in Uganda since 1998 and has approximately 17.1 million subscribers. In 2022, MTN's revenue in Uganda was R10.1 billion.

Lawful interceptions Regulatory framework:

- Article 27(2) and 29 of the Constitution of the Republic of Uganda, 1995.
- The Uganda Communications Act, 2013.
- The National Payment Systems Act, 2020.
- The Anti-Money Laundering Act, 2013 (as amended).
- Sections 2, 3, 4, 8, 10, 11 and 15 of the Regulation of Interception of Communications Act, 2010.
- Sections 7, 9 and 29 Data Protection and Privacy Act, 2020.
- Sections 10, 11, 24, 25 and 26 of the Computer Misuse Act, 2011.
- Section 32(2) of the Electronic Transactions Act, 2011.
- Section 17 of the Anti-Pornography Act, 2014.
- Sections 18 and 19 of the Anti-Terrorism Act, 2002.
- Sections 88 and 91 of the Electronic Signatures Act, 2011.
- The Data Protection and Privacy Regulations, 2020.
- The Uganda Communications (Intelligent Network Monitoring System) Regulations, 2019.
- Uganda Communications (Centralised Equipment Identification Register) Regulations 2019.
- The Uganda Communications (Text and Multimedia Messaging) Regulations, 2019.
- The Uganda Communications (Consumer Protection) Regulations, 2019.
- The Uganda Communications (Content) Regulations, 2019.
- The Uganda Communications (Emergency Response) Regulations, 2019.
- The Uganda Communications (Computer Emergency Response Team) Regulations, 2019.

Authorities:

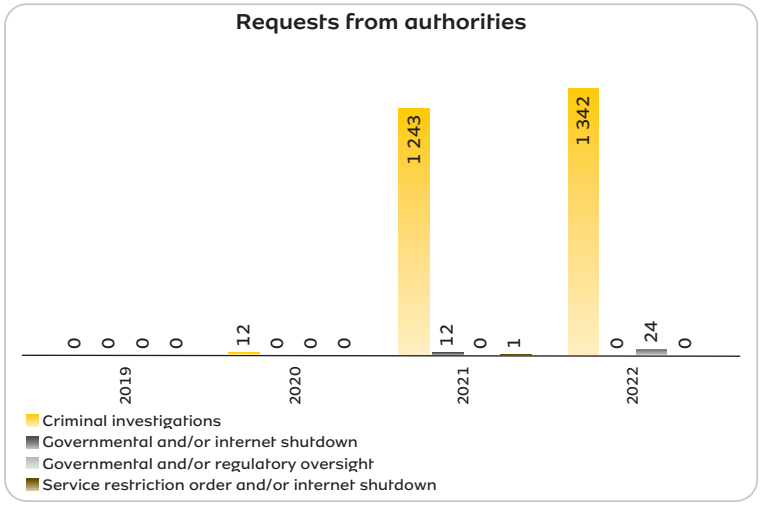
- Uganda Police Force
- Uganda Communications Commission
- National Information Technology Authority
- Central Bank of Uganda
- Ministry of Internal Affairs
- The Ministry of Information, Communications, Technology and National Guidance
- Financial Intelligence Authority
- Personal Data Protection Office
- Uganda's People Defence Forces
- Internal Security Organisation
- External Security Organisation
- Courts of law

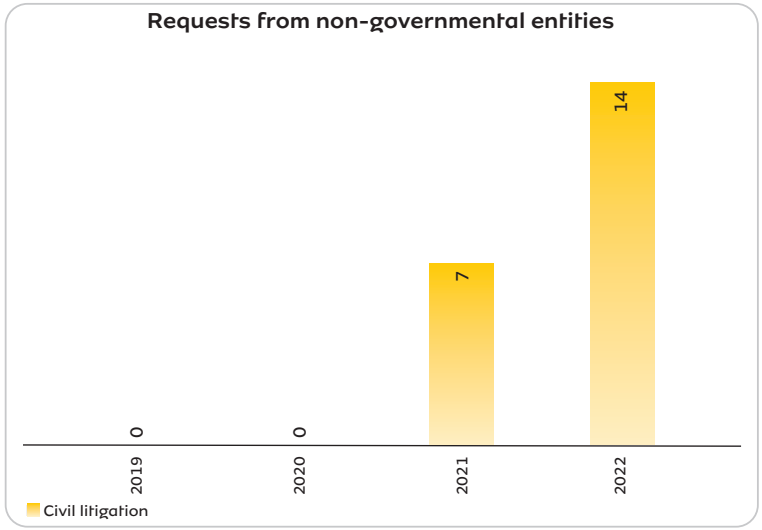
Impact assessment:

