Questionnaire with a view to take stock of the operation on the Retention of Data generated or processed in connection with the provisions of publicly available electronic communications services or of public communications networks and amending Directive 2006/24/EC – partial Slovenian answers from the Ministry of Higher Education, Science and Technology, Information Society Directorate

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

Public authorities have issued approx. 2821 requests to obtain data under the Directive 2006/24/ES in Slovenia in 2008.

1.A.1.c The time elapsed between the date which the data were retained and the date on which the competent authority requested 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]

The information about age of the data in Slovenia is represented below, although it has to be explained that only few Slovenian courts collected that information. Therefore the table provides the estimation of the age of data, calculated on the basis of a representative sample (282 cases that represents more than 10% of the whole statistics) for which the age was known (grouped in 3-months periods).

<table>
<thead>
<tr>
<th>Age of data provided - time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- age of data statistics based on 282 cases which contain all the relevant data that was necessary to calculate the age of data, in three months periods:</td>
</tr>
<tr>
<td>-3 - 0 months</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>2 (0,71%)</td>
</tr>
</tbody>
</table>

- extrapolation obtained from the sample of 282 cases which represent 10,40% of the whole sample that includes 2712 cases in which information was provided to the competent authorities:

<table>
<thead>
<tr>
<th>Age of data provided - time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- age of data statistics based on 282 cases which contain all the relevant data that was necessary to calculate the age of data, in three months periods:</td>
</tr>
<tr>
<td>-3 - 0 months</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>19</td>
</tr>
</tbody>
</table>

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

National legislation concerning electronic communications does not require that a specific communication channel must be used to exchange information between law enforcement authorities and service providers.

Ministry competent for electronic communications does not have relevant information concerning communication channels for exchanging information between law enforcement and service providers in actual use. The mentioned information may provide other ministries and public authorities (Ministry of the Interior, Slovenian Intelligence-Security Agency, Ministry of Justice, Public Prosecutor and Courts of Justice).

1.A.1.e.3 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)

National legislation concerning electronic communications imposes obligation of data retention for purposes of investigation, detection and prosecution of crimes as stipulated by law governing the criminal procedure, for the purposes of ensuring national security and the constitutional order, and the security, political and economic interests of the state, as stipulated by the law governing the Slovenian Intelligence-Security Agency, and for the purposes of national defence as stipulated by the law governing the defence of the state. Data retention obligation is not intended for purposes of investigation, detection and prosecution of misdemeanours.

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

National legislation concerning electronic communications does not require the storage of other categories of data different from the data contained in Article 5 of the Directive 2006/24/ES. All the categories of data that are required to be stored are listed in Article 107.b of the Electronic Communications Act and are in total accordance with the Article 5 of the Directive.

1.A.1.f.2 Did your country standardise or seeking to standardise the format for the acquisition and disclosure of communications data between authorities and the interaction with communications service providers (for instance in service level agreements, or by making reference to relevant ETSI standard)? If so, please provide information about the standard (form or format) for requests, the message format, the technical modalities and/or interface.
Current legislation does not impose any standards for the format for the acquisition and disclosure of communications data between authorities and the interaction with communications service providers, however presently we are in a process of preparing an Implementation Regulation (Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication network) which will replace the current Implementation Regulation - Rules on the method of transmission of retained traffic data in fixed and mobile electronic communications network telephony services (“Pravilnik o načinu posredovanja hranjenih podatkov o prometu telefonskih storitev v mobilnem in fiksnem elektronskem komunikacijskem omrežju, Uradni list RS, No. 31/2008”) and which will require from public authorities and communications service providers that acquisition and disclosure of data is made in a safe way by using electronic communication networks. By doing that public authorities and communications service providers will have to comply with provisions (take into consideration) of the standard ETSI TS 102 657 (v1.1.2 (2008-12)). Implementation Regulation will also determine exceptions from the mentioned rule. It is expected that the Implementation Regulation will come into force by the end of this year.

Time frames

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

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

National legislation concerning electronic communications (Electronic Communications Act, Rules on the method of transmission of retained traffic data in fixed and mobile electronic communications network telephony services) requires that communications service providers deliver retained data immediately (without undue delay) upon receiving a copy of the order of public authority that contains all the necessary data concerning the scope of the access. However, currently we are in a process of preparing an act that will amend Electronic Communications Act (ZEKom-B) and also a new Implementation Rule (Rules on the method of transmission of retained traffic data regarding telephony services and data services in mobile and fixed electronic communication network - look also answ. to 1.A.1.f.2) that will contain a new obligation for communications service providers to deliver retained data immediately or no later that in three day after receiving a copy of the order of public authority.

Ministry competent for electronic communications can not provide relevant information concerning possible time frames determined in orders of public authorities. The mentioned information may provide other ministries and public authorities (Ministry of the Interior, Slovenian Intelligence-Security Agency, Ministry of Justice, Public Prosecutor and Courts of Justice).
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?

