# COMMUNICATIONS TRANSPARENCY REPORT 2022

# TABLE OF CONTENTS



# INTRODUCTION; SCOPE OF THE REPORT

**This Communications Transparency Report (this "Report") is reflective of América Móvil's commitment to protecting the universal rights to privacy and freedom of expression and is intended to assist in developing a more informed society. In this Report, the terms "América Móvil," the "Company," "us" and "our" mean América Móvil, S.A.B. de C.V., individually and/or together with its subsidiaries, as the context may require.**

Our ability to safeguard our customers' rights to the protection of their personal data and the privacy of their communications is critical for retaining their trust in our Company and preserving the reputation by which we have been characterized since our inception.

We reaffirm our commitment to the full satisfaction of all of our obligations under the laws of each of the countries in which we operate. Accordingly, we endeavor to comply with all applicable laws, cooperate with all Competent Authorities in connection with their investigations and enforcement actions, and guarantee the privacy of communications and the protection of the information with which we are entrusted.

Our teams are engaged in an ongoing effort to assess and address all government and court orders for data records and ensure that such data are handled in compliance with our internal security protocols and all applicable laws. This implies, rejecting any demands or requests not originated from a Competent Authority (e.g., private parties or individuals, etc.) and in certain cases, reserving the right of notifying the users involved in the requirements, since it may compromise national security.

This Report is being published in an effort to provide our stakeholders with certainty about the corporate policies and internal procedures followed by our operating divisions as with respect to our cooperation with the Competent Authorities and the discontinuance of service.

Consistent with our commitment to transparency, this Report is comprised of the following sections:

- A shared responsibility.
- Legal framework for our duty of confidentiality obligation in connection with government orders and for the discontinuance of service.
    - América Móvil´s internal process for addressing oficial communications from Competent Authorities[1].
- General provisions that apply in the countries in which we operate.

[1] For purposes hereof, order means one or more requests for information about one or more of our customers.

# A SHARED RESPONSIBILITY

América Móvil has developed a comprehensive security strategy that comprises (i) cybersecurity, (ii) data privacy and (iii) communications privacy, based on three core principles: (a) **integrity**, (b) **availability** and (c) **confidentiality**. Our abidance by these principles is critical to our activities and operations.

This statement is especially relevant where the privacy of our customers' communications is concerned, not just as a matter of corporate principle and legal requirement, but more so because our customers' trust and confidence in us are at stake.

Those of our subsidiaries who hold concessions or authorizations for the provision of telecommunications services are required by law to comply with each and every lawful order of a Competent Authority, whether written or in electronic format, in the manner set forth in the applicable laws of their respective countries.

To meet these obligations, we have assigned dedicated teams and developed a stringent set of security protocols and specific criteria for assuring the validity of every request we receive from a Competent Authority.

Our guidelines principles[2] with respect to the privacy of communications are as follows:

1. No one may listen in any conversation or monitor any transmission of data or other communication, or disclose its existence or contents, except upon a lawful written order of a Competent Authority.
2. We may only turn over personal data or geolocate, block, impose service limitations on or keep track or a log of the communications associated with a mobile telephone line where required by law and upon a lawful order of a Competent Authority.
3. We do not prioritize, block, or delay traffic, applications, protocols, or content for reasons beyond assuring quality of service and network reliability. Our commercial offer for unlimited usage on certain social media apps implies that the user will not be charged for the data used by those applications or web pages. Under no circumstances will the traffic of those apps be prioritized over the rest of the navigation.

América Móvil's Privacy Policy and its enforcement are reviewed annually to ensure that they remain current and effective. If you have any question in regarding with the above, please contact us at privacidad@americamovil.com.

[2] América Móvil's Privacy Policy is available for consultation a: https://sustainability.americamovil.com/portal/su/pdf/10_Privacy-and-Personal-Data-Protection-Policy-(vigente-110522).pdf

# LEGAL FRAMEWORK FOR OUR DUTY OF CONFIDENTIALITY WITH RESPECT TO GOVERNMENT ORDERS AND FOR THE DISCONNECTION OF SERVICES

## NORTH AMERICA AND THE CARIBBEAN

## Statutory obligation to address the requests of Competent Authorities.

### PUERTO RICO

The América Móvil subsidiaries that provide telecommunications services in Puerto Rico (a U.S. territory) are subject to the rules and regulations for the *Federal Communications Commission* ("FCC") and the laws and regulations relating to the privacy of customer information, including Section 222 of the Communications Act of 1934, and are required to comply with the following:

i) **Disclosure of Customer Proprietary Network Information, or CPNI.** Pursuant to the Federal laws and the rules and regulations relating to the authority of the FCC, telephone carriers and VoIP service providers have a duty to protect the confidentiality of their customers' proprietary information and may only use, disclose or permit access to a customer's information (1) where required by law, (2) with the approval of the customer or; (3) in regarding with the provision of the telecommunications service from which such information is derived.

ii) **Geolocation of mobile devices in real time.** The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001.

iii) **Interception of private communications.** The Electronic Communications Privacy Act, or ECPA, regulates law enforcement access to electronic data and addresses certain specific types of data. Title I of the ECPA, which is called the Wiretap Act, regulates the manner in which the government may listen in or intercept the content of private communications, including telephone conversations. Title II of the ECPA is called the *Stored Communications Act, or SCA*. The interception of private communications is also subject to regulation under 18 U.S. Code § 2511 (Interception and disclosure of wire, oral, or electronic communications prohibited).

iv) **Discontinuance of telecommunications services upon court order.** The FCC has established certain procedures to protect customers in the event of discontinuance, reduction or impairment of service by a carrier for any reason. These procedures are intended to protect customers against service discontinuance or sudden changes to contract terms, allowing them a sufficient amount of time to secure service from another carrier. Any U.S. telephone carrier that seeks to discontinue, reduce, or impair the services it provides must:

- Notify its customers in writing and advise them of their right to file comments with the FCC.
- Following the delivery of notice to its customers, file with the FCC an application for authorization to discontinue, reduce or disable its services.
- Continue to provide services during a period of no less than 31 days after the release of a public notice of its discontinuance application by the FCC if the carrier is nondominant, or 60 days if dominant; provided, that such period may be extended by the FCC.

**Competent Authorities:** The heads of the security and law enforcement agencies are responsible for appointing officials authorized to request and receive information from carriers.

**Note:** Pursuant to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, such information must be classified as confidential.

## MEXICO

The América Móvil subsidiaries that provide telecommunications services in Mexico are required to cooperate with national security and law enforcement authorities under Article 189 of the Federal Law on Telecommunications and Broadcasting (*Ley Federal de Telecomunicaciones y Radiodifusión, or LFTR*), and to comply with the following:

i) **Delivery of data records to Competent Authorities**. Article 190-II(a)-(h) and III of the LFTR.
ii) **Geolocation of mobile devices in real time.** Article 190-I of the LFTR, Article 303 of the National Code of Criminal Procedures (Código Nacional de Procedimientos Penales, or CNPP) and item 15 of the Guidelines for Security and Law Enforcement (*Lineamientos de Colaboración en Materia de Seguridad y Justicia, or Cooperation Guidelines*).
iii) **Interception of private communications.** Articles 291-294 and 301 of the CNPP, articles 34-42 of the National Security Law (*Ley de Seguridad Nacional*), Article 24 of the General Law to Prevent and Punish Kidnapping Crimes (*Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro*) and articles 16-21 and 26 of the Federal Law to Combat Organized Crime (*Ley Federal Contra la Delincuencia Organizada*).
iv) **Discontinuance of telecommunications services upon court order.** Article 190-VI of the LFTR**.**
v) **Blocking of communication lines used for the commission of criminal offenses.** Article 190-VII of the LFTR.

