Executive Summary for Law Enforcement Assistance Requests

GLOBAL GUIDELINE

This is a summarized public version of Millicom's internal guideline for procedures relating to law enforcement requests. 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

TABLE OF CONTENTS

I. INTRODUCTION

Any external request for surveillance, customer information or access to communications networks represents an exception or limitation to freedom of expression and privacy of our customers. International conventions demand that any such limitation must always have a legal basis. All countries Millicom Group operates in have ratified the relevant international conventions protecting freedom of expression and privacy.[1]

We have an obligation to do our utmost to protect the integrity and privacy of the information we hold on our customers, and not pass it on to others without authorization to access it.

The purpose of this document is to guide employees involved in receiving and responding to law enforcement assistance requests and support them to create local procedures in a way that best respects the local law, international standards and the privacy of our subscribers.

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

II. DEFINITION OF LAW ENFORCEMENT REQUESTS

Requests for interception	Request for live interception of voice, SMS, fax and data traffic (lawful interception).
Requests for customer metadata	Requests for CDR (call data records) or IP addresses, past call, SMS, email traffic, Internet traffic information, or documents from cloud services, or requests for location information (physical / base station or GPS information).
Requests for Mobile Financial Services (MFS) related data	Requests for information relating to MFS, such as confirming an individual is an MFS customer, transaction data and other account activity.
Take down of data	Requests to block access to specific websites or web pages, including criminal material.

Other types of request relating to shutdown of services, for continuous access to the network, for blocking of subscribers, for implementation of equipment for additional monitoring, or requests to push specific information to subscribers require a separate procedure, in line with existing incident reporting or crisis management procedures.

[1] The right to privacy is enshrined in the Universal Declaration of Human Rights (UDHR), Article 12, and in the International Covenant on Civil and Political Rights (ICCPR), Article 17. The right to freedom of expression is enshrined in the UDHR, Article 19, and the ICCPR, Article 19. See also ITU Constitution: ARTICLE 34, 35, 37.

III. 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 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.

IV. DOCUMENT HISTORY

File Version	Rev 2.0
Full version approved on	27-Apr-2015
File reviewed and updated	12-Dec-2017
File Status	Final

./.