



# National Emergency Telecommunications Plans: Enablers and Safeguards

A brief evaluation guide for  
policy practitioners

December 2021



The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at [gsma.com](http://gsma.com)

Follow the GSMA on Twitter: [@GSMA](https://twitter.com/GSMA)



This initiative has been funded by UK Aid from the UK Government and is supported by the GSMA and its members. The views expressed do not necessarily reflect the UK Government's official policies.

**Author:**

Ken Okong'o (Senior Policy and Advocacy Manager, Mobile for Humanitarian Innovation, GSMA)

**Contributors:**

Kimberly Brown, (Head of Mobile for Humanitarian Innovation, GSMA)

Jenny Caswell, (Insights Director, Mobile for Humanitarian Innovation, GSMA)

Olly Parsons, (Director, Mobile for Humanitarian Innovation Fund, GSMA)

Isaac Kwamy, (Senior Manager, Market Engagement and Strategic Partnerships, Mobile for Humanitarian Innovation, GSMA)

## GSMA Mobile for Humanitarian Innovation

The GSMA Mobile for Humanitarian Innovation programme works to accelerate the delivery and impact of digital humanitarian assistance. This is achieved by building a learning and research agenda to inform the future of digital humanitarian response, catalysing partnerships and innovation for new digital humanitarian services, advocating for enabling policy environments, monitoring and evaluating performance, disseminating insights and profiling achievements. The programme is supported by the UK Foreign, Commonwealth & Development Office.

Learn more at [www.gsma.com/m4h](http://www.gsma.com/m4h) or contact us at [m4h@gsma.com](mailto:m4h@gsma.com)

Follow GSMA Mobile for Development on Twitter: [@GSMAM4d](https://twitter.com/GSMAM4d)

# Contents

---

<b>Overview of the guide</b>	<b>2</b>
Background	2
National Emergency Telecommunications Plans (NETPs)	3
About this guide	5

---

<b>Section 1: Enabling policy environments</b>	<b>6</b>
Purpose	6
Implementation	7
Policy areas of focus	7

---

<b>Section 2: Data infrastructure</b>	<b>8</b>
Purpose	10
Implementation	11
Policy areas of focus	11

---

<b>Section 3: In-depth consultation</b>	<b>12</b>
Purpose	12
Implementation	12
Policy areas of focus	12

---

<b>Conclusion</b>	<b>13</b>
-------------------	-----------

---

<b>Appendix: Assessment framework for an NETP</b>	<b>14</b>
Pillar 1: Policy (“enablers”)	14
Pillar 2: Laws (“safeguards”)	15
Pillar 3: Institutions	16



# Overview of the guide

## Background

Humanitarian needs are on the rise, with 235 million people in need of assistance worldwide.<sup>1</sup> New partnership models and innovative tools and approaches are crucial to address this growing humanitarian challenge. More and more, humanitarian organisations, the private sector and governments are working together to mitigate risk, strengthen disaster preparedness and provide logistical assistance in response to humanitarian crises. Mobile technology has become critical to the success of disaster response efforts and the delivery of humanitarian aid. In low- and middle-income countries (LMICs), better access and increased use of mobile technology has dramatically expanded how countries are preparing for and responding to humanitarian crises.

---

<sup>1</sup> UN OCHA. (2021). [Global Humanitarian Overview 2021](#).

As governments leverage mobile to manage crisis situations, for example, to distribute cash assistance through mobile money, many are developing policies and establishing institutions to enable these new and innovative approaches. In collaboration with the humanitarian community, some governments are developing disaster response frameworks that rely on telecommunications, often referred to as National Emergency Telecommunications Plans (NETPs). These plans provide an opportunity for mobile-enabled emergency telecommunications to play a more expansive and impactful role in disaster preparedness, response and recovery.

## National Emergency Telecommunications Plans (NETPs)

An NETP is a strategy document that outlines telecom-supported activities in times of crisis. It provides a policy and regulatory framework to guide the use of mobile in disaster risk management, and the relevant, step-by-step actions to be taken in each phase of the disaster management cycle beyond the role of the mobile sector.<sup>2</sup> A sound NETP is expected to describe a country's telecommunications landscape and stakeholders, including the potential roles of MNOs and service providers. It may also define Standard Operating Procedures (SOPs) and relevant treaties and international cooperation agreements.