Information Commissioner exercises inspection supervision of the retention of traffic and location data acquired or processed in connection with providing public communications networks or services, including compliances of communication service providers with the provisions of the public authority’s order which can include time frame for disclosing retained data. In cases of non-compliance the Information Commissioner may sanction service provider with a financial penalty.

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 requests or type of data they need? If so, please provide examples of such differentiation.

National legislation concerning electronic communications does not make provisions regarding different time periods for different types of request or different types of data that are requested by public authority.

Ministry competent for electronic communications can not provide relevant information concerning possible different time periods for different types of request or different types of data determined in orders of other public authorities. The mentioned information may provide other ministries and public authorities (Ministry of the Interior, Slovenian Intelligence-Security Agency, Ministry of Justice, Public Prosecutor and Courts of Justice).

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

National legislation concerning electronic communications does not provide for reimbursement of CAPEX or OPEX costs for communications service providers.

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.

---

\(^1\) CAPEX or CApital 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.
According to national legislation concerning electronic communications the reimbursement of cost can not be conditional since the mentioned legislation does not provide for reimbursement of any costs for communications service providers.

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?

National legislation concerning electronic communications does not provide provisions for reimbursement of any costs for communications service providers.

Telecommunications authorities

1.A.3.a.1 Which national authorities are charged with tasks resulting from the Directive (for instance, as appropriate, following up with relevant service 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 standard, managing reimbursement schemes, assessing the economic impact of the implementation and application of the Directive)? Which tasks are assigned to which authority?

Ministry competent for electronic communications is competent for preparing proposals of legal act and regulations regarding the electronic communications. The proposals of acts may include which standards should be respected by national authorities and service providers. As mentioned before Information Commissioner exercises inspection supervision about applicable law concerning the retention of traffic and location data acquired or processed in connection with providing public communications networks or services. In cases of non-compliance the Information Commissioner may sanction service provider with a financial penalty. Police authority, Slovenian Intelligence-Security Agency, Public Prosecutor or Investigating Judge have the competency to submit a request for the handover of retained data which also include the scope and content of data that has to be disclosed by service providers. Since the legislation concerning electronic communications does not reimburse costs for service provider, we do not have an authority who manages reimbursement schemes. To the knowledge of Ministry of Higher Education, Science and Technology there is no public authority that systematically performs tasks concerning assessments of the economic impact of the implementation and application of the Directive.

1.A.3.a.2 When did/will respective authorities start to be operational for these tasks?

All the mentioned authorities in answer 1.A.3.a.1 except the Ministry competent for electronic communications started to be operational for their tasks when the national provisions concerning Data Retention came into force on 15 September 2007 but only regarding tasks relating to telephony services in fixed and mobile electronic communication networks. Since the provisions relating to internet, internet telephony and internet e-mail came into force on 15 March 2009 the authorities became also
competent for these mentioned areas from 15 March 2009 forward. Ministry competent for electronic communications started to be operational for tasks preparing relevant national legislation when the Directive 2006/24/ES came into force.

1.A.3.a.4 Does any authority collect data about the economic effects of measures required under the Directive, including the impact of replying to court orders to provide retained data issued by Civil Courts on the requests 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]

To the knowledge of Ministry of Higher Education, Science and Technology there is no public authority that systematically collects data about the economic effects of measures required under the Directive, including the impact of replying to court orders to provide retained data issued by Civil Courts on the requests of copy right owners in cases brought by them against illicit downloading and file sharing of copy right protected material.

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]

To the knowledge of Ministry of Higher Education, Science and Technology no public authority systematically gathers information concerning the impact of the required measures on competition e.g. on market entry for new operators, on advantages for bigger companies. However, legislation concerning electronic communications allows and encourages so called joint data retention with the aim to reduce costs for smaller companies.

Law enforcement issues

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

Ministry of Higher Education, Science and Technology does not have relevant information concerning the exact costs of the Data Retention obligation for the private sector, however there have been some remarks from service providers and other stakeholders that the Data Retention obligation is related to certain costs and that national legislation should make provisions for reimbursement of costs for service providers.

1.B.2.b Does the authority mentioned in 1.A.3.a. & monitor and enforce national measures on providers or other stakeholders?

The Information Commissioner monitors and enforces national measures on service providers by exercising inspection supervision about applicable law concerning the retention of traffic and location data acquired or processed in connection with providing
public communications networks or services. In cases of non-compliance the Information Commissioner may sanction service provider with a financial penalty.
take stock of the operation on the Retention of Data generated or processed in connection with
the provisions of publicly available electronic communications services or of public
communications networks and amending Directive 2006/24/EC – partial Slovenian answers
from the Ministry of the Interior

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]

Police authorities have issued requests to obtain data for 1580 individual persons.

