# Spain

## International cooperation

### Specific step-by-step procedures and best practices

Version 23 July 2020

## Table of Contents



*This information sheet has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of facilitating international cooperation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.*

# 1. Categories of Data (subscriber information, traffic data, content data)

## 1.1. Definitions under national legislation

| | |
|---|---|
| **Subscriber Information** | The domestic legislation does not provide for a legal definition of what subscriber information is; nevertheless the Budapest Convention, ratified by Spain, applies. |
| **Traffic Data** | Pursuant to art Article 588 ter b) of the Criminal Procedural Law<br><br>*Electronic data, of traffic or associated, refers to all data generated as a result of the communication transmission through a network of electronic communications, the availability to the user, as well as through the provision of a similar service from the company of information or telematic communication of similar kind.*<br><br>A similar definition is provided for in Art. 61 of the Regulation of 15 April 2005 on electronic communication services. |
| **Content Data** | The domestic legislation does not provide for a legal definition of what content data is. |

Back to the Table of Contents

# 2. Procedures for preservation requests of stored computer data

## 2.1 Expedited preservation of stored computer data (Art. 29)

### General remarks

The expedited preservation of stored computer data is not specifically foreseen in the Spanish domestic law as a measure for mutual legal assistance. Nevertheless, the Budapest Convention, ratified by Spain, applies which means that preservation in the international context is affordable to the same extent as if it were a measure to be adopted in a domestic investigation.
Expedited preservation of stored computer data, as an internal investigative measure (Art. 16 of the Budapest Convention) is foreseen in Art. 588 octies of the Criminal Procedural Law as follows:

*Data preservation order*
*The Public Prosecutor or the Judicial Police may request any natural or legal person to retain and protect specific data or information included in a storage computer system available to them, until the corresponding judicial authorisation for their transfer is obtained in accordance with the provisions in the precedent articles.*
*Data shall be retained for a maximum period of ninety days, which may be extended once, until the transfer is authorized or one hundred and eighty days have elapsed.*
*The person requested shall be obliged to cooperate and to maintain secrecy regarding the execution of this measure, under liability described in Article 588 ter e., Subsection 3.*

### Procedures in place

Requests issued: For large service providers (most of them in USA), the requests are addressed directly to them through their email contact points or specific portals for law enforcement.
For the rest of the providers, the regular procedure is to reach them through the SPOC of the 24/7 network, since this national authority acts as an intermediary and improves trust between parties.
Requests received: The requests received through 24/7, are sent to our national service providers to retain and protect the data for the 90+90 days period under Article 588 octies.

## 2.2 Expedited disclosure for stored traffic data (Art. 30)

### General remarks

The expedite disclosure of stored traffic data is neither foreseen as a measure affordable in a domestic investigation (Art. 17 Budapest Convention) nor in the context of mutual legal assistance (Art. 30 Budapest Convention), which does not mean that such measures cannot be adopted, because the Budapest Convention is directly applicable.

Back to the Table of Contents

### Procedures in place

Where executing a preservation request with respect to a specified communication and there is a third party involved in the communication process based in another country, it's possible to disclose enough amount of traffic data to identify the service provider and the path of the communication in order to facilitate the requesting authority to address the order.

## 3. assistance

### 3.1 Requests for stored computer data: subscriber, traffic, content data (Art. 31)

Go to Subscriber information | Traffic Data | Content Data

## Requests for subscriber information

### General remarks

The Spanish Criminal Procedure Law does not provide for special measures for obtaining electronic evidence (subscriber information, traffic data and content data) through mutual legal assistance.
Internally, the procedure for accessing the data stored in the computer files of the service providers is established in Article 588 ter j of the aforementioned Law.

According to this article
*1. Electronic data held by service providers or people who facilitate communication in compliance with the legislation on data conservation related to electronic communications, or on their own initiative for commercial reasons, or not, and that are linked to processes of communication, can only be transferred and included in the file after judicial authorization has been granted.*
*2. 2 If the data is essential for the investigation, the competent judge will be asked to authorize the collection of the information included in the computer files of the service provider, including the intelligent or cross-data search, provided that the nature of the the data to be identified and the reasons that justify the transfer of such data are specified.*

As regard subscriber data, Art. 588 ter m reads as follows:

*Identification of the holders or terminals, or connectivity devices.*
*When, in the exercise of their functions, the Public Prosecutor or Judicial Police need to know the ownership of a phone number or of any other communication means or, in the opposite sense, require the telephone number or the identifying data of any communication means,*

*can turn directly to the providers of telecommunication services, of access to a telecommunications network or of services of the information society who will be obliged to meet the requirement, under penalty of incurring the offence of disobedience*."

