QUESTIONNAIRE
WITH A VIEW TO TAKE STOCK OF THE OPERATION OF
ON THE RETENTION OF DATA GENERATED OR PROCESSED IN CONNECTION WITH THE PROVISION
OF PUBLICLY AVAILABLE ELECTRONIC COMMUNICATIONS SERVICES OR OF PUBLIC
COMMUNICATIONS NETWORKS AND AMENDING DIRECTIVE 2002/58/EC

v 30 09 2009

SPANISH RESPONSES (Qualitative questions):

1 Questions to Member States and and non- EU EEA States

1.A Qualitative and quantitative aspects of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10,

1.A.1 Law enforcement issues

1.A.1.a Total number of requests that are issued by year to obtain data retained under the DRD [Quantitative Reply]

The total number of requests that have been issued to obtain data retained since 2007 is 72.011.

1.A.1.b Number/Percentage of these requests that are generated by type of requesting authority: 1. police, 2. judicial, and 3. other authorities (please specify as relevant) [Quantitative Reply]

All requests are issued always by the judicial authority.

1.A.1.c The time elapsed between the date on which the data were retained and the date on which the competent authority request the transmission of the data, or if unavailable, the average age of the data that are requested, ? The answer to this question may already have been provided in the context of the statistics of Article 10 DRD. [Quantitative Reply]

At present our system doesn’t keep track of this information so we don’t have the means to carry out a statistical report. As an approximation, these requests can delay from several months to a year.

1.A.1.d Which communication channels are used to exchange information between law enforcement authorities and service providers (e-mail, fax, secure network, or other channels)? If certain channels are required to be used, please provide information about the channels to be used

A Secure network connection will be used in the near future. (VPN IPSec).
1.A.1.e Type of crimes
For what types of crime does the national law authorise the acquisition and use of retained data? Please provide a list of these crimes

Según el artículo 1.1 de la Ley 25/2007, de 18 de octubre que transpone la Directiva 2006/24/CE: Delitos graves contemplados en el código Penal o en las leyes penales especiales.

According to the article 1.1 of the Act 25/2007, from October 18th which it is a transposition of the 2006/24/CE Directive: serious crimes defined under Penal Code or penal special laws.

1.A.1.e.1 What is the average age of the data that has been requested for the different types of crime mentioned under I.A.1.e.1? [Quantitative Reply]

At present the average time is seven (7) months.

1.A.1.e.2 Does the national law allow for or prohibit acquisition of data from communications providers of data subservient of the Directive and/or related instruments for purposes other than the investigation, detection and prosecution of serious crime (e.g. copyright infringements). If so, please provide details about the alternative purpose(s) or laws prohibiting such acquisition.

The national law does not allow acquisition of data from communications providers for purposes other than the investigation, detection and prosecution of serious crimes.

1.A.1.e.4 Assessment of the data to be retained
The data to be retained are very important for the investigations of serious crimes.

1.A.1.e.5 Does the national law transposing the Data Retention Directive or a related instrument, require the retention of other categories of data in addition to the data contained in Article 5 of the Directive? If so, please provide details about the additional data as well as the instrument in which this obligation is enshrined.

No

1.A.1.e.6 Adequacy and law enforcement relevance of the data retained under Article 5 of the Data Retention Directive
Please indicate whether the data service providers must retain under Article 5 of the Directive are relevant and sufficient from a law enforcement perspective, and mention which data either should be removed from the list of Article 5 where redundant or be added where relevant data is not yet retained.

Member States are invited to motivate their answer and provide examples of situations that demonstrate the redundancy or the law enforcement requirements.

The data on which we need to apply the retention are suitable. The experience gained with the implementation of the Directive and the national laws will tell us if additional data will be required or if some data should be removed.

1.A.1.f Details of the requests that are issued

1.A.1.f.1 The kind of information that service providers are requested to retrieve; Please provide information about typical search parameters (information selection
criteria) contained in requests for the acquisition of retained data, e.g. listing of the communications made from or to a given phone number, or on certain date, or at a certain hour, or listing of all calls made from a certain location, or of all numbers used by an identified user.

The most important are the incoming and outgoing calls, subscriber identity request, mobile phone location and IP address identification.

1.A.1.f.2 Did your country standardise or seeking to standardise the format for the acquisition and disclosure of communication data between public authorities and communications service providers (for instance in service level agreements, or by making reference to relevant ETSI standars)? If so, please provide information about the standard (form or format) for requests, the message format, the technical modalities and/or interface.