- Progress has been made to socialise the MTN Digital Human Rights Policy among key staff.
- Information security is a high priority for the business and it has heavily invested in this. Child protection online is another priority.
- Civil society is increasingly targeted online, and SROs are limited but becoming more frequent.
- Affordability hampers access to internet, particularly in rural areas. This was compounded by the introduction of a new tax on internet access.
- Civil society supports MTN's efforts but would welcome increased transparency.

In recent years, MTN has made significant strides in establishing digital human rights frameworks, policies and escalation processes, as noted by the DHRIAs. The DHRIAs emphasised that the Company is shifting in the right direction in advancing the implementation and monitoring of these frameworks, policies and processes.

Uganda continued





Zambia

MTN has been present in Zambia since 2005 and has approximately 7.1 million subscribers. In 2022, MTN's revenue in Zambia was R3.3 billion.

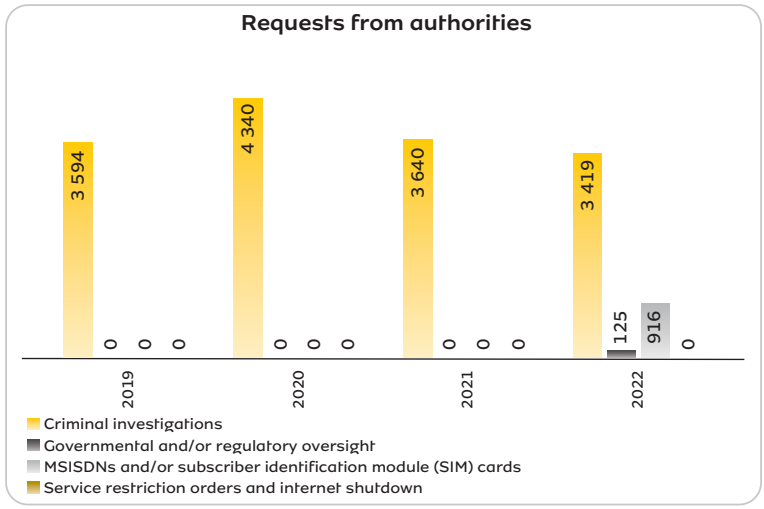
Lawful interceptions
Regulatory framework:

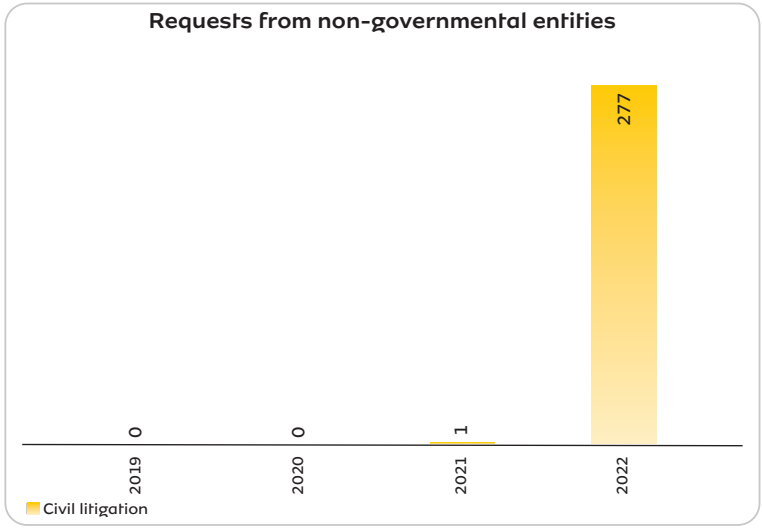
- Constitution of Zambia (Amendment) Act No. 2, 2016.
- The Cybersecurity and Cyber Crimes Act No. 2, 2021.
- The Electronic Communications and Transactions Act No. 4, 2021.
- The Data Protection Act No. 3, 2021.
- The Financial Intelligence Centre Act No. 46, 2010.
- Zambia Information and Communication Technology Agency Network Licence Standard Terms and Conditions.
- Statutory Instrument No. 80, 2015.
- The Information and Communication Technologies (Telecommunication Traffic Monitoring) Regulations issued pursuant to the Electronic Communications and Transactions Act No. 21, 2009.
- Children's Code Act No. 12, 2022.
- Regulation 40 of The Electronic Communications and Transactions (General) Regulations, Statutory Instrument 71, 2011 issued pursuant to the Electronic Communications and Transactions Act No. 21, 2009.