An NETP is intended to promote coordination across all levels of government. Stakeholders become engaged in mapping the life cycle of a potential disaster and identifying the capacities, skills and capabilities required in an emergency response. Part of this process is establishing a governance framework that defines the roles and responsibilities of different players through a multi-stakeholder approach.<sup>3</sup> Another task is creating a clear procedure or plan to use and share information or data with public, private and humanitarian stakeholders, as this is essential to an efficient and resilient approach to disaster response. A thorough and carefully considered NETP should outline effective ways to achieve and communicate expected results. Therefore, the operating environment and

soundness of a country's disaster response policy or plan should be able to be tested across a range of plausible futures or scenarios.

In 2019, the International Telecommunications Union (ITU) published the *ITU Guidelines for National Emergency Telecommunication Plans*, which detail, step-by-step, how to develop an NETP.<sup>4</sup> The Guidelines provide a framework for countries to assess their current policy environment for mobile-enabled emergency telecommunications, evaluate the soundness of a mobile-enabled NETP, chart pathways to refine an existing NETP and maximise the potential of mobile as a lifesaving tool in times of humanitarian crisis. Since every country has unique technological capabilities, institutional and policy requirements, the guidelines were designed to be flexible enough to support national assessments and evaluations, and to develop and implement NETPs tailored to different contexts.

The ubiquity of mobile means mobile is becoming a default method of communication and this offers positive contributions pre-, during and post disaster. This guide was developed by the GSMA Mobile for Humanitarian (M4H) Innovation programme to support regulators and policy makers make a rapid assessment of mobile-enabled NETPs and support structures to mitigate the impacts of disasters.

<sup>2</sup> ITU. (2019). [ITU Guidelines To Prepare a NET Plan](#).

<sup>3</sup> World Bank. (2019). ["Emergency Communications"](#).

<sup>4</sup> ITU. (2019). [ITU Guidelines for National Emergency Telecommunication Plans](#).



# About this guide

The guide is divided into three sections.



**Section 1** focuses on **creating an enabling environment**. Mobile network operators (MNOs) operate in a regulated environment.<sup>5</sup> However, if this environment is not sufficiently enabling to support disaster preparedness, response and recovery, MNOs will encounter challenges when disaster strikes. This section provides a broad overview of a country's mobile landscape by helping practitioners to appraise the policy, legal and regulatory environment and identify key areas for policy intervention.



**Section 2** focuses on **data sharing**. Here, practitioners can take a closer look at the data ecosystem by examining not only the policy and regulations that exist on paper, but also what it takes to implement data infrastructure and policies for using and protecting data across the humanitarian ecosystem. These include institutional mandates, technological options, human capabilities, incentives and enforcement mechanisms. Understanding how infrastructure systems, processes, people and policies support humanitarian innovation in practical ways is key.



**Section 3** provides an analysis of **use cases** in mobile-enabled emergency telecommunications. These use cases help to capture the lived experiences of those in the humanitarian ecosystem and guide policy reviews in support of government priorities, use cases and humanitarian interventions.

This guiding framework (see the Appendix) is intended to be a living document, and questions or policy areas may be refined as the GSMA Mobile for Humanitarian Innovation (M4H) programme continues to seek insights into mobile-supported emergency telecommunications and disaster response frameworks.

<sup>5</sup> GSMA. (2020). [Building a Resilient Industry: How Mobile Network Operators Prepare for and Respond to Natural Disasters](#).



## Section 1

# Enabling policy environments

Policies, laws and rules are central to emergency telecommunications. They are the foundation upon which the roles and responsibilities of stakeholders are defined.<sup>6</sup> The policy environment determines the framework for coordination mechanisms, communication channels and operating procedures. The policies help to identify decision-makers and decision-making structures within relevant agencies and define how best to deliver outcomes for society and the economy.<sup>7</sup> They also help make disaster risk management process more sustainable, as disaster management policies often outlast government administrations. Therefore, policies are not only needed to streamline decision making

and achieve rational outcomes, but also to establish a formal basis for achieving the goals or priorities of a government or institution that adopts and enforces them.<sup>8</sup> For instance, MNOs hold personal and non-personal data of their customers. The data can provide a dynamic and near real-time picture of the mobility of millions of people in a market. These metadata records may be analyzed to extract insights that, in combination with other data sources, can be shared with decision-makers in a timely manner.<sup>9</sup> However, the challenge in many markets is whether the policy environment is supportive of such actions.