- Draft of the Ministerial Order to adopt the ETSI TS 102 657 standard, for Handover Interface.
- Message format in XML

1.A.1.g Details of the replies to the requests mentioned under I.A.1.g

1.A.1.h Does the national law governing the acquisition of communications data enable the public authority to specify the time period within which data must be disclosed, as referred to in the Directive as “without undue delay”. If so:

Yes

1.A.1.h.1 Please provide examples of time frames enforceable within the context of national legislation or by service level agreements between competent authorities and communication providers.

The article 7.3 of the Act 25/2007, from Oct 18th, for data retention relative to the electronic communications..., states:

“The time period to exercise the transfer request will be determined by the judicial warrant, taking in consideration the urgency of the transfer and base of the investigation process, the nature and technical complexity of the operation. If no other period is established, the transfer will be carried out within the 72 hours counted from 8:00 a.m. of the next working day following the day when the Service Provide receives the warrant”

1.A.1.h.2 What measures do competent authorities avail of to ensure the respect of the time period within which they request the reply to be given?

The article 10 of the Act 25/2007, states:

“Non fulfilment of the obligation established in this Act will be penalized according to the stated in the Act 32/2003, from Nov the 3th, without prejudice to the penal responsibilities that arise from the not fulfilment of the data transfer obligation to the LEAs.
1.A.1.h.3 Where relevant, do competent authorities distinguish between time periods within which they require the disclosure of data by communication providers and the type of request or type of data they need? If so, please provide examples of such differentiation.

No

1.A.1.i Reimbursement of costs

1.A.1.i.1 Does your country reimburse CAPEX\(^1\) and/or OPEX\(^2\) incurred by service providers? If so, please provide information about the type of costs that are reimbursed, as well as about the modalities and amount or ratio of reimbursement.

No

1.A.1.i.2 Does your country make the reimbursement of costs conditional on the respect of certain conditions, such as, for instance, guaranteeing a certain quality of service (request profiles, amount of requests to be handled, speed of retrieval)? If so, could you please provide information about the conditions that service providers have to meet and the link between reimbursement scheme.

No

1.A.1.j Effectiveness - What is the success rate of the use of retained data

1.A.1.j.1 Did the use of retained data assist in crimes being detected and/or prosecuted within the courts that otherwise would have failed? If so, please provide examples.

[can entail Quantitative elements]

1.A.1.j.2 How much does the use of retained data cost in terms of deployment of Human Resources and acquisition & maintenance of dedicated equipment? What are the typical cost drivers?

[quantitative Reply]

No human costs

1.A.1.j.3 How can cost-effectiveness of the acquisition and use of retained data be increased?

[entails quantitative elements]

Unknown

1.A.2 National and transnational requests and answers

1.A.2.a Within this questionnaire, a "transnational requests" means a cross-border requests from the acquisition of communications data between EU Member States and non-EU EEA States as appropriate where:

1.A.2.a.1 law enforcement authorities from another country request you to provide data retained by service providers within your country (the “incoming request”) and

---

\(^1\) CAPEX or CAPlital EXPenditure, are expenditures creating future benefits. In concrete terms it is the cost of developing or providing non-consumable parts for the product or system, and may also include the cost of workers and facility expenses such as rent and utilities.

\(^2\) OPEX or OPerational EXPenditure are operating costs or recurring expenses which are related to the operation of a business, or to the operation of a device, component, piece of equipment or facility.
1.A.2.a.2 request initiated by your competent authorities for data held within another country’s jurisdiction (the “outgoing request”).

Having regard to the total number of requests mentioned under section 1.A.1.a:

1.A.2.a.3 how many (a) incoming and how many (b) outgoing transnational requests are processed by your country on an annual basis. When possible, please differentiate between judicial co-operation and non-judicial cooperation [Quantitative Replies]

1.A.2.a.4 what is the ratio between national and transnational requests (total number of transnational requests)? [Quantitative Reply]

We do not have unified statistics yet covering this aspect.

1.A.2.b What is the average time to:

1.A.2.b.1 receive an answer to an outgoing request, between the moment of issuing the request and the reception of the answer (see also A.A.2.f)? What are the elements (for instance: type of procedure) that determine the length of the procedure? [Quantitative elements]

The average time to provide an answer to these requests (outgoing requests) is three (3) months, and it mainly depends on the company, so the bigger troubles are the internal procedures of these companies. The requests are sent to the legal business addresses and the answers are received from the legal departments, which are not usually placed in the same address. Sometimes the companies base the delay on the implementation of the law on the protection of personal data. The INFORMATION OVERLOAD requested also determines the length of the procedure.

