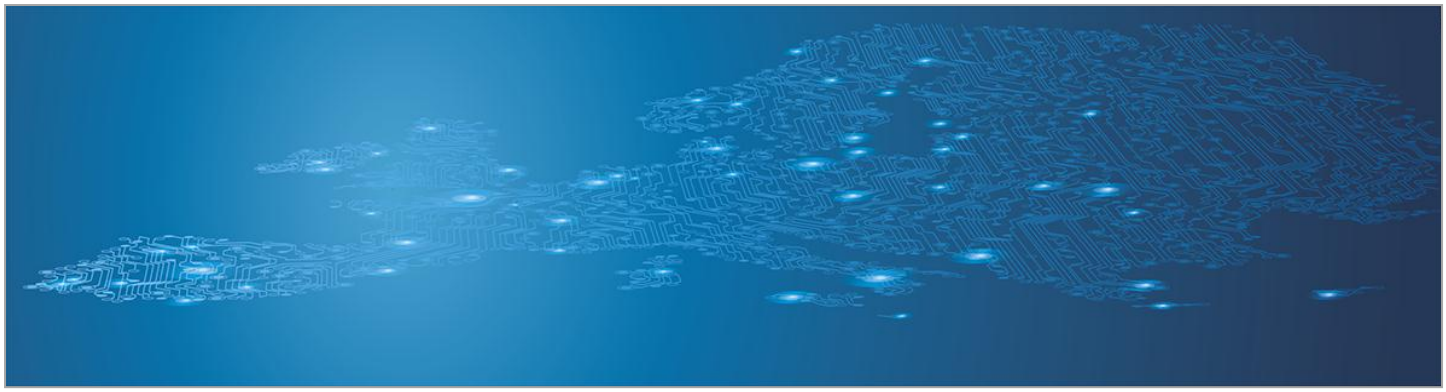

Securing personal data in the context of data retention

Analysis and recommendations

Version November 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

This work was partly commissioned by ENISA under contracts

- ENISA P/18/12/TCD Lot 1, to time.lex, which is the contributor to Section 3 and
- ENISA P/18/12/TCD Lot 2 to the consortium formed for this work by KU Leuven (BE) and University of Bristol (UK), which is the contributor for Section 4

Contributors: Eleni Kosta (time.lex), Vincent Rijmen (KU Leuven), Danny De Cock (KU Leuven), Jos Dumortier (time.lex), Hans Graux (time.lex), Nigel P. Smart (University of Bristol)

ENISA project manager: Rodica Tirtea

Contact

For contacting the authors please use sta@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to extend our gratitude to the respondents to the survey for their collaboration and to the reviewers for their comments, suggestions, feedback. We also thank a number of respondents who provided anonymous input.

Table of Contents

1 Executive summary

Data retention legislation has been adopted to address concerns related to national security and serious criminal activity. The legislation provides access to communication data for law enforcement purposes. However, according to the Data Retention Directive (DRD) [1] personal data collected, stored or in any way processed in most European Union (EU) Member States (MSs) needs to be securely protected, to meet the requirements of data protection legislation.

This document provides the results of (a) a survey on the national implementation of the DRD in six selected Member States on the requirements regarding technical and organisational security measures (in short 'security measures') and the implementation of the data security principles that are provided for in the Directive, and (b) a state-of-the-art analysis of the security measures proposed for the protection of personal data collected and stored in the context of the DRD.

This document aims at providing a set of recommendations for a common European approach on the security measures that should be taken in relation to retained data, taking into account existing specifications on security measures.

In order to realise this goal, this document offers an overview of the current policy context in Section 2; the current revision of the data protection legislation is briefly presented, as well as the most significant documents relevant for this activity covering specifications, comments, opinions or guidance in the frame of securing personal data in the context of DRD. Section 3 contains the survey results, covering Austria, Estonia, France, Spain, Sweden and the United Kingdom. This study aimed mainly at the identification of best practices on data security specifications and standards that are used for securing personal data in the framework of the Data Retention Directive in EU Member States. It will serve as the basis for the drafting of recommendations for a common European approach. In Section 4 existing specifications in the field are reviewed, in particular the European Telecommunications Standards Institute)(ETSI) technical report, ETSI TR 102 661 "Security framework in Lawful Interception and Retained Data environment V1.2.1 (2009-11)" [2]. TR 102 661 is the most relevant document providing security measures in this area. Finally, the findings and the recommendations are summarized in Section 5. Among the recommendations of Section 5 we mention here the proposal for re-phrasing of the text referring to security measures in DRD to better cover the security requirements and general recommendations focusing on security measures for the case that the Data Retention Directive is going to be revised.

Note. *It is outside the remits of this document to address all legal issues beyond what is useful for understanding the context of data retention. The purpose of this document is to propose coherent opinions and recommendations for implementing the appropriate security measures to protect personal data stored and transferred by the systems spawned by DRD. It is beyond the scope of this document to provide a broader perspective on the efficiency, necessity, proportionality and the impact of data retention in general.*

2 Introduction

The transposition of the Data Retention Directive, published in 2006, into national legislation, has been, and still is, a challenging task. In light of the review of the Data Retention Directive an evaluation of the Directive was scheduled by the European Commission (EC) for 2010, aiming towards assessing the application and the impact of its implementation for different stakeholders.

In addition to the evaluation report published by the EC [3], other stakeholders provided opinions and recommendations on this topic

- the Article 29 Data Protection Working Party (Art 29 WP) [4],
- the European Data Protection Supervisor (EDPS) [5], and
- the expert group on the DRD [6].

These contributions raise issues regarding the information security mechanisms in place.

In light of the above, the European Union Network and Information Security Agency (ENISA), based on a request received from Directorate General Home Affairs (DG HOME) of the EC

- Assessed the current implementation of data security measures for data retention in selected Member States and provides "best practice" recommendations in this respect;
- Provides state-of-the art recommendations for security measures in the context of data retention reform.

