Department: External Affairs

MILLICOM'S POLICY FOR LAW ENFORCEMENT ASSISTANCE AND 'MAJOR EVENTS'

This is a summarized public version of Millicom's internal guidelines for procedures relating to law enforcement requests and 'Major Events'. The internal guidelines contain more detailed function-specific guidance at each step. If you wish to discuss further anything contained in this document, please contact CR@millicom.com

Millicom International Cellular S.A.	Title: MILLICOM'S POLICY FOR LAW ENFORCEMENT ASSISTANCE AND 'MAJOR EVENTS'	Version: 2.0
Document Owner: Head of Corporate Responsibility and VP Legal LatAm and Global Chief Privacy Officer	Approvers: EVP Chief External Affairs Officer; EVP General Counsel; and EVP Chief Ethics and Compliance Officer	

I. TABLE OF CONTENTS

II. Overview

External requests for surveillance, customer information or access to communications networks may represent an exception or limitation to freedom of expression and privacy rights of our customers. International conventions demand that any such limitation must always have a legal basis.

At Millicom, we strive to protect the integrity and privacy of the information we hold on our customers and the right to freedom of expression of our customers, as articulated in the Universal Declaration of Human Rights, and the International Covenant on Civil and Political Rights, which are ratified by all countries in which the Millicom Group[1] operates. We disclose customer information only to those who have the legal authority to obtain this information while ensuring that such authority is exercised in a manner that adheres to the law and that any disclosure is responsive to a lawful government request.   We also work diligently to avoid contributing to actions that may interfere with the right to freedom of expression, while complying with lawful government requests.

This is a summarized public version of Millicom's internal guidelines for procedures relating to law enforcement requests and 'Major Events'. The internal guidelines contain more detailed function-specific guidance at each step. The purpose of this document is to guide employees involved in receiving and responding to law enforcement assistance requests in a manner that best respects the local law, international standards, and the privacy of our subscribers and our employees. The policy is also meant as guidance on actions to be taken when an operation receives a government request classified as a 'Major Event' (as per the definition outlined within). While a Major Event is not necessarily in breach of local law, it can nevertheless pose significant risks for financial losses (through service shut down) or reputational damage.

As local laws regarding exceptions and limitations to freedom of expression and privacy vary, local procedures need to be tailored to those requirements. This document defines key steps that all local operations should take into consideration with respect to these procedures.

III. Definitions

Requests for lawful interception	Request for live interception of voice, SMS, fax and data traffic (lawful interception), i.e., live surveillance.
Requests for customer metadata	Requests for CDR (call data records) or IP addresses, SMS, email traffic, Internet traffic information, or documents from cloud services, or requests for location information (physical / base station or GPS information).
Requests for MFS related data	Requests for information relating to MFS, such as confirming an individual is an MFS customer, transaction data and other account activity.

[1] Group refers to Millicom, the parent company of the local Tigo companies – which are referred to as the "operations".

These requests do not always only relate to financial crime.

These requests can come from public prosecutors or court orders, or any other authority legally authorized to make such requests. In the case of MFS, the requests can come from the central bank or the financial intelligence regulator or, in certain cases, the ICT regulatory authority.

Other types of requests relating to shutdown of services, continuous access to the network, blocking of subscribers, implementation of equipment for additional monitoring, or requests to push specific information to subscribers are defined separately as 'Major Events'. These are defined below and follow a separate procedure outlined throughout this document and in line with existing incident reporting and/or crisis management procedures.

Major Events

While their motivations may be valid and legal and/or be in line with regulatory instruments/frameworks in a local context, 'Major Events' can include clearly politically motivated requests which contradict internationally recognized norms and commitments in the areas of Privacy rights and Freedom of Expression, as well as international norms more generally, such as:

- shut down of base stations / entire network
- service denial or restriction (SMS, mobile/fixed internet, social media, blocking of international gateway(s)
- targeted take-down or blocking of content, including access to broadcasting and other forms of news media
- denial of access for specific individuals (with intent to limit their freedom of expression)
- significant operational changes relating to surveillance techniques (direct access / new technical implementations)
- impromptu/unannounced audits that go beyond the regulator's right to audit as defined in the license and/or telecom law and/or other regulatory instruments[2]
- requests for lawful interception without the appropriate authorizations as spelled out in the applicable LI regulations
- significant changes to local laws relating to government powers of surveillance or data retention
- instructions to send politically motivated messages to customers (targeted and/or mass messaging) on behalf of the government.
- seizing of equipment such as company laptops and computers

IV. Roles and Responsibilities

Law enforcement assistance requests can relate to extremely sensitive matters of national security or organized crime, and in certain cases, can give the designated person(s) access to private information of Millicom/Tigo customers.

