Electronic Evidence Fiche: PHILIPPINES

1) DEFINITIONS

Philippines
What are the definitions in your laws/regulations, if any, of:
Electronic evidence
According to Section 3 [u] of the Implementing Rules and Regulations of Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012"), electronic evidence "refers to evidence, the use of which is sanctioned by existing rules of evidence, in ascertaining in a judicial proceeding, the truth respecting a matter of fact, which evidence is received, recorded, transmitted, stored, processed, retrieved or produced electronically".
Computer system
According to Section 3 [l] of the Implementing Rules and Regulations of Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012"), computer system refers to "any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities, including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components, which may stand alone or be connected to a network or other similar devices. It also includes computer data storage devices or media".
Computer data
According to Section 3 [j] of the Implementing Rules and Regulations of Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012"), computer data refers to "any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function, and includes electronic documents and/or electronic data messages whether stored in local computer systems or online"
Categories of computer data (e.g. basic subscriber information, traffic data and content data)
According to Section 3 [o] of The Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012"), subscriber's information refers to "any information contained in the form of computer data or any other form that is held by a service

provider, relating to subscribers of its services other than traffic or content data and by which identity can be established: (1) The type of communication service used, the technical provisions taken thereto and the period of service; (2) The subscriber's identity, postal or geographic address, telephone and other access numbers, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement; and (3) Any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement" According to Section 3 [p] of The Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012"), traffic data or non-content data refers to "any computer data other than the content of the communication including, but not limited to, the communication's origin, destination, route, time, date, size, duration, or type of underlying service" Content data refers to "the communication content of the communication, the meaning or purport of the communication, or the message or information being conveyed by the communication, other than traffic data" - Section 3 [m] of The Rules and Regulations Implementing Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012")
Electronic surveillance or real-time collection of computer/communication data
According to Section 3 [m] of The Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012"), interception refers to "listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring". Real-time collection of traffic data was regulated in Section 12, Paragraph 1 of The Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012"): "Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system". However, the legal provision was declared unconstitutional in the case of Disini v. SOJ.
Service provider (e.g. ISP, hosting)
According to Section 3 [n] of The Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012"), service provider refers to: "(1) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and (2) Any other entity that processes or stores computer data on behalf of such communication service or users of such service."

2) DATA RETENTION REGIME

Philippines
Do you have any domestic laws that stipulate a mandatory retention period of electronic data? If so, for what types of data and for how long?
The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved for a minimum period of six (6) months from the date of the transaction according to Section 13 of The Republic Act no. 10175 (“The Cybercrime Prevention Act of 2012”). It is stated in the same section that “content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation. Law enforcement authorities may order a one-time extension for another six (6) months: Provided, that once computer data preserved, transmitted or stored by a service provider is used as evidence in a case, the mere furnishing to such service provider of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case.”

3) ADMISSIBILITY OF ELECTRONIC EVIDENCE IN A CRIMINAL TRIAL

Philippines
What is the requirement under your domestic law for electronic evidence to be admissible in a criminal trial?
According to Section 2, Rule 3, A.M. No. 017-01-SC or the Rules on Electronic Evidence, an electronic document is admissible in evidence if it complies with the rules on admissibility prescribed by the Rules of Court and related laws and is authenticated in the manner prescribed by these Rules. If the evidence was obtained through mutual legal assistance, the authentication requirements under the treaty, if met, are sufficient for the said evidence to be admissible in criminal trial in the Philippines.

4) RECEIVING REQUESTS FOR ELECTRONIC EVIDENCE FROM OTHER STATES

4.1. **Direct requests** from foreign authorities to service providers

4.1.1. Requests for preservation

Philippines
What legal framework(s) is/are applicable, if any?
The Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012") and the Budapest Convention on Cybercrime
Are the service providers in your country prohibited from or have limited capacity for executing such requests from foreign authorities?
They have limited capacity since local service providers merely accommodate direct requests for preservation from foreign authorities.
If they are prohibited or if there are limitations, are there any alternative options to preserve the data from your country, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or mutual legal assistance (MLA)?
As a matter of procedure, foreign authorities coordinate through the 24/7 Point-of-Contact (Office of Cybercrime, Department of Justice - DOJ) under the purview of the Budapest Convention for purposes of preservation
Is a judicial order required from the requesting state?
A judicial order from the requesting state is not required.
Are there any time limits for data preservation? Any possibility of extension?
The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved for a minimum period of six (6) months from the date of the transaction according to Section 13 of The Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012") It is stated in the same section that "content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation. Law enforcement authorities may order a one-time extension for another six (6) months: Provided, that once computer data preserved, transmitted or stored by a service provider is used as evidence in a case, the mere furnishing to such service provider of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case."