2.1 The Data Retention Directive in brief

The DRD was adopted in 2006 [1] and aimed at harmonising the obligations of providers with respect to the retention of traffic and location data for the purpose of investigation, detection and prosecution of serious crime. Although the Directive is seen as an exceptional measure regarding the retention of specific categories of data for law enforcement purposes, it shall still comply with the basic principles of European data protection and privacy legislation. The data to be retained are traffic and location data as well as data necessary to identify the subscriber or registered user, while no content data shall be retained.

The retained data shall be provided only to the competent national authorities in specific cases and in accordance with national law. The retention of data, as described in Article 7 of the Data Retention Directive, imposes specific security obligations to providers. The data do not need to be of evidential quality in order to be retained, but they shall be of the same quality and subject to the same security and protection as those data on the network. Furthermore the data shall be subject to appropriate technical and organisational measures to protect them against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure. Appropriate measures shall also be taken in order to ensure that they can be accessed by specially authorised personnel only. Finally all other data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

This last obligation requires in several cases certain effort from the provider. The retained data shall be deleted upon expiration of the retention period foreseen in the national legislation (i.e. after a period of between six months and two years). It goes without saying that companies should store data in such a way that will allow their transmission upon request to the competent authorities, without delay. In simple words the provider is responsible for the storage of the data, their authenticity, accuracy and security, for the prevention of loss of the data as well as for their timely and proper transmission to the competent authorities.

2.2 Considering the overall picture

The DRD was designed, as specified in Article 1, "[…] *in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law"*. Further, in the next alignment, it is specified that "*[t]his Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.*"

The DRD makes references to the Data Protection Directive 1995/46/EC[1]. However *the data protection framework is currently undergoing a reform*. In January 2012[2] the EC proposed a new Regulation to replace the existing Data Protection Directive and a new Directive aimed at replacing the Framework decision 2008/977/JHA[3] for personal data processed in the framework of police and judicial cooperation in criminal matters. Furthermore, new provisions have been recently published by the European Commission in the regulation (EU) No 611/2013[4] on the measures applicable to the notification of personal data breaches.

From a technical perspective, while specifications, standards and best practices are developed by different bodies, the challenges that need to be addressed every day are becoming more demanding. As such, a revision of such specifications is needed on a permanent basis. Furthermore, security and privacy measures are not always completely and correctly implemented for a number of reasons, such as the incurred costs or the lack of expertise within the responsible organisation. ENISA published at the end of 2011 a study on the cryptographic recommendations and specifications that EU Member States promote for e-Government services that have a direct impact on the privacy of European citizens[5]. The study noticed that the surveyed specifications in general recommend good practice cryptographic algorithms, however, in contrast, the survey of the IT industry experts identified that many of the cryptographic solutions that they audit and test are poorly deployed and insecure. As such, from this perspective there is further work needed to reach a minimum level of security deployed in non-classified eGovernment services.

While the current document focuses on the retained data for the purpose of DRD, it should be noted that telecom service providers may collect and store a broader range of traffic data (including personal data for the purposes of the conveyance of the communication and for the billing thereof), even if only temporary. As such, the retained dataset is only a subset of traffic data. Although the storage of traffic data that are not retained under the DRD goes beyond the scope of this study, considerations should be given to this stage as well. *The protection not only of the data stored for DRD purposes but also of the initial dataset is essential in order to meet the need for personal data protection.* Furthermore, we are not going to address the handling of retained data once they have been handed over to LEA (Law Enforcement Authorities). *The transfer process and the storage at*

[1] European Parliament & the Council of the European Union, Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995, [7].
[2] European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) [8].
[3] Council Framework Decision 2008/977/JHA of 27 November 2008, on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [9].
[4] Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, OJ L173/2 [10].
[5] ENISA, Study on the Use of Cryptographic Techniques in Europe [12].

LEA side should also be secured. Data security measures in all these stages must be proportional to the risk and potential damage.

2.3 Security measures for data retention in the policy documents, reports and opinions

In this section we identify key documents that refer to security measures related to data retention.

2.3.1 Security measures in the text of Data Retention Directive

For a better understanding of the context we include below the most relevant paragraphs[6] from the DRD relating to security measures.

Preamble

"(16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, ***and their obligations concerning measures to ensure confidentiality and security of processing of data****, which derive from Articles 16 and 17 of that Directive,* ***apply in full to data being retained within the meaning of this Directive****."*

Article 4. Access to data

"Member States shall ***adopt measures to ensure that data*** *retained in accordance with this Directive* ***are provided only to the competent national authorities in specific cases and in accordance with national law.*** *The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights."*

Article 7. Data protection and **data security**

"Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network ***respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive****:*

(a) the retained data shall be of the same quality and subject to the ***same security and protection as those data on the network****;*

(b) the data shall be subject to appropriate technical and organisational measures ***to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure****;*

(c) the data shall be subject to appropriate technical and organisational measures ***to ensure that they can be accessed by specially authorised personnel only****;*

and

(d) the data, except those that have been accessed and preserved, shall ***be destroyed at the end of the period of retention****."*

Article 9. Supervisory authority

"1. Each Member State shall designate ***one or more public authorities to be responsible for monitoring the application*** *within its territory of the provisions adopted by the Member States* ***pursuant to Article 7 regarding the security of the stored data****. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.*

2. The authorities referred to in paragraph 1 shall act with complete independence in ***carrying out the monitoring*** *referred to in that paragraph."*

Article 13. Remedies, liability and penalties

[6] Emphasis in all following paragraphs is added by ENISA.