1.A.2.b.2 provide an answer to an incoming request, between the moment of reception of the request and the sending of the answer? What are the elements (for instance: type of procedure) that determine the length of the procedure? [Quantitative elements]

The average time from the incoming request to the sending of the answer is three (3) months, and it depends on the reception of the requested data.

1.A.2.b.3 Which strategies could be deployed to reduce the time it takes to answer an incoming request?

For example, the effective application or use of the Mutual Legal Convention?

1.A.2.c Which authority takes the decision in your country to issue a transnational request? Are all law enforcement authorities entitled to make or prompt to make a transnational request?
The authority is a Judge from the National Court, who can request a “Rogatory Commission” or can work with a warrant inside of the EuroJust framework.

1.A.2.d Does your country have a central point that issues outgoing requests or receives incoming requests? If so, please provide details about these central points.
No.

1.A.2.e Costs

1.A.2.e.1 If your country reimburses OPEX (see 1.A.1.k) do you reimburse national service providers in the same way for replying to transnational requests? Do you or do you plan to ask other Member States to share the costs?
No.

1.A.2.f Language

1.A.2.f.1 Does your country impose linguistic conditions to incoming requests (e.g. translation in a national or vehicular language? If so, please provide details about those conditions.
No.

1.A.2.f.2 What means does your country deploy to comply with linguistic conditions imposed by other countries to outgoing requests? Do you have a central facility to provide linguistic support?
We have translator resources in case of need.

1.A.2.g Data security

Which measures (rules, procedures, audit provisions) are enforced to protect data against misuse?
The measures are the Directive and the National Act of Data Protection. The access to this data will be available under judicial authorization.

1.A.3 Telecommunications authorities

1.A.3.a Allocation of tasks

1.A.3.a.1 Which national authorities are charged with tasks resulting from the Directive (for instance, as appropriate, following up with relevant services providers about applicable law, specifying content of data to be retained e.g. in CDRs, providing for a certain standardisation e.g. on the basis of ETSI standards, managing reimbursement schemes, assessing the economic impact of the implementation and application of the Directive)? Which tasks are assigned to which authority?
The Handover Interface format for the data delivery will be specified by Ministers of Interior, Defence and Economy and Treasury.

1.A.3.a.2 When did/will the respective authorities start to be operational for these tasks?
It is currently under implementation

1.A.3.a.3 For each authority: Did/does the authority need to acquire additional expertise in order to perform its tasks under the Directive? Which? How was this implemented (e.g. new staff, reorganisation, special training) or how will it be implemented?
No

1.A.3.a.4 Does any authority mentioned under this section collect data about the economic effects of measures required under the Directive, including the impact of replying to court orders to provided retained data issued by Civil Courts on the request of copy right owners in cases brought by them against illicit downloading and file sharing of copy right protected material. If the answer to this question is affirmative, please provide details about the authority as well as about the data that are collected? [May entail Quantitative elements]
No, it is not mentioned in the Act 25/2007, from 18th October, on “Data Retention related to Electronic Communications”.

1.A.3.a.5 Does any authority mentioned under this section engage in cross-border co-operation relating to the Directive? If so, please provide details about 1. those authorities 2. the type of action or activity that these authorities undertake in this context. [may entail Quantitative elements]
Not specifically.

1.A.3.a.6 Do the authorities mentioned under this section gather data concerning the impact of the required measures on competition e.g. on market entry for new operators, on advantages for bigger companies? Please provide details about the kind of data that are being collected? [last par may entail Quantitative elements]
No.

1.A.3.a.7 Centralised storage of data by Service providers

Does your country have problems (e.g. time to obtain an answer, quality of the reply) to obtain retained data that are stored by service providers outside of your country. Please provide details of problems you may have experienced and means deployed to redress these problems. [can entail Quantitative elements]

There were no problems.
1.B Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards (cfr Council Conclusions in Annex)

1.B.1 Law enforcement issues

1.B.1.a Which means (technical, operational) or measures (procedural, law-based) does your country deploy to increase the traceability of users of communication services so as to assist law enforcement authorities in the attribution of end-user devices to the person using them? Among the measures mentioned are those that take account of data that are presently held by communication providers, such as customer service notes, payment history, insurance agreements, IMEI history, but also supermarket loyalty cards associated to the top-up history, use of e-top-up linked to debit or credit cards, information held by credit reference agencies and mobile device given as contact point, forensic examination of mobile devices? Please provide a description of these measures.

