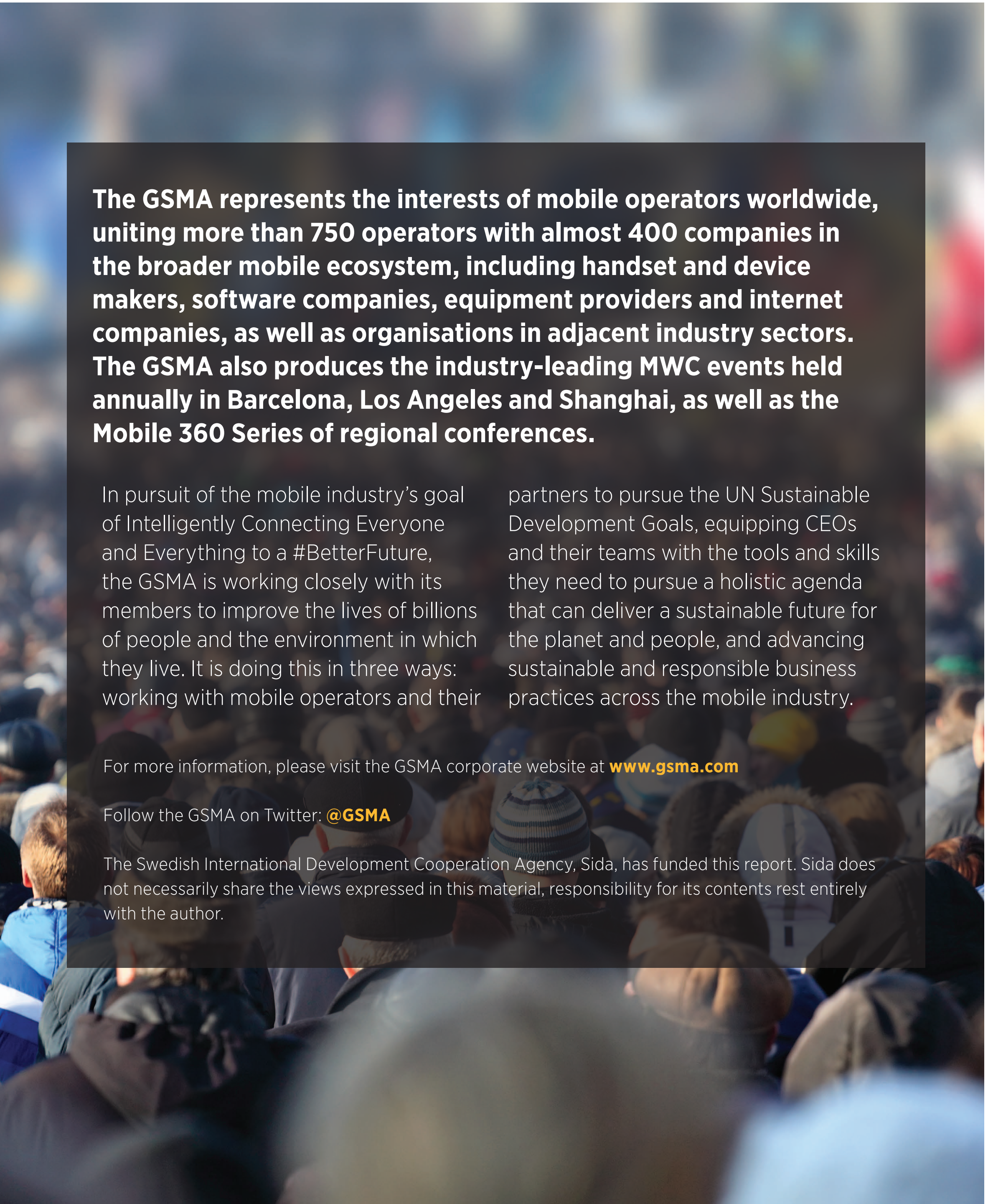
HUMAN RIGHTS GUIDANCE for the mobile industry



The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

In pursuit of the mobile industry's goal of Intelligently Connecting Everyone and Everything to a #BetterFuture, the GSMA is working closely with its members to improve the lives of billions of people and the environment in which they live. It is doing this in three ways: working with mobile operators and their partners to pursue the UN Sustainable Development Goals, equipping CEOs and their teams with the tools and skills they need to pursue a holistic agenda that can deliver a sustainable future for the planet and people, and advancing sustainable and responsible business practices across the mobile industry.

For more information, please visit the GSMA corporate website at **www.gsma.com**

Follow the GSMA on Twitter: **@GSMA**

The Swedish International Development Cooperation Agency, Sida, has funded this report. Sida does not necessarily share the views expressed in this material, responsibility for its contents rest entirely with the author.

Contents

This guidance document has been created by Threefold Sustainability Advisory Services. Threefold is led by Milka Pietikainen and Annette Fergusson, two telecoms executives with over 30 years of combined practical experience leading, creating and implementing sustainability programmes within large multinational companies. www.threefoldsustainability.com

Human rights issues guidance

This guidance follows and should be viewed together with the GSMA publication "An introduction to human rights for the mobile sector." The Introduction provides necessary context and introduces wider human rights frameworks and processes that will help structure the implementation of company approaches to the specific issues presented here.

As highlighted in the Introduction, the focus of this guidance is purposefully on operating responsibly with respect to human rights and not on the significant positive contribution that the sector and its services can make in enabling human rights. This positive contribution is addressed by a number of GSMA and industry initiatives and publications, such as the 2019 Mobile Industry Impact Report, the GSMA's Enhancing Children's Lives Through Mobile initiative and GeSI's Innovators Network Enabling Human Rights.

The aim of this document is to provide an introduction for companies to consider the relevance of the following issues for their operations, as well as inspiration and resources to begin to formalise their management of human rights. It is recognised that many of these issues cannot be solved by one company alone and require collaboration across the mobile sector and working with other stakeholders.

For each of the human rights issues covered here, the guidance:

- Explains and defines what the human rights issue is and why it is salient for the mobile industry;
- Outlines steps mobile operators can consider taking to operate responsibly and manage related risks;
- Suggests examples of potential indicators that could be used to measure and report progress;
- Briefly introduces supporting initiatives and resources in the sector that address these issues; and
- Provides some case studies from GSMA members on addressing the topic.

This guidance covers the following issues:

- Privacy and freedom of expression;
- Child rights and safety online;
- Child labour;
- Forced labour, modern slavery and human trafficking;
- Other labour standards;
- Conflict minerals; and
- Community impacts from building and maintaining infrastructure.

> "For business to fully realise its contribution to sustainable development, it must put efforts to advance respect for human rights at the heart of the people part of sustainable development."

JOHN RUGGIE,
author of the guiding principles and chair of shift

Privacy and freedom of expression

The issue

The human rights of privacy and freedom of expression are enshrined in the Universal Declaration of Human Rights (Articles 12 and 19 respectively) and repeated in the International Covenant on Civil and Political Rights (Article 17 and 19). These are very relevant human rights in the online world and in 2016, the UN Human Rights Council passed a resolution stating that "the same rights that people have offline must also be protected online".