*"1. Each Member State shall take **the necessary measures to ensure that the national measures** implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions **are fully implemented with respect to the processing of data** under this Directive.*

*2. Each Member State shall, **in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained** in accordance with this Directive **that is not permitted** under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive."*

2.3.2 Standardisation activities

ETSI has issued the technical report ETSI TR 102 661 version 1.2.1 in 2009[7]. This ETSI technical report proposes an integrated Security Policy. This Security Policy contains a number of security measures and controls, necessary for the secure (in terms of confidentiality, integrity, availability) provision of Lawful Interception (LI) and Data Retention (DR) services of Communication Service Providers. More analytically, it contains a set of security categories where most of the controls for each of these categories, are indispensable security controls while some others can be optionally chosen for creating a tighter security framework. Finally, the Technical Report provides four Annexes with specific solutions. Initially, a summary table of security controls is recommended that can be applied to specific functional blocks of a data retention environment. Moreover, a generic methodology and architectural solution are provided for implementing a secure logging procedure for a DR environment. An encryption solution is also provided for securely Storing and Querying the retained data. The report includes also a guide for selecting cryptographic algorithms and minimum key sizes in DR systems is also proposed.

ENISA considers this technical report as a good reference/benchmark for implementation of security measures in the context of DRD. In Section 4 we provide an analysis of this document with respect to state-of-the-art security recommendations. In Section 4, we will also compare the published opinions and the recommendations mentioned in the following sub-section with these technical recommendations published by ETSI in TR 102 661.

2.3.3 Public opinions on security measures

As already mentioned, opinions and recommendations on security measures and on DRD in general have been formulated in the evaluation report published by the EC [3], in the Article 29 Data Protection Working Party (Art 29 WP) opinion WP 172 [4], in the opinion of the European Data Protection Supervisor (EDPS) [5] and in the publications of the expert group on the DRD [6].

2.3.3.1 Report of the Article 29 Data Protection Working Party

In section "*iii. Technical and Organisational Security Measures*" of the Art 29 WP Report on the second joint enforcement action [4], reference and opinions are provided to the technical and organisational measures in place to minimise the risks of accidental and/or unauthorised destruction or alteration of retained data, and 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.

[7] Version 1.1.1 was published in 2008, [2].

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.****"* [4]

Besides this, the report has an Annex with the findings in a selection of MSs. The findings cover: the types of data retained, the retention periods and the technological solutions implemented for retention purposes, along with especially important issues from a data retention perspective (e.g., IT security, logical protection, authentication/authorisation, logs, encryption, disclosure/transmission protocols, physical protection, back-up/disaster recovery).

The findings of this opinion are:

"*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." [4]

The outsourcing issues are also mentioned in the Art.29 WP report "*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 is also mentioned that for Data Protection Authorities (DPAs) it was "*difficult […] to accurately monitor the processing operations performed by the outsourcee*". The conclusion for the topic of outsourcing is "*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.*" [4]

2.3.3.2 DATRET Expert Group report

The guidance document 7 on a "Closer understanding of the term 'Data Security' in relation to its application in Directive 2006/24/EC" that is produced by the Data Retention Expert Group [6] lists in page 10 security measures that are needed in the DRD context:

"***Examples of data security measures which may help address the exceptional risk potential of data retained pursuant to the Directive***

By way of indication only the following are examples of data security measures which could help address the heightened risk surrounding data retained pursuant to the DRD:

- *Documented security policies specifically covering the retained data, defining responsibilities, roles and organisational and technical measures;*
- *Retained data to be stored in a secure physical environment;*
- *Retained data to be stored separately from commercial data (or, at least, effective separation among the different sets of data, including strict access controls);*
- *Effective back up and recovery mechanisms to secure system content;*
- *Technical measures designed to prevent unauthorized access to or alteration of retained data during transfer or back up storage, including by use of cryptographic algorithms.*
- *High level intrusion controls from external attacks and to limit access to duly authorised persons;*
- *Automated logging of all access to, searches and other processing of retained data;*
- *Documented instructions to all authorized personnel on how to avoid security risks and breaches;*
- *Clear distinction of functions and competences concerning the categories of persons responsible for managing the system and those authorised to access and use the system with a view to liability for system failure;*
- *Regular independent audit of all data security measures.*"

2.3.3.3 European Data Protection Supervisor opinion

This section covers the opinion of the European Data Protection Supervisor (EDPS), on the Evaluation report on the Data Retention Directive [5].

In the opinion, the part referring to security measures can be found in paragraph 62:

"Does the Data Retention Directive meet privacy and data protection requirements?

[…] the level of security is not sufficiently harmonised. One of the main conclusions of the Article 29 Working Party in its report of July 2010 was that ***there is a patchwork of security measures in place*** *in the different Member States. The Commission seems to consider the security measures in the current Directive as sufficient, as "there are no concrete examples of serious breaches of privacy". It appears however that the Commission has only asked Member States' governments to report on this. In order to evaluate the suitability of present security rules and measures, a broader consultation and more concrete investigation into instances of abuse is needed. Even if no specific instances of security breaches are mentioned in the context of the report, data security breaches and scandals in the area of traffic data and electronic communications in some Member States also serve as illustrative warnings. This issue cannot be taken lightly, as the security of the retained data is of crucial importance to a system of data retention as such, as it ensures respect for all other safeguards*."[8]

2.4 Reactions on the Directive

This subsection presents a short overview of national court cases on the national implementations of the DRD, as well as of requests for preliminary rulings that are sent to the Court of Justice of the European Union (CJEU) by national courts, aiming at the drafting of a complete picture of the current regime with regard to data retention in Europe. This presentation of the national jurisprudence of the EU Member States is not aimed at criticising the DRD, as an overall evaluation of data retention in general and of the DRD in particular goes beyond the scope of this document.

[8] See [5], paragraph 62 (p. 12).

The DRD, as well as its transposition by the EU Member States, has been heavily criticised by human rights organisations and privacy activists and there is an increasing number of national court decision that have ruled on the compatibility of specific provisions of the national data retention laws with fundamental rights.