**Competent Authorities:** The heads of the security and law enforcement agencies are responsible for appointing officials authorized to request and receive information from carriers, through the publication of a resolution to such effect in the Official Gazette of the Federation (*Diario Oficial de la Federación*).

**Note:** Pursuant to the Cooperation Guidelines, such information must be classified as confidential.[3]

[3] *"**SEVENTH.** The concessionaires and Licensees are required to address the requests of the Designated Authorities in accordance with the foregoing guidelines:*

## DOMINICAN REPUBLIC

America Movil subsidiaries that provide telecommunication services in the Dominican Republic are required to cooperate with the Prosecuting Attorney´s (Ministerio Público) and its ancillary agencies under Article 44(3) of the Constitution of the Dominican Republic (*Constitución de la República Dominicana*), which provides that the secrecy of communications is inviolable except upon a lawful order of a competent court for the seizure, interception or recording of communications in the interest of justice.

Pursuant to the Organic Law for the Prosecuting Attorney's Office (*Ley Orgánica del Ministerio Público*), or Law No. 133-11, the Prosecuting Attorney's Office is responsible for all practical aspects of the criminal investigations conducted by such Office, the police and any other executive, security or government agency responsible for performing ancillary investigation activities for judicial system purposes.

**Applicable Laws:**

- Article 44 of the Constitution of the Dominican Republic;
- Article 192 of Law No. 76-02, Which Contains the Code of Criminal Procedure for the Dominican Republic (*Ley No. 76-02 que Establece el Código Procesal Penal de la República Dominicana*);
- Article 6 of General Telecommunications Law No. 153-98 (*Ley General de Telecomunicaciones No. 153-98*);
- Law No. 53-07 on High Technology Crimes and Misdemeanors;
- Resolution No. 2043-2003 of the Supreme Court of Justice, which contains the Regulations Relating to Court Authorizations for the Electronic Surveillance and Interception of Communications (Reglamento Sobre Autorización Judicial para la Vigilancia e Interceptación Electrónica de Comunicaciones); and
- Decision No. 0200-13 of the Constitutional Tribunal, which provides that the duty of confidentiality owed by telecommunications carriers is not limited solely to the data derived from communication processes but, rather, is extensive to any personal information or data provided by their customers at any public or private telecommunications service center as a condition for accessing such information or data.

In addition, such subsidiaries must comply with the following:

i) **Delivery of data records to Competent Authorities.** Article 56 of Law No. 53-07 on High Technology Crimes and Misdemeanors (Ley No. 53-07 Sobre Crímenes y Delitos de Alta Tecnología).

ii) **Geolocation of mobile devices in real time.** Article 56 of Law No. 53-07 on High Technology Crimes and Misdemeanors.

iii) **Interception of private communications.** Article 192 of the Code of Criminal Procedure for the Dominican Republic (Código Procesal Penal de la República Dominicana).

---

*A. About the Authorized Department responsible for addressing requests for the real-time geolocation of Mobile Devices or Terminals, the delivery of data records and the interception of private communications:*
*The information provided by such Authorized Department must be classified by such authorities and by the Institute as confidential or reserved in accordance with the applicable laws, and ..."*

iv) **Real-time interception of telecommunications**. Article 192 of the Code of Criminal Procedure for the Dominican Republic (Código Procesal Penal de la República Dominicana).
v) **Discontinuance of telecommunications services upon court order**[4]. Article 6 of General Telecommunications Law No. 153-98 (Ley General de Telecomunicaciones No. 153-98).
vi) **Blocking of communication lines used for the commission of criminal offenses.** Article 6 of General Telecommunications Law No. 153-98 and Article 14 of the Regulations Relating to the Rights and Obligations of Users and Carriers (*Reglamento de Derechos y Obligaciones entre Usuarios y Prestadoras*).[5]

**Competent Authorities:** The Prosecuting Attorney's Office and its ancillary agencies.

**Nota:** Pursuant to the Cooperation Guidelines, such information must be classified as confidential.[6]

## Procedure for Addressing Requests from Competent Authorities in North America and the Caribbean

In general terms, under the legal framework in effect in these regions, information may be disclosed, and communications may be intercepted only upon a lawful written request of a Competent Authority or order of a competent court in connection with matters submitted to the justice system, through lawful procedures that ensure the preservation of the secrecy of such information or communications.

Our subsidiaries perform a detailed review and analysis of each request in order to ensure our compliance with the law and ascertain that the human rights of our customers will be respected. This procedure entails the following:

- A legal analysis of the orders of Competent Authorities to determine whether they are valid and lawful.
- Upon verification of the satisfaction of all legal requirements, the preparation and processing of the information requested by the Competent Authorities.
- The preparation of an official response to the Competent Authorities.
- The delivery of the relevant information to the Competent Authorities through procedures that ensure that such information cannot be altered and will remain confidential.

[4] In the event of the commission of a criminal offense relating to telecommunications services or involving the use thereof, the Prosecuting Attorney's Office may move the relevant court to consider authorizing the suspension or cancellation of such services and, if such motion is granted, such services may be canceled upon such decision.
[5] A carrier is entitled to disconnect or remove from its network any customer who has used its services in a manner not consistent with the applicable laws and regulations, public order, and good customs. Similarly, under Article 8 of the Regulations for Telephone Services (*Reglamento de Servicio Telefónico*) carriers may discontinue the provision of services to any customer who is found to have set up clandestine or unauthorized connections to telephone services or to have used or gained access to such services in an unlawful or fraudulent manner (which constitutes a telecommunications crime under Law No. 53-07 on High Technology Crimes and Misdemeanors), whereupon such customer shall cease to be regarded as a primary user.
[6] Pursuant to Article 44.4 of the Constitution of the Dominican Republic, all official data and information obtained by the authorities responsible for the prevention, prosecution and punishment of criminal offenses must be handled, used, disclosed, or stored thereby in a manner such that it remains confidential and may only be disclosed to public registries upon commencement of a court action in accordance with the law.

**More specifically:**

## PUERTO RICO

The process for complying with the subpoenas and requests for customer records is managed by our Legal Department. Our Executive Resolutions Department is responsible for ascertaining the authenticity of each request for information and the identity of the customer (where applicable), and for gathering the relevant information and delivering such information to the agency or customer who requested it. The administrators of our Legal and Executive Resolutions departments oversee the enforcement and observance of our policies and procedures for addressing official and customer requests for information.