[2] e.g., request by a telecom regulator for an audit of MFS processes/ information when the oversight of MFS is the remit of a different regulator

These issues should be taken into account in the designation of responsibilities, noting that there may be restrictions on the nationality or other attributes of the person(s) handling such requests defined within the local law. There may also be the need to protect the identity of person(s) involved in processing such requests.

Legal department	Should always be involved in assessing the legality of requests as defined in the local law before requests are processed. In some countries, specific teams handle such requests – such teams should always include a legal professional.
Corporate Affairs / Regulatory staff	Should always be involved with legal and compliance in assessing and responding to requests.
Compliance department	Should always be involved with legal and corporate affairs in assessing and responding to requests.
Country Corporate Security Manager	Should own the relationship with the local law enforcement agencies to promote clear processes that allow Tigo to respond to requests quickly and within the law.
Anti-money laundering control officers	Receive and process requests relating to MFS, following a similar process as defined for the legal department.

V. Local Processes for Law Enforcement Assistance

1) MAPPING

Identify local laws that outline in which cases it is legal for law enforcement to make requests for surveillance, customer metadata or MFS information.

The laws should specify which authorities are allowed to issue requests, and in what format.

Clarify also whether the government has other powers to make requests, e.g. in the case of a state of emergency and how this may change the “usual process”.

Document this information for the use of the teams who are assessing requests to help them assess and respond to requests quickly.

2) RECORDING

Log and keep secure copies of all requests received in the four categories:

- Requests for interception
- Requests for customer metadata
- Requests for MFS information

- Requests for take-down of content

Log whether requests have been approved or rejected.

3) ASSESSMENT

Always only accept written requests. Reject any request that is not written, unless the situation is defined as urgent. Urgent requests should be accepted only from a restricted predetermined number of sources permitted by local law. In case of urgent requests, ask for a written request to be sent without delay.

Accept only requests that have been granted by authorised entities, as defined in local law.

If urgent requests relate to any ‘Major Events’, follow Millicom’s crisis process to escalate to global teams through GMs, security or business continuity teams [separate process exists].

4) ACTIVATION

Only persons internally identified and authorized should be involved in collecting and processing the information requested.

Strictly only information that has been requested should be searched and collected.

5) DELIVERY

The requested information should always be sent in as secure a manner as possible, in encrypted format whenever possible. In some countries information is delivered in person.

Protect any copies of the information and limit access only to persons who are internally authorized to process such requests.

Keep records of the receipts that have been obtained from law enforcement when information has been delivered.

VI. Major Events Reporting Template

After initial consultation with the senior management escalation group, a more formal communication channel must be established to report the Major Event incident as soon as feasibly possible. The following form will be sent by all local legal/regulatory teams in order to follow up and share the most relevant details concerning the incident:

The following form[3] must be sent to all relevant staff outlined in the 'Major Events Flowchart' as per region. Prior to formal reporting of the Major Event incident, actions taken must already have been communicated to and approved by the senior management escalation group.

Type	Briefly outline what type of Major Event has occurred, using language outlined in Millicom's definition of a Major Event
Form	Indicate if the request has been made orally, electronically or in writing
Source	Define which requesting authority or authorities are involved
Dates/Duration	Indicate date received and any other dates relevant to the request e.g., period/length of time for which the request is valid; deadline for reply and execution of request, etc.
Recipients	Indicate, if known, whether the request has been made to all operators or not
Scope	Indicate the geographical areas and services affected if applicable
Legal and regulatory assessment	• Describe whether the legality and validity of this request has been/has not been confirmed (explain further in the case of the latter). • Indicate whether the request is binding or possible to appeal/challenge. • Indicate whether the request is clearly defined and exact, or whether there is any room for narrower interpretation
Business impact	Describe the potential business impact of rejecting and/or executing request
Risk to safety of employees	Describe possible risks and define as High / Medium / Low
Actions taken	Describe any actions taken in relation to this request e.g., this request has been rejected or executed because… / we have contacted our local telecoms chamber contact to discuss this request, etc.

****

[3] When and if legally possible, please attach all relevant requests and government orders to form.