In the end of 2008 the Bulgarian Supreme Administrative Court found that the provisions of the law transposing the Directive in Bulgaria on access to the retained data contradicted Article 8 of the European Convention of Human Rights.[9] In 2009 the Romanian Supreme Court declared the law transposing the Data Retention Directive into Romanian law as unconstitutional because it breached the right to correspondence and to privacy[10]; the German Constitutional Court found in 2010 that the way the DRD was implemented in Germany infringed the privacy of telecommunications protected in Art. 10(1) of the German Constitution (GG)[11]; the Supreme Court of Cyprus found that the provisions on access to the data and on the transmission of data to law enforcement authorities were in violation to the right to secrecy of communications[12]; the Czech Constitutional Court found in 2011 the law transposing the Directive into the Czech Republic as interfering with fundamental rights as it was not precise and clear in its formulation[13]. It is interesting to point out that the Czech Constitutional Court focused its decision on the fact that the Czech law implementing the DRD had failed to define sufficiently, unambiguous and detailed rules containing minimum requirements concerning the **security of the retained data**, in particular, taking the form of restricting third-party access, the procedure of maintaining data integrity and credibility, or the procedure for the deletion of the retained data.[14]

Besides the national court decisions mentioned above, there are pending cases in Poland, Slovakia and Slovenia. In 2008 the Hungarian Civil Liberties Union (HCLU) filed an *actio popularis* in front of the Hungarian Constitutional Court requesting the examination of the constitutionality of the relevant provisions of Hungarian telecom data retention regulations.[15] However, Hungary adopted a new Constitution, which entered into force in January 2012 and abolished the *actio popularis*.[16] The HCLU pending case was then terminated.

[9] Bulgarian Supreme Administrative Court, No 13627, 11 December 2008, available only in Bulgarian at http://www.capital.bg/getatt.php?filename=o_598746.pdf (last accessed 16.07.2013)..

[10] Decision of the Romanian Constitutional Court 1258, 08 October 2009. The original decision in Romanian is available at http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf (accessed 10 July 2013) Unofficial translation by Bogdan Manolea and Anca Argesiu, available at http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf (last accessed 16.07.2013).

[11] German Constitutional Court (Bundesverfassungsgericht), Decision of 02 March 2010, NJW 2010, 833.

[12] Supreme Court of Cyprus, Decision of civil applications 65/2009, 78/2009, 82/2009 & 15/2010-22/2010, 01 February 2011, available only in Greek at http://www.supremecourt.gov.cy/judicial/sc.nsf/0/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf (last accessed 16.07.2013).

[13] Czech Constitutional Court, Decision of 22 March 2011 on petition Pl. ÚS 24/10, available online in Czech at http://www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Aktualne_prilohy/2011_03_31b.pdf. Translation by the Constitutional Court in English, available online at http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=40&cHash=bbaa1c5b1a7d6704af6370fdfce5d34c (last accessed 16.07.2013). .

[14] idem, para. 50.

[15] Constitutional complaint filed by HCLU against Hungarian telecom data retention regulations, 02 June 2008, available at http://tasz.hu/en/data-protection/constitutional-complaint-filed-hclu-against-hungarian-telecom-data-retention (accessed 08 Jul 2013)

[16] K. Kelemen, "The Hungarian Constitutional Court in the new constitutional framework" (2012) Paper presented at the III Colloquio biennale dei giovani comparatisti, Aosta (Italy) on 28-29 June 2012, organised by the Italian Association of Comparative Law, available at

In 2012 the DRD, as well as the relevant Irish legislation transposing it, was challenged in front of the Irish High Court by the civil and human rights advocacy group, Digital Rights Ireland. The Irish High Court granted the relief for a preliminary ruling to the Court of Justice of the European Union on the validity of the DRD, which was submitted in June 2012[17]. Among other questions, the Court of Justice is called to give answer on the compatibility of the Directive with the right to privacy laid down in Article 7 of the Charter and Article 8 ECHR and with the right to the protection of personal data laid down in Article 8 of the Charter. Moreover, in November 2012 the Austrian Constitutional Court published a decision seeking a preliminary ruling by the Court of Justice on whether data retention is compatible with the European Charter of Fundamental Rights, the European Convention on Human Rights and the right to data protection, as specifically protected in the Austrian Constitution[18].

More recently, on 28th January 2013 a request for a preliminary ruling was submitted to the Court of Justice of the European Union by the Austrian Data Protection Commissioner, dealing **specifically with the interpretation of Article 7(c) of the DRD**.[19] The Austrian Data Protection Commissioner asked if Article 7(c) of Directive 2006/24/EC is to be interpreted as meaning that natural persons affected by the retention of data within the meaning of the Directive do not fall into the category of 'specially authorised personnel' within the meaning of that provision and may not be granted a right to receive information on data relating to their own person from the provider of a publicly available communications service or a public communications network. And if this question is answered at least partly in the affirmative, the Court is asked whether Article 7(c) of Directive 2006/24/EC is compatible with the fundamental right laid down in the second sentence of Article 8(2) [of the Charter of Fundamental Rights of the European Union] and thus valid. Although the Court has not dealt with this case yet, it is interesting to anticipate the impact it may have on the interpretation of this data security principle.

http://academia.edu/1760644/The_Hungarian_Constitutional_Court_in_the_new_constitutional_framework (accessed 08 Jul 2013).

[17] Reference for a preliminary ruling from High Court of Ireland made on 11 June 2012 — Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, Case C-293/12, O.J. C258/11 (25.08.2012)

[18] Request for a preliminary ruling from the Verfassungsgerichtshof (Austria) lodged on 19 December 2012 — Kärntner Landesregierung and Others, Case C-594/12, O.J. C79/7 (16.03.2013).

[19] Case C-46/13: Request for a preliminary ruling from the Datenschutzkommission (Austria) lodged on 28 January 2013 — H v E (Pending Case), OJ C147/3 (25.05.2013)

3 Implementation of security measures at MSs level

3.1 Introduction

One of the goals of this report is to provide a set of recommendations for a common European approach on the technical and organisational security measures (in short 'security measures') that should be taken in relation to data that are retained in accordance with Article 7 of the DRD. For the realisation of this goal, the identification of best practices on data security specifications and standards that are used for securing personal data in the framework of the DRD in EU Member States will serve as the basis for the drafting of recommendations for a common European approach.