The Spanish Legislation requires the identification for users having mobile prepaid services (prepaid mobile phone SIM cards), according to the Act 25/2007, from 18th October, about “Data Retention related to Electronic Communications”. The Sole Additional Legal Disposition, about Mobile Telephony Service provided through prepaid SIM cards, states:

“1st. The mobile telephony service operators, which supply services whose way of activation is based on prepaid cards, will have to create a compulsory register-book where client identity can be found for those who purchase an intelligent card with this type of payment.

The identification will be done through a legally proved personal identity document for registering on the compulsory register-book, the customer’s name, surnames or lastnames and nationality, the document’s identification number, its nature and its official denomination...

1.B.1.b What is the scope of these means or measures in terms of contribution to increasing the traceability of users? Please provide details about the legal justification or administrative motivation and as well as about the scope of these instruments, i.e. whether they are aiming to assist the prevention of crime, or its detection, investigation or prosecution. Which crimes are specifically addressed by the means and measures that your country deploys.

These measures will avoid the existence of anonymous subscribers with prepaid cards which use them to perform serious crimes, therefore these measure are aiming to assist the prevention of crime, or its detection, investigation or prosecution.

These measures are aiming to fight against terror, drug traffic, and organize crime and people kidnapping.
1.B.1.c  Efficiency

1.B.1.c.1  Are the measures imposed by your country efficient in terms of achieving the aim for which they have been put in place? Please provide details about results obtained as a result of the deployment of the relevant means or measures [may entail Quantitative elements].

It is very premature to assess the effectiveness of the measures.

1.B.1.c.2  Did your country assess the effectiveness of the measures? If so, please provide details of this assessment.

It is very premature to value the effectiveness of the measures.

1.B.1.c.3  What is the added efficiency of the measures deployed by your Member State in terms of improvement of your capabilities to detect, investigate or prosecute of terrorism and other serious forms of crime that go beyond the results obtained with the data obtained under Article 5(1)(e)(2) of the Directive and in particular its paragraph (vi)? [can entail Quantitative elements].

The measures are still being implemented. It is very premature to assess them.

1.B.1.c.4  What are the costs or these measures for the private sector? [can entail Quantitative elements]

Unknown.

1.B.1.d  Should measures be taken at European level to increase the traceability of users of communication devices? If so, which measures should be taken, at European level? How would these measures improve the efficiency of the means and measures that you deploy at national level?

Yes. If a country enforces the prepaid cards buyers to register, the subscribers can buy them in other countries that do not have such obligation, therefore, the measures will be more efficient if other countries in the EU will also implement such measures.

1.B.1.e  Which training or skill-development scheme, if any, does your Member State provide for law enforcement authorities to train them in attributing (linking) end-user devices (e.g. mobile phones) to data that are held by communication providers to identify the end-users?

The personnel in each police organization, working in these matters receive specified training.

1.B.2  Telecommunications authorities

1.B.2.a  Which impacts on the market do the means or measures mentioned in section 1.B.1 have?

The impact will be non relevant since all the operators have the same obligation.
1.B.2.b Does the authority mentioned in 1.A.3.a. & monitor and enforce national measures on providers or other stakeholders?

No

1.B.2.b.1 Did the authority mentioned in the previous question investigate any cases of non-compliance with national means or measures? Please provide details, if relevant. [can entail Quantitative elements]

Unknown.

1.B.2.b.2 If the national law provides for measures to ensure the identification of users of prepaid SIM cards, what treatment is given to the cards acquired before the entry into force of the law? Are these cards cancelled after a certain period in use?

The Act 25/2007, from 18th October, about “Data Retention related to Electronic Communications”. The Sole Additional Legal Disposition, about Mobile Telephony Service provided through prepaid SIM cards, states:

8th. Nevertheless, regarding the cards being purchased before this Act has been put in place, Mobile Telephony Operators will have a period of two years long, counting it since the date this Act has come into effect, to comply with the registering obligations.

Once this mentioned period is over (on 8th November 2009), Operators will be obliged to cancel or deactivate those prepaid cards whose users have not carried out their own identification.”

**COMMENTS:**

The questionnaire is very lengthy and detailed. But at the present time there are many issues that have no answers because they are still implementing the technical functionalities of DR systems and have not come into operation.

Spain has transposed the Directive into a national law, but they aren’t asking data to operators en masse and at present there is no relevant statistics.