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." (ICCPR, Article 17)

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." (ICCPR, Article 19)

Mobile network operators use a limited set of personal data to enable the provision of communications services. Taking proactive steps to respect consumers' privacy and enabling them to make informed choices about what data is collected and how their personal data is used while also protecting it from external attacks or intentional or unintentional leaks is important in maintaining consumer trust and their right to privacy. At the same time, in accordance with local regulation and legislation including licence obligations, operators may be required to share some of this data to assist governments and their law enforcement agencies in their objective to protect public health and safety.

From time to time, mobile network operators may also receive orders from government authorities to shut down or restrict services on their networks, including blocking signals around, for example, prisons. These service restriction orders (SROs) may include blocking particular mobile or internet services or content, restricting data bandwidth or degrading the quality of SMS or voice services. They are often referred to as network shutdowns or internet shutdowns.

The core challenge for operators is that they are required by local laws, regulations and licence obligations to comply with government demands, while also having a responsibility to respect internationally recognised human rights.

While some countries have well-established and transparent laws and processes relating to government powers to access communications data or restrict services, in others relevant laws and processes are ambiguous, overbroad or they do not exist. This can make it difficult for operators to assess the legal basis of such demands, including whether they are made by those authorised in law to make them.

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks

(ICCPR, Article 17)

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

(ICCPR, Article 19)

Privacy and freedom of expression

International conventions[1] state that governments can limit the right to privacy of individuals only in narrowly defined circumstances. Even in countries with established rule of law, in some situations, proposals for access by the government are seen by some as overreaching these limitations. Complying with such requests and orders may put mobile operators in a difficult position as they may be seen as complicit in governments overstepping their powers. At the same time, in some cases, operators would risk fines or criminal sanctions (including imprisonment of staff) or even the loss of their licence if they refused to carry out demands or even disclose that they had been issued.

Some of these considerations may further increase in importance as technology and systems advance, for example, as AI and big data become more ubiquitous. AI systems rely on collecting and processing large quantities of data and that data needs to be secure and protected and individuals' right to privacy respected. While AI-enabled applications should have a positive purpose, there may be scenarios where AI data could be misused and/ or result in unintended consequences. Companies can follow a "Trustworthy AI" approach and seek to apply privacy and ethics principles to help mitigate any risks.

Operating responsibly

Solid data protection and security policies and processes, audits and vulnerability testing, as well as providing consumers with information about privacy and security issues are key to protecting consumers' rights.

While mobile network operators are obliged by local law and/ or licence obligations to comply with orders from government authorities, when faced with a law enforcement assistance request or a service restriction order they also have a responsibility to determine the legitimacy of the demand and minimise any negative impacts on their consumers. To do this, and to enable quick response time, mobile operators can:

- Carry out a risk assessment of potential scenarios;
- Advocate for clear laws and government transparency, jointly with other operators if possible
- Identify a (dedicated) team to assess and respond to requests;
- Establish a process to escalate difficult cases to senior management;
- Map government's legal powers and who is allowed to make requests and under which laws;
- Put in place controls to protect consumer data at each step of responding to a request;
- Keep good records of requests received and responses;
- Train relevant personnel on policies and encourage escalation of any issues; and
- Regularly audit compliance to processes and policies.

Companies can also (where legally possible and where doing so does not pose threat to personnel or company operations) be transparent about the numbers and types of requests and orders they have received from the authorities and advocate for clear laws and government transparency, jointly with other operators if possible. This is something that many external stakeholders with concerns about these issues value.

The GSMA has published a set of AI ethical principles which set out the issues operators should consider to ensure they are operating trustworthy and are ensuring responsible use of data with regards to AI.

[1] The International Covenant on Civil and Political Rights, Article 4 and Article 19. The UN Human Rights Committee, General comment no. 34.

Privacy and freedom of expression

Example KPIs

Where it is legal to disclose this information, indicators for law enforcement assistance requests could include:

- The numbers of lawful interception requests received (by country); and
- The number of consumer data disclosure requests received (by country).

Where it is legal to disclose this information, indicators for service restriction orders could include:

- The number of requests to restrict access to specific websites or content (by country);
- The number of lawful requests to restrict access to services; and
- The number of consumers affected by each request.

Supporting initiatives and resources

The GSMA's positions on mandated government access (p186); privacy (p204), mandated SROs (p190) and signal inhibitors (p210) are available in the Mobile Policy Handbook.

The GSMA provides a wealth of information for mobile operators on the issues of privacy and data protection on its Privacy website. Further background information on protecting consumer privacy, law enforcement assistance requests and service restriction orders is also available in the GSMA Safety, Privacy and Security Across the Mobile Ecosystem report (from pages 28, 38 and 43 respectively). The GSMA GSMA has also published AI Ethics Principles.

The GSMA has published specific privacy guidance relating to COVID-19 and collaboration with governments in such emergency situations.

The GSMA also provides practical guidance for mobile operators relating to managing law enforcement requests, service restriction orders and signal blocking requirements, both internally and with external stakeholders. These toolkits are available for GSMA operator members on the GSMA Infocentre.

The Global Network Initiative (GNI) is a multi-stakeholder forum that brings together telecommunications operators, major internet companies, civil society, academics and investors to work together to protect and advance freedom of expression and privacy. The GNI has a set of principles and implementation guidelines for companies and has also issued a statement expressing concern over the increasing number of government orders to shut down or restrict access to communication networks and services, and a one-page guide available in 12 languages on the consequences of network shutdowns.

Legal Frameworks on Freedom of Expression and Privacy in Telecommunications published by the GNI includes a summary of legal frameworks relating to government access and surveillance powers in over 50 countries.

The Ranking Digital Rights (RDR) project publishes an annual ranking of telecoms and internet companies' disclosed commitments, policies and practices affecting users' privacy and freedom of expression.

The nongovernmental organisation (NGO) Access Now maintains a database called the Transparency Reporting Index, which includes links to the reports of mobile operators and other companies, to provide information on, for example, the numbers of data access requests they receive from governments. They also track internet shutdowns across the world as part of their Keep It On campaign.

There are also a number of organisations and events that address these issues:

- The Freedom Online Coalition is a group of 31 governments promoting internet freedom. It organises regular meetings hosted by member governments and attended by all stakeholder groups.
- The Internet Governance Forum is an annual event led by the UN and hosted by national governments.
- RightsCon is an annual civil society-led conference bringing together a diversity of local and global human rights organisations and other stakeholders.

Privacy and freedom of expression

Case study: Transparency report by Verizon

Every six months, Verizon publishes a detailed transparency report providing details of the number of different types of requests and national security demands it receives for consumer data in the United States and internationally. The report is very clear on what services and requests the reported numbers cover and under what circumstances Verizon would reject requests from the authorities.

