00068/10/EN
WP 172

Report 01/2010 on the second joint enforcement action:

Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive

Adopted on 13 July 2010

Executive Summary

- This enforcement action by the Article 29 Working Party was set up to investigate compliance with the provisions introduced by directive 2006/24/EC, taking into account the recommendations and concerns voiced by the Working Party in its previous opinions on this matter.

- Implementation of the DR directive by electronic communications and Internet service providers is associated with an inherently high risk level that requires appropriate technical and organisational security measures. This is due to the circumstance that availability of traffic data allows disclosing preferences, opinions, and attitudes and may interfere accordingly with the users' private lives and impact significantly on the confidentiality of communications and fundamental rights such as freedom of expression.
- Based on both a questionnaire and on-site inspections addressing the main national operators and ISPs so as to cover significant market shares, the action shows a patchwork of implementation measures, with particular regard to the security measures in place.

- There are significant discrepancies as for the retention of Internet services traffic data categories, and the retention periods are also found to vary significantly in the individual Member States, whilst a more uniform picture emerges as far the retention of telephone traffic data categories is concerned. Of note, in many Member States' national laws a shorter retention period than the maximum allowed by the Directive proves to be the preferred option.

- In this connection, the Article 29 Working Party is concerned to find that the directive does not seem to have been consistently implemented at domestic level. In particular it appears that it has been interpreted by Member States as if it was leaving open the decision on its scope – that is, whether the directive was meant to derogate from the general obligation erase traffic data upon conclusion of the electronic communication or to mandate retention of all those data providers were already empowered to store for the purposes laid down in Article 6(2) of directive 2002/58. The latter interpretation is supported by the WP29 as well as being upheld in the recent judgment by the ECJ in the Ireland v. Commission case (C-301/06).

- The security measures appear to vary with the providers' business size; logical security measures are not always appropriate to take care of the highly sensitive information contained in traffic data. Importantly, the handover procedures applying to the traffic data requested by LEAs are found to be considerably inhomogeneous, including a wide gamut of solutions and different levels of transmission security.

- The action highlights additionally that only a few Member States have provided the Commission with the requested statistics on the use of traffic data retained under the directive, and that outsourcing is a widespread practice especially among smaller operators, the latter casting some doubts as for the effective compliance with data protection requirements.

- The lack of available sensible statistics hinders the assessment of whether the Directive has achieved its objective. The findings of the report clearly show a lack of harmonization and diversity in national implementation. Awaiting the decision of the EU Commission whether or not to amend or repeal the Directive[1], the Working Party considers it appropriate to lay down specific recommendations to ensure increased harmonization, more secure data transmission and standardized handover procedures.

- They include, in particular, the following:
  - ***Categories of retained data***: The list of traffic data that are to be retained on a mandatory basis is to be regarded as exhaustive. Accordingly, no additional data retention obligations may be imposed on providers pursuant to the DR directive.
  - ***Retention periods:*** in order to attain a level playing field the maximum retention period should be reduced and to set a single, shorter term to be complied with by all providers throughout the EU as stated in Opinion WP113 by the Article 29 Working Party. In a broader perspective, the overall security of traffic data "per se" should be re-considered by the Commission.
  - ***Technical and Organisational Security Measures:*** specific additional measures have been detailed (such as strong authentication, detailed access log management) and a proposed standard for data handover to LEAs has been developed in order to achieve faster, more reliable data transfers enabling the collection of statistical information and accountable data accesses. In this connection, the concept of "serious crime" would appear to require clarification at Member State level and the list of the entities authorised to access the data should be disclosed to all the relevant stakeholders.

[1] In this respect the Article 29 Data Protection Working Party recalls its previous opinions on this directive

I. Background – Enforcement

Following the first Report on the implementation of the Data Protection Directive in May 2003, the European Commission requested the Article 29 Working Party to consider the launching of sector-related investigations at EU level and the approximation of standards in this regard. The Article 29 WP, in a Declaration of 25 November 2004, stated that the promotion of uniform application and harmonised compliance with data protection legislation is one of its strategic and permanent goals.

After the first joint enforcement action on private health insurance companies (Report 1/2007 adopted on 20th June - WP137) and on the basis of the experience gathered on that occasion, the Article 29 WP decided to implement a second joint inquiry and chose to investigate the compliance at national level of Telecom Providers and ISPs with the obligations arising from national traffic data[2] retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC – as part of the priorities set forth in its Work Programme to verify the uniform application of the data protection principles harmonised at Community level.

The Enforcement Task Force (ETF) was mandated in July 2008 by the WP 29 to plan and implement the steps required to carry out the action in accordance with the terms of reference detailed in WP152.

The combination of criteria identified in WP101 pointed to the selection of this topic even though the Working Party was aware that the transposition process of the DR Directive was not over – whether on account of national delays or because of the different deadlines set for Member States to introduce retention obligations also in respect of Internet traffic data.

This decision was made because Directive 2006/24/EC is quite specific in scope and derogates from the general principle laid down in the e-privacy directive (2002/58/EC) – under whose Article 6(1) "traffic data relating to subscribers and users processed and stored by the providers of a publicly available electronic communications service must be erased or made anonymous… when it is no longer needed for the purpose of the transmission of a communication." The only general obligation to store traffic data is set forth in paragraph 2 of Article 6, to the extent such data is necessary "for purposes of subscriber billing and interconnection payments" – however, this is only permissible "up to the end of the period during which the bill may be lawfully challenged or payment pursued." It should be recalled that the objective pursued by directive 2006/24/EC (see its Article 1) consists in "harmonis(ing) provisions …with respect to the retention of certain data which are generated or processed by [providers of publicly available electronic communications services or of public communications networks]". The data in question may be retained "for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law."

[2] For the sake of clarification, "traffic data" in this opinion encompasses the data referred to in Article 5 of directive 2006/24/EC.

Furthermore, the Article 29 WP had issued three opinions on the Data Retention Directive and the drafts preceding the final instrument.[3] In these opinions, in particular in documents WP113 and WP119, reservations were voiced since the provisions of the Directive have far reaching consequences for all European citizens and their privacy as the decision to oblige telephone and Internet service providers to retain traffic data of all their subscribers and users was and is an unprecedented one. It encroaches into the daily life of every citizen and may endanger the fundamental values and freedoms all European citizens enjoy and cherish. Consequently, the WP29 in its opinions "considers crucial that the provision of the Directive are interpreted and implemented in an harmonized way to ensure that the European citizens can enjoy throughout the European Union the same level of protection".

The WP29 was concerned about the rather vague purpose consisting in "combating serious crime", given the lack of a shared definition of serious crime, as well as about the lack of specific guidance on the authorities entitled to access the retained data and the retention mechanisms of such data by providers to ensure that the information would only be available for the purposes laid down in directive 2006/24. The WP29 asked that safeguards be introduced at least with regard to purpose specification, access limitation, data minimization, prohibition on data mining, judicial/independent scrutiny of authorized access, ban on the use by providers of the data that is retained solely for public order purposes under the DR Directive – which led to the request for system separation and the definition of minimum standards for the security measures to be taken by providers.

The retained traffic data allow monitoring and tracing the whole relational network of individuals as well as mapping their movements and the tools used in doing so. Any restrictions on individuals' rights of privacy and data protection must be necessary, appropriate and proportionate within a democratic society and serve specific order public purposes – national security, defence, public security, or the investigation, detection and prosecution of crimes. As a bare minimum, such restrictions must respect the rights, freedoms and principles laid down in the Charter of Fundamental Rights of the EU as well as in the European Convention for the protection of human rights and fundamental freedoms.

Looking at the way the directive has been implemented so far in domestic laws was accordingly a tool to verify the reservations of the Article 29 WP and the harmonization achieved so far.

Although the transposition process has yet to be completed in the EU, the findings of this enquiry now enable the WP29 to provide helpful information to the Commission, which is expected to submit its assessment report by 15 September 2010.

II. The Legal Framework

As said, the objective of directive 2006/24/EC (hereinafter, the DR directive) consists in harmonising the national provisions on the retention obligations that apply to certain traffic data. Reference can be made in this connection to Articles 5, 6 and 7 of the DR directive, which lay down the categories of data to be retained, the relevant retention periods, and the data protection and security measures, respectively. It should also be recalled that the obligation introduced by the directive may have and has a different impact depending on how

[3] Opinions 9/2004, 4/2005 and 3/2006

Article 3 thereof is construed and implemented – i.e. on whether it is established that the directive derogates from the general principle whereby traffic data should be erased when it is no longer needed for the purpose of the communication (as per Article 6(1) of directive 2002/58), or rather that it only introduces a mandatory retention period for such traffic data as already collected and stored by providers for the purposes mentioned in Article 6(2) of the 2002/58 directive ("billing purposes and interconnections payments").[4]

Given these premises, it should be recalled that the provisions contained in the above Articles are to be applied restrictively by Member States – i.e., domestic legislation implementing the directive may only be introduced by Member States to the extent such legislation is strictly in line with the requirements made in the DR directive.

It should also be pointed out that the DR directive requires each MS to designate a public authority to be responsible for monitoring the application of the provisions laid down in directives 95/46/EC and 2002/58/EC as well as the data protection and security measures mentioned in Article 7 of the DR directive. The security measures mentioned in Article 7 are to be regarded as the minimum level to be afforded by each MS. Of note, the DR directive expressly provides in article 9 that the public authorities in question may be the national DPAs, and should be fully independent in their monitoring activities.