Pursuant to the abovementioned Article and to Articles 18 (1) (b) and 35 of the Budapest Convention subscriber data can be obtained through the 24/7 Network: no MLA formal request is needed, but such formal request can be issued by a competent authority of another jurisdiction according to its domestic requirements and it will be also executed.

In compliance with Article 35 of the Budapest Convention Spain has two 24/7 points of contact. Each point of contact corresponds to one of the national law enforcement forces in charge of fighting cybercrime. In both cases, the e-mail address and office telephone numbers are included for ease of contact in case of absence. Both police forces share competence in this subject. When reporting information, these two points of contact can be used, as the allocation of cases between them is carried out based on rules and criteria previously agreed by them.

As regards international police cooperation, Guardia Civil and National Police participate in the most relevant international agencies as EUROPOL or INTERPOL. Their presence in the Joint Cybercrime Action Task Force (J-CAT) of EC3-EUROPOL should be highlighted.

## Competent Authorities

The content of this section is applicable to all subsequent sections under "competent authorities".
In the execution of MLA request for the gathering of subscriber, traffic or content data, the competent authorities are as follows:

Unless otherwise provided by an international convention ratified by Spain, the central authority is responsible for receiving incoming and outgoing requests from and to any country other than those of the EU, where the direct communication principle applies. In the context of the CoE, the second additional protocol to the 1959 Convention has been ratified by Spain but a reservation to Article 4.8 has been notified: according to this reservation, direct communication is only possible in urgent cases. As for the rest of the world, UN Conventions, bilateral agreements or reciprocity principle applies, via diplomatic channel or central authority, depending on the applicable Convention. In some exceptional cases direct communication is allowed. The Spanish Central authority is the Sub Directorate General for International Legal Cooperation of the Ministry of Justice.

Incoming requests related to subscriber data can be executed by the competent law enforcement agencies or by the prosecutor; for all other requests, traffic data or content data, judicial authorization issued by the investigative judge should be granted.

The authorities responsible for issuing a European Investigation Order are the judges or courts in charge the criminal proceedings where the investigative measure is to be adopted. The issuing authorities are also the public prosecutors in their proceedings (pre-procedural

Back to the Table of Contents

investigations), provided that the measure contained in the European investigation order does not affect fundamental rights.

The Public Prosecutor's Office is the competent authority in Spain to receive all European investigation orders issued by the competent authorities of other Member States. The receiving prosecutor will be competent to execute the request provided it does not affect fundamental rights: in case of electronic data, the prosecutor will be competent to execute a EIO where subscriber data is requested; other than that, judicial authorization is needed.

In all other contexts (non-EU CoE members and non-EU, non-CoE States), rogatory letters could be received either by Prosecution Services or Investigative Courts. The rules on competent authorities for executing these requests are similar: prosecutors would be competent only if subscriber data has been requested.

## Relevant contact points

The 24/7 CPs Network in the context of the CoE, EJCN or EJN CPs in the context of the EU, CiberRed CPs in the context of the Ibero American region, are always available. In addition, two domestic networks are working in the field of judicial cooperation and cybercrime: CPs of these two networks are deployed across country ; central coordination units for these two domestic networks in the Prosecutor General´s Office can be easily reached.

## Prior consultations

Any prior consultation can be carried out through informal ways, e.g. via EJN CPs (listed on its website) or all other abovementioned international networks. The province-based internal network of specialised prosecutors in the field of MLA can also be contacted for any aspect related to their field of expertise.