## Purpose

Given the critical role of MNOs in disaster response and the proliferation of mobile connections around the world, mobile networks can be a lifesaving tool when disaster strikes.<sup>10</sup> Mobile technology can be used to amplify the voices of those affected by disaster, facilitate more dignified aid delivery, monitor disaster-affected environments and anticipate crises and hazards.<sup>11</sup> Mobile networks assure the timely flow of vital and lifesaving data and information, but this depends on the policies and standards that guide service provision. This highlights the need to strengthen regulatory foundations to make MNO infrastructure more resilient, to build trust in the system and to enable MNOs to provide value to the humanitarian community.<sup>12</sup>

This assessment considers a country's emergency telecommunications policy and governance landscape. It examines a spectrum of issues, distilling the complexities of the digital ecosystem and identifying key areas for policy intervention. This assessment can ultimately support the mobile industry in saving lives and providing essential services in humanitarian contexts. The assessment is not prescriptive, rather, it documents the current state of policy and regulation on mobile-enabled emergency telecommunications and humanitarian innovation in general.

6 United Nations Office for Disaster Risk Reduction. (2018). [Annual Report](#).

7 GSMA. (n.d.). [GSMA Mobile Policy Handbook: Business Environment](#).

8 UNHCR. (2019). [Connectivity for Refugees](#).

9 World Bank. (2010). [Natural Hazards, Unnatural Disaster: The Economics of Effective Prevention](#).

10 Granryd, M. (22 August 2017). "[Five ways mobile can help in humanitarian emergencies](#)". [World Economic Forum Global Agenda](#).

11 GSMA. (2020). [Partnering During Crisis](#).

12 GSMA, ITU, World Bank and WEF. (2020). [Digital Development Joint Action Plan and Call for Action](#).



## Implementation

The assessment is conducted primarily through desk research of existing or proposed policies, plans and regulations. A formal survey may also be conducted

in collaboration with the telecommunications regulator or government agency that oversees disaster response work, or with a local policy expert.

## Policy areas of focus

Pillar to assess	Components and elements
<b>Policy</b>	<ul style="list-style-type: none"><li>• Vision of digital transformation (e.g., leaders or champions)</li><li>• Mobile connectivity (e.g., access, affordability, availability and quality)</li><li>• Data governance and cybersecurity (e.g. data privacy and data-sharing policy)</li><li>• Whole-of-government approach (e.g., systems interoperability and open data sets)</li></ul>
<b>Laws</b>	<ul style="list-style-type: none"><li>• Legal systems (e.g. international conventions and treaties)</li><li>• Personal data protection (e.g. soundness and robustness of the data protection policies)</li></ul>
<b>Institutions</b>	<ul style="list-style-type: none"><li>• Governance, coordination and partnerships (e.g., mandates, interactions and resource capacities)</li><li>• Digital skills and human capital development (e.g. continuous training and capacity building plans)</li></ul>



## Section 2

# Data infrastructure

Data frameworks define who has authority and control over data assets, both personal and non-personal. The frameworks also describe how data assets may be used, including the people, processes and technologies needed to manage and protect them.<sup>13</sup> Every country must execute decision rights and accountability for data infrastructure and processes in line with agreed-upon models. For instance, data from MNO call detail records (CDR) may provide valuable insights into population flows. Flowminder uses an open-source code installed at MNO data centres to enable them to analyse their CDRs. These can be used to monitor population flows pre- and post-disaster and have been used to support targeted relief efforts.<sup>14</sup> Since this data could then be repurposed to infer patterns of human mobility and support decision making in a crisis, there is not only a need for a documented set of policy guidelines, but also data infrastructure to ensure that data or information assets are managed, stored and processed properly. This may require creating policies on data quality, standards, protection, security, privacy, access or data-sharing platforms, as well as defining the roles of each actor in the data ecosystem, including those responsible for implementing and monitoring compliance.