Additionally, the DR directive provides that the Commission should submit to the European Parliament and the Council, by 15 September 2010, an evaluation of the application of the directive and the impact of its provisions with a view to determining whether it is necessary to amend the directive by having regard, in particular, to data categories and retention periods. In performing this evaluation, the Commission should take account of the observations submitted by Member States and the Article 29 WP as well as of the statistics on data retention Member States are required to provide to the Commission on a yearly basis as provided in Article 10 of the said Directive. These statistics should report, in particular, the cases where information was transmitted to LEAs, the time elapsed from the date on which the information was retained and the date on which LEAs requested such information, and the cases where the data requests could not be complied with.

As said, at the time of drafting this report, not all Member States had transposed the DR directive. In some MS (Germany, Romania), the Constitutional or Supreme Courts have ruled that the respective transposition legislation was in breach of constitutional principles.

---

[4] In *Opinion 1/2003 on the storage of traffic data for billing purposes, adopted 29 January 2003* WP29 gave guidance in the harmonisation of the period during which traffic data may lawfully be processed for billing purposes. Storage for billing purposes should normally involve a storage period of 3-6 months at most. Only traffic data that are adequate, relevant and non-excessive for billing and interconnection purposes may be processed. Other traffic data must be deleted or anonymised.

Practices that are inconsistent with these principles as well as practices that are not clearly authorised by legislative provisions under the conditions of Article 15 of Directive 2002/58/EC are, prima facie, incompatible with the requirements of EC Data Protection Law.

III. The Enforcement Action

A. Rationale

The enforcement action was aimed at assessing how the providers of electronic communications services and Internet service providers had transposed the obligations arising out of the DR directive as for the categories of retained traffic data (Article 5), retention periods (Article 6) and technical and organizational security measures (Article 7). In those Member States that had not yet transposed the directive into national law, account was taken of the obligations imposed on the aforementioned providers by the national legislation in force pursuant to the e-privacy directive (directive 2002/58/EC) – with particular regard to Articles 6 and 9 thereof. Reference was also made to the minimum safeguards proposed in Opinion 3/2006 (WP 119).

Under directives 2006/24/EC and 2002/58/EC, the security of personal data must be proportionate to the risks arising from the processing of such data and the features of the data in question. From this standpoint, it is unquestionable that the implementation of the DR directive carries specific risks to data subjects on account of the nature of traffic data. For this reason, the enquiry carried out by the Article 29 Working Party's members was meant more specifically to gather concrete information about these risks in order to investigate whether the concerns voiced by the Working Party on earlier occasions would still apply.

As said, the availability of traffic data allows disclosing preferences, opinions, and attitudes and may interfere accordingly with the users' private lives and impact significantly on the confidentiality of communications and fundamental rights such as freedom of expression. These scenarios are unfortunately likely to occur both because of intentional activities and on account of negligent retention mechanisms. The unauthorised disclosure of and/or access to information related to electronic communications – which may be associated with location data – can affect data subjects' privacy considerably. In the light of the above circumstances, implementation of the DR directive by electronic communications and Internet service providers is associated with an inherently high risk level such as to require appropriate technical and organisational security measures.

Regarding the risks, it should be recalled that the directive bans the retention of data related to the contents of communications; additionally, the mere availability of traffic data (i.e. those referred to in Article 5 of the DR directive) allows tracing several items of personal information related to data subjects (including sensitive information) based on the overall picture (e.g. behavioural profiles of individual users) that can be derived of their social interactions. This information can be put in a time and space context and categorized in a highly detailed manner via data mining tools that benefit from the major computing power that is currently available through servers and personal computers. These techniques prove especially effective in the presence of massive amounts of traffic data covering a large time span. As for Internet-based services, further risks can arise compared to telephone traffic data because information such as the destination IP address can disclose the respective contents per se; as well as the social graph, they may also unveil information on the data subjects' most intimate preferences. One of the objectives of this enforcement action consisted accordingly in assessing to what extent electronic communications and Internet service providers were aware of these specific risks and live up to the safeguards put in place to avoid these risks.

B. Methodology and Stages

The investigation was carried out by the Data Protection Authorities of: *Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Lithuania, Malta, Netherlands, Poland, Romania, Slovak Republic, Slovenia, Spain, and the United Kingdom.* It should be recalled that comments on the findings of the investigation were also submitted by the Swedish Post and Telecom Agency as well as by the European Commission.

Based on the experience gathered from the first enforcement action as well as on the suggestions contained in the final report of that action, the Article 29 Working Party decided the second enforcement action to consist in two steps – namely, the administration of a questionnaire followed by the assessment of the replies by DPAs, also by means of on-site inspections.

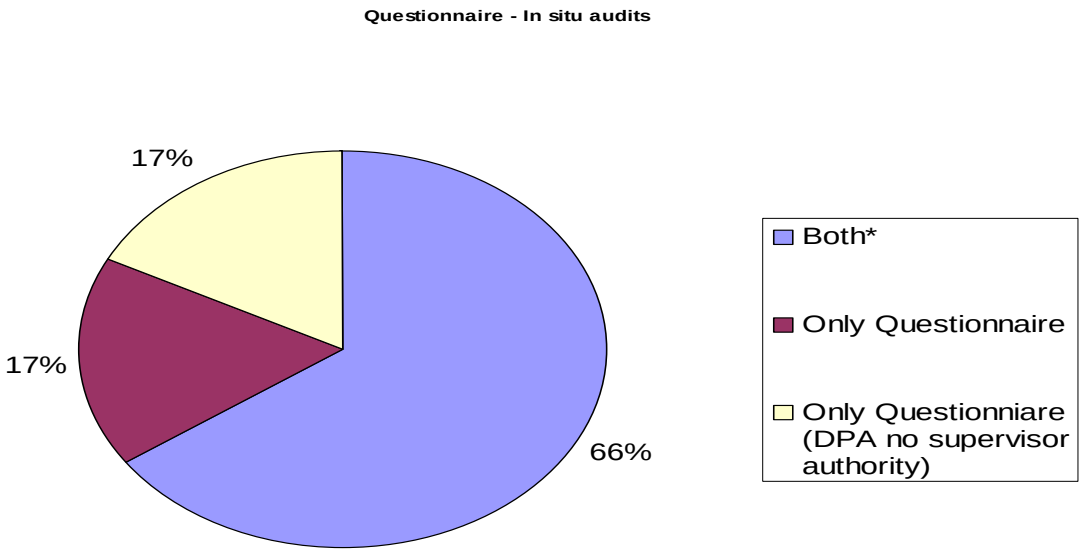
A standard questionnaire (adopted by the WP in December 2008) was administered on the basis of a standard letter to all the electronic communications and Internet service providers that had been selected in the individual Member States. The selection of investigated companies was based on criteria of addressable market (fixed vs. mobile telephony, convergent operators, pure internet service providers), size (small providers and big Telco operators) in order to cover a significant national market share.

The questionnaire included 10 sections addressing the type of data retained, the retention periods, and the technological solutions implemented for retention purposes along with especially important issues in a data retention perspective (e.g., IT security, logical protection, authentication/authorisation, logs, encryption, disclosure/transmission protocols, physical protection, back-up/disaster recovery). The number of questions was kept small and their contents was specified as clearly as possible, taking account of the issues reported following the first enforcement action as also related to the selection criteria of the respondents.

On-the-spot inspections were carried out whenever this was found necessary by DPAs and allowed in pursuance of the inspection powers conferred on DPAs by national laws as well as in the light of the availability of experienced staff. Such inspections were aimed at evaluating reliability of the replies to the questionnaire and obtaining more detailed information on implementing issues and proved fundamental to assess compliance by data controllers with the applicable requirements.

A national report was subsequently drawn up by each of the participating DPAs to take stock of the respective situation and the main criticalities. A Table summarising the information provided by the participating DPAs can be found in Annex 1 to this Report.

The diagram below shows the statistical distribution of the DPAs that performed on-the-spot inspections compared to that of the DPAs that administered the questionnaire and that of the DPAs which do not have the required enforcement powers.



C. Findings[5]

Generally speaking, the replies to the questionnaire showed a patchwork of implementing measures, with particular regard to the security measures in place (see Annex 1, Columns P and Q). Only through in-depth, on-the-spot inspections was it possible to establish that some of the replies were inaccurate and/or imprecise, which resulted into the imposition of ad-hoc sanctions and specific technical and organisational measures.

Taking account of the different information value provided by inspections compared to the administration of a questionnaire, especially the DPAs empowered to carry out inspections should be conscious of the inherent risks of a general obligation to retain traffic data, by recommending awareness campaigns and if necessary continuing their monitoring of the systems at the premises of electronic communications and Internet service providers; additionally, it would be necessary to prevent the enforcement activities of DPAs from being limited by possible constraints, including those related to business/industry confidentiality, where such constraints may be relied upon by the said providers in order to not disclose the requested information. It is necessary to give broad enforcement powers to DPAs, including the power to demand access to business/industry confidentiality. Otherwise, a full-fledged picture will be difficult to obtain.

[5] See the Table in Annex I to the Report for a detailed overview of national replies.

i. Categories of Retained Data

As for the categories of traffic data subject to the retention obligation, it was found that the telephone traffic data retained by the individual providers (Annex 1, Columns I and J) were basically in line with those listed in Article 5 of the DR directive. Conversely, there were some significant discrepancies as for the retention of Internet services traffic data (Annex 1, Column K).

Subject to few exceptions (in particular a case where in a MS the contents of sms messages were found to be retained and accessed for several months to facilitate the activity of security services), the data required to identify source and destination of the communications, beginning and end of the communications, the service and terminals employed by users are retained with regard to telephone services. A particular cause for concern is related to the retention of location data, where such data are collected continuously during a call or an internet session, due to the potential for tracking user mobility.