## Accepted legal basis / mechanisms for MLA requests

- Budapest Convention (Ratified on 03/06/2010);
- European Convention on Mutual Assistance in Criminal Matters, done at Strasbourg, 20th April 1959 (Instrument of Ratification 14Th July, 1982);
- Additional Protocol on Mutual Assistance in Criminal Matters, 17.III.1978 (Ratified on 2-8-91);
- Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, done at Strasbourg, 8th November, 2001 (Ratified on 1-6-2018);
- Convention on Mutual Assistance in Criminal Matters between the EU countries, 12th of July, 2000;
- Convention implementing the Schengen Agreement of 14 June 1985;
- United Nations Convention against Transnational Organized Crime and its Protocols.

Back to the Table of Contents

- Directive 2014/41/EU regarding the European Investigation Order in Criminal Matters
- Law 23/2014, Nov 20 on Mutual recognition of criminal decision in the EU (Spanish Legal framework).

## Content of the request

The request will observe the specific requirements, prescribed in the different tools.
For the EIO, the form should be filled out (Annexes). No need for attachments. Tidy description of the request and the crimes involved in separate windows. It is important to indicate the references to domestic (issuing state) criminal code in order to check whether the crimes are offences under the law of executing State and whether the EIO is related to one sent before.

For MLA, according 2000 Convention indications set out in Arts. 3 and 6 should be followed. No mandatory form. Attachment should be inserted when is requested by the executing authority.

For 1959 Convention:

a) Description of offences subject to investigation and/or prosecution, applicable law. Identification of domestic criminal proceeding
b) Statement of relevant facts, which is sufficient 1. to invoke the applicable criminal law, and 2. to reasonably infer the need for the requested assistance

## Applicable legal requirements

In case of execution of EIO, it should be verified that it has been issued in compliance with Art. 6 of the Directive and Art.189 of the Spanish Law 23/2014: a) necessity and proportionality, b) applicable to a similar domestic case. In addition, special verification of Art. 11 (grounds for non-recognition or non-execution) in order to refuse its execution. Similar provision as are in the Spanish law, since the Directive was implemented in the Law 23/2014, Nov 20.
For MLA, where 2000 Convention applies, all the requests will be executed according formalities and procedures indicated by the requesting state (Art. 4).
For 1959 Convention, see full text and Protocols. It will be underlined that the grounds for refusal are in Art. 2 (political offence, harm to sovereignty…) and the execution will be according to the law of the requested state. It is important to consult in advance the reservations made by Spain to the Convention and first/second Protocols, basically related to the concept of judicial authority, the special position of Gibraltar and the role of the central authority.
The Budapest Convention set out in Art. 23 onwards provisions related to international cooperation that have to be understood as an extension of the provisions of the 1959 Convention in order to allow for cooperation to the widest extent possible. In this regard, the reservations made by Spain are: identifies the Subdirectorate General of International Cooperation of the Ministry of Justice as the central authority for Arts. 24 and 27, set some

Back to the Table of Contents

provisions about the non-autonomous role of Gibraltar, and identifies the National Police as central authority for Art. 35.

### Confidentiality requirements

The execution of an EIO is confidential except to the extent necessary to execute the investigative measure (Art. 19 EIO Directive). It has been implemented literally in Art. 194 of the Spanish Law.

The execution of an MLA request under the 2000 Convention and to any other MLA instrument will be confidential; the requesting authority may make explicit the need to keep the execution of the MLA confidential. Art. 25 of the Second Protocol to the 1959 Convention on Judicial Assistance and 27.8 of the Budapest Convention include specific provisions in this field; therefore, Spain is bound by these provisions.

### Urgent requests

In the context of the EU, direct transmission applies, but the urgency of the request should be highlighted in the EIO or in the MLA and the reasons thereto.
As for the CoE, see above references as regards the 1959 Convention and the reservations made by Spain to the Second Protocol. The rest of MLAs where the central authority intervenes for the channelling of the requests, such requests can be sent in advance to the requested authority or in parallel to the central authority in order to speed up the process, as a best practice.

### Translation

According the Spanish legal framework any MLA request shall be translated into Spanish unless otherwise stated in a bilateral agreement. Portuguese is admissible under the 1959 Convention and the EIO regime.

### Limitations

## Requests for Traffic Data

### General remarks

Pursuant to Art 588 ter b, mentioned above, the legal regimes for the gathering of traffic data and content data are equivalent.

Back to the Table of Contents

## Competent Authorities

See above.