In order to achieve this goal, a study was carried out examining the transposition of Article 7 in six European Member States, based on the collection of information on the security measures that are applied to protect user data that have been retained in the frame of the DRD, as well as on the supervisory authorities that are entrusted with the monitoring of the implementation and application of these measures in accordance with Article 9 of the DRD. The provisions of these Articles have been presented in Section 2.3.1. Article 7 stipulates **four data security principles** that should be adopted by the Member States and foresees that appropriate technical and organisational measures should be in place for the protection of the retained data of the users. These principle can be broken down to (a) the principle that data shall be of the same quality and enjoy the same security protection, as the security protection measures on the network, (b) the principle that the data shall be protected against accidental or intentional destruction, loss or manipulation, (c) the principle that data shall be accessed only by specially authorised personnel, and (d) the principle of data destruction at the end of the retention period. Article 9 provides for the designation of a **supervisory authority** that will be responsible for the monitoring of the application of the data security principles.

The study was based on the collection of information from six EU Member States, namely Austria, Estonia, France, Spain, Sweden and the United Kingdom. Based on available resources for this study we aimed at having a small but representative sample of EU Member States. These Member States represent different legal, administrative and socio-political cultures and ensure an adequate population and geographic coverage.

Austria is a continental Germanic law country that was chosen over Germany, as the latter has not duly transposed the DRD. **France** has a strong continental Napoleonic law tradition, while the **United Kingdom** is the largest common-law country in the European Union. **Spain** is a country from the south of Europe. **Estonia** is a Baltic country, while **Sweden** is a Scandinavian country that recently transposed the Directive.

These countries form an interesting mix of prior experiences with the DRD, and furthermore contain both common law and continental law, western and central European, larger and smaller countries.

The information was collected through a questionnaire that was dispatched to and collected from a selected list of representatives in these Member States (see Annex I). The answers focused on providing information on whether and how the data security principles are implemented in these countries and on the supervisory authority that has been established (if any), as well as on the auditing procedures and mechanisms.

3.2 Security measures

All surveyed countries have implemented Article 7 of the DRD. However, **Spain** and **Estonia** have transposed only three of the four data security principles, not providing explicitly for the destruction of data at the end of the retention period.

Spain transposed the data security principles via Article 8 of the Spanish Data Retention Act[20], according to which providers who are to retain user data shall implement technical and organisational measures to prevent accidental erasure, manipulation or misuse of the data. Specific security measures applicable to retained data are set forth in the Spanish Data Protection Act[21] and in Royal Decree 1720/2007[22]. Art. 81.4 of Royal Decree 1720/2007 provides that retained data shall be protected by medium-level security measures, which are specified in Articles 82-100 of the same Royal Decree. More specifically the following main security measures should be applied to retained data: data processors shall sign special data processing agreements (Art. 82), non-qualified workers (i.e. cleaning staff) accessing provider's premises should sign special non-disclosure agreements (Art. 83), delegation of authorisations should specifically be described in a security document (Art. 84); the Decree also provides for the implementation of security policies and procedures (Art. 88), incident management systems (Art. 90), access control (Art. 91), document and device management systems (Art. 92, 101), identification and authentication (Art. 93), backup policies (Art. 94, 102); moreover security officer must be appointed (Art. 95), bi-yearly audit must take place (Art. 96), physical restricted access to data centres must be ensured (Art. 99) and log files records must be kept (Art. 103).

The data security principles have been implemented in **Estonia** by adding Section 111^1(9) to the Electronic Communications Act.[23] Section 111^1 regulates the obligation of a communications undertaking to preserve data, while subsection 111^1 (9) specifically implements Article 7 of the Data Retention Directive. Clause 111^1 (9) 1) of the Electronic Communications Act implements Article 7 a) of the Directive and prescribes the obligation to ensure the same quality, security and data protection requirements as those applicable to analogous data on the electronic communications network. Clause 111^1 (9) 2) of the Electronic Communications Act implements Article 7 b) of the Directive and requires that the data are protected against accidental or unlawful destruction, loss or alteration, unauthorised or unlawful storage, processing, access or disclosure. Clause 111^1 (9) 3) of the Electronic Communications Act implements Article 7 c) of the Directive and prescribes that

[20] Law 25/2007, of 18 October, on the retention of data related to electronic communications and public communication networks [Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones"], available in Spanish at http://www.boe.es/aeboe/consultas/bases_datos/act.php?id=BOE-A-2007-18243 (accessed at 16.07.2013).

[21] Organic Law 15/1999 of 13 December, on Personal Data Protection [Ley Orggánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal], available in Spanish at http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/Ley-15_99.pdf. Unofficial translation in English available at: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs_ingles/Ley_Orgnica_15-99_ingles.pdf (last accessed 16.07.2013).

[22] Royal Decree 1720/2007 of 21 December which approves the Regulation implementing Organic Law 15/1999 of 13 December on the protection of personal data [Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de *la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal], available in Spanish at* http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf. *Royal decree nofficial translation in English available at* http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/reglamentolopd_en.pdf (last accessed 16.07.2013).

[23] Estonian Electronic Communications Act from 8 December 2004 [Elektroonilise side seadus. State Gazette: RT I 2004, 87, 593] regulates the field of electronic communications. The Data Retention Directive was implemented into Estonian national law via an amendment to the Electronic Communications Act on 15 November 2007 (RT I 2007, 63, 397). Several new Sections were added with this amendment in order to take over the provisions of the Data Retention Directive. The Electronic Communications Act is available in Estonian at the official webpage of the State Gazette (Riigi Teataja): https://www.riigiteataja.ee/akt/107112012003. English translation of the Electronic Communications Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X90001K7&keel=en&pg=1&ptyyp=RT&tyyp=X&query=elektroonilise+side+seadus (last accessed 16.07.2013).

necessary technical and organisational measures must be in place to restrict access to the data. The wording of Clause 111[1] (9) 3) *differs from* Article 7 c) of the Directive – the underlined part below has not been implemented in the wording of Estonian Electronic Communications Act: "the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only". Clause 111[1] (9) 4) of the Electronic Communications Act requires that no data revealing the content of the communication are preserved. Therefore this clause does not provide for the destruction of data upon the end of the retention period. A Regulation was adopted by the Minister of Economic Affairs and Communications on 25 June 2008 regarding the procedure for the preservation and delivery of data, applications, log files and requests to the Technical Surveillance Authority, their deletion and destruction.[24] This Regulation stipulates the general principles for security measures on the preservation of retained data.