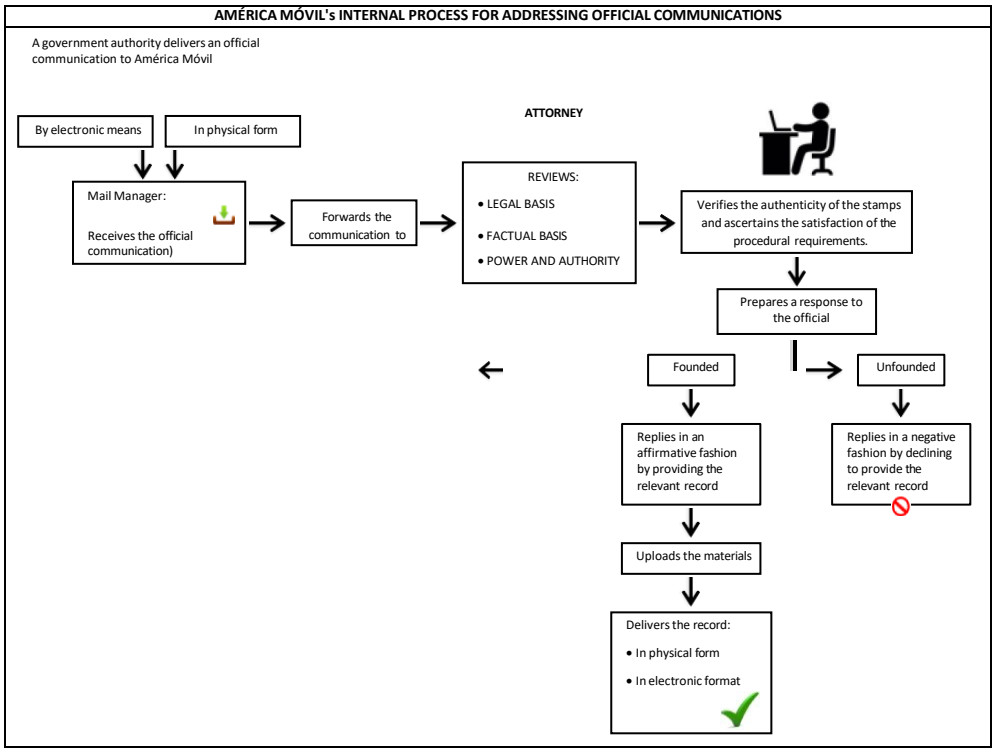
The Request Management Analyst and the Custodian of Records are the only individuals authorized to provide to any government authority any call detail record, credit card information, CPNI, personal identifiable information of customers, IP address information or any other information which is protected by law.

Subpoenas, orders for records and court orders may be delivered to the Request Management Analyst by hand, mail, email, fax or other means. Upon receipt of a subpoena, order for records or court order, the relevant document is reviewed to ascertain its authenticity and validity. All orders for records, grand jury subpoenas and court orders must be signed by a judge, magistrate, or other authorized court official and must include a docket or order number.

**More specifically:**

## MEXICO

The following flowchart depicts our process for addressing official communications from Competent Authorities:




# Number of Requests Processed in North America and the Caribbean

In 2022, our subsidiaries in **North America and the Caribbean** received an aggregate of **138,564** requests for customer proprietary information from government authorities. We fulfilled **137,354** requests for information or **99.2%** of the requests we received from Competent Authorities upon determining that such requests had been issued in accordance with the applicable law. The remaining **0.8%** (**1,210** requests) was not fulfilled either because the issuing authority was not a Competent Authority, or the request did not comply with all applicable legal requirements.

## CENTRAL AMERICA

# Statutory obligation to address the requests of Competent Authorities.

## COSTA RICA

The América Móvil subsidiary that provides telecommunications services in Costa Rica is required to cooperate with national security and law enforcement authorities under the Law to Combat Organized Crime (*Ley Contra la Delincuencia Organizada*), or Law No. 8754, the Law that Creates a Jurisdiction Specializing in Organized Crime in Costa Rica(*Ley de Creación de la Jurisdicción Especializada en Delincuencia Organizada en Costa Rica*), or Law No. 9481, the Law on the Registration, Seizure and Examination of Private Documents and the Interception of Communications (*Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones*), or Law No. 7425, and the General Telecommunications Law (*Ley General de Telecomunicaciones* ), as amended by Law No. 9597, and to comply with the following:

i) **Delivery of data records to Competent Authorities.** Law to Combat Organized Crime (*Ley Contra la Delincuencia Organizada*), or Law No. 8754.
ii) **Geolocation of mobile devices in real time.** Law on the Registration, Seizure and Examination of Private Documents and the Interception of Communications, or Law No. 7425.
iii) **Interception of private communications.** Law on the Registration, Seizure and Examination of Private Documents and the Interception of Communications, or Law No. 7425.
iv) **Discontinuance of telecommunications services upon court order.** Criminal Code (*Código Penal*), or Law No. 4573.
v) **Blocking of communication lines used for the commission of criminal offenses.** Law on the Registration, Seizure and Examination of Private Documents and the Interception of Communications, or Law No. 7425; and General Telecommunications Law, as amended by Law No. 9597.

**Competent Authorities:** The heads of the security and law enforcement agencies are responsible for appointing officials authorized to request and receive information from carriers.

**Note:** Pursuant to Article 24 of the Political Constitution of Costa Rica (*Constitución Política de Costa Rica*), Article 20 of the Law on the Registration, Seizure and Examination of Private Documents and the Interception of Communications, and Article 15 of the Law to Combat Organized Crime, such information must be classified as confidential.

## GUATEMALA

The subsidiary of América Móvil that provides telecommunications services in Guatemala is obliged to cooperate with the authorities to exercise criminal action and the pursuit of justice, by virtue of the provisions of: (i) The Political Constitution of the Republic, (ii) Decree 51-92, Criminal Procedure Code, (iii) Decree 21-2006, Law Against Organized Crime and its regulations included in Governmental Agreement 158-2009; (iv) Decree 55-2010, Law of Extinction of Ownership; (v) Decree 6-91, Tax Code; (vi) Decree 8-2013, Law of Mobile Terminal Equipment; being obliged to the following:

i) **Delivery of retained data to the competent authorities:** Decree 21-2006, Law Against Organized Crime; Governmental Agreement 158-2009, Regulations for the Application of Special Investigation Methods; Decree 55-2010, Law of Extinction of Ownership; Decree 6-91, Tax Code.
ii) **Real time geographic location of mobile equipment:** Decree No. 21-2006, Law against Organized Crime, and Governmental Agreement 158-2009, Regulations for the Application of Special Investigation Methods.
iii) **Intervention of private communications:** Political Constitution of the Republic, Decree No. 21-2006 Law Against Organized Crime and Government Agreement 158-2009 Regulation for the Application of Special Investigation Methods.
iv) **Suspension of telecommunications services by judicial order:** Decree 8-2013, Law of Mobile Terminal Equipment. The judicial authority issues a suspension order based on its powers, which must be complied. Otherwise, the crime of disobedience is incurred in accordance with Article 414 of the Penal Code.
v) **Blocking of communication lines involved in the commission of crimes:** Mobile Terminal Equipment Law. Decree 8-2013, Article 17.

**Competent Authorities:** The prosecutors of the Public Ministry and Judges of the criminal judicial system are the competent authorities to manage and authorize the requirements made to the operators to request the information related to the clients.

**Note:** The Political Constitution of the Republic of Guatemala, Article 24; the Code of Criminal Procedure, Decree 51-92, Article 314; the Law against Organized Crime, Decree 21-2006 and the Law on Extinction of Ownership, Decree 55-2010, Article 19, stipulate that such information must be classified as confidential during and after the entire criminal process.