Authorities:

- Zambia Information and Communication Technology Agency established under the Information and Communication Technologies Act No. 15, 2009.
- Zambia Police Service established under the Constitution.
- Anti-Corruption Commission established under the Anti-Corruption Act No. 3, 2012.
- Zambia Security Intelligence Service established under the Zambia Security Intelligence Service Act, Chapter 109 of the Laws of Zambia.
- Drug Enforcement Commission.
- Human Rights Commission.
- Financial Intelligence Centre.
- Anti-Money Laundering Investigations Unit.
- Zambia Revenue Authority.
- Child Development Department.

Zambia continued





Glossary

Explanations of acronyms and terms:

Term	Definition
Human rights impact assessment (HRIA)	An HRIA provides a consistent, efficient and systematic way to identify, prioritise and address human rights risks and opportunities at a corporate, country, site or product level. An HRIA is one part of a human rights due diligence system.
Freedom of Expression (United Nations Articles)	The use of digital communications to freely express views, opinions and information, informed by Article 19 of the United Nations Universal Declaration on Human Rights.
Human rights due diligence	A continuous management process to identify, prevent, mitigate and account for how we address the adverse human rights address, manage and remedy potential adverse human rights risks.
ICT	Information and Communication Technology
Information security	As defined in the Group Information Security Policy, information security is the preservation of confidentiality, integrity and availability of information. In addition, other properties such as authenticity, accountability, no-repudiation and reliability can also be involved.
Limitations on freedom of expression	This can assume numerous forms including interception, pausing, disrupting, service blocking, throttling, tracking, surveillance, slowing down or stopping/ shutting down, taking down content or otherwise intentionally disrupting communications from use or transmission for the purposes intended by users. Also see 'SRO'.
Mobile access	Ability to use voice, data, short messaging service (SMS) and internet services and receive, view or respond to communications via mobile networks.
Personal information	Personal information is any factual or subjective information, whether recorded or not, about an identifiable, living natural person, and where applicable, an identifiable, existing juristic person, including but not limited to, information relating to an individual's ethnicity, race, social origin, nationality, colour, sexual orientation, age, disability, religion, conscience, belief, mental and physical wellbeing, colour and marital status; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person; and the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person; and/or Special Personal Information, as defined in the MTN Group Data Privacy and Protection Policy.
Privacy	The reasonable expectation of users that their digital communications and personal information is not used and shared for purposes other than as authorised, and that such communications and information are protected, secured and remain confidential between the user and recipient of communications.
Remedy	Counteract or make good any digital human rights harms that have occurred.
UN Universal Declaration of Human Rights	Thirty articles proclaimed by the United Nations General Assembly on 10 December 1948 as the basic concepts of dignity, liberty and equality for all people and nations.
UN Guiding Principles on Business and Human Rights	Principles universally established by the United Nations in 2011 that set out the duty of governments to ensure protection against human rights violations, the responsibility of corporates to respect human rights, and ensure access to effective judicial and non-judicial remedies for victims of human rights violations.
UN Sustainable Development Goals (UNSDGs)	Goals adopted by all United Nations in 2015 with a vision to end poverty, protect the planet and ensure all people enjoy peace and prosperity by 2030.
Stakeholders	A person, groups of persons or institutions who are directly or indirectly affected by MTN, including those who may have interests in MTN's business activities and/or the ability to influence MTN's business outcomes, either positively or negatively.
Centre for Internet Security	A 501 non-profit organisation, formed in October 2000. Its mission is to make the connected world a safer place by developing, validating and promoting timely best practice solutions that help people, businesses and governments protect themselves against pervasive cyber threats.
Child sexual abuse material (CSAM)	CSAM has different legal definitions in different countries. The minimum defines CSAM as imagery or videos that show a person who is a child and engaged in or is depicted as being engaged in explicit sexual activity.
Digital human rights	Digital technologies provide new means to exercise human rights, but they are too often also used to violate them. Data protection and privacy issues, digital identity, the use of surveillance technologies, online violence and harassment are of particular concern (https://www.un.org/techenvoy/content/digital-human-rights).
GSMA	Global Systems of Mobile Communications
GNI	Global Network Initiative