Sweden has introduced higher security requirements for retained data compared with users' regular data kept by providers of electronic communications. A new Section was added to the Electronic Communications Act, Chapter 6 Section 3a.[25] The new provision prescribes that providers who are to retain users' data according to Chapter 6 Section 16 of the same Act (general data retention obligation) shall implement technical and organisational measures necessary to protect the retained data during processing. In contrast, Section 3 (security measures for general user's data) leaves some leeway to the providers as available techniques and costs associated with the measures can be taken into consideration in a risk analysis.

Section 3a does not stipulate any specific rules regarding the security measures for retained data, but leaves such regulation to the government or the relevant supervisory authority. This was realised in 2012 by amending Section 37 of the Electronic Communications Ordinance.[26] Section 37 of the Ordinance prescribes detailed requirements, in line with Article 7 of the Data Retention Directive: Section 37(1) stipulates that providers (i.e. providers obliged to retain data) shall implement the necessary measures to ensure that the retained data has the same quality and is subject to the same security and protection it had before the retention. Para 1 reflects in this sense point a) of Article 7 in the Directive. Section 37(2) specifies that the provider shall implement the necessary measures to protect the data against accidental or unlawful destruction, accidental loss or alteration. Such measures shall further be implemented to prevent unlawful storage, processing of or access to and unlawful disclosure of the data. The data shall only be made accessible to personnel with specific authorisation. Para 2 reflects points b) and c) of Article 7. Section 37 furthermore gives the right to the Swedish Post and Telecom Authority[27] to adopt more specific regulations about the measures mentioned in Para 1 and 2.[28] This should be done in cooperation with the Swedish Data Inspection Board (*Datainspektionen*) and the Swedish National Police Board (*Rikspolisstyrelsen*).

[24] Regulation by the Minister of Economic Affairs and Communications regarding the procedure for the preservation and delivery of data, applications, log files and requests to the Technical Surveillance Authority, their deletion and destruction [Andmete, järelpärimiste, logifailide ja taotluste säilitamise, Tehnilise Järelevalve Ametile üleandmise ning kustutamise ja hävitamise kord. RTL 2008, 56, 774], available in Estonian at the official webpage of the State Gazette: https://www.riigiteataja.ee/akt/13100712 (last accessed 16.07.2013).

[25] Swedish Electronic Communications Act [Lag (2003:389) omelektroniskkommunikation], available in Swedish at http://www.notisum.se/rnp/sls/lag/20030389.HTM. English version of the act **not** yet updated is available at http://www.government.se/sb/d/2025/a/18454 (last accessed 16.07.2013).

[26] Electronic Communications Ordinance [Förordning (2003:396) om elektronisk kommunikation], available in Swedish at http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/_sfs-2003-396/ (last accessed 16.07.2013).

[27] Swedish Post and Telecom Authority (PTS;*Post- ochtelestyrelsen*), www.pts.se (last accessed 16.07.2013)

[28] Electronic Communications Ordinance [Förordning (2003:396) om elektronisk kommunikation],Section 37, available in Swedish at https://lagen.nu/2003:396#P37S1 (last accessed 16.07.2013).

Based on Section 37 of the Electronic Communications Ordinance, the Swedish Post and Telecom Authority (PTS)[29] adopted on 1 December 2012 regulations and general advice on security measures concerning retention and other processing of data for crime prevention purposes (PTS regulation PTSFS 2012:4)[30]. Section 3 of the PTS regulation stipulates the obligation for the provider to perform regular and systematic security work taking into consideration the specific risks of data retention. The security work should contain at least the measures mentioned below and the provider must have routines and processes in place to implement the protective measures. The regulation also suggests a risk analysis for the activities in question and that specifically appointed personnel should monitor the security operations. In specific PTS regulation PTSFS 2012:4 prescribes that routines must be in place that ensure that only personnel with specific authorisation have access to the data and the system (Section 4), any equipment being used for the retention must be placed in spaces protected against electronic outage, fire, flooding and unauthorised access to prevent loss of or unlawful access to the retained data (Section 5), all processing of retained data must be documented through logs. Logging information must include who had access to which data and when. Personnel accessing the data must not have access to the logs (Section 6), the logs shall be used for regular and systematic follow-ups and control (Section 6), logging information must be protected through encryption during storage and transfer. For the encryption a generally accepted encryption method with a sufficient key length must be used. Encryption keys must be handled in a secure way (Section 6), retained data and logs must be backed up often enough to prevent accidental or unlawful destruction or accidental loss or change (Section 6), back up copies must be physically stored away from the retained data (Section 6) and back up copies must be deleted at the same time as the retained data (Section 6). The PTS regulation PTSFS 2012:4 also suggests that non-disclosure agreements between the provider and its employees who process the retained data (Section 4); authorisation control for the entire system, equipment and places being used for the retention; authorisations should be evaluated on a regular basis (Section 4); back up copies should be checked on a regular basis (Section 6).

In the **United Kingdom**, Article 7 of the Directive is implemented by regulation 6 of the Data Retention (EC Directive) Regulations 2009[31]. In large part this follows the approach of the DRD but does make some changes in terminology. In respect of paragraph (a) of the Directive, the Regulations add reference to public communications networks although this limitation is clear from the opening sentence of the Directive. Paragraph b of the Directive is implemented without any changes, as is paragraph (c). There is a slight change in terminology as respects paragraph (d). The UK Regulations provide that "except in the case of data lawfully accessed and preserved, the data retained solely in accordance with these Regulations must be destroyed at the end of the retention period". This provision is similar to but marginally more restrictive than the provisions of the Directive due to the addition of the requirement that data must be "lawfully accessed". There are no specific provisions relating to the technical and organisational security measures required in respect

[29] The Swedish Post and Telecom Authority (PTS) provides a specific website for data retention (in Swedish) at http://www.pts.se/sv/Bransch/Internet/Integritet/Regler/Trafikdatalagring/(last accessed 16.07.2013).