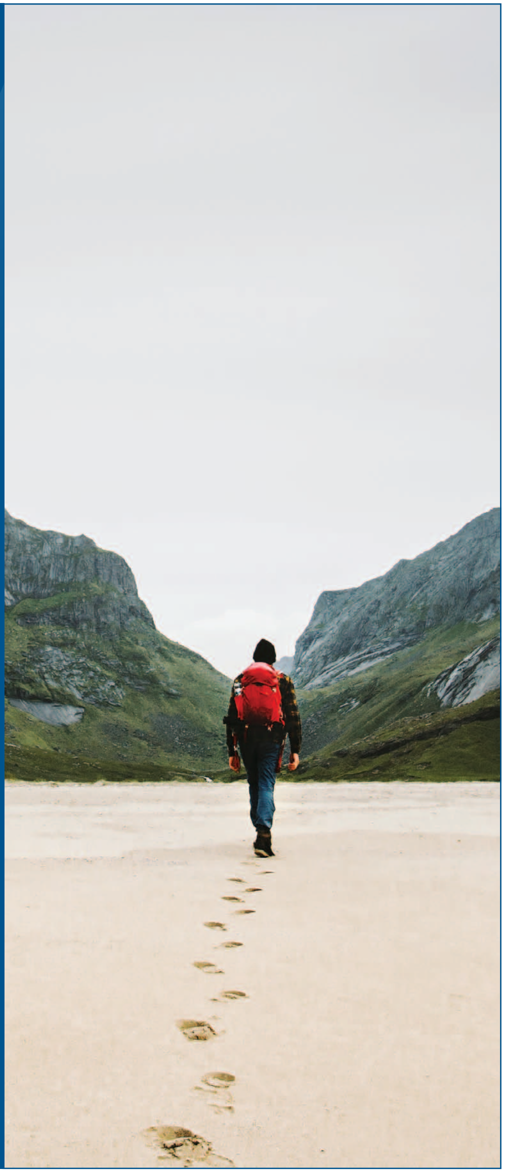
The report also includes helpful questions and answers on Verizon's approach and the different types of requests. Verizon explains the current requirements for governments to be transparent about the requests they make to telecommunications and internet service providers.

Case study: Telia Company's Policy on freedom of expression & surveillance privacy

Telia Company's policy addresses the company's commitments and advocacy position in relation to requests or demands with potentially serious impacts on freedom of expression and surveillance privacy. See the Telia Company policy for the full text of the company's commitments, which include:

- Striving to act in the best interest of customers and the company;
- Advocating clear and transparent legal provisions on proportionality and necessity for all government surveillance of communications, pointing to that vague, non-transparent and broadly conceived legal provisions are not appropriate when freedom of expression and surveillance privacy is at stake;
- Complying with requests or demands only to the extent required by law, including binding regulations and licence requirements. Telia Company will also argue that all such requests or demands are submitted in writing and are signed by the appropriate government official;
- Enhancing internal decision making to efficiently determine whether a request or demand could be in conflict with international standards of human rights because of serious impacts on freedom of expression and surveillance privacy;
- Defining clear criteria, processes and responsibilities for assessing and determining the likelihood and seriousness of impacts on freedom of expression and surveillance privacy; and
- Always prioritising the safety and liberty of company personnel who could be put at risk when applying the policy.

Telia Company has also shared an internal tool it uses to assess and escalate government requests and demands that potentially could have serious impacts on the freedom of expression and/or surveillance privacy rights of individuals.



Privacy and freedom of expression

Case study: Telefónica's transparency report

Telefónica was commended in the 2018 Ranking Digital Rights assessment as the company that disclosed the most about its policies affecting freedom of expression, including information on how it handles government requests to restrict content and accounts and to restrict services.

Telefónica's 2018 Report on Transparency in communications includes – for Telefónica's countries of operation – information on:

- The commitments, policies and processes that following when responding to these requests from the Competent Authorities;
- The legal framework and competent authorities for law interceptions, access to metadata, blocking and filtering of content and for geographical or temporary suspension of services;
- Requests from the competent authorities in terms of law interceptions;
- Requests from the competent authorities in terms of access to metadata;
- Requests from the competent authorities in terms of blocking access to specific websites or content;
- Requests from the competent authorities to temporarily or geographically limit the provision of a service;
- The number of times requests were rejected; and
- The number of customers affected by each request, taking into account that a single request may affect one or several customers.

It also seeks to inform in a transparent manner about Telefonica's efforts regarding those requests that may have a potential impact on the rights of privacy and/ or freedom of expression as they are framed within so-called "major events".

Child rights and safety online

The issue

In an increasingly connected world, mobile operators play a key role in contributing to positive outcomes for children in terms of their rights, development and well-being, for example by enabling access to information and learning, and supporting communication and the exchange of ideas.[2]

However, in order to be able to enjoy these opportunities, children also need the digital skills to thrive online as well as the knowledge and tools to navigate potential issues - such as inappropriate content and grooming - and to protect their privacy and reputation online. Mobile operators and other players such as social media platforms are in a key position to help children and their guardians to understand how to keep safe online and address concerns.

Balancing these risks and opportunities is key to ensuring that concerns for child safety online do not over-ride other rights children have; to access information, culture and entertainment, and make their voices heard.

Mobile operators and other companies in the sector can also uphold children's right to protection from abuse by taking steps to make their services hostile to those who wish to sexually exploit children by accessing or sharing child sexual abuse material online.

All of these efforts will help protect the rights of children to be free from violence, abuse and commercial exploitation. In addition, other child rights impacts mobile operators should consider include:

- Responsible marketing practices, to protect children's right to be free from commercial exploitation;
- Practices in relation to family leave and flexible working of employees that may have significant indirect impact on their children.

Child labour in relation to mobile operators is covered in detail in the following chapter.

[2] See: GSMA / UNICEF "Enhancing Children's Lives through Mobile: Opportunities to improve children's lives, development and well-being, using the Convention on the Rights of the Child (CRC) as a foundational framework – a Guide for Mobile Network Operators" which maps relevant SDGs and articles of the CRC to mobile operator activities, showing how mobile operators can support Child Rights from 'protection to participation'. This document, along with a series of mobile operator case studies, can be found on: https://www.gsma.com/mpoweryouth/

Child rights and safety online

Operating responsibly

Tools for parents and materials to educate children, guardians, and teachers

Operators can create or signpost 'parental control' solutions to give their parent consumers more control of what their children see and do online. These controls can be activated at device or (home) network level.

Many operators have partnered with expert child rights organisations to develop or make available activities and educational materials for children, guardians and teachers to jointly learn about risks online and how to address them. These can range from school talks to flyers and online materials available to consumers. Many operators are also partnering and supporting various child helplines, which can also guide children with issues they face online.

Fighting child sexual abuse content

Mobile operators that provide hosting services should develop 'Notice and Takedown' processes, where they remove any child sexual abuse content (CSAC) from their servers at the demand of the appropriate authority, retain evidence if required and post a notice that the content has been removed. Companies for whom content sharing is a main part of their business should also consider using 'digital fingerprinting' tools (e.g. Photo DNA), hash lists or other solutions that could be used to identify known CSAC before it is uploaded to servers.[3]

Where available, mobile operators should work with the national internet reporting hotline[4] responsible for handling reports of potential CSAC and working with law enforcement to ensure they are investigated. Operators can help raise awareness of their national reporting hotline.

Whilst CSAC is often shared in ways that cannot be disrupted by mobile operator measures, for example via encrypted messages, there are steps which can help make it harder to access known illegal child sexual abuse content online: operators can put in place processes to help limit access to lists of known child sexual abuse content at network level. Guidance for mobile operators on key considerations, including technical and legal, as well as trusted international sources of such lists (including INTERPOL) has been created by the GSMA Mobile Alliance Against Child Sexual Abuse Content (see below).

Other issues

Some companies have established responsible marketing guidelines covering child rights specific issues such as not targeting advertising to children, avoiding the use of stereotyped representation or promotion of dangerous or unhealthy behaviours. Such guidance can also consider the appropriate use of images of children in advertising.