## EL SALVADOR

The América Móvil subsidiary that provides telecommunications services in El Salvador is required to cooperate with national security and law enforcement authorities under the Constitution of El Salvador, the Telecommunications Law (*Ley de Telecomunicaciones*) and the Special Law on the Interception of Telecommunications (*Ley Especial para la intervención de las Telecomunicaciones*), and to comply with the following:

i) **Delivery of data records to Competent Authorities.** Article 42-A of the Telecommunications Law; Article 47 of the Special Law on the Interception of Telecommunications.
ii) **Geolocation of mobile devices.** Article 42-A of the Telecommunications Law.
iii) **Interception of private communications.** Article 24 of the Constitution of El Salvador; Special Law on the Interception of Telecommunications.

iv) **Discontinuance of telecommunications services upon court order.** Article 42-A of the Telecommunications Law.

**Competent Authorities:** The Prosecuting Attorney's Office is responsible for appointing officials authorized to request and receive information from carriers.

**Note:** Pursuant to articles 2-A and 29-B of the Telecommunications Law, such information must be classified as confidential.

## HONDURAS

The América Móvil subsidiary that provides telecommunications services in Honduras is required to cooperate with national security and law enforcement authorities under the Constitution of the Republic of Honduras, Article 100 of the Law that Sets Forth the Legal Framework for the Telecommunications Sector (*Ley Marco del Sector Telecomunicaciones*), the General Regulations (*Reglamento General*) issued thereunder, the Special Law on the Interception of Private Communications (*Ley Especial para la Intervención de las Comunicaciones Privadas*) and the Criminal Code (*Código Penal*), and to comply with the following:

i) **Delivery of data records to Competent Authorities.** Article 100 of the Constitution of the Republic of Honduras; Code of Criminal Procedure.
ii) **Geolocation of mobile devices in real time.** Code of Criminal Procedure.
iii) **Interception of private communications.** Article 100 of the Constitution of the Republic of Honduras; Code of Criminal Procedure.
iv) **Discontinuance of telecommunications services upon court order.** Code of Criminal Procedure.
v) **Blocking of communication lines used for the commission of criminal offenses.** Code of Criminal Procedure.

**Competent Authorities:** The heads of the security and law enforcement agencies are responsible for appointing officials authorized to request and receive information from carriers.

**Note:** Pursuant to Article 278 of the Code of Criminal Procedure, such information must be classified as confidential.

## NICARAGUA

The América Móvil subsidiary that provides telecommunications services in Nicaragua is required to cooperate with national security and law enforcement authorities under the Code of Criminal Procedure for the Republic of Nicaragua (*Código Procesal Penal de la República de Nicaragua*), or Law No. 406, the Law for the Prevention, Investigation and Prosecution of Organized Crime and for the Administration of Seized, Confiscated and Abandoned Property (*Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados*), or Law No. 735, the Special Law on Cybercrimes (*Ley Especial de Ciberdelitos No. 1042*) and the Rules for the Preservation of Data and Information (*Normativa para Preservación de Datos e Información*), or Administrative Resolution AA 001-2021, and to comply with the following:

i) **Delivery of data records to Competent Authorities.** Rules for the Preservation of Data and Information (AA 001-2021); Code of Criminal Procedure for the Republic of Nicaragua (Law No. 406); Law for the Prevention, Investigation and Prosecution of Organized Crime and for the Administration of Seized, Confiscated and Abandoned Property (Law No. 735); and Special Law

on Cybercrimes (*Law No. 1042)*; and Rules for the Preservation of Data and Information (AA 001-2021).

ii) **Geolocation of mobile devices in real time.** Law for the Prevention, Investigation and Prosecution of Organized Crime and for the Administration of Seized, Confiscated and Abandoned Property (Law No. 735). Special Law on Cybercrimes (Law No. 1042).

iii) **Interception of private communications.** Code of Criminal Procedure for the Republic of Nicaragua (Law No. 406); Law for the Prevention, Investigation and Prosecution of Organized Crime and for the Administration of Seized, Confiscated and Abandoned Property (Law No. 735); and Special Law on Cybercrimes (Law No. 1042).

iv) **Discontinuance of telecommunications services upon court order.** Code of Criminal Procedure for the Republic of Nicaragua (Law No. 406); and Special Law on Cybercrimes (Law No. 1042).

v) **Blocking of communication lines used for the commission of criminal offenses.** Code of Criminal Procedure for the Republic of Nicaragua (Law No. 406); and Special Law on Cybercrimes (Law No. 1042).

**Competent Authorities:** The judicial authorities responsible for prosecuting cases involving actions that constitute criminal offenses; and the authorities or officials assigned to the criminal divisions of police agencies.

**Note:** Pursuant to the Special Law on Cybercrimes, such information must be classified as confidential.

# Procedure for Addressing Requests from Competent Authorities in Central America.

In general terms, under the legal framework in effect in this region, information may be disclosed, and communications may be intercepted only upon a lawful written request of a Competent Authority or order of a competent court.

Our subsidiaries perform a detailed review and analysis of each request in order to ensure our compliance with the law and ascertain that the human rights of our customers will be respected. This procedure entails the following:

- A legal analysis of the orders of Competent Authorities to determine whether they are valid and lawful.
- Upon verification of the satisfaction of all legal requirements, the preparation and processing of the information requested by the Competent Authorities.
- The preparation of an official response to the Competent Authorities.
- The delivery of the relevant information to the Competent Authorities through procedures that ensure that such information cannot be altered and will remain confidential.

# Number of Requests Processed in Central

In 2022, our subsidiaries in **Central America** received an aggregate of **46,843** requests for customer proprietary information from government authorities. We fulfilled **46,303** requests for information or **98.8%** of the requests we received from Competent Authorities upon determining that such requests had been issued in accordance with the applicable law. The remaining **1.2%** (**540** requests) was not fulfilled either because the issuing authority was not a Competent Authority, or the request did not comply with all applicable legal requirements.

## SOUTNER CONE

# Statutory obligation to address the requests of Competent Authorities.

## BRAZIL

The América Móvil subsidiaries that provide telecommunications services in Brazil are required to cooperate with national security and law enforcement authorities under sections 5 (XII) [7] and 136[8] of the Constitution of the Federal Republic of Brazil (*Constituição da República Federativa do Brasil*) [9], Section 1 of the Federal Telecommunications Law (*Lei Geral das Telecomunicações*), or Law No. 9.472/1997, the Brazilian Telecommunications Code (*Código Brasileiro de Telecomunicações*), or Law No. 4.117/1962, and the Civil Rights Framework for the Internet (*Princípios, Garantias, Direitos e Deveres para o Uso da Internet no Brasil*), or Law No. 12.965/2014, and to comply with the following:

i) **Delivery of data records to Competent Authorities.** Article 15 of the Law to Combat Organized Crime (*Lei de Combate ao Crime Organizado*), or Law No. 12.850/2013; Article 17-B of the Law on the Prevention of Money Laundering (*Lei de Lavagem de Dinheiro*), or Law No. 9.613/1998; Section 13-A of the Code of Criminal Procedure (*Código de Processo Penal*), or Decree-Law No. 3.689/1941; and Article 10 of the Civil Rights Framework for the Internet, or Law No. 12.965/2014.

ii) **Geolocation of mobile devices in real time**. Article 10 of Law No. 13.812/19 and Section 13- B of Decree-Law No. 3.689 of 1941 - Code of Criminal Procedure (*Decreto-Lei No. 3689 de 1941, Código de Processo Penal*).

iii) **Interception of private communications.** Law No. 9.296/96;

iv) **Discontinuance of telecommunications services upon court order.** Article 136 of the Constitution of the Federal Republic of Brazil, which provides that, in the event of a state of siege or defense, the President of Brazil may limit the privacy of the communications of any person on a temporary basis.