Glossary continued

Explanations of acronyms and terms:

Term	Definition
Information Security Forum	An independent information security body. Its membership includes Fortune 500 and Forbes 2000 listed corporations to public sector organisations.
IWF	Internet Watch Foundation
JAC	Joint Audit Co-operation
Operating markets	Benin, Cameroon, Congo-Brazzaville, Côte d'Ivoire, eSwatini, Ghana, Guinea-Bissau, Guinea-Conakry, Liberia, Nigeria, Rwanda, South Africa, South Sudan, Sudan, Uganda and Zambia.
Sustainability Network	A non-profit capacity builder that has been serving the environmental non-profit community for almost 25 years.
SRO	Service restriction orders
UNGC	United Nations Global Compact
VASP	Value-added Service Providers
WASP	Wireless Application Service Providers
RDR	Ranking Digital Rights

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^
RT Mupita[1]
TBL Molefe[1]
NP Gosa^
PB Hanratty[2]^
S Kheradpir[3]^
SN Mabaso-Koyana^
SP Miller[4]^
CWN Molope^
N Newton-King^ (appointed 1 January 2023)
T Pennington[5]^ (appointed 1 August 2022)
NL Sowazi^
SLA Sanusi[6]^
VM Rague[7]^

[1] *Executive*
[2] *Irish*
[3] *American*
[4] *Belgian*
[5] *British*
[6] *Nigerian*
[7] *Kenyan*

^ Independent non-executive director
 # Non-executive director

Group Company Secretary

PT Sishuba-Bonoyi
Private Bag X9955, Cresta, 2118

Registered office

216 – 14th Avenue
Fairland
Gauteng, 2195

American depository receipt (ADR) programme

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 2004/003647/070
Rosebank Towers, 15 Biermann Avenue
Rosebank, 2196
PO Box 61051, Marshalltown, 2107

Joint auditors

PricewaterhouseCoopers Inc.
4 Lisbon Lane, Waterfall City, Jukskei View,
Johannesburg, South Africa, 2090

Ernst & Young Inc.
102 Rivonia Road, Sandton, Johannesburg,
South Africa, 2146

Lead sponsor

JP Morgan Equities (SA) Proprietary Limited
1 Fricker Road, cnr Hurlingham Road,
Illovo, 2196

Joint sponsor

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

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
E-mail: investor.relations@mtn.com
Website: http://www.mtn.com
Date of release: 26 April 2023

Forward-looking information

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.

Mapping our SDG impact:

In 2021, MTN Group implemented an SDG prioritisation tool to determine the SDGs and SDG Ambition Benchmarks on which we could deliver the biggest impact, while creating business value. It considers three dimensions – impact potential, strategic alignment and risk management potential – for which scores are attributed against defined qualitative criteria. The tool considers various internal and external assessments such as our risk register and industry research. It also incorporates stakeholder views collected through surveys, workshops and materiality assessments. The results are then refined to ensure alignment with our strategy.

www.mtn.com

Tel: +27 83 869 3000/+27 11 912 3000
Innovation Centre
216 14th Avenue
Fairland, 2195
South Africa