Some mobile operators have adopted global family leave policies beyond local legal requirements, in some cases applicable for both parents as well as adoptive parents. Companies can also support employees returning from family leave with shortened

[3] Further information can be found at https://www.projectvic.org/technology-2/photodna/ and GSMA's guidelines on Notice and Takedown processes.
[4] See: www.inhope.org

Child rights and safety online

Example KPIs

- Per cent of operations providing materials to education and advise children, parents and carers on child online safety;
- Number of children reached by child online safety training.

Supporting initiatives and resources

The GSMA Mobile Alliance Against Child Sexual Abuse Content is a GSMA-led initiative founded by a group of mobile operators to obstruct the use of the mobile environment by individuals or organisations wishing to consume or profit from child sexual abuse content. The Mobile Alliance had produced a range of materials for all GSMA members, some of which are listed below and publically available. Additional materials are available to members – for example, on technical solutions for blocking CSAC – by contacting the GSMA directly (mpoweryouth@gsma.com)

- Hotlines: Responding to reports of illegal online content
- Notice and Takedown: Company policies and practices to remove online sexual abuse material
- Preventing mobile payments services from being misused to monetise child sexual abuse content

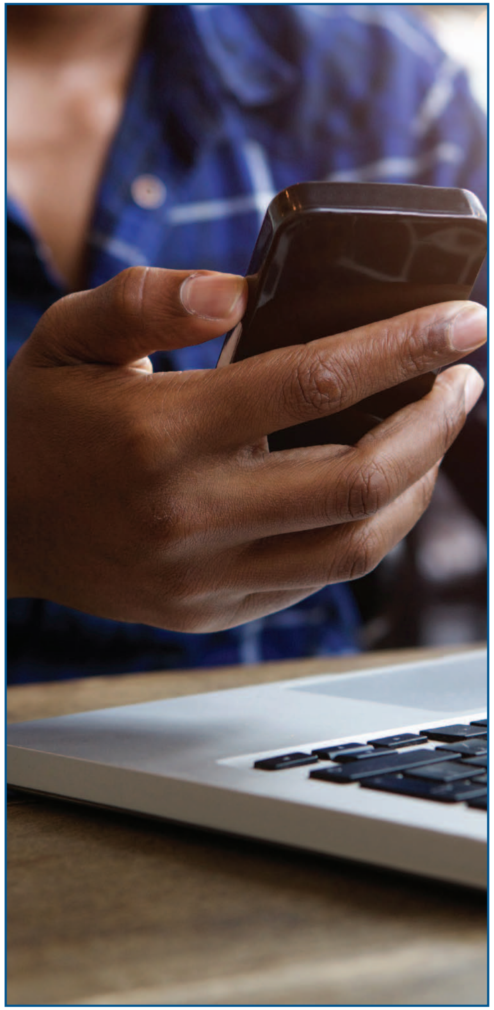
In partnership with Child Helpline International, the GSMA developed a practical guide for how mobile operators can work together with helplines as well as high level guidance for helpline personnel to deal with issues relating to online safety.

The International Telecommunication Union, with a range of partners including UNICEF, has published a series of guidelines on Child Online Protection for a range of stakeholders, including policymakers and industry.

UNICEF's Children Are Everyone's Business is an introduction to companies on how to better take into account children's rights in company policies and processes and the UNICEF Mobile Operator Child Rights Self-Assessment tool helps operators understand how they may impact children in their day-to-day operations and how well they are currently managing the risks. The tool is specific to mobile operators and has been developed together with the industry. There is also a series of UNICEF discussion papers highlighting the numerous issues children face in the digital world.

Case study: Telenor's #Digiworld curriculum

Digiworld is an interactive game launched by Telenor in 2018 and designed to help children become safer and more confident digital citizens. It is available in multiple languages and contains quizzes, a resource library and worksheets for children, parents and schools.



Child labour

The issue

The International Labour Organization (ILO) defines child labour as "work that is mentally, physically, socially or morally dangerous and harmful to children; and interferes with their schooling".

As part of the SDGs, the international community has committed to end child labour in all its forms (Target 8.7). The ILO Minimum Age Convention, 1973 (No. 138) sets the minimum age of employment to 15 years (and 13 for light work). Virtually all countries in the world have ratified the convention into law and local laws usually define minimum age between 14 to 16. In many countries, child labour is punishable by serious fines and imprisonment. The Netherlands is introducing a law, coming into force in 2020, imposing duty of care on all companies selling goods and services in the country to ensure they have been produced without child labour.

The ILO Minimum Age Convention also defines 18 as the minimum age for hazardous work. This can be work that is physically demanding, happens at night, lasts long hours, or which can expose children to dangerous substances or situations.

For mobile operators, risks of child labour usually relate to activities of subcontractors. These can range from children being involved in the sale of mobile SIM cards and top-up cards; child labour in the supply chains supporting the manufacture of mobile equipment or infrastructure; children working at construction sites in network deployment; or children participating in taking apart electronic waste for resale. There are also a range of jobs that would be unsuitable for children under 18, such as those relating to security, driving, network maintenance or any positions that require or incentivise long hours or night-time work.

Operating responsibly

Mobile operators can put in place policies and programmes to minimise the risk of child labour across the value chain and focus efforts on countries where the risk of child labour is high. As minimum age limits and restrictions for young workers vary, it is important that policies account for the specific requirements in each of their operating jurisdictions and good practice would be to align policies either with local law or the ILO conventions, whichever is higher.

Policies and processes – within the company and towards suppliers – should clearly prohibit the use of child labour and include proof of age requirements, including defining a process for when official personal identification documents may not exist. Similarly, a remediation process should be defined for cases where children below the minimum age are discovered. This would include investigating the child's overall family situation and finding solutions to support the child to continue their schooling.

When procuring security services for base station sites, offices, shops or marketing events, companies should require that providers have experience and are trained in situations involving children and that children are not used in security arrangements.

Child labour

Example KPIs

Information should be provided on the risks of child labour in the supply chain and potential indicators include:

- Number of supplier site assessments conducted;
- Number of issues relating to child labour identified (and number followed up and resolved);
- Number of reports to whistleblowing hotlines related to child labour concerns; and
- Number of suppliers that have received training on child labour.

Supporting initiatives and resources

The Global Child Forum maintains a Children's Rights and Business Atlas that helps companies easily identify the key risks by operating country.