**Competent Authorities:**

- Judiciary.
- At the request of the Public Prosecutor's Office, Public Prosecutor's Office.
- Police Authority or Police Commissioner.
- Regulatory Agencies.

**Note:** Pursuant to the Cooperation Guidelines, such information must be classified as confidential[10].

[7] Under the Constitution of the Federal Republic of Brazil as it relates to the privacy of telecommunications, communications may only be intercepted based upon a court order or in the event of a presidential declaration of a state of siege or defense.
[8] Every person is entitled to the protection of the privacy of his communications absent a court order to the contrary.
[9] In the event of a declaration of a state of siege or defense.
[10] Article 20 of Decree-Law No. 3.689 /41 - Code of Criminal Procedure. Under Brazilian law, judges, delegates, and other authorities may seal a proceeding in order to preserve evidence, preclude the obstruction of investigations or preserve the honor and intimacy of a victim or the subject of an investigation. The disclosure of sealed court records is prohibited.

## ARGENTINA

The América Móvil subsidiaries that provide telecommunications services in Argentina are required to cooperate with national security and law enforcement authorities under Article 18 of the Constitution of the Argentine Nation (*Constitución de la Nación Argentina*) and Article 18 of the National Telecommunications Law No. 19.798 (*Ley Nacional de Telecomunicaciones No. 19.798*), and to comply with the following:

i) **Delivery of data records to Competent Authorities.** Article 236 of the Code of Criminal Procedure for the Nation (*Código de Procedimiento Penal de la Nación*).
ii) **Geolocation of mobile devices in real time.** Article 236 of the Code of Criminal Procedure for the Nation.
iii) **Interception of private communications.** National Telecommunications Law No. 19.798, as amended; National Information and Communication Technologies Law No. 27.078; and Article 236 of the Code of Criminal Procedure for the Nation.
iv) **Discontinuance of telecommunications services upon court order**. Article 236 of the Code of Criminal Procedure for the Nation.
v) **Blocking of communication lines used for the commission of criminal offenses.** Article 236 of the Code of Criminal Procedure for the Nation.

**Competent Authorities:** The interception of any communication must be expressly authorized by a judge or, if intended for purposes relating to a kidnapping for ransom in progress, only, by the Prosecuting Attorney's Office, provided that the relevant order is ratified by a competent judge within 24 hours. Notwithstanding the above, the Office of Judicial Assistance in Connection with Complex Criminal Offenses and Organized Crime (*Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado, or DAJUDECO*), an agency of the Supreme Court of Justice, is the only Competent Authority for purposes of the delivery of interception orders to carriers.

**Note:** Pursuant to the Cooperation Guidelines, such information must be classified as confidential[11].

## PARAGUAY

The América Móvil subsidiaries that provide telecommunications services in Paraguay are obliged to cooperate with national security and law enforcement authorities, pursuant to the provisions of the National Constitution of Paraguay, Law No. 642/1995 on Telecommunications and Decree No. 14135 - Regulatory Rules of the Telecommunications Law; Law 4739/2013 that creates the 911 System for the attention, dispatch and monitoring of emergency communications, as well as The Paraguayan Code of Criminal Procedure, which establishes in its Article 228 is obliged to the following:

i) **Delivery of retained data to the competent authorities**. Criminal Procedural Code, Article 228.
ii) **Real-time geographic location of mobile equipment.** Law 4739/2013, Article 12.
iii) **Intervention of private communications.** National Constitution, article 36.
iv) **Blocking of communication lines.** Upon a court order requested by the Prosecuting Attorney Office and/or a competent judge.

[11] Article 5 (Consent) of Law No. 25326. It shall not be necessary to obtain the subject's consent to the use, disclosure, or storage of his or her personal data where the intended purpose of the collection of such data is the performance of government functions or the satisfaction of an obligation of law, among other things.

**Competent Authorities:** Judges and the Prosecuting Attorney´s Office.

**Note:** Pursuant to the Cooperation Guidelines, such information must be classified as confidential.[12]

## URUGUAY

The América Móvil subsidiaries that provide telecommunications services in Uruguay are required to cooperate with national security and law enforcement authorities under Article 28 of the Constitution of the Oriental Republic of Uruguay (*Constitución de la República Oriental del Uruguay*) and articles 297 and 298 of the Criminal Code, and to comply with the following:

i) **Delivery of data records to Competent Authorities.** Article 5 of Law No. 18.494.
ii) **Geolocation of mobile devices in real time.** Article 5 of Law No. 18.494.
iii) **Interception of private communications.** Article 5 of Law No. 18.494.
iv) **Discontinuance of telecommunications services upon court order.** Article 166 of Law No. 19.355[13].

**Competent Authorities:**

- For purposes of any data record, geolocation or communications interception, the judge presiding over a criminal investigation, upon request from the Prosecuting Attorney's Office.
- For purposes of any order for the disconnection of telecommunications services, the Ministry of the Interior.

**Note:** Pursuant to the Cooperation Guidelines, such information must be classified as confidential.

# Procedure for Addressing Requests from Competent Authorities in the Southern Cone.

In general terms, under the legal framework in effect in this region, information may be disclosed, and communications may be intercepted only upon a lawful written request of a Competent Authority or order of a competent court.

Our subsidiaries perform a detailed review and analysis of each request in order to ensure our compliance with the law and ascertain that the human rights of our customers will be respected. This procedure entails the following:

- A legal analysis of the orders of Competent Authorities to determine whether they are valid and lawful.

[12] *"A person's documentary heritage is inviolable. No record, regardless of technique, printout, correspondence, writing, telephone, telegraphic or other conversation, collection or reproduction, testimonial or object of testimonial value or copy of any of the above may be examined, reproduced, intercepted or seized except upon court order in the events expressly set forth in the law and provided that it is indispensable for shedding light on matters within the jurisdiction of the relevant authorities. The law will establish special methods for examining commercial accounting records and the requisite legal records. Any documentary evidence obtained in violation of the above shall be of no value at trial. In any event, any item determined to be unrelated to the subject matter of the investigation shall be kept strictly confidential."*

[13] Specifically, to deter irregular or repeated calls to the 911 emergency telephone number.

- Upon verification of the satisfaction of all legal requirements, the preparation and processing of the information requested by the Competent Authorities.
- The preparation of an official response to the Competent Authorities.
- The delivery of the relevant information to the Competent Authorities through procedures that ensure that such information cannot be altered and will remain confidential.

**More specifically:**

## ARGENTINA

Pursuant to the National Intelligence Law (*Ley de Inteligencia Nacional*), or Law No. 25.520, Decree No. 256/2015 and decisions Nos. 2/2016 and 30/2016 of the Supreme Court of Justice, the power and authority to demand compliance with a request relating to an order for the interception of communications in Argentina is reserved to the *DAJUDECO*. Claro Argentina and the *DAJUDECO* have established an interconnection link to facilitate the exchange of data records, thereby allowing Claro Argentina to receive requests for such records or disconnection orders and to deliver the relevant information to the *DAJUDECO*. Pursuant to Resolution No. 15/2017 of the *DAJUDECO*, the report generated upon an interconnection request shall have the same effect as the "synthetic official communication" otherwise required by the second paragraph of Article 22 of the National Intelligence Law, or Law No. 25.520.