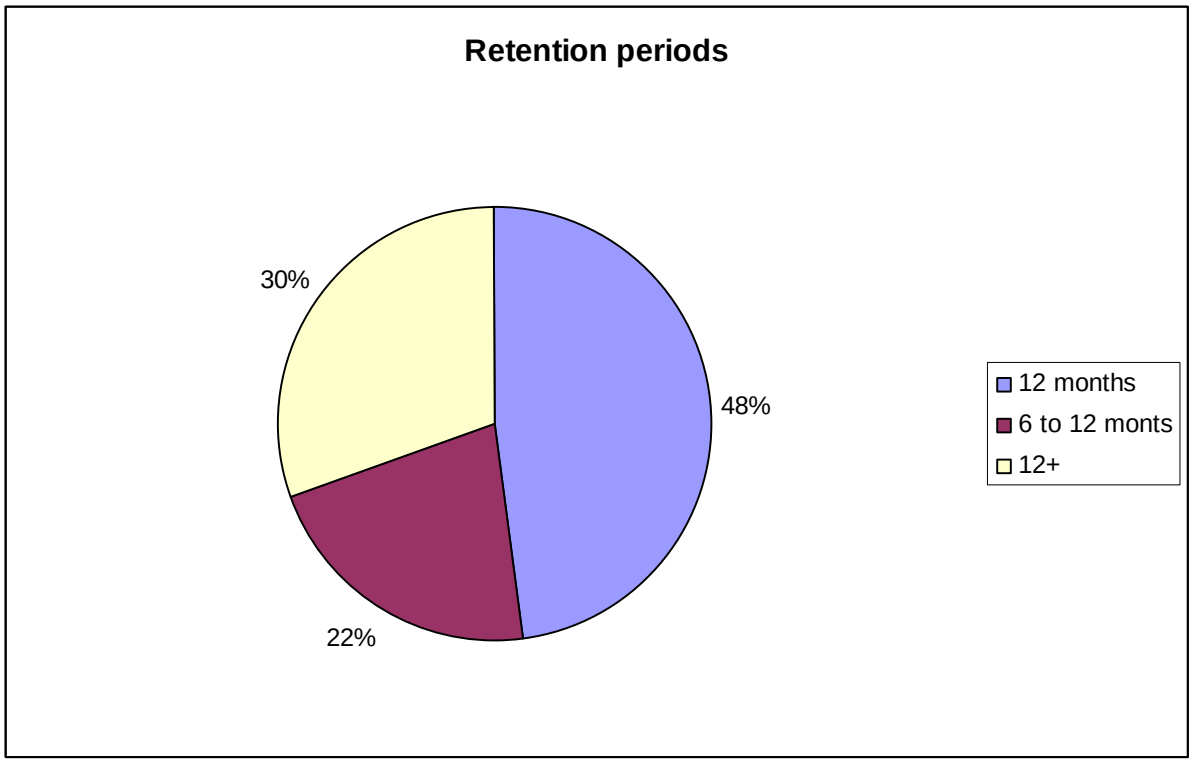
The situation is different as regards the retention of Internet traffic data. As well as the data categories listed in Article 5 of the directive, additional data categories are retained in some cases that have to do with the contents of communications and thereby fall outside the scope of the current regulatory framework (see Annex 1, Column K). Reference can be made in this regard to the destination IP address and the URLs of web sites, the headers of e-mail messages, the list of all the recipients of e-mail messages in "CC" mode at the destination mail server, the port number allocated to users by the ISP.

In this connection, it should be recalled that directive 2006/24/EC derogates from the provisions of directive 2002/58/EC and the list of traffic data that have to be retained on a mandatory basis is to be regarded as exhaustive – i.e., no additional data retention obligations may be imposed on providers pursuant to the DR directive.

On the other hand, the Article 29 WP is aware of the issues related to the possible extension of the scope of application of the DR Directive under national law – in particular whether LEAs may only gather the traffic data that providers are allowed to retain under paragraph 2 of article 6 of Directive EC/2002/58 or also additional traffic data which are not mentioned in the relevant provisions of directive 2002/58/EC.

ii. Retention Periods

For the purposes of this analysis and based on the achievements of the enforcement action, the potential retention range (6 to 24 months) was broken down into three time sets, namely: a. 12-month retention; b. less than 12-month retention; and c. over 12-month retention. It was found that 48% of the responders retained data for a 12-month period, with significant, comparable percent rates as for "fresh data" (b. group) and "tail data" (c. group) – which were 22% and 30%, respectively. The diagram below shows the percent distribution for the EU Member States:



The retention periods set by the national legislators in transposing the DR Directive were found to vary significantly in the Member States (see Annex 1, Column L, M, N), although in many countries (see the diagram below) a shorter period than the maximum allowed proved to be the preferred practice, which would suggest that the retention period range laid down in the DR directive can be harmonized further.

To that end, ***it would be preferable to consider reducing the maximum retention period and to set a single, shorter term to be complied with by all providers throughout the EU as stated in Opinion WP113 by the Article 29 Working Party***[6]***.***

Based on the findings of this enforcement exercise, the providers contacted and/or inspected/audited complied with the retention obligations as above. However, in very few cases the de facto situation proved different on account of the different storage practices and/or obligations applying to traffic data for business/commercial purposes, whereupon such data are actually stored for longer periods than those set forth in the DR directive. In some cases such periods span as many as 36 months, and in one case the storage period was found to amount to 10 years.

Furthermore, it was found that in many cases no automated data erasure procedures were in place upon expiry of the relevant retention periods. It must be recalled in this regard that the adoption of manual and/or human-initiated procedures is not to be considered in line with the DR directive as it allows extending the retention periods for the uncertain time span ranging from the lapse of the retention period to the start of the manual erasure procedure.
Automated procedures should also be applied to backup copies.

[6] WP 113 "In any event, a general retention period must be clearly regulated. Such retention period should be as short as possible and should be as close as possible to the retention period for the original purposes for which communication service providers recorded those data."

It should also be pointed out in this regard that electronic communications and Internet service providers store traffic data in several systems and use that data for multifarious operational and management purposes, which are provided for by law in some cases as well as being regulated via SLAs and service provision contracts. Additionally, any traffic data stored in LEA-accessible systems were actually also stored in other systems beforehand; such systems were accessible for various purposes such as troubleshooting, fraud detection, billing, etc. by multifarious entities in the provider's organisation that were subject most frequently to less stringent controls.

Therefore, it would be appear to be necessary to emphasize the need for the Commission and the other institutions in charge of assessing operation of the data retention directive to take account of the overall sensitivity of traffic data per se and re-consider their overall security – regardless of whether such data is stored in systems and for purposes other than those referred to in the DR directive - with a view to the overall assessment of the implementation of the DR directive. Allowing the systems containing the categories of traffic data mentioned in the DR directive to implement different security levels and retention periods compared to those systems that contain traffic data used for different, business-related purposes means lowering the overall security of the traffic data and failing ultimately to meet the requirements made by the DR directive – i.e. that traffic data should be retained for limited periods and accessed on the basis of specific constraints.

iii. Technical and Organisational Security Measures

Article 7(b) of the DR directive requires traffic data to be retained in such a way as to ensure that appropriate technical and organisational measures are in place in order to minimise the risk of accidental and/or unauthorised destruction or alteration of the data along with the risk of unauthorised access and/or processing.
The DR directive does not require additional security measures to be in place on top of those provided for by directive 2002/58/EC and directive 95/46/EC. However, as already pointed out in the aforementioned WP29 opinions, it should be considered that it is the risk level associated with traffic data *per se* that mandates strict, risk-adjusted security standards to be implemented by having regard to the nature of such data, the amount of stored data, and the retention periods.
In this connection, the enforcement action has shown that the technical and organisational security measures implemented by electronic communications and Internet service providers mirror their awareness of the risk(s) associated with telephone and Internet traffic data. If no detailed guidance is provided, or if the attending risks are underestimated, it is highly likely that inadequate measures are taken.

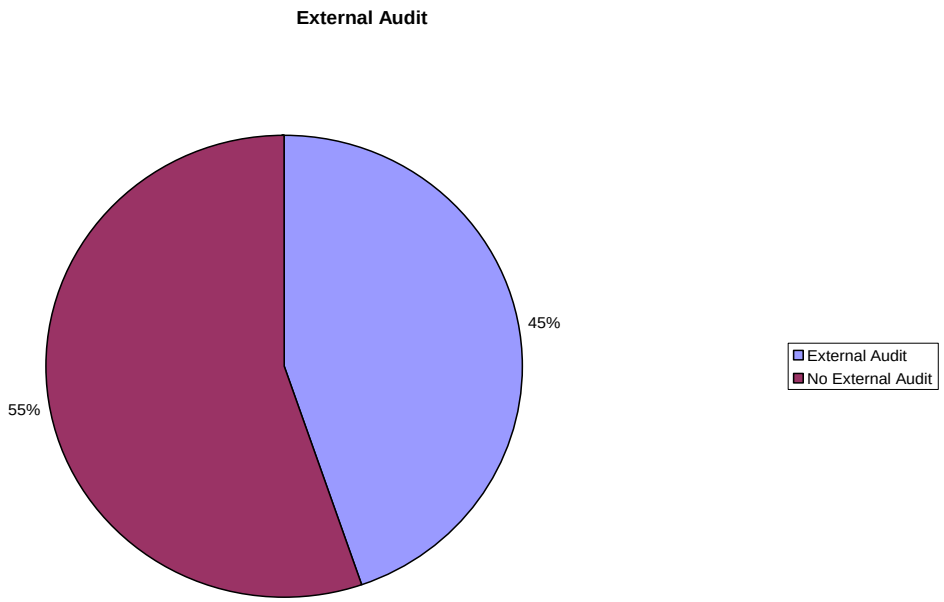
In order to comply with the requirements in the DR directive, electronic communications and Internet service providers should assess the risks associated with traffic data on a regular basis and as objectively as possible, in order to detect all the relevant risk factors and their possible impact, and by paying special attention to access control and data availability. Regular external audits could contribute to an independent and objective risk assessment.