When designing and implementing humanitarian activities at the country level, discussions on data infrastructure and privacy typically include the following stakeholders:

- Governments, including national and local government ministries, departments, secretaries and other public bodies. They are responsible for providing the enabling conditions and resources for the development of a data protection and privacy regime; appropriate and secure hardware systems; and a structure to enforce data protection legislation.
- Policymakers and lawmakers, who are responsible for drafting data protection and privacy laws, which can be sectoral, cross-cutting or comprehensive. They also create legislation that defines the obligations and rights of different stakeholders and sanctions for violations. In a humanitarian context, this includes violation of data of persons of concern.
- Data protection authorities (DPAs), which are an independent public authority that supervises compliance with data protection and privacy legislation. These authorities are generally responsible for providing guidance on national data protection legislation, enforcing data protection laws by investigating alleged privacy violations and imposing sanctions when the law is breached.

<sup>13</sup> GSMA. (2018). [Regional Privacy Frameworks and Cross-Border Data Flows](#).

<sup>14</sup> Migration Data Portal. (2021). [The "FlowKit": Tool for rapid and near real-time assessments of population displacement after natural disasters using mobile phone data](#).

- Data subjects, who, in this context, may be the recipients of humanitarian aid and whose personal data is being processed. They should be enabled to become active stakeholders, taking control of their personal data and privacy by understanding the risks involved and exercising their rights related to personal data and privacy.
- Data controllers and processors, which include any stakeholder that controls and/or processes personal data (e.g., social protection schemes and programmes, private sector companies, development agencies, governments and MNOs). They are responsible for safeguarding personal data, respecting the rights of data subjects and demonstrating compliance with data protection and privacy principles and legislation.
- Development and humanitarian agencies and other partners, which may be dedicated to distributing aid and promoting economic growth and development in the areas they serve. Externally, their role is to advise and support country governments to develop and/or improve their data protection and privacy frameworks and enforcement mechanisms. Internally, they are responsible for demonstrating compliance with data protection and privacy principles and internal guidelines, and with the legislation to which they are subject.
- Civil society, which may include activists, academics, employers' and workers' organisations or consumer protection organisations that lobby governments, lawmakers or other stakeholders. These groups ensure that data subjects have rights to their personal data, supervise respect for these rights, report violations and raise public awareness of data protection and privacy.

Timely, accurate and reliable data are vital to an effective and efficient response in humanitarian emergencies.<sup>15</sup> To ensure that data is transparent and processed in a way that supports humanitarian outcomes, the stakeholders and partners in humanitarian action listed above need to apply a critical lens to every aspect of the process.<sup>16</sup> These analyses create a complete picture and understanding of data processes. Therefore, disaster risk reduction operations need to be carried out collaboratively by humanitarian organisations, MNOs, government and emergency units on various administrative levels using accurate and reliable information, as there is a direct link between disaster risk reduction and data frameworks.<sup>17</sup>

However, there are several barriers to data use and interoperability that can stagnate response and information flows. These barriers are often complex and intertwined.<sup>18</sup> The reasons for this complexity may differ at the local, national, regional and global level, including the number of actors involved, such as civil protection, firefighters, health care services, municipalities and non-profit organisations, among others. Effective cooperation between these actors requires an enabling environment, efficient data exchange platforms and a collaborative mechanism.<sup>19</sup>

<sup>15</sup> LODGD. (2019). [Next Generation Disaster Data Infrastructure](#).

<sup>16</sup> DSEG. (2020). [Framework for Ethical Use of Advanced Data Science Methods in the Humanitarian Sector](#).

<sup>17</sup> GSMA. (2019). [Mobile Big Data Solutions for Better Future](#).

<sup>18</sup> GSMA. (2019). [Data Privacy Frameworks in MENA](#).

<sup>19</sup> World Bank. (2016). [Open Data for Resilience : Policy Notes and Principles](#).