**More specifically:**

## URUGUAY

Under current laws and regulations, all requests for compliance with court orders relating to the interception of communications or the provision of commercial information, historical records, or geolocation (ERB traffic) data must be delivered to Claro Uruguay through the Lawful Interceptions Management System (*Sistema de Administración de Interceptaciones Legales*, or *SAIL*). Upon receipt of any such request, the Legal Department performs a review and analysis thereof. Absent any irregularity, the request is accepted, and the information required by the relevant authority is automatically processed and delivered by the system. Claro Uruguay files with the Supreme Court of Justice a quarterly report on the number of requests for lawful interceptions, historical records and ERB traffic data received, processed, and rejected by it during the relevant quarter.

# Número de solicitudes atendidas en Cono Sur.

In 2022, our subsidiaries in the **Southern Cone** received an aggregate of **394,601** requests for customer proprietary information from government authorities. We fulfilled **381,159** requests for information or **96.5%** of the requests we received from Competent Authorities upon determining that such requests had been issued in accordance with the applicable law. The remaining **3.5%** (**13,442** requests) was not fulfilled either because the issuing authority was not a Competent Authority, or the request did not comply with all applicable legal requirements.

## ANDEAN REGION

# Statutory obligation to address the requests of Competent Authorities.

## COLOMBIA

The América Móvil subsidiaries that provide telecommunications services in Colombia are required to cooperate with national security and law enforcement authorities under the Political Constitution of Colombia (*Constitución Política de Colombia*), Law No. 1341 of 2009 and Decree No. 1704 of 2012, and to comply with the following:

i) **Delivery of retained data to the competent authorities**: Law 906 of 2004, article 234 and 235 (selective search in database); Law 1621 of 2013, article 44; and decree 1704 of 2012 article 4; numeral 9 of article 277 of the Political Constitution (request of the Attorney General of the Nation); articles 631 and 684 of the Tax Statute (DIAN) and Coactive Collection of public entities (Law 1066 of 2006).
ii) **Geolocation of mobile devices in real time**. Article 235 of Law No. 906 of 2004, Article 44 of Law No. 1621 of 2013 and Article 5 of Decree No. 1704 of 2012
iii) **Interception of private communications.** Article 15 of the Political Constitution of Colombia, Article 2 of Decree No. 1704 of 2012, Article 235 of Law No. 906 of 2004 and Article 44 of Law No. 1621 of 2013
iv) **Discontinuance of telecommunications services upon court order**. Article 8 of Law No. 1341 of 2009[14].

**Competent Authorities:** The Office of the Attorney General for the Nation (*Fiscalía General de la Nación),* acting through the division of the judicial police responsible for investigating the relevant case; and the directors of the intelligence agencies or the persons to whom such individuals may delegate their authority.

**Nota:** Pursuant to the Cooperation Guidelines, such information must be classified as confidential.[15]

## CHILE

The América Móvil subsidiaries that provide telecommunications services in Chile are required to comply with the requests of the judicial authorities under the Political Constitution of the Republic of Chile

[14] *"Article 8 (Telecommunications in Cases of Emergency, Commotion or Calamity and the Prevention of Such Events). In response to cases of emergency, internal and external commotion, disaster or public calamity, the providers of network and telecommunications services shall make available such networks and services to the authorities, free of charge and in a timely fashion, and shall assign priority to the transmission of all such communications as such authorities may require. The transmissions relating to the protection of human life shall be assigned absolute priority in any such event. In addition, the authorities shall be assigned priority as with respect to the transmission of free and timely communications intended to prevent disasters, if such transmissions are believed indispensable."*

[15] Article 6 (Confidentiality) of Decree No. 1704 of 2012 provides the following: *"The providers of network and telecommunications services, the officials of the Office of the Attorney General for the Nation and the members of the Judicial Police who have access to any type of information or data by reason of the nature of their duties or the performance thereof, or who engage in activities involving the interception of communications, covenant and agree to regard as reserved such data and as confidential such information under penalty of criminal investigation and disciplinary action.".*

(*Constitución Política de la República de Chile*), the mandatory resolutions of the judicial authorities and the Code of Criminal Procedure, as well as with the following:

i) **Delivery of data records to Competent Authorities**. Regulations on the Interception and Recording of Telephone Conversations and Other Forms of Telecommunications, or Decree No. 142 of 2005, issued by the Ministry of Transportations and Telecommunications; and articles 222 and 224 of the Code of Criminal Procedure.
ii) **Geolocation of mobile devices in real time.** Articles 222 and 244 of the Code of Criminal Procedure.
iii) **Interception of private communications.** Article 19(4) and (5) of the Political Constitution of the Republic of Chile; Regulations on the Interception and Recording of Telephone Conversations and Other Forms of Telecommunications (*Reglamento sobre Interceptación y Grabación de Comunicaciones Telefónicas y Otras Formas de Telecomunicación*), or Decree No. 142 of 2005, issued by the Ministry of Transportations and Telecommunications (*Ministerio de Transporte y Telecomunicaciones*); and articles 222 and 224 of the Code of Criminal Procedure.

**Competent Authorities:** The authority to issue requests for data records, geolocation data and the interception of communications is reserved to the courts of the judicial branch, including the Courts of Appeals (*Cortes de Apelaciones*) and the Most Excellent Supreme Court (*Excelentísima Corte Suprema*), Local Police Court (*Juzgado de la Policia Local*), the Prosecuting Attorney's Office (*Ministerio Público*) and the National Economic Prosecutor (*Fiscalía Nacional Económica*).

**Note:** Pursuant to the Cooperation Guidelines, such information must be classified as confidential[16].

## ECUADOR

The América Móvil subsidiaries that provide telecommunications services in Ecuador are required to cooperate with national security and law enforcement authorities under the Constitution of the Republic of Ecuador (*Constitución de la República del Ecuador*), the Organic Law on Telecommunications (*Ley Orgánica de Telecomunicaciones*), the General Regulations Under the Organic Law on Telecommunications (*Reglamento General a la Ley Orgánica de Telecomunicaciones*), the Law on Public and National Security (*Ley de Seguridad Pública y del Estado*) and the Comprehensive Organic Criminal Code (*Código Orgánico Integral Penal*), and to comply with the following:

i) **Delivery of data records to Competent Authorities.** Organic Telecommunications Law, article 77; General Regulations to the Organic Telecommunications Law: articles 117, 118 and 119; Concession Contract and the Comprehensive Organic Criminal Code, articles 230, 476 and 477; Organic Law for the Protection of Personal Data, article 11.
ii) **Geolocation of mobile devices in real time.** Organic Telecommunications Law, article 77; General Regulations to the Organic Telecommunications Law: articles 117, 118 and 119; Concession Contract and the Organic Integral Criminal Code, articles 230, 476 and 477.
iii) **Interception of private communications**. Organic Telecommunications Law, article 77; General Regulations to the Organic Telecommunications Law, articles 118 and 119; Concession Contract; Regulations for the subsystem of Interception of communications or

[16] *Absent a duty of confidentiality or access restriction, or if the period of time for complying with the request for information has expired, Claro Chile reserves the right to give its customers notice of its provision of personal data of such customers to the relevant authority.*

computer data, articles 4 and 5; and the Organic Integral Criminal Code, articles 230, 476 and 477; Resolutions of the Public Prosecutor's Office and Resolutions of ARCOTEL.

iv) **Suspension of telecommunications services upon court order**. Constitution of the Republic of Ecuador, articles 164 and 165; Concession Contract, clause 34.7.

v) **Blocking of communication lines used for the commission of crimes.** Concession Agreement and Section 34.7 thereof.[17]

**Competent Authorities:** Any competent judge upon a lawful request from a prosecuting attorney in the Attorney General´s Office (*Fiscalía General del Estado*).

