Questionnaire Dataretention Directive 2006/24/EC
Input Law Enforcement, National Public Prosecotor's Office in asociation with the Ministry of Justice
Date: 04-03-2010

1.A Qualitative and quantative 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.
Since the DRD has only entered into force on 1 September 2009, there is no complete view on the number of requests issued by year.

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)
Since the DRD has only entered into force on 1 September 2009, there is no complete view on the number of requests issued by year. We don't have numbers or percentages of requests that are generated by type of requesting 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 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.
The time elapsed can vary from less than 1 day to 6 months (retentionperiod for internet data) or a year (retentionperiod for telecommunication data). Because of the fact that in The Netherlands, the DRD has only been entered into force since 1 September 2009, there is no complete view on the quantitative questions in this questionnaire.

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.
E-mail, fax, secure network or physical hand over of data.

1.A.1.e Type of crimes

1.A.1.e.1 For what types of crime does the national law authorise the acquisition and use of retained data? Please provide a list of these crimes.
All crimes of Article 67 of the Code of Criminal Procedure.

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.1.e.1?
See response on question 1.A.1.c.

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.

The Dutch national law does not allow for acquisition of data from communication providers for other purposes other than the investigat of serious crime. (Article 67 of the Code of Criminal Procedure)

1.A.1.e.4 Assessment of the data to be retained

1.A.1.e.5 Does the national law transposing the DRD or a related instrument, require the retention of other categories of data in addition 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.

Telecommunications Act.

1.A.1.e.6 Adequacy and law enforcement relevance of the data retained under Article 5 of the DRD. Please indicate whether the data the service providers must retain under Article 5 of the Directive are relevant and suff ient 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 exampes of situations that demonstrate the redundancy or the law enforcement requ ts.

Since the DRD has only entered into force on 1 September 2009, there is no complete view on the relevancy of the retained data. LE and the largest providers have decided to set a standard and evaluate over time what data is usefull and what data should be removed from the list of retained data.

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

1.A.1.f.1 The kind of information that service provide quested 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.

If available at the police, the typical search parameters are:

- name
- address
- used number (telephone or IP-address)
- date, time

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

SLA based on ETSI standards. There are formats for the requests.
Besides that: standardized via CIOT-interface as far as the identifying data are concerned. There is a business case to try and get the historical identifying data in this system as well. With regard to the communicationsdata, this is not standardized yet.

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

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.
There is no formal time frame, but in the formats used, a time frame of 5-7 days within which the data must be disclosed is used.

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?
SLA and formal, periodic deliberation with the providers.

1.A.1.h.3 Where relevant, do competent authorities dis inguish 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.
Not usually, but depending on the (urgency of the) case and the type of data needed. Probably more time to disclose if it is known beforeha disclosing the data will take more time than usual.

1.A.1.i Reimbursement of costs à BZK/ Justitie

1.A.1.i.1 Doe your country reimburse CAPEX and/or OPEX incurred by service providers? If so, please provide information about the type of casts that are reimbursed, as well as about the modalities and amount or ratio of reimbursement.
We do not reimburse CAPEX. OPEX is only reimbursed as far it concerns direct costs of personell that is working on the request. With the largest 5 service providers we have a contract based on a lump sum.

1.A.1.i.2 Does your country make the reimbursement of costs conditional on the respect of certain conditions, such as, for instance, quaranteeing a certain quality of service(request profile, amount of requests to be handled, speed re rieval)? If so, could you please provide information about the conditi that service providers have to meet and the link between reimbursement scheme.
With the 5 largest service providers we have a contract in which quality standards are mentioned. If the service providers meet the standards for 100% they are entitled to a lump sum on which they agreed before. If they do not meet de quality standards we are entitled to shorten the service provider by utmost 10% of the lump sum in that year.

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.
The DRD has not been entered into force long enough to answer this question.

1.A.1.j.2 How much does the use of retained data cost n terms of deployment of Human Resources and acquisition & maintenance of dedicated equipment? What are the typical cost drivers?
We have no figures on that.

1.A.1.j.3 How can cost-effectiveness of the acquisition and use of retained data be increased?
By automatising the process of disclosure and standardizing as much as possible.

1.A.2 National and transnational requests and answers

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 country requests you to provide data retained by service providers within your country (the "incoming requests") and

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

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) outgo g transnational requests are processed by your country on an annual basis? When possible, please differentiate between judicial cooperation and non-judicial cooperation.
There are no figures on that.

1.A.2.a.4 what is the ratio between national and transnational requests (total number of transnational requests)?
There are no figures on that.

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?
There is no insight, since it is not registered at a central point and not dealt with by a central organ.

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 pr ure?

There is no insight, since it is not registered at a central point and not dealt with by a central organ.

1.A.2.b.3 Which strategies could be deployed to reduce the time it takes to answer an incoming request?
Try to have a central authority dealing with transnational requests. This authority should also know what data has to be retained for which period in other countries.

1.A.2.c Which authority takes the decision in your country to issue a transnat onal request? Are all law enforcement authorities entitled r prompt to make a transnational request?
The prosecution service (prosecutors).

1.A.2.d Does your country have a central point that issues outgoing requests or receives incoming requests? If so, please provide deta t these central points.
Yes.
AIRS (Ministry of Justice)
Department of International Assistance
PO Box 20301, 2500 EH The Hague
The Netherlands

LIRC:
Europaweg 45, 2711 EM Zoetermeer
PO Box 891, 2700 AW Zoetermeer
The Netherlands

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?
The service providers are reimbursed in the same way for replying to transnational costs. We have not yet a policy on sharing costs with member states.

1.A.2.f Language

1.A.2.f.1 Does your country impose linguistic conditio to incoming requests (e.g. translation in a national or vehicular language)? If so, please provide details about those conditions.
Dutch translation (or English in urgent matters). If not provided for, the request will be translated.

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?
Central database of translators, obliged to use them for translations.

1.A.2.g Data security
Which measures (rules, procedures, audit provisions) are enforced to protect data against misuse?

SLA: encryption, procedures.

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 byy communicat on 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.
There is no registration of prepaid SIM cards and we don't feel the need to change that yet. However, the date and time of first activation are a ilable. No other means or measures to trace users of prepaid SIM cards.

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 aimed 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?
It remains difficult to trace users of prepaid SIM cards.

1.B.1.c Efficiency

1.B.1.c.1 Are the measures imposed by your country eff ient 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.
The DRD has not been entered into force long enough to answer this question.
Misschien nog wel een mooi voorbeeld?

1.B.1.c.2 Did your country assess the effectiveness of the measures? If so, please provide details of this assessment.
The DRD has not been entered into force long enough to answer this question.

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)?
The DRD has not been entered into force long enough to answer this question.

1.B.1.c.4 What are the costs of these measures for the private sector?
Implementation of the DRD costs the private sector 75 million on CAPEX and 20 million on OPEX .

1.B.1.d Should measures be taken at European level to ase 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?
Registration of users could improve the efficiency.

1.B.1.e Which training or skill-development scheme, if any, does your Member State provide for law enforcement authorities to train them ttributing (linking) end-user devices (e.g. mobile phones) to data that are held by communication providers to identify the end-users?
Police officers dealing with telecommunication data are all trained by having had a course called 'DCS' (Digitale Communicatie Sporen, Digital Communication Leads). Employees of the prosecution service (legal officers, prosecutors) and judges are trained by being able to take a course named 'Interception and Investigation'.