## Purpose

Mobile network data or mobile big data represent vast amounts of information, and can be transformative resources for social good.<sup>20</sup> For example, MNO data can be used to predict disease outbreaks or to respond more effectively in humanitarian crises.<sup>21</sup> However, mobile data is more meaningful when policy environments and data platforms are enabling and allow data to be shared in the right format and benefit the private sector, humanitarian organisations and government. Reusing this data repeatedly may also help to extract a range of informative insights for aid and relief agencies. For instance, in 2020 during the early stages of the COVID-19 pandemic, Flowminder, in partnership with Vodafone Ghana and the Ghana Statistical Service, released useful insights on population mobility. The analyses provided responders with timely information that alerted policymakers to areas needing attention in a fast-changing situation.<sup>22</sup>

Creating a data-sharing environment in which transactions between MNOs, other data aggregators and data users are trusted requires the right mix of data governance practices, institutional frameworks and technical architecture. These “enablers” and “safeguards” are important when leveraging

mobile data for humanitarian action and ensuring that the benefits of data are shared by diverse groups of stakeholders. They must also ensure data transactions with third-party data brokers are secure.<sup>23</sup> In fact, without adequate safeguards, MNOs, data users, data subjects and other data aggregators may not trust the system or have confidence that data can be shared without the risk of abuse. Without enablers such as frameworks for interoperability and data portability, it may become a challenge for responders and aggregators to share data in an agile manner.

Therefore, an inclusive mobile-enabled disaster response framework requires understanding the factors that create a trusted data-sharing environment, which may be different for every country. These factors include the extent to which the regulatory environment defines and enacts the rights of the vulnerable over their data, the institutional capabilities to enforce the rules while offering humanitarian actors effective support, the technical architecture to standardise data sharing across humanitarian organisations, the human and organisational capabilities, as well as additional safeguards for government overreach.<sup>24</sup>

---

20 GSMA. (2017). [State of Mobile Data for Social Good](#).

21 GSMA. (2021). [Developing Guidelines for Cash Transfers in Somalia](#).

22 GSMA. (2021). [Building Resilience Through Mobile Enabled Solutions](#).

23 GSMA. (2018). [Guidelines on Mobile Money Data Protection](#).

24 GSMA. (2017). [Safety, Privacy and Security across the Mobile Ecosystem](#).



## Implementation

This assessment may be conducted through desk research and/or direct engagement with policy actors and regulatory authorities. The exercise

requires a local expert with deep relationships across the digital and data ecosystem who can facilitate connections and navigate local dynamics.

## Policy areas of focus

To understand data frameworks, it is necessary to focus on policy approaches relevant to data across the government, to political will and to the existing or aspirational national data agenda. To understand the policies or regulations governing data sharing and the conditions shaping those policies, questions

will need to be posed to relevant stakeholders. These stakeholders must include government, MNOs and humanitarian organisations, with a special focus on policy priorities, institutions and data or technology architecture.

### Pillars to assess

### Components/elements

#### Priorities and Goals

- Shared vision of stakeholders involved in the national data agenda
- Nature of data handled and data policy concerns (e.g., security and privacy)
- Data protection regulations

#### Institutions

- Overseer or supervisor of data policy
- Clarity of institutional mandates – regulatory, policy or implementation
- Data-sharing policy across government and between government and the private sector, including MNOs
- Resource capabilities (e.g., budgets, skilling and reskilling)
- A whole-of-government approach to data governance

#### Technology

- Investment in technology to facilitate data sharing
- Interoperability of data systems
- Specific investment in open data, digital ID and payment systems



### Section 3

# In-depth consultation

## Purpose

An in-depth consultation assesses the practical provision of emergency telecommunications services, logistics and data sharing in the context of specific government priorities. It captures a use case or the lived experience of actors in the ecosystem, and a detailed analysis of use cases that feature mobile technology used in humanitarian contexts,

for example, information as aid<sup>25</sup> or mobile money-enabled cash assistance. The consultation may provide an overview of the practical challenges facing the humanitarian sector or identify how impact could be enhanced through regulatory interventions or conducive policies.

## Implementation

This exercise may be conducted through direct engagement and focus groups with experts or stakeholders in the humanitarian sector, policymakers or those implementing the specific use

cases. However, it is important to have a government champion to identify government priorities, and a representative of the humanitarian sector to highlight use cases of interest.