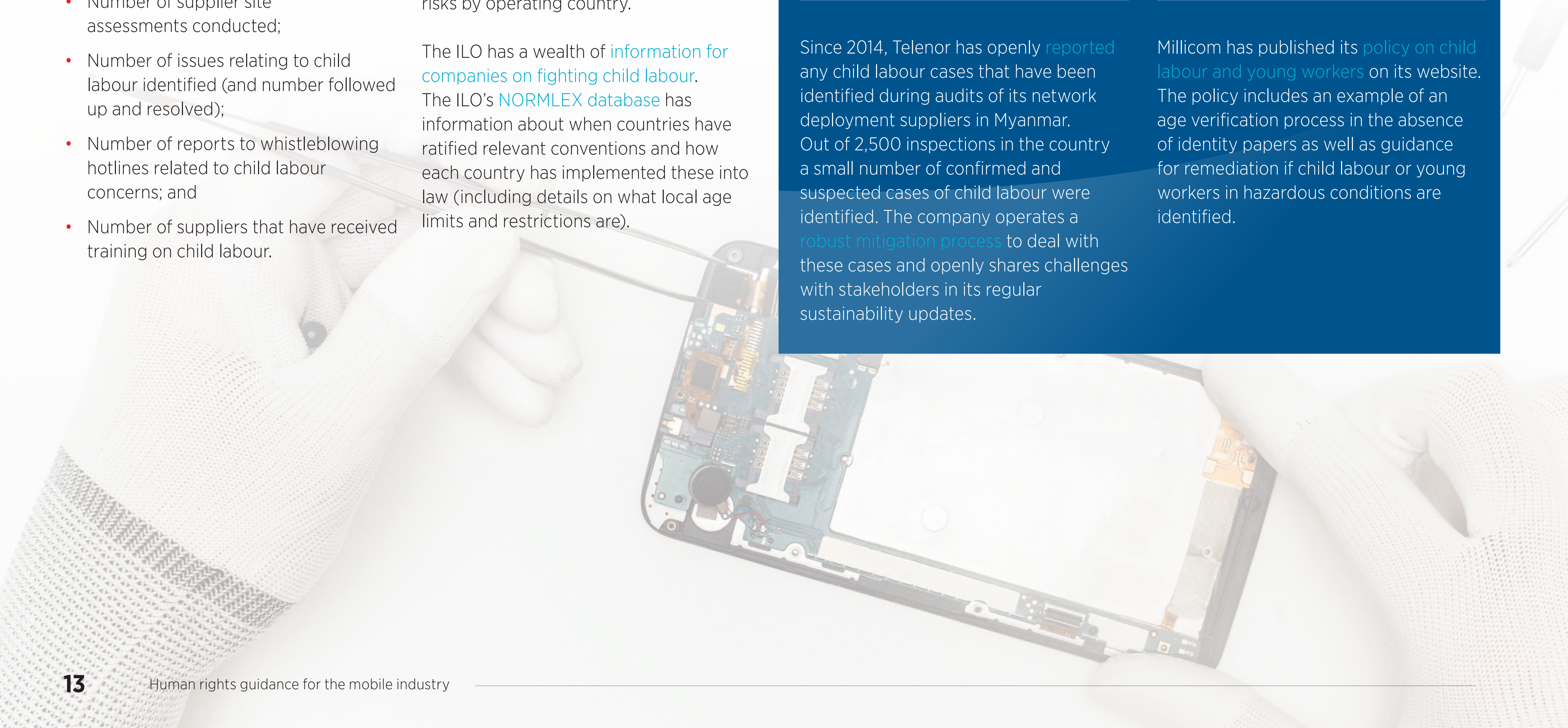
The ILO has a wealth of information for companies on fighting child labour. The ILO's NORMLEX database has information about when countries have ratified relevant conventions and how each country has implemented these into law (including details on what local age limits and restrictions are).

Case study: Managing child labour in network deployment – Telenor

Since 2014, Telenor has openly reported any child labour cases that have been identified during audits of its network deployment suppliers in Myanmar. Out of 2,500 inspections in the country a small number of confirmed and suspected cases of child labour were identified. The company operates a robust mitigation process to deal with these cases and openly shares challenges with stakeholders in its regular sustainability updates.

Case study: Child labour and young workers policy – Millicom

Millicom has published its policy on child labour and young workers on its website. The policy includes an example of an age verification process in the absence of identity papers as well as guidance for remediation if child labour or young workers in hazardous conditions are identified.



Forced labour, modern slavery and human trafficking

The issue

The ILO estimates that there are approximately 40 million victims of modern slavery around the world and 16 million of these victims are exploited in the private economy.

Human trafficking and forced labour are both forms of modern slavery.

- Human trafficking involves transporting, recruiting or harbouring people for the purpose of exploitation, using violence, threats or coercion.
- The ILO Forced Labour Convention, 1930 (No. 29), defines forced labour as: “all work or service which is exacted from any person under the menace of any penalty and for which the person has not offered himself voluntarily”. Forced labour is different from sub-standard working conditions or underpayment of workers. Indicators include restrictions on workers’ freedom of movement, withholding of wages or identity documents, physical or sexual violence, threats and intimidation, or fraudulent debt from which workers cannot escape.

As part of the SDGs, the international community has committed to end modern slavery by 2030 (Target 8.7). There are also a number of legal disclosure requirements for companies that relate to modern slavery and forced labour. These include:

- The California Transparency in Supply Chains Act (2010) requires certain companies (manufacturers and retail sellers) doing business in California to disclose the extent of their efforts, if any, to ensure that the goods they sell are not produced by workers who are enslaved, coerced, or otherwise forced into service or who have been the victims of human trafficking. See more information on the five areas of disclosure.
- Section 54 of the UK Modern Slavery Act requires commercial organisations that operate in the UK and have an annual turnover above £36 million to produce a statement setting out the steps they are taking to address and prevent the risk of modern slavery in their operations and supply chains. Over 10,000 companies have already produced statements and guidance has been published by the UK Home Office.
- The Australian Commonwealth Modern Slavery Act 2018 establishes a requirement for large businesses to publish annual Modern Slavery Statements on an online, central register. These statements must explain what the business is doing to assess and address the risks of modern slavery practices that may be occurring in its global and domestic operations and supply chains. The government has produced Guidance for Reporting Entities.

Operating responsibly

Mobile operators, like other companies, should put in place policies and programmes to minimise the risk of modern slavery, forced labour and human trafficking within their business and across the value chain. These would usually sit within broader labour standards policies and programmes (see section on Other labour standards).

Once a policy is in place, companies should engage with suppliers to communicate their expectations and assess and audit suppliers to enforce the policy. Operators should also put in place monitoring, reporting and remediation process where cases of forced labour, modern slavery and human trafficking have been identified.

Forced labour, modern slavery and human trafficking

Example KPIs

Information should be provided on the risks of modern slavery in the supply chain and potential indicators include:

- Number of supplier site assessments conducted;
- Number of issues relating to forced labour, human trafficking and modern slavery identified (and number followed up and resolved);
- Number of reports to whistleblowing hotlines related to modern slavery concerns; and
- Number of suppliers that have received training on modern slavery.

Supporting initiatives and resources

The Responsible Labor Initiative (launched by the Responsible Business Alliance) is a multi-industry initiative focused on ensuring that the rights of workers vulnerable to forced labour in global supply chains are respected and promoted. See more details on the Responsible Business Alliance in the section on Other labour standards.

KnowTheChain is a benchmarking of companies' practices and transparency in relation to forced labour risks in supply chains. It is focused on three sectors, including information and communications technology. The 2018 benchmark covered 40 companies, including 20 headquartered in the US (e.g. Apple and Microsoft), 14 in Asia (e.g. Foxconn and Canon) and six in Europe (e.g. ASML Holding and Ericsson).

There are several non-sector specific initiatives on modern slavery, particularly in those countries where there are legal disclosure requirements for companies. For example, a coalition of NGOs has established the Modern Slavery Registry, a central registry that tracks compliance with the UK Modern Slavery Act and hosts modern slavery statements. The registry also includes an assessment of the reporting of FTSE 100 companies.