Regarding information security, no homogeneous picture was found based on the enforcement exercise; indeed, the security measures can be said to vary with the providers' business size – based both on the replies to the questionnaire (see Annex 1, Columns P and Q) and on the in-situ inspections.

High security levels could be found with regard to physical accesses to traffic data retention systems (see Annex 1, Column Q). Apart from minor differences, most electronic communications and Internet service providers rely on video surveillance, dedicated surveillance staff, access control systems and emergency-triggered escalation procedures to ensure the continued monitoring of the said systems.

Whilst larger providers were found to deploy technical and organisational measures that could ensure the appropriate security level for the retained traffic data, smaller providers would appear to afford lower security standards; indeed, most of them - mainly on account of cost-containment strategies - are unable to implement top IT security solutions protecting the traffic data to the same degree of complexity as the industry leaders use to. In the latter case, the tasks committed to the staff processing the personal data in question may overlap, whereby some members of the staff can access different systems storing traffic data for different purposes. Not all the systems processing traffic data for commercial purposes were designed and/or implemented by keeping in mind the need to ensure adequate security levels for traffic data. There appears to be no standard awareness of the risks related to traffic data retention.

As regards, in particular, the preliminary risk assessment phase, it was found that this was a task performed as a rule internally to the given company – which may foster biased views and entails the risk of underestimating vulnerabilities. The diagram below shows the percent rates of providers relying on external audits and/or third-party security certifications compared to the total number of providers taken into consideration.



Traffic data are by their nature to be regarded as very sensitive. They should therefore be treated in a way comparable to the special categories of data mentioned in article 8 of Directive 95/46/EC. Not only should the retention of the data be adapted to their sensitive nature, but also extra attention is required as to their access by and onward transfer to the LEAs. In order to ensure that this is the case, the conditions for access and onward transfer of retained data should be clearly specified in the law. The DR Directive is an instrument developed in the pre-Lisbon Treaty years, pursuant to a different separation of legal competences, and does not include specific rules on that point – even though the WP29 had called for the development of such rules. Additionally, it might be argued that self-regulation does not suffice in this context, primarily because of the uneven balance of power between the service providers on one side and the LEAs on the other side. Service providers are not in a position to 'enforce' their own security policies when dealing with LEAs.

Some measures can be suggested, in addition to other security measures currently in place, which can be adopted in full compliance with the technology neutrality principle, in order to ensure that the data may only be accessed by duly authorised staff pursuant to Article 7(c) of the DR directive, whilst they are currently not adopted by all the providers in question:

- ***strong access control to the retained data, via the definition of user responsibilities and profiles with different user privileges;***
- ***strong authentication for system access, based on dual authentication mechanisms (i.e. password + biometrics, or password + token), to ensure physical presence of the person in charge of processing traffic data;***
- ***detailed tracking of accesses and processing operations by way of log retention, via logs recording at least user identity, access time, file acceded;***
- ***deployment of log management solutions to ensure log integrity by means of encryption technology or measures that provide equivalent protection;***
- ***logical separation from other systems processing traffic data for commercial purposes;***
- ***such additional measures as may be necessary to ensure confidentiality of data .***

Additionally, from an organisational/management standpoint, special importance should be attached to system administrators dealing with systems where traffic data are stored for LEA-related purposes; ***the roles and functions pertaining to such administrators should be detailed, also by means of ad-hoc policy documents, and all the maintenance activities performed on such systems should be the subject of in-depth controls***.

To enhance the security measures applying to traffic data, multiple and co-ordinated actions are necessary; ***their implementation by providers may be facilitated if both in-house policies and strictu sensu technological measures are incorporated in a security certification programme to be run at regular intervals – preferably by an external third party – in accordance with internationally agreed standards to assess robustness of the measures deployed vis-à-vis the changing pattern of risks and vulnerabilities. Other measures might also prove viable for this purpose, such as enabling DPAs to carry out audits or making audits available to DPAs.***

The non-homogeneous compliance with technical and organisational security obligations translates into the failure to fully meet the harmonisation objective pursued by the directive and impacts on the costs incurred by the individual players due to their different size and market position as well as altering market dynamics, which ultimately results into a non-harmonized application of the DR Directive, and prevents EU citizens from being afforded the same level of protection.

The Case of Article 7(d) of the DR directive (Accessed Data) - Article 7(d) of the DR directive envisages an exception applying to retention of the data accessed by LEAs, which may be stored *de facto* for an indefinite additional period.

One might consider whether electronic communications and Internet service providers should be called upon to develop additional security measures targeted to this category of "accessed data", as no specific requirements are laid down in the directive, or whether these data are subsequently to be included into the relevant case files and the applicable security measures committed to the competent authorities (which appears to be the case). The data in question are fraught with considerable criticalities both because they can disclose important information on users (which may also include sensitive information).

Massive accesses to traffic data and the extended retention of such data might be regarded as mechanisms to dodge the obligations laid down in the directive. ***The need for envisaging extended retention periods for accessed data should be assessed according to well defined criteria which, at all events, should provide for the deletion of accessed data in the light of the requirements made in both directive 95/46/EC and international instruments (including Council of Europe's Recommendation R(87)15).***

iv. Handover Procedures

The handover procedures applying to the traffic data requested by LEAs were found to be considerably inhomogeneous. A wide gamut of solutions were reported and described both via the questionnaire and on the occasion of in situ inspections – including handover procedures based on hand-written documents, courier or standard mail – along with different levels of transmission security ranging from the delivery of email and/or fax messages to the use of dedicated, encryption-protected transmission channels. ***Special importance should be attached to achieving harmonization in this area by developing standardised data handover procedures for LEAs.***

In this connection, it should be pointed out that the DR directive contains an exhaustive list of the data that may be transmitted to LEAs by providers, which data make up a finite set of elements; additionally, the serious crimes underlying the handover requests should be clearly set forth by domestic laws, whilst the entities (judicial authorities) empowered to authorise access to such data or the specific possibilities of access provided for by the law should be specified clearly and exhaustively.

A data exchange protocol based on the above assumptions could be developed into a standard IT procedure, whereas this is currently left to the discretion of the individual stakeholders – at least pursuant to the available information. Defining a standard handover procedure, which takes into account also the directionality of the transfer (which should be based on PUSH protocols) would enable faster, more reliable data transfers with

lower costs incurred by all the relevant stakeholders (providers and LEAs); indeed, the latter could benefit from standard solutions that would be designed on the basis of a unified reference framework and implemented on a large scale. This would be a far cry from the solutions currently available on the market, which are both different in nature and more expensive.

- It should be emphasized that clearly specifying both the stakeholders and the data sets these stakeholders may exchange would significantly enhance the overall security level of the handover procedure. This can be accounted for on several grounds: mutual authentication would be enabled; the preconditions would be met for implementing encrypted connections and trusted and secure communication channels based on key and digital signature certificate exchanges, which would ensure integrity, confidentiality and non-repudiation of data transfers; the risks of man-in-the-middle-type attacks – to intercept the communication channel and appropriate and/or duplicate the transferred contents – would be reduced significantly; all the tools required to enable effective data access accounting could be introduced; the individual stakeholders could categorize the requests by purpose and/or category of requested data, which can be reasonably expected to facilitate drawing up homogeneous statistical reports in Member States. All these options, where implemented, would allow reducing the number of inappropriate data accesses and enable DPAs to effectively audit data accesses. Judicial authorities should be involved in the handover process as well – namely, in their capacity as trusted entities that could decide on a case-by-case basis which data under which circumstances may be provided to LEAs. The purposes should be selected out of a known list of serious crimes, so as to faithfully mirror the communication procedure envisaged in the directive regarding traffic data.

For the above reasons, a pan-European handover standard could include the following items:

- a single contact point at each service provider;
- a single data handover format including, at least, the following fields allowing a secure, reliable traffic data interchange/access among the stakeholders:
    - User data, containing a known, finite number of fields related to service subscription and the terminals made available to users;
    - Traffic data, containing a known, finite number of fields related to national transposition of the data list set forth in Article 5 of the DR directive;
    - Provider code, containing a unique EU-wide ID to identify the electronic communications service provider and/or the Internet service provider;
    - LEA code, containing an ID to identify the authority empowered to access traffic data;
    - Judiciary code, containing a unique EU-wide ID to identify the judicial authority empowered to authorise access to traffic data;
    - Timestamp & request number, to identify timing and sequence of the data access requests and the respective authorisations;
    - Request type, to specify the data request category (e.g. by serious crime, or by amount of requested traffic data).

Introducing a data exchange protocol with the above features would allow minimizing some criticalities a few DPAs pointed out in the course of this enforcement action – such as the pressure exerted by LEAs on providers to acquire additional user-related data that are not listed in the DR directive, the submission of access requests in the absence of formal warrants, or the lodging of access requests by unauthorised (i.e. non-LEA) entities.

It is appropriate to recall in this connection that ***the list of serious crimes justifying retention under the directive should be laid down at domestic level based on national law, taking into account the considerations made in documents WP113 and WP119 as for the need to clearly define and delineate what is meant by "serious crime. An exhaustive list of the entities enabled to access the data retained pursuant to the DR directive should be disclosed to all the relevant stakeholders.***

It is worth mentioning in this regard that the European Telecommunications Standards Institute (ETSI) has been working effectively on a reference template for the handover of traffic data to LEAs, and this model can be further studied and evaluated..