## Policy areas of focus

Given the intended level of detail, interview guides may need to be tailored to specific use cases. The following is an example of a script to assess policy concerns with cash and voucher assistance (CVA) programming:

1. Understand the experience of combining and sharing personal data across humanitarian organisations to register customers and recipients without proof of identification (ID). Does the existing policy framework support this? What key factors make this a success? What are the difficulties and hurdles with the policy?
2. How did the telecommunications sector or custom regulations impact cross-border flows of personnel and equipment? These may include many factors that are unique to a country and that emergency telecommunications policy should anticipate.
3. What public sector institutions are key in coordinating MNO forces in a crisis situation? What are the critical success factors that drive the coordination?
4. What key factors enable or hinder the sharing of data, infrastructure or other support services? Is it technology architecture, inter-agency coordination mechanisms or human capital or leadership?
5. How would you characterise overall trust in infrastructure and data sharing? Between government agencies, between the government and the private sector (e.g., MNOs)?

<sup>25</sup> NetHope. (2019). "Centre for Disaster Philanthropy Grant Drives Information as a Form of Aid". NetHope Blog.



## Conclusion

This guide has aimed to help identify the gaps, opportunities and weaknesses in the system to inform a more coherent national strategy and position mobile to support disaster preparedness, response and recovery. A full assessment of the needs and capabilities of a country, its agencies and the state of its policies form the basis for refining existing emergency telecommunications strategies and plans, as well as integrating mobile-enabled NETP aspirations in an overall country disaster response or national development plan.



# Appendix: Assessment framework for an NETP

## Pillar 1: Policy (“enablers”)

	Question	Yes/No	Comments
1	Does the government have a shared vision for digital transformation?		
2	Is the digital transformation linked to a development agenda?		
3	Does the government have a humanitarian innovation agenda?		
4	Is (3) linked coherently to (1) and (2)?		
5	Is there a clear national humanitarian innovation implementation road map?		
6	Are there clear policy provisions for incentives to expand and accelerate the impact of digital humanitarian assistance? (e.g., tax credits, relaxed SIM registration rules)		
7	Does the National Critical Infrastructure Plan articulate emergency telecommunications?		
8	Does the country have a plan for a data-sharing infrastructure?		





Question	Yes/No	Comments
9   If Yes to 8, does the accessibility include access by international (commercial) and/or local (government and commercial) to government data infrastructure?		
10   Does 8 include the storage, analysis and sharing of data to promote quicker and/or more flexible delivery of humanitarian services?		
11   Does the government have an interoperability framework with mandatory standards for its agencies' systems?		
12   Does the government have an open data policy?		
13   Does the government have a National Emergency Telecommunications Capacity Development Plan?		

## Pillar 2: Laws (“safeguards”)

Question	Yes/No	Comments
1   Do the law or enabling legal instruments provide for an agency to oversee or supervise the provision of emergency telecommunications services?		
2   Do the law/implementing regulations provide for an agency to oversee or supervise the provision of emergency telecommunications services?		
3   Is the entity in (2) sufficiently resourced to undertake its functions effectively?		
4   Is there a general data protection law or specific instruments governing the processing of personal and sensitive data of a vulnerable population?		



## Pillar 3: Institutions

	Question	Yes/No	Comments
1	Do relevant ministries, departments and agencies have clear mandates and appropriate capabilities, supervisory and oversight functions for emergency telecommunications services?		
2	Is there an entity with clear authority over personal data protection?		
3	Are there training opportunities or roundtables for MNOs, regulators and policymakers?		
4	Are there specific initiatives to raise awareness or train citizens on emergency telecommunications and/or data protection laws?		
5	Do the existing plans articulate clear responsibilities and roles for relevant public sector agencies responsible for: <ul style="list-style-type: none"><li>• Health</li><li>• Security</li><li>• Air travel</li><li>• Ambulance</li><li>• Power supply</li><li>• Refugee affairs</li><li>• Identity issuance</li><li>• Customs clearance</li><li>• Immigration services</li><li>• Disaster management</li><li>• Drought management</li><li>• Personal data protection</li><li>• Transportation and roads</li><li>• Telecommunications regulation</li><li>• NGO coordination or regulation</li><li>• Capacity building for policymakers</li><li>• Universal service fund for connectivity</li><li>• Foreign affairs and international linkages</li><li>• Financial sector regulations (e.g., mobile financial services)</li></ul>		

**gsma.com**



For more information, please visit the  
GSMA website at [www.gsma.com](http://www.gsma.com)

**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