Case study: Vodafone Group's approach to modern slavery reporting and training

Vodafone Group's Modern Slavery Statement provides details of the company's relevant policies, governance, risk assessment, supplier selection and monitoring and grievance mechanisms.

It also describes efforts the company has made to train its employees and suppliers on modern slavery. This includes a publicly available interactive modern slavery online training module launched in 2017–18 to help build awareness and understanding of modern slavery in the ICT supply chain. It helps suppliers to spot 'red flags' within their business operations and supply chain.

The course uses examples from a range of high-risk sectors – such as recruitment fees in the construction sector and passport retention in electronics manufacturing – and highlights both Vodafone's expectations and international standards in relation to these issues.

It is available in English, Mandarin Chinese and Hindi and since its launch in 2018 has been distributed to over 11,000 suppliers. Anyone can register and access the free training on their desktop or mobile device via http://modernslavery.vflearning.com.

Other labour standards

The issue

There are material risks to the human rights of people working in the mobile sector value chain beyond child and forced labour.

These range from, for example, the risk of harmful effects of working long hours in electronics factories; risks of injury to people working in field operations and network deployment; and risks of poor living conditions for workers housed in factory dormitories.

The ILO has identified eight fundamental Conventions covering subjects that are considered to be fundamental principles and rights at work. The categories are:

- Freedom of association and the effective recognition of the right to collective bargaining;
- The elimination of all forms of forced or compulsory labour;
- The abolition of child labour; and
- The elimination of discrimination in respect of employment and occupation.

These conventions are widely ratified by the vast majority of countries across the world. They are also the origin of the four labour principles of the UN Global Compact and are referred to by many companies in their codes of conducts, human rights policies and supplier codes of conducts.

Although terminology and scope vary, supplier codes of conduct tend to also go beyond just the fundamental conventions and set standards across the following labour and working condition issues:

- Child labour;
- Forced labour;
- Working hours;
- Freedom of association and the right to collective bargaining;
- Health and safety;
- Non-discrimination;
- Humane treatment; and
- Wages and benefits.

Operating responsibly

The first step for companies to manage labour standards risks in their supply chains is to set clear expectations and requirements for suppliers through, for example, a supplier code of conduct that forms part of the contractual agreement with the supplier.

The supply chains of companies in the mobile sector are complex and therefore companies should take a risk-based approach to focus efforts on those product categories, regions and suppliers where the risk of non-compliance is greatest.

Companies should conduct due diligence on their suppliers starting at the prequalification stage before a potential supplier is approved. This can be done through risk assessments, information gathering, supplier self-assessments and/or in-depth analysis such as site audits.

Good practice would involve site audits using experts in labour standard audits who would, for example, interview workers directly. It is also critically important to follow up with corrective actions plans.

However, responsible sourcing is not just about audits and assessments. Working with suppliers, including those further down the value chain, to build understanding and capacity and support the improvement of standards is critical. This is an area (as well as assessments) where industry collaboration is more efficient and effective than companies working alone.

Other labour standards

Example KPIs

- Number of supplier site audits conducted;
- Number of non-conformances to supplier code of conduct identified (and number followed up and resolved); and
- Per cent of relevant employees (for example, procurement staff) completing training on the company supplier code of conduct.

Supporting initiatives and resources

The Joint Audit Cooperation (JAC) is an association of 17 telecom operators that aims to verify, assess and develop the corporate social responsibility performance (including labour standards) of shared suppliers in the sector. This is done through coordinated on-site audits of suppliers based on a common verification, assessment and development methodology. Each member company has the responsibility, acting on behalf of the others, to lead a complete audit and corrective action process with a number of suppliers, sharing the results between JAC members. JAC has also launched a supplier academy focused on developing training to help suppliers assess and improve performance within their own supply chains.

The Responsible Business Alliance (RBA, formerly the Electronic Industry Citizenship Coalition) is a coalition of over 150 companies primarily in the electronics industry, and so includes many companies that are suppliers (and consumers) to mobile operators.

RBA members commit to a common Code of Conduct that establishes standards (including on working conditions) that members and their suppliers must implement. There are three primary initiatives of the RBA:

- The Responsible Minerals Initiative (see section on Conflict Minerals for more information);
- The Responsible Labour Initiative (see section on Forced labour, modern slavery and human trafficking for more information); and
- The Responsible Factory Initiative, which provides tools and programmes for members, such as a facility-level self-assessment questionnaire and audit programme.

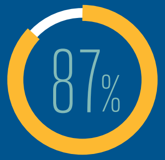
Case study: Telenor’s approach to supplier capacity building and monitoring

Telenor combines compliance monitoring and capacity building with suppliers and sub-suppliers to drive continuous improvements in its supply chain.

Telenor reported that during 2018 its business units organised more than 20,000 man-hours of various capacity building initiatives. The activities varied from supplier to supplier depending on the most relevant and salient risk of the business unit and included on-site briefings, awareness sessions, workshops, forums, process support, online portals and resource guides. Topics covered were broader than just labour rights and health and safety,

3,500+ SUPPLIER INSPECTIONS CONDUCTED

(ranging from simple site visits to more comprehensive inspections or audits) across the Group.



OF THE INSPECTIONS WERE UNANNOUNCED.

450+ MAJOR NON-CONFORMITIES IDENTIFIED

during the inspections. These are followed up with mitigation plans and processes aiming to address these non-conformities until they are resolved and can be closed.

Conflict minerals

The issue

Mobile phones and other electronics contain a wide range of metals that allow them to function properly. Operators are unlikely to directly buy any of these metals but many of the products that operators use or sell will contain them.

'Conflict minerals', as defined in US legislation, include tin, tantalum, tungsten and gold (collectively known as 3TG) and can be extracted in many locations all over the world. Mining of these metals in the Democratic Republic of the Congo (DRC) and adjoining countries has been linked to armed conflict by financially benefiting armed groups in the region. It has also been linked to human rights abuses such as child and forced labour.

There are a number of legal requirements relating to conflict minerals, including:

- The US Dodd-Frank Act (section 1502), which requires companies that are publicly traded in the U.S. to disclose the use of 3TG metals in their products and describe the process used to ensure that the purchase of these minerals does not fund illegal armed groups operating in the DRC; and
- The EU Conflict Minerals Regulation, which will apply from January 2021, will require EU importers of 3TG to carry out due diligence on their supply chain. This regulation does not solely focus on the DRC and surrounding countries, but all conflict-affected or high-risk areas globally. It only applies mandatory actions to upstream and some downstream imports (for example, alloys and chemicals), leaving due diligence by downstream product manufacturers and importers voluntary.

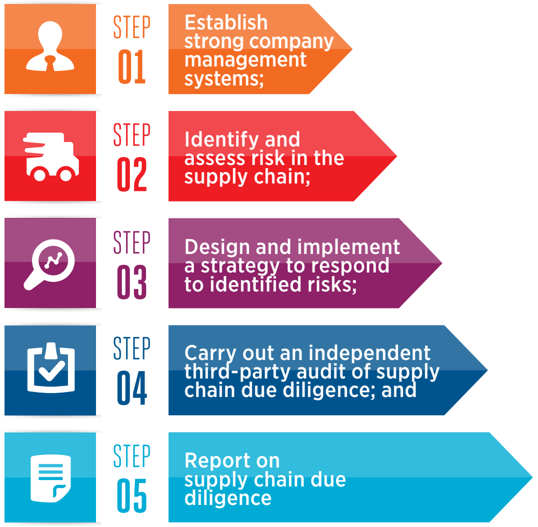
Although these two legal requirements are focused on 3TG metals, voluntary responsible mineral sourcing initiatives extend to include other metals, most notably cobalt.