D. Statistics under Article 10 of the DR Directive

Under Article 10 of the DR directive, Member States shall ensure that the Commission is provided on a yearly basis with statistics on the use of the traffic data retained as per the relevant provisions; Article 14 provides that any amendments to the directive should take account of those statistics (made available by Member States). Apart from very few exceptions, compliance with this notification obligation could not be confirmed.

Only few Member States did provide the requested information, which concerned the number of requests submitted to providers; the cases where the requested information was provided and those where the provider was unable to make available the requested data; the time elapsed between the date on which the data were stored and the date on which the competent authorities requested transmission of the said data.

Even though the statistics under Article 10 cannot be the only basis used to determine the future of the DRD, the availability and adequate assessment of the information in question is fundamental to gauge whether the objectives underlying the directive have been achieved including the need for introducing harmonised principles applying to all EU Member States – partly in the light of the criticalities that have been pointed out throughout the debate that led to its adoption as well as thereafter (see the decisions by some European Constitutional and Supreme Courts).

The lack of sound statistics might hinder the whole assessment exercise, as it is an important precondition to possibly amend the directive – in particular as far as the list of data in Article 5 and the retention periods set forth in Article 6 thereof are concerned.

The use of partial and/or inhomogeneous statistics may result into decisions that impact markedly on data subjects' privacy without making any difference as to the better harmonization that is pursued by the directive.

Again, it is appropriate to consider that several hindrances could be removed if a standardised handover procedure were developed. Given the availability of specific data handover rules, each player could produce statistics that would be consistent with those released by the remaining players – which would enable an improved reliable overview of the use and effectiveness of traffic data to prosecute "serious crimes".

With a view to the first assessment of implementation of directive 2006/24/EC the Commission is required to carry out by 15 September 2010, it is fundamental for each and every Member State that has implemented the directive to provide the necessary statistics. The Article 29 Working Party deems it absolutely necessary that this information be provided in order to objectively help establishing the need for and effectiveness of the Data Retention Directive.

Furthermore it will be also fundamental for those statistics to be accompanied by information on the impact produced by the data in question, broken down by age of the data, on the tackling of serious crimes.

E. Outsourcing Issues

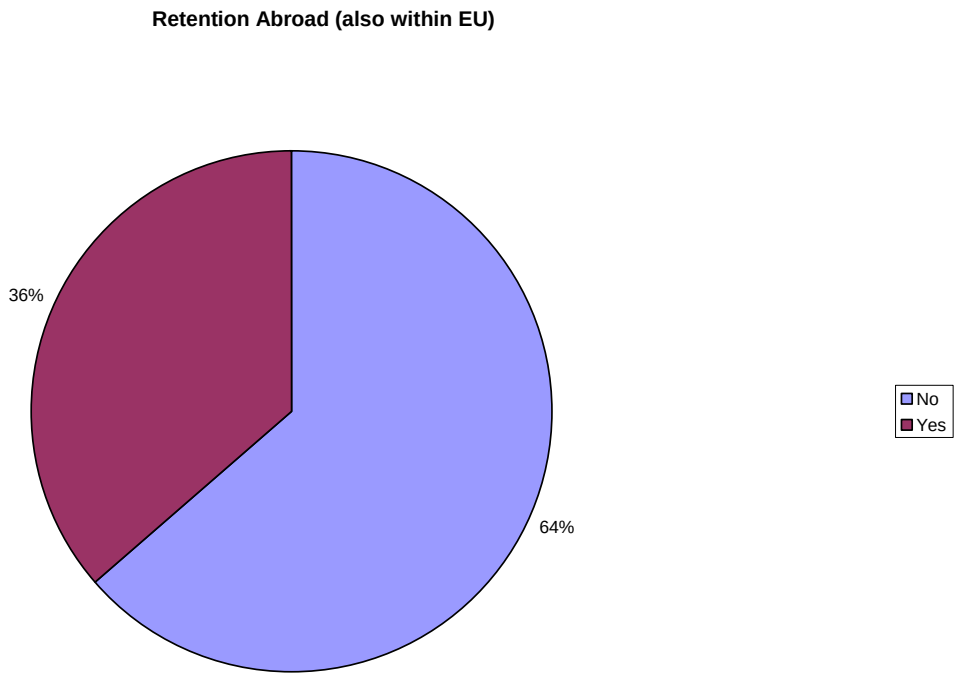
This enforcement action has found that outsourcing is increasingly relied upon to carry out several activities related to the retention of traffic data – especially as regards smaller operators pursuing a cost-containment policy. Not always does this practice go hand in hand with the accurate definition of the respective roles, in particular as for compliance with national data protection legislation and the appointment of data processors and/or the allocation of processing tasks to the staff in charge.

It should be recalled that the market of electronic communications networks and services is made up of multifarious entities that can count on markedly different human and financial resources; this is clearly an obstacle to achieve the harmonisation objective pursued by the DR directive. For instance, it was found that the business size of the entity retaining the data was in some cases markedly larger than that of the electronic communications service provider – which obviously makes it difficult for the latter, i.e. the data controller, to accurately monitor the processing operations performed by the outsourcee. Additional criticalities arise if the traffic data are retained outside domestic borders, which is not that unusual (see the diagram below) even though it is mostly limited to some large-sized players working in smaller Member States and availing themselves of the services afforded by their respective headquarters. This is an option also relied upon by smaller providers and/or virtual operators that resort to the services of multinational companies specializing in IT solutions. In these circumstances the supervisory authorities are called upon to an increased level of mutual assistance and cooperation in order to allow access to data and exercise of necessary enforcement powers.

In order to meet the requirements set forth in the Directive with limited impact on costs, reference could be made to federated solutions that have already been implemented mainly at domestic level by small ISPs – whereby one of the federated ISPs, or a delegated third party, designs and implements the traffic data retention system, manages the authentication phases, and partitions the memory allocated to each ISP. This approach should be viewed favourably although it requires a sufficiently harmonised, formalised and detailed set of rules.

At all times the transfer of retained data to other countries should meet the conditions set out in Directive 95/46/EC. Especially transfer of traffic data generated within EU territory that is to be used outside EU territory has to be subject to an adequacy assessment pursuant to the Directive.

Furthermore, the provisions of the Directive 95/46/EC relating to transfers of personal data to third countries cannot be applied separately from other provisions of the Directive, including those regarding the relations between controllers and processors.[7]



The outsourcing issue should be the subject of more in-depth analysis by DPAs to more effectively assess compliance with domestic obligations (e.g. as for the appointment of data processors) including contractual clauses – which should envisage specific, appropriate security measures.

[7] For a more in-depth analysis of the legal side of the outsourcing issues, the Article 29 WP refers to paragraph 4.6 Transborder Data Flows of Opinion 10/2006 on the processing of personal data by SWIFT. Reference can also be made to the WP29's Opinion no. 1/2010 (WP169) on the concepts of "controller" and "processor".

IV. Further Actions and Recommendations

In the light of the findings of this joint enquiry, the following specific recommendations can be put forward by having regard to the individual issues considered. Whilst most of them are addressed to providers, which have the technical means for implementing them, they nevertheless call into play the role of public authorities including the European Commission, Member States and national DPAs – not least on account of cost issues, which may entail reduced attention to the deployment of the necessary privacy protection and security tools, on the one hand, and may also give rise to market distortions on the other hand. **Furthermore, the Working Party would like to recall that self-regulation alone does not suffice in this context, primarily because of the uneven balance of power between the service providers on one side and the LEA's on the other as well as because issues related to costs and competition may not lead to a self-regulatory approach ensuring high security standards.**

- Categories of retained data

Since directive 2006/24/EC derogates from the provisions of directive 2002/58/EC, the list of traffic data that have to be retained on a mandatory basis is to be regarded as exhaustive. Accordingly, no additional data retention obligations may be imposed by national laws on providers pursuant to the DR directive. On the other hand, the Article 29 WP would like to emphasize that on the basis of the DR Directive LEAs are not allowed to ask service providers to gather data that fall outside the scope of the categories mentioned in the directive.

- Retention periods

a. The lack of harmonisation pointed out by this inquiry in terms of retention periods markedly impacts on the principle whereby EU citizens "can enjoy throughout the European Union the same level of protection", partly because it may affect considerably the individual stakeholders in economic terms as also related to costs and competitiveness. In this connection, the WP29 considers that it would be beneficial to consider reducing the maximum retention period and to set a single, shorter term to be complied with by all providers throughout the EU as stated in Opinion WP113 by the Article 29 Working Party.

b. Due to the existence of different retention purposes and periods (commercial vs. law enforcement), it would appear appropriate to suggest that the Commission re-consider the overall security of traffic data "per se" with a view to the overall assessment of the implementation of the DR directive. It should not be permitted that different security levels and retention periods apply depending on the different underlying purposes. The DR directive provides that law enforcement traffic data should be retained for limited periods and accessed for specific law enforcement purposes and on an explicit legal basis.