**Note:** Pursuant to the Cooperation Guidelines, such information must be classified as confidential

## PERÚ

The América Móvil subsidiaries that provide telecommunications services in Peru are required to cooperate with national security and law enforcement authorities under the Political Constitution of Peru (*Constitución Política del Perú*), the Amended and Restated Telecommunications Law (*Texto Único Ordenado de la Ley de Telecomunicaciones*), or Supreme Decree No. 013-93-TCC, and the Amended and Restated General Regulations Under the Telecommunications Law (*Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones*), or Supreme Decree No. 020- 2007-MTC, and to comply with the following:

i) **Delivery of data records to Competent Authorities.** Articles 230 and 231 of the New Code of Criminal Procedure (*Nuevo Código Procesal Penal*).

ii) **Geolocation of mobile devices in real-time.** New Criminal Procedural Code, articles 230 and 231. Also, Legislative Decree 1182, which regulates the use of data derived from telecommunications for the identification, location, and geolocation of communication equipment in the fight against crime. This regulation requires 24/7 attention for geolocation requests under penalty of fine.

iii) **Interception of private communications.** Article 2(10) of the Political Constitution of Peru; Article 4 of the Telecommunications Law; Article 13 of the General Telecommunications Regulations; Article 4 of the Regulations Under the Law that Provides for the Creation of the Financial Intelligence Unit - Peru (*Reglamento de la Ley que crea la Unidad de Inteligencia Financiera - Perú*), or Supreme Decree No. 020-2017-JUS; articles 230 and 231 of the New Code of Criminal Procedure; and articles 230 and 231 of the Law to Combat Organized Crime (Ley Contra el Crimen Organizado).

[17] *Pursuant to Section 34.7 of the Concession Agreement, services may be discontinued for the following reasons: (a) the occurrence of the conditions set forth in the service contract, including, among others, the theft or loss of the equipment, if the information provided is proven false, the occurrence of an event of force majeure or act of God or if the customer jeopardizes the security or quality of the network; (b) the unlawful or fraudulent use of the service; and (c) if the ARCOTEL determines that the relevant lines have been used in connection with unauthorized services.*

iv) **Discontinuance of telecommunications services upon court order**. Articles 18[18] and 19 of the General Regulations Under the Telecommunications Law. [19]

v) **Blocking of communication lines used for the commission of criminal offenses**. Articles 18 and 19 of the General Telecommunications Regulations

**Competent Authorities:** The Prosecuting Attorney, either directly or through an official of the Attorney General's Office or a police officer. The authority to issue disconnection and blocking orders is reserved to the National and Civil Defense Systems and the Ministry of Transportation and Communications (*Ministerio de Transportes y Comunicaciones*).

**Note**: Pursuant to the Cooperation Guidelines, such information must be classified as confidential[20].

## Procedure for Addressing Requests from Competent Authorities in the Andean Region.

In general terms, under the legal framework in effect in this region, information may be disclosed, and communications may be intercepted only upon a lawful written request of a Competent Authority or order of a competent court.

Our subsidiaries perform a detailed review and analysis of each request in order to ensure our compliance with the law and ascertain that the human rights of our customers will be respected. This procedure entails the following:

- A legal analysis of the orders of Competent Authorities to determine whether they are valid and lawful.
- Upon verification of the satisfaction of all legal requirements, the preparation and processing of the information requested by the Competent Authorities.
- The preparation of an official response to the Competent Authorities.
- The delivery of the relevant information to the Competent Authorities through procedures that ensure that such information cannot be altered and will remain confidential.

[18] *"In the exceptional cases set forth in the Constitution or declared to be such in accordance with the law, all providers of carrier services, teleservices or final services shall assign priority to the voice and data transmissions that are necessary to the National Defense System and the Civil Defense System. In the event of an external war upon a declaration issued in accordance with the law, the National Defense Council (Consejo de Defensa Nacional), acting through the Joint Armed Forces Command (Comando Conjunto de las Fuerzas Armadas), shall be authorized to assume the direct control of the telecommunications services and to issue operations-related directives. (…).""*

[19] *"In the event of occurrence of a local, regional or national emergency or crisis, such as earthquakes, floods or other similar events requiring of special attention from the telecommunications carriers, such carriers shall provide all such telecommunications services as may be necessary and shall assign priority to the support actions aimed at resolving the emergency situation. To such effect, all holders of concessions and licenses shall abide by the provisions issues by the Ministry."*

[20] Article 231(3) of the New Code of Criminal Procedure*: "Following the implementation of the intervention measure and the completion of a preliminary investigation of its effects, the affected party shall be given notice of all the actions taken in connection therewith and shall be entitled to request, within three days from the receipt of such notice, a judicial reexamination thereof.*

**More specifically:**

## CHILE

Under the legal framework described above, the delivery of information and the interception of communications may only occur upon a written request from a Competent Authority (i.e., the Prosecuting Attorneys´ Office, the National Economic Prosecutor and the Court of Appeals), accompanied by a court resolution authorizing the relevant action.

**More specifically:**

## PERÚ

Requests relating to:

a) The unveiling of the secrecy of telecommunications and other related data

The aforementioned process has become automated as a result of the implementation of an information technology system known as the System for Unveiling the Secrecy of Telecommunications *(Sistema de Levantamiento del Secreto de las Telecomunicaciones*), which extracts the requisite information directly from the data bases upon entering the telephone numbers identified in the official communication. This system allows us to ascertain which employees entered which numbers. The security loop is closed when the scanned copy of the official communication made by our mail manager is uploaded to the system, which then generates a record of the document delivered in response to the original request. All the information has been uploaded to the system.

The annual statistics, authorized entities and the established protocol to address the process of lifting the secrecy of telecommunications, are publicly available at Claro's webpage.

b) The location and geolocation of equipment in real time.

We have developed an application for addressing official communications relating to the delivery of data records and/or the geolocation of a telephone line in real time. This application allows us to perform location and geolocation searches immediately upon request from the Specialized Unit of the National Police of Peru (*Unidad Especializada de la Policía Nacional del Perú*). This unit is devoted to addressing certain specified types of crimes, including extortion, kidnapping, and organized crime, among others. The application does not allow for the performance of searches for other related data such as ownership records, call logs or other data.