Operating responsibly

The first step a company should take is to adopt a public, company-wide policy for the supply chain of minerals originating from conflict-affected and high-risk areas. Companies should consider not simply banning minerals from such areas but actively supporting responsible sourcing through robust, internationally recognised schemes.

Companies also need to work with suppliers to improve traceability of minerals and identify and assess risk in their supply chains.

The OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas provides internationally accepted guidance for managing this issue and identifies five due diligence steps:


STEP 01 Establish strong company management systems;

STEP 02 Identify and assess risk in the supply chain;

STEP 03 Design and implement a strategy to respond to identified risks;

STEP 04 Carry out an independent third-party audit of supply chain due diligence; and

STEP 05 Report on supply chain due diligence

No one company can solve the issue of responsible mineral sourcing alone and so companies need to work together with their suppliers, other players in their sector and more widely. Companies should therefore consider supporting and actively participating in established industry and multi-stakeholder initiatives.

Conflict minerals

Example KPIs

Indicators should focus on those products that contain relevant metals (in the case of the US and EU legislation this is tin, tungsten, tantalum and gold) and the suppliers that provide these products. For these products and suppliers, potential indicators include:

- Number/per cent suppliers that have:
  - Their own conflict minerals policy;
  - Provided information on the smelters in their supply chain; and
  - Identified all of the smelters providing 3TG in their supply chain.
- Number of suppliers and/or products that are conflict free for all minerals.

Supporting initiatives and resources

The Responsible Minerals Initiative (RMI, formerly the Conflict Free Smelter Initiative) has over 380 companies and associations from across 10 different industries as members. It is one of the most well-established resources for companies addressing responsible mineral sourcing issues in their supply chains. The RMI's scope is broader than 3TG from the Great Lakes region of Central Africa, addressing, for example, cobalt sourcing. There are two primary components:

- The Responsible Minerals Assurance Process, which offers companies an independent, third-party audit that determines which smelters and refiners can be verified as having systems in place to responsibly source minerals; and
- The Conflict Minerals Reporting Template, which helps companies collect and disclose information about smelters in their supply chains.

There are also initiatives in place to responsibly source minerals from conflict affected and high-risk areas while avoiding funding illegal armed groups. The Public–Private Alliance for Responsible Minerals Trade (PPA) is a multi-sector and multi-stakeholder initiative to support supply chain solutions to conflict minerals challenges in the Great Lakes Region of Central Africa. The PPA provides funding and coordination support to organisations working in the region to improve the due diligence and governance systems and develop verifiable conflict-free supply chains. Members include Apple, Nokia, Telefónica and Verizon.

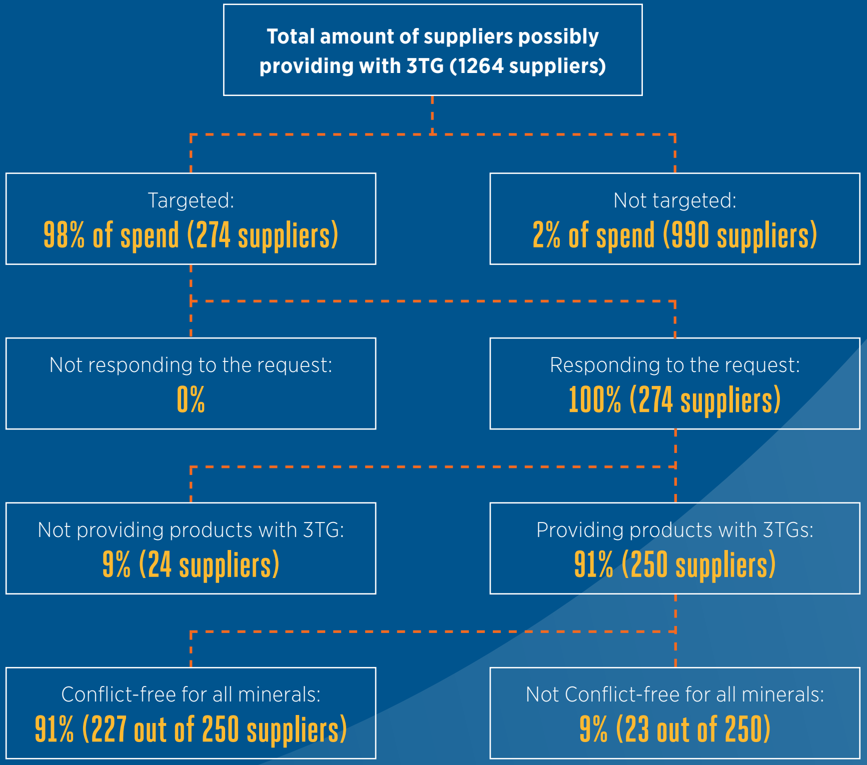
Conflict minerals

Case study: Nokia's conflict minerals due diligence and reporting

Nokia has designed its conflict minerals due diligence process and approach to conform to the internationally recognised due diligence framework provided by OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas. The Nokia Conflict Minerals Report for 2018 sets out the actions the company has taken against each of the five steps of the Guidance including, among other things:

- Setting up governance system in line with OECD Guidelines
- Putting in place a policy and working group;
- Being a member of the RMI, contributing to joint industry efforts, and using its tools and resources;
- Conducting a reasonable country of origin inquiry survey with direct suppliers;
- Engaging in stakeholder collaboration upstream of the supply chain via Public Private Alliance; and
- Publishing results of its due diligence efforts.

The figure opposite is taken from Nokia's 2018 Conflict Minerals report and summarises the results of its due diligence efforts.



Total amount of suppliers possibly providing with 3TG (1264 suppliers)

Targeted:
98% of spend (274 suppliers)

Not targeted:
2% of spend (990 suppliers)

Not responding to the request:
0%

Responding to the request:
100% (274 suppliers)

Not providing products with 3TG:
9% (24 suppliers)

Providing products with 3TGs:
91% (250 suppliers)

Conflict-free for all minerals:
91% (227 out of 250 suppliers)

Not Conflict-free for all minerals:
9% (23 out of 250)