- Technical and Organisational Security Measures

a. Electronic communications and Internet service providers should assess the risks associated with traffic data on a regular basis and as objectively as possible, in order to detect all the relevant risk factors and their possible impact, and by paying special attention to access control and data availability. Regular external audits could contribute to an independent and objective risk assessment.

b. The following measures can be suggested, in addition to other security measures currently in place, which can be adopted in full compliance with the technology neutrality principle, in order to ensure that the data may only be accessed by duly authorised staff pursuant to Article 7(c) of the DR directive, whilst they are currently not adopted by all the providers in question:

- strong access control to the retained data, via the definition of user responsibilities and profiles with different user privileges;
- strong authentication for system access, based on dual authentication mechanisms (password + biometrics, or password + token), to ensure physical presence of the person in charge of processing traffic data;
- detailed tracking of accesses and processing operations by way of log retention, via logs recording at least user identity, access time, file acceded;
- deployment of log management solutions to ensure log integrity by means of encryption technology;
- logical separation from other systems processing traffic data for commercial purposes;
- such additional measures as may be necessary to ensure confidentiality of data.

c. The roles and functions pertaining to system administrators should be detailed, also by means of ad-hoc policy documents, and all the maintenance activities performed on such systems should be the subject of in-depth controls.

d. To further enhance the security measures applying to traffic data, multiple and co-ordinated actions are necessary; their implementation by providers may be facilitated if both in-house policies and *strictu sensu* technological measures are incorporated in a security certification programme to be run at regular intervals – preferably by an external third party – in accordance with internationally agreed standards to assess robustness of the measures deployed vis-à-vis the changing pattern of risks and vulnerabilities. Other measures might also prove viable for this purpose, such as enabling DPAs to carry out audits or making third party audits available to DPAs.

e. The need for envisaging extended retention periods for accessed data should be assessed according to well defined criteria which, at all events, should provide for the deletion of accessed data in the light of the requirements made in both directive 95/46/EC and international instruments (including Council of Europe's Recommendation R(87)15).).

- Handover procedures

a. Standardised data handover procedures for LEAs should be developed at European level to enhance harmonization. A data exchange protocol could be developed into a standard IT procedure, taking into account also the directionality of the transfer (which should be based on PUSH protocols). This would enable faster, more reliable data transfers with lower costs incurred by all the relevant stakeholders (providers and LEAs). Such

handover standard should keep track of at least the following parameters or events: user data, type of traffic data, service provider code, LEA code, judiciary code, timestamp, number and type of request.

b. The list of serious crimes should be laid down at domestic level based on national law, taking into account the considerations made in documents WP113 and WP119. An exhaustive list of the entities enabled to access the data retained pursuant to the DR directive should be disclosed to all the relevant stakeholders.

- Statistics

Member States should provide the necessary statistics to the Commission as expeditiously as possible; at all events suitably in advance of the deadline for the assessment report the Commission is required to draft on the DR directive. Such statistics should possibly come along with information on the impact produced by retained traffic data on the tackling of serious crimes, broken down by age of the data.

- Outsourcing

a. The outsourcing issue should be the subject of more in-depth analysis by DPAs to more effectively assess compliance with domestic obligations (e.g. as for the appointment of data processors) including contractual clauses – which should envisage specific, appropriate security measures

b. Reference could be made to federated solutions that have already been implemented at domestic level by small ISPs.

ANNEX I

Data Retention_DraftFinall

		Implementation directive 2006/24/CE	National law reference	Onsite Inspections/Questionnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
1	Belgium	No		Questionnaire	Yes	Yes	Yes
2	Bulgaria	Yes	Law on Electronic Communications (LEC)- Art. 250a-f,251 and 251a	Yes. Inspections of the mobile operators were conducted and the questionnaire on the first joint investigation action was sent to them.	Yes	Yes	Yes
3	Cyprus	Yes		Both	Yes	Yes	Yes

		Implementation directive 2006/24/CE	National law reference	Onsite Inspections/Questionnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
4	Czech Republic	Yes	Act No. 127/2005 Coll, as amended	both	Yes	Yes	Yes
5	Denmark	Yes	Danish Ministerial Order 988/2006	Questionnaire	Yes	Yes	Yes
6	Estonia	Yes	Estonian Electronic Communications Act	Questionnaire	Yes	Yes	Yes

		Implementation directive 2006/24/CE	National law reference	Onsite Inspections/Questionnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
7	Finland	Yes	Protection of Privacy in Electronic Communication 343/2008	Questionnaire	?	?	?
8	France	Yes	decree n° 358/2006	Onsite Inspections	Yes	Yes	Yes
9	Germany	Yes	Sections 113a and 113b of the Federal Telecommu-nications Act (TKG)	both	Yes	Yes	Yes

		Implementation directive 2006/24/CE	National law reference	Onsite Inspections/Questionnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
10	Greece	No		both	Yes	Yes	Yes
11	Hungary	Yes	ACT C /2003	Both	Yes	Yes	Yes
12	Ireland	No		Both	Yes (no SMS)	Yes	Yes

		Implementation directive 2006/24/CE	National law reference	Onsite Inspections/Questionnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
13	Italy	Yes	Decree no. 109/2008	both	Yes	Yes	Yes
14	Latvia	Yes	Electronic Communications Law	both	Yes	Yes	Yes

Num	Countries	Implementation directive 2006/24/CE	National law reference	Onsite Inspections/Questionnaire	Type of services (Y/N)		
					Mobile	Fixed	Internet
15	Liechtenstein	No		Questionnaire	Yes	Yes	Yes
16	Lithuania	Yes	Law on electronic communications n° IX 2135	Both	Yes	Yes	Yes.Pursuant to Article 15(3) of the Directive 2006/24/EC Lithuania has declared that it will postpone the application thereof to the retention of communications data relating to internet access, internet telephony
17	Luxembourg	No		Both	Yes	Yes	Yes

		Implementation directive 2006/24/CE	National law reference	Onsite Inspections/Questionnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
18	Malta	Yes	LN 198/2008 and LN 199/2008	Questionnaire	Yes	Yes	Yes
19	Netherlands	Telecommunicatio Data Retention Act July 7th 2009	31.145	both	Yes	Yes	Yes
20	Poland	No		both	Yes	Yes	Yes

		Implementation directive 2006/24/CE	National law reference	Onsite Inspections/Questionnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
21	Romania	Yes	Act no. 298/2008 (Constitutional Court has declared unconstitutional)	Both	Yes	Yes	?
22	Slovak republic	Yes	No. 610/2003 Coll. on electronic communications	Questionnaire	Yes	Yes	Yes
23	Slovenia	Yes	Electronic Communications Act ZEKom-UPB1(Off. Gaz. of RS, no. 86/04, 129/06 and 110/09)	both	Yes	Yes	Yes

		Implementation directive 2006/24/CE	National law reference	Onsite Inspections/Questionnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
24	Spain	Yes	Act 25/2007	both	Yes	Yes	Yes
25	UK	Yes	Data Retention Regulations 2009	Questionnaire	Yes	Yes	Yes

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
1	Belgium	Load ID, Record Type, served IMSEI, served IMEI, cell identity ci served MSISDN, served Ip-address, client Ip-address	start date, start time, call duration	login, logout, duration, in/out, IP no content data collected
2	Bulgaria	number of the caller, ID data of subscriber or user; dialed number, number to which the call was transmited; date and hour of the beginning and the ending of the call; type of the used public telephone service; IMSI, of the caller and the calling, IMEI, date and hour of service activating and location	IP addresses, telephone number of user and ID data, caller and called telephone number	User ID, number of any message entering the public telephone network, number of the receiver of Internet telephone call, date and hour of entering or exiting the Internet (logs), dynamic and static IP address for Internet access, ID of user and subscriber, date and hour of entering or exiting e-mail, caller telephone number, DSL and other connection end point.
3	Cyprus	CDR (part A-part B) callID, duration, time , cellID, subscriber identity, IMSI, IMEI	CDR (part A-part B) callID, duration, time	IP address e-mail headres

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
4	Czech Republic	telephone number of the calling party and the called party, date and time of commencement of traffic, duration of traffic, the IMEI number, the StartBTS station number and, as appropriate, the StopBTS station number, destination	telephone number of the calling party and the called party or the identifier of the telephone card for use in a public pay phone, date and time of commencement of traffic, duration of traffic	IP address, PORT NUMBER user account, identifier of the message on the mail server, date and time of commencement of traffic, sender's electronic mail addresses, recipients' electronic mail addresses, identifier of the electronic mail protocol, quantity of transferred data
5	Denmark	no details	no details	no details
6	Estonia	• the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended IMSI, IMEI, cell-ID	• the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended	the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, allocated by the Internet access service provider to a communication, and the user ID of client

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
7	Finland	no details	no details	no details
8	France	day, hour, incoming and outgoing phone numbers, IMSI, type call		IP addresses (no content, no email)
9	Germany	• A, B and (if applicable) C number • date and time when the call started and ended • IMSI, IMEI, cell-ID • all above mentioned applies to regular calls as well as SMS or MMS • if different services are available as part of the telephone service, data on the service used	• A, B and (if applicable) C number • date and time when the call started and ended • if different services are available as part of the telephone service, data on the service used	email: • identifier of electronic mailbox and IP of the sender and recipient • identifier and Internet Protocol address used to access electronic mailboxes • date and time of the log-in and log-off intenet access: • IP assigned to the subscriber • unequivocal identifier of the end point of the originator used to access • date and time of the log-in and log-off

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
10	Greece	calling and called number, date, time and duration of the call, IMSI and IMEI codes of calling and called number as well as the antenna (cell)	CDR, identification of the caller and the recipient of the telephone call, the duration of the call, the cause of call termination and some data about the internal routing of the call	a timestamp, the username, the assigned IP address SMTP, POP3 and IMAP protocol logs the header of the email message
11	Hungary	dialing and the called numbers, discrete technological identifiers, user identifiers, the type of the electronic telecommunicational service, date, the time, when it started and ended, incidentally the transmitter calls, IMEI, IMSI, the network and cell-identifier, and the data necessary for geographical identification	calling and the called number, discrete technological identifiers, user identifiers, the type of the electronic telecommunicational service, date, the time, when it started and ended, incidentally the transmitter calls	sender and destination, address of origin and type, discrete technological identifiers, user identifier, the type of the electronic telecommunicational service, date, the time, when it started and ended (for emails too), IP adress, user identifier
12	Ireland	no details	no details	no details