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

The Slovene Police attains information through the use of secure network or personal
service.

1.A.1.e Type of crimes

1.A.1.e.1 For what types of crime does the national law authorize the acquisition and use of
retained data? Please provide a list of these crimes

The police acquires data for the all types of criminal offences that are prosecuted ex
officio and listed in the Criminal Code, but most frequent requests are for following
criminal offences: Larceny/Grand Larceny, Drug trafficking, Joy Riding, Extortion and
Blackmail, Illegal Crossing of the State Border or State Territory, Manufacture and
Acquisition of Weapons and Instruments Intended for Committing of Criminal
Offence.

1.A.1.e.2 What is the average age of the data that has been requested for the different types of
crime mentioned under 1.A.a.a.? [Quantitative Reply]

In connection with our legislation we can request for data between 0 and 24 months
for all types of criminal offences. It is not possible to properly present the average
age of data, suffice it to say that the average age of data does not reach 24 months.

1.A.1.e.3 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. copy
right infringements). If so, please provide details about the alternative purpose(s) or laws prohibiting such acquisition.

No, Slovene legislation permits to acquire these data only for investigation and prosecution of criminal offences - which follows also prohibitory rules from Article 37 of the Constitution of the Republic of Slovenia.

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 the 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.

We find that the current data retention under Article 5 is appropriate.

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 identifiable user.

The police typically requests data necessary to trace and identify the source of a communication, data necessary to identify the destination of a communication, data necessary to identify the date, time and duration of a communication, data necessary to identify users’ communication equipment or what purports to be their equipment. The typical search parameters for the above mentioned requested data are: specific phone numbers, date, time period, etc.

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.

National legislation concerning electronic communications requires that communications service providers deliver retained data immediately, but the Police request the data delivery from providers to be implemented in the time frame between immediately and 1 month at the latest.

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]
The retained data is very important for the prosecution by the state prosecutor and in a later instance for the decision-making of the courts.

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]

The data retention is part of the common police investigation process and therefore does not entail any additional costs.

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

See answer 1.A.1.j.2.

1.A.2.a Within this questionnaire, a "transnational request" means a cross-border request for 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 county requests you to provide data retained by service providers within your country (the "incoming requests ") and

Based on the request of the law enforcement authorities from another country the police submit the request to the state prosecutor who in his turn passes the request to the competent court that formulates the request to the specific service provider. The answer to the authority from another country is passed by the police or by the court (sometimes via the Ministry of Justice).

1.A.2.a.2 requests initiated by your competent authorities for data held within another country's jurisdiction (the "outgoing requests ").

The Slovene police use the appropriate international channels of the Ministry of Justice.

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)

The police cannot provide relevant information concerning numbers of incoming and outgoing transnational requests.

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

See answer 1.A.2.a.3

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.J)? What are the elements (for instance: type of procedure) that determine the length of the procedure? [Quantitative elements]

The police cannot provide relevant information concerning time frames between an outgoing request and the reception of the answer.

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 police cannot provide relevant information concerning time frames between an incoming request and the sending of the answer.

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 state prosecutor and the courts can make the decision to issue a transnational request.

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.

Slovenia does not have a central point for issuing outgoing and receiving incoming requests. In most instances the Ministry of Justice is the focal point for those requests.

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.

The Slovene Police does not impose linguistic conditions on incoming requests.

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?

The Slovene Police has its own linguistic/translation unit to comply with potential linguistic demands in other countries.

1.A.2.g Data security

Which measures (rules, procedures, and audit provisions) are enforced to protect data against misuse?
Slovene police and other participants in this process (courts, state prosecution) use national legislation about secret (confidential) data and legislation protecting personal data, which are used against misuse.

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 reorganization, special training) or how will it be implemented?*

The Slovene Police has the needed know how and human resources to perform tasks under the Directive.

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 Slovene Police uses the measures included in the Criminal Procedure Act which are comparable with Directive 2006/24/EC

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.

The information on detection of a committed crime, for all types of criminal offences, is the basis on which the courts in the Slovene legal system authorize the implementation and use of measures as described in the Slovene Criminal Procedure Act. The evidentiary standard is grounds for suspicion (in Slovene language: "razlog za sum"), assessed by courts.

1.B.1.e **Efficiency**

1.B.1.e.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.*

The measures imposed by our country are efficient and do help in strengthening the prosecution of suspects who supposedly committed criminal offences.
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(l)(e)(2) of the Directive and in particular its paragraph (vi)? (can entail Quantitative elements)

The Slovene Police strictly abides to the measures only included in the Criminal Procedure Act which is similar to the Article 5(1)(e)(2), paragraph (vi).

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 Slovene Police regularly performs specialized trainings to improve the overall skill and knowledge of the police staff.