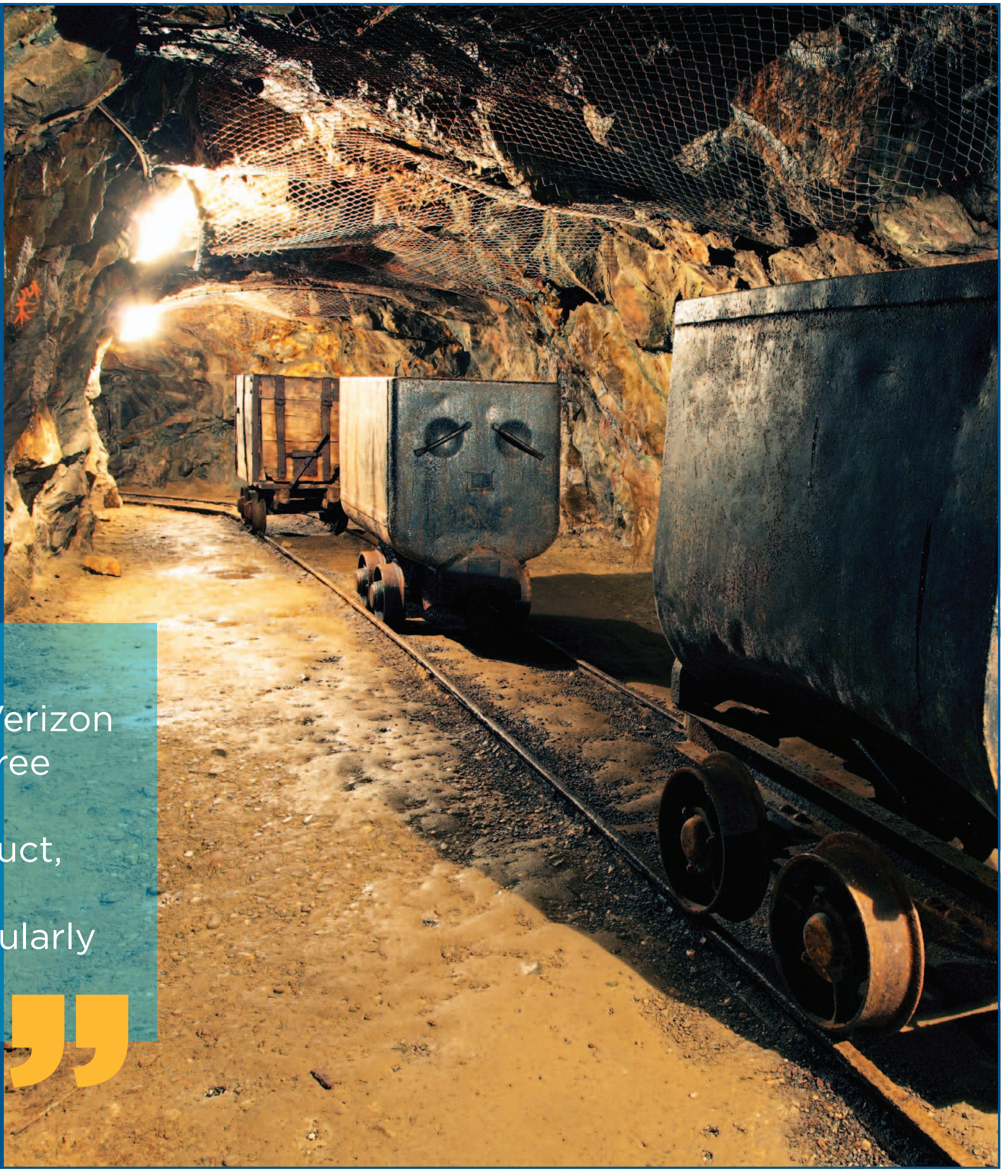
Conflict minerals

Case study: Verizon's conflict minerals policy statement

Verizon's conflict minerals policy acknowledges concerns around conflict minerals and states the company's support for the goals of section 1502 of the Dodd-Frank Act. As well as highlighting its involvement in joint initiatives (Verizon is a member of GeSI and the Public–Private Alliance for Responsible Minerals Trade), the policy sets out clear expectations for suppliers including:

- Establishing policies, due diligence frameworks and management systems consistent with the OECD due diligence guidance;
- Working with sub-suppliers to attain traceability of conflict minerals to the smelter level; and Communicating their own policies and expectations to their sub-suppliers and establishing appropriate objectives and monitoring of sub-supplier performance.
- Although the policy acknowledges that Verizon does not typically manufacture its own products, it states that "in those cases where Verizon exercises a higher degree of influence over the manufacture of a product, our engagements with suppliers will be particularly robust".

> "in those cases where Verizon exercises a higher degree of influence over the manufacture of a product, our engagements with suppliers will be particularly robust"



Community impacts from building and maintaining infrastructure

The issue

Companies' due diligence processes should "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". (Principle 18 (b) of the UN Guiding Principles on Business and Human Rights).

Article 32 of the United Nations Declaration on the Rights of Indigenous Peoples reaffirms that states must seek *"free and informed consent prior to the approval of any project affecting their [indigenous peoples] lands or territories and other resources".*

While mobile phone base stations, masts and antennas do not require large plots of land, mobile phone operators may be faced with various land rights challenges during network deployment and site acquisition. The use and ownership of land is often linked to livelihoods and can be a source of conflict. In some countries, people's rights to land ownership are restricted; land ownership may not be documented; people may have been displaced from their rightful lands in conflict; or there may be ongoing disputes over indigenous land rights.

These are all issues that may complicate and delay site acquisition but also place mobile operators leasing and buying land in a challenging position regarding land and human rights. Anti-corruption and bribery; the environment, especially relating to running remote diesel-generator sites and potential impacts on food and water sources; and potential health concerns of communities are related issues that may present human rights risks or concerns for communities local to sites.

In addition, some multilateral financial institutions, notably the IFC, focus heavily on land rights in their required due diligence and reporting, and their loans may be conditional on reporting how these issues have been addressed.

Once sites are operational, there are certain circumstances where armed security personnel are required to protect sites from access and theft. In other sectors, there have been a number of cases where security services have been implicated in human rights abuses or have used excessive force. These are considerations to take into account particularly when operating in areas of conflict and heightened violence.

Operating responsibly

When planning network deployment and new sites, mobile operators should consider including appropriate risk assessments to understand any land rights-related risks in the targeted areas, and how the placement of the site(s) and any access roads may affect local communities and their access to vital resources such as water or agriculture.

Mitigation strategies should then be implemented to minimise any risks and these should be followed up as part of site maintenance visits. Good practice would involve consulting with communities to understand and address concerns at the planning and acquisition phase and this can also help to avoid costly delays and issues when running the sites.

When subcontracting security services, in particular armed guards, companies should take specific care that they carry out proper due diligence of their personnel, that personnel follow principles of minimum use of force and are properly trained, including for interactions with vulnerable populations – such as young people and indigenous people.

Community impacts from building and maintaining infrastructure

Example KPIs

- Number of identified incidents relating to land rights and network deployment (and details of how land rights issues are assessed and managed).
- Number of per cent of security personnel who have been trained on the company's policies and procedures for interactions with local communities.

Supporting initiatives and resources

There is little documented guidance specific to mobile operators on land rights and provision of security services, with most existing good practice and guidance relating to the extractives industry. Some of this guidance can be applied to mobile operators, although issues around environmental impact and, for example, population displacement, will be at a completely different scale. Well-known resources for the extractives industry to draw inspiration from include:

- OECD's Due Diligence Guidance for Meaningful Stakeholder Engagement in the Extractives Sector; and
- Indigenous peoples and mining good practice guide by the International Council on Mining and Metals.

The IFC Performance Standards on Environmental and Social Sustainability require steps to be taken on stakeholder engagement to understand impacts on communities prior to deployment. The standards also include specific sections on land rights and indigenous rights.

The Voluntary Principles on Security and Human Rights were originally developed by the extractives sector and highlight several areas for companies to take into account when subcontracting and using armed guards and security services. The Danish Institute of Human Rights has also published a compliance assessment tool for security arrangements.

For more information please visit the GSMA website at
https://www.gsma.com/betterfuture/sustainable-leadership

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601