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
13	Italy	CDR (part A-part B) callID, duration, time , cellID, subscriber identity, IMSI, IMEI	CDR (part A-part B) callID, duration, time	a timestamp, the username, the assigned IP address the header of the email message (1 case)
14	Latvia	• the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended IMSI, IMEI, cell-ID	• the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended call transfer	One operator retained content (1 month)

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
15	Liechtenstein	no details	no details	the records of the RADIUS server no data as to contents
16	Lithuania	- the number making the call (A number); - the number receiving the call (B number); - subscriber identity; - date and time when the call started; - duration of the call and /or date and time when the call ended VOIP, SMS, EMS (2 inspected companies providing mobile telephony services)	- the number making the call (A number); - the number receiving the call (B-number); subscriber identity; - date and time when the call started; - duration of the call and/or date and time when the call ended	IP address, e-mail logs (source, destination, date and time)
17	Luxembourg	CDR	CDR	CDR

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
18	Malta	timestamp, location	timestamp	IP address Radius log e-mail logs (source, destination, date and time)
19	Netherlands	The categories of data that are to be retained under the Telecommunications Data Retention Act are the same categories of data that are listed in article 5 of the Data Retention Directive 2006/24/EC.	The categories of data that are to be retained under the Telecommunications Data Retention Act are the same categories of data that are listed in article 5 of the Data Retention Directive 2006/24/EC.	The categories of data that are to be retained under the Telecommunications Data Retention Act are the same categories of data that are listed in article 5 of the Data Retention Directive 2006/24/EC.
20	Poland	MSISDN (mobile telephone number), IMEI number (telephone serial number), IMSI (number connected with telephone serial card number), roaming number, data and time when a call starts and ends, LAC/CELL ID (location area code/cell identifier), user's contact details (name, surname, place of residence)	source of call (caller telephone number), data necessary to establish a recipient (recipient telephone number), data essential do establish date, time and duration of call, as well as data necessary to identify type of call (type of telephone service being used e.g. 'alarm clock', forwarding).	session start/end (date, time), IP number, login and parameters of access and service router which enable to identify TP subscribers CONTENT ON REQUEST BY PUBLIC AUTHORITY

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
21	Romania	• the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended IMSI, IMEI, cell-ID	• the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended IMSI, IMEI, cell-ID	no details
22	Slovak republic	(for details see Annex4 of the Act No 610/2003 Coll.); CDR (part A-part B) callID, duration, time , cellID, subscriber identity, IMSI, IMEI	(for details see Annex4 of the Act No 610/2003 Coll.); CDR (part A-part B) callID, duration, time	(for details see Annex4 of the Act No 610/2003 Coll.);IP addresses (type of service data), IPDR, Internet telephony CDR
23	Slovenia	• the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended IMSI, IMEI, cell-ID	• the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended call transfer	e-mail: date and time of communication, message ID, sender e-mail, recipients' e-mail, status (e.g. sent) internet access: calling telephone number (dial-up), IP address, the digital subscriber line (DSL) or MAc address (end point), date and time of the log-in and log-off of the Internet access service, user ID, type of communication

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
24	Spain	MSISDN, IMEI, IMSI the origin cell from which the call was initiated and the destination cell of the call -and those indicated in the Directive	CDR (part A-part B) callID, duration, time	IP address, email sender-destination timestamp
25	UK	Calling Telephone (Source of communication) Name & address of the subscriber or registered user of any such telephone Telephone No dialled including where appropriate the telephone number to which the call is forwarded or transferred (Destination of communication) Name & address of the subscriber or registered user of any such telephone. Date, time, start and end of call. The telephone service used International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity of the telephone from which the call was made	Calling Telephone No (Source of communication) Name & address of the subscriber or registered user of any such telephone Telephone No dialled including where appropriate the telephone number to which the call is forwarded or transferred (Destination of communication) Date, time, start and end of call. The telephone service used (type of communication)	iThe user ID allocated The user ID and telephone number allocated to the communication entering the public telephone network. The name and address of the subscriber or registered user to whom an IP address, user ID or telephone number was allocated at the time of the communication. In the case of Internet telephony, the user ID or telephone number of the intended recipient of the call. In the case of internet e-mail or internet telephony, the name and address of the subscriber or registered

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
1	Belgium	it varies (12-->24 months)			fax/mail/specific section
2	Bulgaria	12	12	12	The access to the data is performed after court decision and is exercised by the submission of motivated written request for inquiry by the competent authorities. The data can be provided to competent authority from other country if foreseen in international agreement, entered in force in the Republic of Bulgaria.
3	Cyprus	6	6	6	provided in person

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
4	Czech Republic	6-->12	6-->12	6-->12	Mostly specific encrypted channels; in one company data were handed over to the appointed police agent
5	Denmark	12	12	12	data based on requests at the operator's address
6	Estonia	12	12	12	paper inside closed envelope, direct access, protocol HTTPS

Num	Countries	Retention period (months)			Communication channel towards LEAs
		Mobile	Fixed	Internet	
7	Finland	no details	no details	no details	PGP
8	France	12	12	12	fax/ encrypted mail
9	Germany	6	6	6	• FAX • PGP email • CD-ROM or DVD-ROM via snail mail

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
10	Greece	retention periods vary drastically (2 years-- >5 yeras)			sealed envelopes, registered mail, fax (in one case also encrypted mail)
11	Hungary	retention periods vary depending on internal orders in the investigated companies			Open and Classified requests are divided depending on national security screening. Online data requests of NSS and National Security Authority (NSA) are provided by a service provider - Lawful Data Providing System.
12	Ireland	36	36	6	encrypted e-mail

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
13	Italy	24	24	12	certified email/FAX
14	Latvia	In most cases 18 Up to 36	In most cases 18 Up to 36	In most cases 18 Up to 36	in writing (by post) and electronically

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
15	Liechtenstein	6	6	6	the data are handed over either personally or in encripted form
16	Lithuania	6+6	6+6	6+6	Encrypted e-mail, hard copy, web interface secured by https protocol (the transmission channel is encrypted by SSL channel)
17	Luxembourg	6	6	6	In general, operators follow the instructions received from Law Enforcement Authorities without further analysis. Authorised staff provides the required information on paper, CD or USB stick directly to the requesting agent.

Num	Countries	Retention period (months)			Communication channel towards LEAs
		Mobile	Fixed	Internet	
18	Malta	12	12	6	e-mail, CD, hard copy format, soft copy through a single contact point
19	Netherlands	12	12	12 -> 6	There are existing protocols and procedures for handling information requests from the authorities. PGP is used when transmitting traffic data, and the encrypted traffic data is always sent to (previously known) named individuals.
20	Poland	it varies from provider to provider for each service (longest 10 years)			electr. mail and encryption/authent. with public key

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
21	Romania	6->36	6->37	6->38	in electronic format, encrypted by courier by mail
22	Slovak republic	6 - Mobile services : Internet access , Iternet e-mail, Internet telephony ; 12 - other types of mobile services	6 - Fixed neetwork services : Internet access , Iternet e-mail, Internet telephony ; 12 - other types of fixed network services ;	6 - Internet access service , Iternet e-mail, Internet telephony	Personal receipt by the authorised LEA Officer, Encrypted e-mail
23	Slovenia	14	14	8	paper or portable electronic media, by courier, secure e-mail

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
24	Spain	6<12	6<12	6<12	certified email/encrypted mail/hand deliver
25	UK	12	12	10-->12	SSL preferred method, fax and email. Pre directive / existing methods of transferring traffic related data to specified authorities

Num	Countries	Logical security measures	Physical security measures
1	Belgium	no encryption of traffic data access to data is strictly restricted (id/pw) risk assessment (50%) Security certification (50%) Appointed CISO penetration test access log management No logging of system admin	access control through cards systems against intruders Video Surveillance Closed Circuits alarm response centres Security guards UPS (50%) fire detection systems, flood protection (50%)
2	Bulgaria	Obligation for implementation of necessary technical and organizational measures, forbiden listening, recording, storing and other ways of intersepting or tracking of messages of other individuals. No retention of content data. Deletion of data after the set period. Only the authorised persons have access to the data that are necessary for thier work There is access log management for traffic data No encryption	alarm system, physical control of an entrance video-surveillance, anti-incendiary measures premise with limited entrance, guard
3	Cyprus	risk assessment (50%) audit (50%) no security certification no CISO penetration test (no specific) access to data is strictly restricted (id/pw) access log management (50%) - no encryption (only in trasmission)	Access control through cards Systems against intruders Video surveillance Security guards

Num	Countries	Logical security measures	Physical security measures
4	Czech Republic	IT expert appointed security audit (50%) security certification (50%)	No details
5	Denmark	risk assessment (2/3) audit (2/3) security certification (1/3) CISO appointed vulnerability assessment (1/3) access to data is strictly restricted (id/pw) access log management (2/3)	access control through cards systems against intruders
6	Estonia	No specific procedures specific risk assesment (one case) internal audit no security certification CISO appointed (1 case) access to data is strictly restricted (id/pw) access log management (not all the companies) only partially encrypted	physically protected server rooms Limited access, fire alarm and break-in alarm

Num	Countries	Logical security measures	Physical security measures
7	Finland	Risk analysis IT security audits access to data is restricted (id/pw) no consolidated log handling for auditing purposes no encryption (only in transmission)	Yes Written procedures
8	France	No specific security for traffic data penetration test/vulnerability assessment access to data is strictly restricted (id/pw) access log management no encryption (only in transmission)	Alarms against intruders Access control through cards or special keys Closed Circuits TV Fire safety system for the servers and backups protection
9	Germany	• risk assessments • penetration tests • access to data is strictly restricted (id/pw) • access log management	data centers are highly secured: • alarm • complete video surveillance • automatic fire extinguishing systems • etc...