Would service providers in your country notify the data subjects of the request?
No. The service provider ordered to preserve computer data shall keep confidential the order and its compliance according toSection 13 of The Republic Act no. 10175 (“The Cybercrime Prevention Act of 2012”)

4.1.2. Requests for voluntary disclosure

Philippines
What legal framework(s) is/are applicable, if any?
The Republic Act no. 10175 (“The Cybercrime Prevention Act of 2012”), A.M. No. 17-11-03-SC on the Rule on Cybercrime Warrants (RCW) and the Budapest Convention on Cybercrime
Are the service providers in your country prohibited from or have limited capacity for executing such requests from foreign authorities?
Service providers are prohibited from executing such requests from foreign authorities.
If they are prohibited or if there are limitations, are there any alternative options to obtain the data from your country, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or mutual legal assistance (MLA)?
As a matter of procedure, foreign authorities coordinate through the 24/7 Point-of-Contact (DOJ Office of Cybercrime) under the purview of the Budapest Convention or mutual legal assistance for purposes of voluntary disclosure.
Is a judicial order required from the requesting state? Are there any time limits?
Yes, since under the A.M. No. 17-11-03-SC on the Rule on Cybercrime Warrants (RCW) all types of computer data require warrant for disclosure.
Would service providers in your country notify the data subjects of the request?
No.
How can the process be simplified or quickened in emergency situations?
By using the 24/7 Point-of-Contact (DOJ Office of Cybercrime).

4.2. Requests received by your central authority for **Mutual Legal Assistance (MLA)**

Philippines
How do you execute MLA requests for electronic evidence stored by domestic service providers (e.g. through a domestic court order or a search warrant)?
Cybercrime Warrant duly issued by courts pursuant to the A.M. No. 17-11-03-SC on the Rule on Cybercrime Warrants (RCW). The Rules on Cybercrime Warrants (A.M. No. 17-11-03-SC) provide: "Section 4. Disclosure of Computer Data "Section 4.1. Disclosure of Computer Data. – Pursuant to Section 14, Chapter IV of RA 10175, law enforcement authorities, upon securing a Warrant to Disclose Computer Data (WDCD) under this Rule, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/her or its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation." "Section 4.2. Warrant to Disclose Computer Data (WDCD). – A WDCD is an order in writing issued in the name of the People of the Philippines, signed by a judge, upon application of law enforcement authorities, authorizing the latter to issue an order to disclose and accordingly, require any person or service provider to disclose or submit subscriber's information, traffic data, or relevant data in his/her or its possession or control."
Can you provide assistance in real-time collection of non-content and/or content data (e.g. through electronic surveillance) upon the receipt of a MLA request? If yes, are there any limitations or conditions (e.g. limited to certain crime types or penalties thresholds)?
Yes, provided that the requirements under the A.M. No. 17-11-03-SC on the Rule on Cybercrime Warrants (RCW) are met.
What are the central and competent authorities in your country to: **a) Receive a request for MLA in criminal matters?** **b) Execute/recognize the measure (if other than the receiving authority)?**
a) Department of Justice (DOJ) Office of the Chief State Counsel

b) Department of Justice (DOJ) Office of Cybercrime, National Bureau of Investigation (NBI), Philippine National Police (PNP), and other competent authorities as the case may be.
What are the accepted languages for MLA requests?
English
Can the request be submitted electronically to the central authority?
In urgent situations, the request may be transmitted by any means of communication that affords a record in writing, including, but not limited to, by facsimile or electronic mail (e.g., in a "pdf" format via e-mail). The requesting Party shall confirm the request in writing within thirty (30) days from receipt thereof by the Philippine Central Authority - Part IV, II(D)(3), DOJ Mutual Legal Assistance in Criminal Matters, A Guide for Domestic and Foreign and Competent Authority (DOJ MLA Guide) For urgent requests, the requesting law enforcement or prosecuting authority may send an advance copy of the request by fax to +632 8525-2218 or email at ocsc@doj.gov.ph. The original hard copy of the request must be submitted within fifteen (15) days from the date the advance copy was sent through facsimile or email - Part V, II (E)(1), DOJ Mutual Legal Assistance in Criminal Matters, A Guide for Domestic and Foreign and Competent Authority (DOJ MLA Guide)
Can the request be submitted directly to the central authority?
It is suggested that the requesting Party consult first the Philippine Central Authority, Department of Justice - Office of the Chief State Counsel (DOJ-OCSC), before submitting the request for assistance to determine if the assistance to be requested, based on the legal basis for the request, is available under the laws of the Philippines, and the request meets the requirements not only of the applicable treaty or convention but also the relevant Philippine laws. Part V, II (A)(1 and 2) of DOJ Mutual Legal Assistance in Criminal Matters, A Guide for Domestic and Foreign and Competent Authority (DOJ MLA Guide) states: "To ensure that the request meets all the requirements that will enable the Philippine authorities to effectively and promptly execute the same, the requesting Party may submit first to the DOJ-OCSC a draft of the request, especially those requiring compulsory process or court order for their execution".
What are the specific requirements (e.g. dual criminality, minimum penalty thresholds, etc.) that the requesting states have to meet under your domestic laws for MLA requests seeking for the provision of electronic evidence?
Generally, the legal provisions could be found in DOJ Mutual Legal Assistance in Criminal Matters, A Guide for Domestic and Foreign and Competent Authority (DOJ MLA Guide) 1. Treaty-based cooperation