[30] Regulations and general advice of the Swedish Post and Telecom Authority (PTS) on security measures concerning retention and other processing of data for crime prevention purposes (PTSFS 2012:4, Post-ochtelestyrelsensföreskrifterochallmännarådomskyddsåtgärderisamband med lagringochannanbehandlingavuppgifterförbrottsbekämpandeändamål), available in Swedish at http://pts.se/sv/Dokument/Foreskrifter/Tele/PTSFS-20124---foreskrifter-och-allmanna-rad-om-skyddsatgarder-i-samband-med-lagring-och-annan-behandling-av-uppgifter-for-brottsbekampande-andamal/ (last accessed 16.07.2013).

[31] The DRD is implemented in the United Kingdom by secondary legislation in the form of the Data Retention (EC Directive) Regulations 2009 (SI 2009/859) which revoked previous regulations – The Data Retention (EC Directive Regulations 2007 (SI 2007 No 2199), available at http://www.legislation.gov.uk/uksi/2009/859/contents/made (last accessed 16.07.2013). The 2007 Regulations implemented the Data Retention Directive in respect of telephone communications and the 2009 Regulations extended the scope of coverage to include Internet communications.

of data retained under the Directive's provisions. However, guidance has been issued by the Information Commissioner[32] and also by the Department for Business and Skills[33] regarding the manner in which compliance with the general data protection requirements relating to security may be assured. Where data is outsourced there is guidance from the Information Commissioner's Office regarding the measures that should be taken to ensure its security[34]. The Information Commissioner has recommended that data held in storage should where practical be encrypted[35].

Austria adopted the text of Article 7 (b) and (c) of the Directive in Sec 102c TKG (TelekommuniKationsGesetz) 2003[36], which generally regulates data security, logging and statistics. Pursuant to Sec 102a para. 8 TKG 2003, retained data has to be destroyed after expiration of the storage period (six months) and in practice at the latest within one month after the end of the retention period. The provision of information after the end of the retention period shall not be permissible. This reflects Article 7(d) of the DRD. With regard to the first data security principle that the retained data shall be of the same quality and subject to the same security and protection as those data in the network, the Austrian legislation did not contain an explicit principle. However, the Austrian legislation required that the retained data have to be retained in a way that differentiates them from other stored data. The Austrian legislator has exercised the option to go beyond the requirements of the Directive (as foreseen in Article 7 of the Directive) by

(i) establishing a "dual control principle" in Sec 102c para 1 TKG 2003: Access to data retained is reserved exclusively to duly authorised persons under strict adherence to the dual control (= four eyes) principle;

(ii) the obligation that protocol data have to be retained for a period of 3 years from expiration of the data retention period;

(iii) the requirement stipulated in Sec 102c para 2 TKG 2003 for audit-proof listing of every access and every information provided to security authorities;

(iv) stipulating in Sec 102c para 3 TKG 2003 that retention must occur in a manner that retained data can be distinguished from other data;

(v) authorizing the Federal Minister of Transport, Innovation and Technology to issue regulations for further specifications as to the security measures for retained data[37].

---

[32] UK ICO, The Guide to data protection, available at http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.ashx. The guidance on principle 7 on information security can also be found at http://ico.org.uk/for_organisations/data_protection/the_guide/principle_7 (last accessed 16.07.2013).

[33] Department for Business and Skills, Information security and assurance
Information security and assurance are the processes and mechanisms needed to build a secure and reliable ICT infrastructure, 4 October 2010 available at https://www.gov.uk/government/publications/information-security-and-assurance and Cyber security guidance for business, available at https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility (last accessed 16.07.2013).

[34] See above footnote 36. UK ICO, The Guide to data protection.

[35] UK ICO, Our approach to encryption, available at http://ico.org.uk/news/current_topics/Our_approach_to_encryption (last accessed 16.07.2013).

[36] The Directive was implemented into Austrian national law via an amendment to the Austrian Telecommunications Act 2003 (Telekommunikationsgesetz - TKG 2003), particularly by implementing the Sec 102a, 102b and 102c TKG 2003. At the same time, the Austrian Code on Criminal Procedure (Strafprozessordnung - StPO) and the Security Police Law (Sicherheitspolizeigesetz - SPG) were amended in order to adjust the powers of federal authorities regarding the access to the data retained. The Act is available in German at https://www.rtr.at/?id=2545 and in English via https://www.rtr.at/en/tk/TKG2003 (last accessed 16.07.2013).

[37] Austrian Data Security Regulation [Datensicherheitsverordnung - TKG-DSVO, BGBl. II Nr. 402/2011], available only in German at http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007596 (last accessed 16.07.2013). .

This option was used by adopting the Regulation on Data Security Measures (Telekommunikationsgesetz TKG 2003) which provides details regarding the protection standards of the data retained.

The TKG 2003 contains only general requirements as to the security measures for retained data. Pursuant to Sec 102c para. 1 TKG 2003, providers are obliged to implement "appropriate technical and organisational security measures". More detailed specifications regarding the safety standard for the retention of data are laid down in Sec 14 of the Austrian Data Protection Act 2000[38] and Sec 95 TKG 2003. These provisions contain data security requirements on providers of electronic telecommunications services, depending on type and purpose of the data used. More specifically, these provisions demand (a) implementation of security policies, (b) logging of every access, (c) definition of internal access rights, (d) technical measures.