Num	Countries	Logical security measures	Physical security measures
10	Greece	access control, log files audit trail and use of secure communication channels general risk analysis Internal audits security certification (only one) CISO appointed independent penetration test/vulnerability assessment (30%) access to data is strictly restricted (id/pw) access log management (login-logout not actions) no encryption	no specific physical protection measures for traffic data. The physical protection measures are included in the general IT security policy.
11	Hungary	Regarding measures taken against unauthorized access it can be reported that all steps are logged, and IT systems are divided into basic, medium and high profile systems.	Servers are situated in a highly secured place, the entrance is secured by a proxy, hierarchic key, video surveillance and live security protection.
12	Ireland	Access to traffic data is restricted to limited number of users and logs of access are kept No specific studies in relation to security risks regarding traffic data Security certification CISO appointed Encryption in transmission	Data is stored on a number of dedicated system CCTV

Num	Countries	Logical security measures	Physical security measures
13	Italy	secure data transmission protocols; risk assessment; strong authentication; and the use of biometric tokens patch management procedures; use of anti-virus software; analysis of abnormal traffic via intrusion detection systems access log management no encryption (only in trasmission)	H24 monitoring; Access via badges; Centralised intrusion (detection) alarm; Video surveillance Fire detection systems; Restricted access areas
14	Latvia	the handling with traffic data is included in general IT security policy general IT audits External audits are selected only by large companies no operator has obtained a certification there aren't clear answers on regularity of tests carried out by providers only authorized persons have access to traffic data Almost 1/3 of providers are not recording the log files 10% encrypted storage (all in transmission)	access control to facilities (secured by key code, magnetic cards etc.), video surveillance / monitoring, alarm systems, security staff/guards

Num	Countries	Logical security measures	Physical security measures
15	Liechtenstein	internal audit company risk assessment no security certification CISO appointed access to data is strictly restricted (id/pw) access log management no encryption	secure data centre security personnel video surveillance intruder alarm system fire alarm system
16	Lithuania	Antivirus software, access to data is restricted, access log management,internal security, penetration tests(one company), audits (no audit in some cases), encryption (not in all cases), ISO 27001 certification (one company), CISO appointed, no IDS.	Entrance (Passing) control system (magnetic cards); premises surveyed by surveillance cameras; 24/7 hour security on duty; fire alarm sensors and automatic fire extinguisher system; continuous electric power supply
17	Luxembourg	No specific security for traffic data no risk assesment - security audit (only one) No operator is certified Encryption Access control and authentication Logs are not checked but only stored for investigation	Written policy (only two operators) IT security manager (only three) Access control through personnel cards Fire protection and intrusion detection systems. Storing of backups in a different place than the server itself (not all)

Num	Countries	Logical security measures	Physical security measures
18	Malta	No specific security for traffic data internal audit/risk assesment CISO appointed (only one) no security certification IDS access to data is strictly restricted (id/pw) access log management encryption (only pw)	Access control through swipe cards Video Surveillance Closed Circuits Security Personnel Systems against intruders written policy
19	Netherlands	Risk assessments are part of the general IT security internal and external information security audits one operator 27001 certified CISO appointed vulnerability assessments on a regular basis access log management not all use encryption	Various physical security measures, e.g. all operators that were investigated store their traffic data in heavily secured data centres
20	Poland	None of them developed a separate IT security policy for traffic data information security risk analysis ICT security audits, both internal and external secirity certification CISO appointed intrusion detection/intrusion prevention systems access to data is strictly restricted (id/pw) access log management (inalterable in one case) no encryption (only in trasmission)	alarm system, CCTV, access control system isolated security zones redundant power supply fire alarm detectors

Num	Countries	Logical security measures	Physical security measures
21	Romania	There are companies that have adopted specific procedures for traffic data periodic risk assessment Only one company security certified No security manager No independent penetration test or vulnerability assessment access to data is restricted (id/pw) data base/system administrators are authenticated on the basis of user name and password log of primary activities (login, logout, change of password) no encryption	badges, video surveillance, anti seismic supports, fire detection and extinction system equipment are installed in specially arranged rooms no written policy
22	Slovak republic	IT security procedures directly applicable to the traffic data security audits and security analyses are performed regularly One company security certified CISO appointed independent penetration tests regularly access to data is strictly restricted (id/pw/token) access log management (except one) DB encryption (except two. all in transmission)	The entry is permitted for authorized persons only The policies are business secret; they may not be published nor given to external subjects
23	Slovenia	major providers: Information Security Management System (ISMS) adapted from ISO 27001 and dedicated Data Retention Solution (WORM CAS-type storage)	major providers: Information Security Management System (ISMS) adapted from ISO 27001 and dedicated Data Retention Solution (WORM CAS-type storage)

Num	Countries	Logical security measures	Physical security measures
24	Spain	No specific security for traffic data internal audits no security certfication CISO appointed penetration tests IDS access to data is strictly restricted (id/pw) access log management no encryption (except one)	Access control through cards. Systems against intruders. Video Surveillance Closed Circuits. Alarm response centres. Security guards Written procedures
25	UK	No separate security procedures for traffic data risk assessments 50% of organisations certified ISO 27001 CISO appointed IDS access to data is strictly restricted (id/pw) access log management no encryption (only in trasmission)	Perimeter fencing. Secure hosting environments. Alarms. CCTV. Personnel access control systems 24 hour police protection

		Specific personnal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
Num	Countries				
1	Belgium	Yes	back-up (100%) disaster recovery (50%)	YES	NO
2	Bulgaria	no details. The authorized persons that have access to the data are those responisible for: managing of traffic data, users' enquires, misuse detections, market studies and provision of added value services,requiring additional processing of traffic and localization data	back-up (100%) recovery systemes (no details)	YES	In accordance with the international agreement
3	Cyprus	Yes	back-up (100%) disaster recovery (only one no details)	YES (2/3)	NO

Num	Countries	Specific personnal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
4	Czech Republic	Yes	contingency plan	YES	NO
5	Denmark	Yes	back-up (100%)	YES (2/3)	No
6	Estonia	not specific	back-up copies are taken centrally, existing policy for rotating back-up copies, automatically administrated lifecycle of back-up copies	yes, data are separated phisically and logically in different databases	only one case but situated in EEA

Num	Countries	Specific personnal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
7	Finland	Yes	Back up	No	No
8	France	not specific	back-up (100%) recovery systemes (no details)	YES	NO
9	Germany	Yes	back-up systems – some actually in encrypted form	YES	NO

Num	Countries	Specific personnal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
10	Greece	not specific	back-up (100%) recovery systemes (no details)	NO	ONE CASE WITHIN EU
11	Hungary	classified data requests are compiled by a person having passed the „C" type national security clearance. In case of open data requests, most of the companies organise compulsary tranings about the specific knowledge	only a few comanies have their own recovery plan but first they were not willing to show these documents. Many companies have security archiving separeted from the servers	most of the companies store the data related to invoices logically or physically separated from the data stored in connection with criminal investigations	No
12	Ireland	Yes	Back-up (1001%) No specific continuity / disaster recovery procedures in place for traffic data	No	No

Num	Countries	Specific personnal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
13	Italy	Yes	back-up (100%) recovery systemes	Yes	No
14	Latvia	not specific	The back-up system is implemented by 81 % of providers few small providers that do not have back-up systems in operation	62 % do not separate the data	Yes (in EU)

Num	Countries	Specific personnal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
15	Liechtenstein	Yes	back-up (100%) recovery systemes (50%)	Yes (50%)	Yes
16	Lithuania	not specific	back-up (100%) recovery systems (except 1 company)	Yes, data are stored separately	One company providing mobile telephony services stores traffic data not only in Lithuania, but also in others EEA countries (Latvia, Estonia, Sweden)
17	Luxembourg	Yes (not all)	Operators use back-up systems. Copies are deleted by overwriting in a general rotation of supports.There are no formal Business Continuity Process in place. Three operators however, store backup on a remote site.	Yes (only two)	All operators store all their data in Luxembourg, except for two that also store some data in Belgium

Num	Countries	Specific personnal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
18	Malta	Yes	Only one operator has back-up procedures	Yes (not all)	Yes (in EU)
19	Netherlands	Handling of traffic data for law enforcement purposes is done by specific group of personnel.	Different strategies, e.g. parallel processing at two different locations	3 telecom providers that were investigated store, or are planning to store, the traffic and location data that is retained under the TLC Data RetentionAct in separate databases.	Data that is retained under the Telecommunications Data Retention act is stored, or will be stored, in the Netherlands
20	Poland	Yes	back-up (100%) disaster recovery (only one no details)	NO	NO

Num	Countries	Specific personnal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
21	Romania	Yes	periodic backup, DR equipment located in another city in "hot back up". The backs up copies are in constant synchronisation	Yes	No
22	Slovak republic	Yes	back-up (100%) recovery systemes	Yes	Yes (in EU)
23	Slovenia	Yes	Yes	Yes	No

		Specific personnal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
Num	Countries				
24	Spain	Yes	back-up (100%) recovery systemes (except one)	Yes	No
25	UK	not specific	back-up (100%) recovery schemes (off-site back up)	Mixed situation with some physical separations already in place and one being implemented	NO