The Philippines may seek or provide assistance pursuant to its bilateral Mutual Legal Assistance Treaties (MLATs) in Criminal Matters and relevant international conventions to which it is a Party.

2. Law

The Philippines does not have a comprehensive law on mutual legal assistance and is able to seek and provide assistance on the basis of a treaty or convention, or reciprocity. The Anti-Money Laundering Act of 2001, as amended, authorizes the Anti-Money Laundering Council (AMLC), the Philippines' financial intelligence unit (FIU), to seek and provide assistance from a foreign State.

3. Principle of Reciprocity

The extent of assistance that the Philippines can seek or grant on the basis of reciprocity will depend on the nature of the assistance being requested.

A request for assistance requiring compulsory processes for its execution may not be made on the basis of reciprocity, as requests of this nature can only be made on the basis of a treaty. An example would be a request for search and seizure, freezing, forfeiture or confiscation of assets which are generally of a more intrusive nature and, therefore, would require going to court and necessarily needs legal basis and supporting evidence.

4. Letters Rogatory

Similar to the principle of reciprocity, this form of assistance is founded upon the customary principle of courtesy and good will between nations. The scope of assistance for requests made through letters rogatory is generally much more restricted, often limited to service of documents or obtaining testimony and documents from a witness.

Dual criminality is generally needed for requests which require coercive action for their execution, such as search and seizure, production orders for bank records, and restraint and confiscation. The "conduct-based approach" to determine the existence of dual criminality is applied by the Philippines. Under this approach, the dual criminality requirement is met if both the Philippines and the foreign State or jurisdiction criminalize the conduct or activity underlying the offense, regardless of whether both States or jurisdictions place the offense within the same category, or denominate the offense under the same nomenclature.

5) REQUESTING ELECTRONIC EVIDENCE ACROSS BORDERS

5.1. **Direct requests** to foreign service providers

5.1.1. Requests for preservation

Philippines
What legal framework(s) is/are applicable, if any?
The Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012") and the Budapest Convention on Cybercrime
Which authority(ies) in your country is/are allowed to request data preservation to foreign service providers?
Law enforcement authorities and the DOJ Office of Cybercrime as the 24/7 Point-of-Contact in the Philippines, within the purview of the 24/7 Network under the Budapest Convention on Cybercrime
If the requested foreign service providers are prohibited or limited to preserve the data, are there any alternative options to preserve the data, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or MLA?
As a matter of procedure, foreign authorities coordinate through the 24/7 Point-of-Contact (DOJ Office of Cybercrime) under the purview of the Budapest Convention for purposes of preservation. Police-to-police cooperation is also an option, if the requested party is not a member of the Budapest Convention. Mutual legal assistance can also be pursued but it could be impractical since it is only mere preservation.
Can a court order or a search warrant be issued for data preservation by foreign service providers? If not, what are the reasons?
Preservation requests issued by Philippine authorities do not require court intervention.

5.1.2. Requests for voluntary disclosure

Philippines
What legal framework(s) is/are applicable, if any?
The Republic Act no. 10175 ("The Cybercrime Prevention Act of 2012") and the Budapest Convention on Cybercrime
Which authority(ies) in your country is/are allowed to request data disclosure to foreign service providers?
Law enforcement authorities and the DOJ Office of Cybercrime as the 24/7 Point-of-Contact in the Philippines, within the purview of the 24/7 Network under the Budapest Convention on Cybercrime
If the requested foreign service providers are prohibited or limited to voluntarily disclose the data, are there any alternative options to obtain the data, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or MLA?
The 24/7 Point-of-Contact network or mutual legal assistance are alternative options
Can a court order or a search warrant be issued for data disclosure by foreign service providers? If not, what are the reasons?
Yes, pursuant to the A.M. No. 17-11-03-SC on the Rule on Cybercrime Warrants (RCW).

5.2. Requests sent by your central authority for **Mutual Legal Assistance (MLA)**

Philippines
What is your central authority to send requests for MLA in criminal matters?
Department of Justice (DOJ) Office of the Chief State Counsel
Are informal contacts with the central authority of the requested states allowed and used?
Yes, it is actually preferred before sending the formal request.