## Relevant contact points

See above.

## Prior consultations

See above.

## Accepted legal basis / mechanisms for MLA requests

- Budapest Convention (Ratified on 03/06/2010);
- European Convention on Mutual Assistance in Criminal Matters, done at Strasbourg, 20th April 1959 (Instrument of Ratification 14Th July, 1982);
- Additional Protocol on Mutual Assistance in Criminal Matters, 17.III.1978 (Ratified on 2-8-91);
- Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, done at Strasbourg, 8th November, 2001 (Ratified on 1-6-2018);
- Convention on Mutual Assistance in Criminal Matters between the EU countries, 12th of July, 2000;
- Convention implementing the Schengen Agreement of 14 June 1985;
- United Nations Convention against Transnational Organized Crime and its Protocols.
- Directive 2014/41/EU regarding the European Investigation Order in Criminal Matters
- Law 23/2014, Nov 20 on Mutual recognition of criminal decision in the EU ( Spanish Legal framework).

## Content of the request

See above.

## Applicable legal requirements

See above.

## Confidentiality requirements

See above.

## Urgent requests

See above.

Back to the Table of Contents

### Translation

See above.

### Limitations

See above.

## Requests for Content Data

### General remarks

As mentioned above, the procedure for international access to stored data is the same for all kinds of data.

### Competent Authorities

The Subdirectorate General for International Legal Cooperation of the Ministry of Justice is responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution

The Public Prosecutor or the Judicial Police are the authorities to ask for data retention for any natural or legal person for purposes of investigation.

See above references related to judicial investigative powers for the execution of these requests

### Relevant contact points

See above.

### Prior consultations

See above.

### Accepted legal basis / mechanisms for MLA requests

Back to the Table of Contents

- Budapest Convention (Ratified on 03/06/2010);
- European Convention on Mutual Assistance in Criminal Matters, done at Strasbourg, 20th April 1959 (Instrument of Ratification 14Th July, 1982);
- Additional Protocol on Mutual Assistance in Criminal Matters, 17.III.1978 (Ratified on 2-8-91);
- Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, done at Strasbourg, 8th November, 2001 (Ratified on 1-6-2018);
- Convention on Mutual Assistance in Criminal Matters between the EU countries, 12th of July, 2000;
- Convention implementing the Schengen Agreement of 14 June 1985;
- United Nations Convention against Transnational Organized Crime and its Protocols;
- Directive 2014/41/EU regarding the European Investigation Order in Criminal Matters
- Law 23/2014 , Nov 20 on Mutual recognition of criminal decision in the EU ( Spanish Legal framework).

### Content of the request

See above.

### Applicable legal requirements

See above.

### Confidentiality requirements

See above.

### Urgent requests

See above.

### Translation

See above.

### Limitations

See above.

## 3.2 Requests for real time collection of traffic data (Art. 33)

Back to the Table of Contents

## General remarks

The interception of telephone and telematic communications (content data, traffic data, associated data) is foreseen in Articles 588 ter a) to 588 ter i) of the Criminal Procedure Law. Judicial authorization will always be needed.
Article 588 ter b of the Spanish Procedural Criminal Code specifies that the scope of the interception of communications can be extended to the content of the communication itself and to 'electronic traffic data or data associated with the communication process'
According to this Article, section 2:
*The court-granted intervention may authorize the access to the content of the communications and traffic electronic data, or associated with the communication process, as well as to those occurring regardless of the establishment or not of a specific communication, involving the investigated individual, either as transmitter or receiver, and can affect terminals or the media of which the person under investigation is the owner or user.*
Article 588 ter a establishes that "*Authorisation to intercept telephone and telematic communications may only be granted when the purpose of the investigation is one of the crimes referred to in article 579.1 of this law, or crimes committed using computer equipment or any other information, communication or communication service technology*"
Article 579.1 refers to the following offences:
1. Deliberate offences punishable by a maximum of at least three years' imprisonment.
2. Offences committed within a criminal group or organization
3. Terrorist offences.

In addition to the above requirements, judicial authorisation will be required, subject to the principles of speciality, appropriateness, exceptionality, necessity and proportionality.