The system may only be accessed through América Móvil Perú's VPN and includes a two-factor authentication: to access the VPN and to allow access to the user of the application. In addition, the system keeps a record of the MAC addresses of the equipment in which the application is enabled. Each police officer assigned to perform location searches by the Specialized Unit of the National Police of Peru is provided with a unique username and an unconventional password that is reset on a monthly basis. The system is available to the Specialized Unit of the National Police of Peru 24 hours a day, seven days a week, solely and exclusively for purposes of ascertaining the location of the telephone lines being targeted by an investigation upon entering the number of the official communication that contains the order for the geolocation search; provided that such investigation relates to conducts amounting to

flagrant criminality, that is, criminal offenses committed within 24 hours of the search or which constitute continuing crimes such as kidnapping and extortion.

América Móvil Perú audits on both a regular and random basis the numbers entered the system based upon the court orders received by its mailing desk, for internal control purposes and to ensure that the system is used in an adequate manner.

## Number of Requests Processed in the Andean Region.

In 2022, our subsidiaries in the **Andean Region** received an aggregate of **97,459** requests for customer proprietary information from government authorities. We fulfilled **80,720** requests for information or **82.8%** of the requests we received from Competent Authorities upon determining that such requests had been issued in accordance with the applicable law. The remaining **17.2%** (**16,739** requests) was not fulfilled either because the issuing authority was not a Competent Authority, or the request did not comply with all applicable legal requirements.

# GENERAL PROVISIONS THAT APPLY IN THE COUNTRIES IN WHICH WE OPERATE

### *Service Restriction Orders*

As a telecommunications carrier, América Móvil may receive orders for the imposition of network restrictions from the Competent Authorities.

These orders, which are known as "*service restriction orders*," or SROs, constitute lawful demands of the Competent Authorities from the Company, requiring the Company to block or restrict the access to its network or the services provided by third parties over such network, block certain specified services, content, URLs or domains, restrict its data bandwidth or degrade the quality of its voice or SMS services.

As members of the GSMA, we encourage governments to become more transparent about their role in the disconnection or restriction of networks and services and their legal arguments in support of such measures, in an effort to ensure that any limitation on the right to freedom of expression imposed by their national laws is due to security reasons, and that any government intervention is limited in scope and complies with the international laws and standards relating to human rights. We reject requests for service restrictions that contravene human rights, as set forth in the Universal Declaration of Human Rights; the International Covenant on Civil and Political Rights; the International Covenant on Economic, Social and Cultural Rights; and the Ten Principles of the United Nations Global Compact. Notwithsatnding, as concessionaires of telecommunications services, we must abide with the Competent Authorities' orders, even when they are related to service restriction orders.

### *Requisition of Operations by the Government*

Under the legal framework in effect in each of the countries in which we operate, the federal government may effect the requisition of general means of communication and of the assets, rights and elements necessary to operate such networks in the event of (1) a natural disaster, (2) war, (3) a material disruption of the public order or (4) in anticipation of an imminent danger to national security, the internal peace of the country or the domestic economy, or to ensure the continuity of the services.

Under the aforementioned framework, upon any such requisition the personnel assigned to the operation of the relevant network must be made available to the administrator appointed by the government for the duration of the contingency. Such administrator shall be responsible for complying with the relevant presidential order in every respect.

### *Repossession of Frequencies and Public Telecommunications Networks*

Under the legal framework in effect in each of the countries in which we operate, the federal government may reclaim the frequencies assigned or the concessions granted to our Company (1) in the public interest, (2) for national security reasons at the request of the executive branch of the federal

government, (3) to introduce new technologies, (4) in response to interferences, (5) to comply with the international treaties to which the relevant country is a party, (6) to reconfigure the radioelectric spectrum or (7) to ensure the continuity of a public service.

Lastly, in the event of cancellation of a concession by reason of a requisition, the federal government must determine the measures that are necessary to ensure the continuity of the services.

### *Network Restrictions Within the Prison System.*

Under the legal framework in effect in each of the countries in which we operate, all holders of telecommunications concessions are required to block or restrict the access to their networks and services from within penitentiary facilities, thereby limiting the inmates' ability to communicate by wireless telephone, in order to preclude the commission of criminal offenses inside such facilities.

In addition, under the legal framework in effect in each of the countries in which we operate, all holders of telecommunications concessions and providers of telecommunications services are deemed to have agreed to commit themselves to the cause of national security. Accordingly, all network operators and providers of telecommunications services are required to adopt and implement all such procedures and technical solutions as may be necessary to preclude the provision, within penitentiary facilities, of wireless telecommunications services otherwise available to the public. The violation of this obligation may give rise to the imposition of penalties by the Competent Authorities.

In accordance with the previous sections on requests for service restriction, seizure or requisition, frequency rescue and network restriction within the prison systems, it is important to mention that they are applicable only to some jurisdictions where orders or requirements could be received from competent authorities, as detailed in the following table:

| | Puerto Rico | Mexico | Dominican Republic | Costa Rica | El Salvador | Guatemala | Honduras | Nicaragua | Brazil | Argentina | Paraguay | Uruguay | Colombia | Chile | Ecuador | Peru |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Confidentiality** | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| **Imposition of service restrictions** | Yes | Yes | No | Yes | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| **Requisition** | No | Yes | No | No | No | No | Yes | Yes | No | Yes | Yes | No | No | No | Yes | Yes |
| **Repossession of frequencies** | No | Yes | No | No | Yes | No | Yes | Yes | No | Yes | No | Yes | Yes | No | Yes | Yes |
| **Network restrictions within the prison system** | No | Yes | No | Yes | Yes | No | Yes | No | No | No | Yes | Yes | Yes | No | No | No |
| **Disconnection of services as a result of the disruption of the normal operation of the telecommunications network** | Yes | No | No | Yes | Yes | No | No | No | No | No | No | No | No | No | No | No |
| **Reassignment of frequencies and public telecommunications networks** | Yes | No | No | Yes | No | No | No | No | No | No | No | No | Yes | No | Yes | No |
| **Limitation of unrestricted-use rights** | No | No | No | No | No | No | No | No | No | No | No | Yes | Yes | No | No | No |
| **Domain blocking** | No | No | No | No | No | No | No | No | No | No | No | Yes | No | No | Yes | No |
| **State intervention in the information and communications technology industry** | No | No | No | No | No | No | Yes | No | No | No | No | Yes | Yes | No | No | No |
| **Emergencies, commotions or calamities** | No | No | No | No | No | No | No | No | No | No | Yes | Yes | Yes | No | Yes | No |
| **Content blocking** | No | No | No | No | No | No | No | No | No | No | No | Yes | No | Yes | Yes | No |
| **Cancellation of the concession agreement** | No | No | No | No | No | No | Yes | No | No | No | No | Yes | No | Yes | No | Yes |

# GLOSSARY

**ARCOTEL. -** means the National Telecommunications Regulation and Control Agency (*Agencia de Regulación y Control de las Telecomunicaciones*), the authority empowered to regulate and exercise the technical control of telecommunications in Ecuador.

**Competent Authority. -** means an authority empowered by current law to perform a designated function.

**Concessionaire. -** means a person to whom a government agency or a company has granted the exclusive right to develop or exploit a business or sell a product in a given region.

**Court Order. -** means a decision issued by a court or agency of the judicial branch with jurisdiction over a given matter.

**Legal Framework. -** means the set of laws, regulations and rules that apply in a particular country.

**Data Subject. -** means any individual maintaining ownership over personal data.