Article 588 ter d regulates the content of the judicial authorization request for the interception of telephone or telematics communications. The requirements contained in this provision must be added to those generally provided for in article 588 bis b for the application of any technological research measure.

The application for judicial authorisation must, apart from the requirements mentioned in article 588 bis b, contain the following:
a) identification of the subscriber's number, the terminal or the technical label,
b) identification of the connection subject to intervention, or
c) the data needed to identify the means of telecommunication in question.

To determine the extent of the measure, the application for judicial authorisation may have any of the following ends as its purpose:
a) Registering and recording the content of the communication, with an indication of the manner or type of communications affected.
b) Knowledge of its origin or destination, at the time the communication is made.
c) The geographic location of the origin or destination of the communication.
d) Knowledge about other associated traffic data, non-associated but of added value to the communication. In this case, the application will specify the precise data to be obtained.
Article 588 bis b: Where the Public Prosecution Service, or the Judiciary Police, apply to the Examining Magistrate for a technological investigation measure, the application must contain:

Back to the Table of Contents

1. The description of the event under investigation and the identity of the person under investigation, or any other affected by the measure, as long as this data is known.
2. A detailed description of the grounds justifying the need for the measure in accordance with the guiding principles provided for in article 588 a. i., and the evidence of criminality which was discovered during the investigation prior to the application to authorise the interception.
3. The identification data of the accused and, as appropriate, the means of communication used which allow enforcement of the measure.
4. The extent of the measure and specification of its content.
5. The investigation unit of the Judiciary Police that will be in charge of the intervention.
6. The manner in which the measure will be enforced.
7. The duration of the measure applied for.
8. The person in charge of carrying out the measure, if known.

Telephone and telematics interceptions are subject to the general provision of judicial control applicable to any technological investigation measure.

As for judicial cooperation, the Spanish Criminal Procedural Law doesn´t provide for specific rules for MLA regarding the interception of traffic data (Art. 33 of the Budapest Convention); only, in the context of the EU, Art. 219 of the 23/2014 Law, allowing for the real time collection of criminal data, via EIO.
For the rest of MLA requests, they will be executed provided an applicable international instrument is in place or upon the reciprocity principle.

## Competent Authorities

See above.

## Relevant contact points

See above.

## Prior consultations

See above.

## Accepted legal basis / mechanisms for MLA requests

See above.

Back to the Table of Contents

### Content of the request

See above.

### Applicable legal requirements

Articles 33 and 34 of the Budapest Convention refer to the conditions and procedures provided for under domestic law. Pursuant to the Spanish law, the regulation of the interception of telephone and telematics communications is provided for the above mentioned in Articles 588 ter a et seq. of the Spanish Criminal Procedural Code.

### Confidentiality requirements

See above.

### Urgent requests

See above.

### Translation

See above.

### Limitations

See above.

## 3.3 Requests for interception of content data (Art. 34)

### General remarks

The Spanish Criminal Procedural Law doesn´t provide for specific rules for mutual legal assistance regarding the interception of content data (Art. 34 of the Budapest Convention).
As mentioned above, the interception of telephone and telematics communications (content data, traffic data, associated data) is provided for in Articles 588 ter a) to 588 ter i) of the Criminal Procedure Law.
As for judicial cooperation, the Spanish Criminal Procedural Law doesn´t provide for specific rules for MLA regarding the interception of traffic data (Art. 33 of the Budapest Convention);

Back to the Table of Contents

only, in the context of the EU, Art. 219 of the 23/2014 Law, allowing for the real time collection of criminal data, via EIO.
For the rest of MLA requests they will be executed provided an applicable international instrument is in place or upon the reciprocity principle.

## Competent Authorities

Same than for real-time interception of traffic data

## Relevant contact points

Same than for real-time interception of traffic data

## Prior consultations

Same than for real-time interception of traffic data

## Accepted legal basis / mechanisms for MLA requests

Same than for real-time interception of traffic data

## Content of the request

Same than for real-time interception of traffic data

## Applicable legal requirements

Same than for real-time interception of traffic data

## Confidentiality requirements

Same than for real-time interception of traffic data

## Urgent requests

Same than for real-time interception of traffic data

## Translation

Same than for real-time interception of traffic data

## Limitations

Same than for real-time interception of traffic data

Back to the Table of Contents