In addition, the Federal Minister of Transport, Innovation and Technology adopted a regulation on security measures concerning retention and other processing of data for crime prevention purposes, which entered into force on 1 April 1 2012 (*Datensicherheitsverordnung, TKG-DSVO*).[39]

Sec 5 TKG-DSVO ("technical and organisational security measures") stipulates that retained data have to be stored in such a way that a clear distinction between operating and retained data is maintained at all times (physical separation is not necessary); the method of the technical and organisational separation of the data has to be documented; retained data have to be deleted in case the provider loses its operational justification.

Sec 7 TKG-DSVO ("audit-proof logging and dual control principle") provides that access to retained data is reserved for duly authorized personnel under strict adherence of the dual control principle, and that all processing of retained data must be documented through logs. Logging information must include who (identity of the requesting persons) had access to which data, why (reference to the underlying offence and the respective orders of the court/security authority) and when.

The Austrian Regulation is further explained in sections 3.4 and 3.5.

France already had statutory provisions in place that reflected the principles contained in Articles 7 a), b) and c) of the Data Retention Directive and were codified in Article L.34-1 of the Code of Posts and Electronic Communications (hereafter "CPEC").[40] According to Article L.34-1-VI-§3, the data retention shall be made in compliance with the Law No 78-17[41]. Article 34 of the Law No 78-17 provides in particular that the data controller shall take all useful precautions to preserve the security of the data – in particular, prevent their alteration and damage, or access by non-authorised third parties. The "useful precautions to preserve the security of the data" set forth by Article 34 of the Law No 78-17 are not defined. As such, there is no legal provision for specific technical and organisational security measures for retained users' data under French law.[42]

[38] Austrian Data Protection Act [Datenschutzgesetz 2000 - DSG 2000],available in German at http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597. Unofficial English translation is available at http://www.dsk.gv.at/DocView.axd?CobId=41936 (last accessed 16.07.2013).

[39] See above footnote 41 Austrian Data Security Regulation.

[40] French Code of Posts and Electronic Communications (Code des postes et des communications électroniques), available at http://www.legifrance.gouv.fr/affichCode.do;jsessionid=82DAAD03B742A91264B188B742394AB6.tpdjo07v_1?cidTexte=LEGITEXT000006070987&dateTexte=20130527 (last accessed 16.07.2013)..

[41] Law No 78-17 dated 6 January 1978 on Information Technology, Data Files and Civil Liberties [Loi relative à l'informatique, aux fichiers et aux libertés], available in French at http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf and an unofficial translation in English at http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf (last accessed 16.07.2013).

[42] General principles however remain applicable. For example, encryption was allowed by Article 30 of the Law No 2004-575 of 21 June 2004 for trust in digital economy [Loi pour la confiance dans l'économie numérique - LCEN] providing for

Article 7 d) of the DRD was codified by the Decree No 2006-358[43] under Articles R.10-13-III (setting the principle that the retention is limited to one year from the recording of the data) and R.10-14 of the CPEC (providing specific measures for the application of Article L.34-1 of the CPEC and for networks and equipment security). Decree No 2006-358 also introduced new provisions in the Code of Criminal Procedure (CCP) at Article R.213-1 pertaining to the rates that may be applied by electronic communications operators for the provision of the retained data.[44] According to Article 226-17 of the Criminal Code[45], five years' imprisonment and a fine of €300,000 can be ordered if the measures provided by Article 34 of the Law No 78-17 are not implemented. Although there is no specific legislation defining the technical and organisational security measures for retained data, the French Data Protection Authority (CNIL) [46] published different guidelines on technical and organisational security measures for retained data.[47]

Summary of findings

All surveyed countries have implemented Article 7 of the Data Retention Directive. **Sweden** and **Austria** have introduced higher security requirements for retained data compared with regular data kept by providers of electronic communications. More specifically, although Austria does not explicitly require that the retained data shall be of the same quality and subject to the same security and protection as those data in the network, the Austrian law stipulates that retained data have to be stored in such a way that a clear distinction between operating and retained data is maintained at all times (physical separation is not necessary), the method of the technical and organisational separation of the data has to be documented and retained data have to be deleted in case the provider loses its operational justification.

However, **Spain** and **Estonia** have transposed only three of the data security principles, not providing explicitly for the destruction of data at the end of the retention period. The Estonian act requires that no data revealing the content of the communication are preserved; therefore this clause does not provide for the destruction of data upon the end of the retention period. Even when the

free use of encryption technologies, available in French at http://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=EC95AAA48B99B4568B2930DF7DBE479B.tpdjo13v_1?idArticle=LEGIARTI000006421577&cidTexte=LEGITEXT000005789847&dateTexte=20130530 (last accessed 16.07.2013)..

[43] Decree No 2006-358 dated 24 March 2006 on the retention of electronic communications data [Décret relatif à la conservation des données des communications électroniques], available in French at http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=3D64C166849818E56C96B316FC942DEE.tpdjo13v_3?cidTexte=JORFTEXT000000637071&dateTexte=20130526 (last accessed 16.07.2013).

[44] Article R213-1 of the French Code of Criminal Procedure [Code de procédure pénale - Article R213-1] available in French at http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=D4B096673ADF3C9687AC1EB658C5276E.tpdjo07v_1?idArticle=LEGIARTI000006518197&cidTexte=LEGITEXT000006071154&dateTexte=20130527 (last accessed 16.07.2013).

[45] Article 226-17 of the Criminal Code [Code pénal - Article 226-17], available at http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=7F043BD72C11400DAB14554D2B073869.tpdjo05v_2?idArticle=LEGIARTI000006417964&cidTexte=LEGITEXT000006070719 (last accessed 16.07.2013).

[46] French National Commission for Information Technology and Civil Liberties (*Commission Nationale de l'Informatique et des Libertés* – CNIL), www.cnil.fr (last accessed 16.07.2013).

[47] In 2010, the CNIL published a first guide on security of personal data. A more detailed guide was made available in 2012 with regards to the methodology for privacy risk management. On the basis of the said methodology, the CNIL also disclosed a catalogue of good practices suggesting measures for the privacy risk treatment: "Guide security of personal data" available in French at http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf and in English at http://www.cnil.fr/fileadmin/documents/en/Guide_Security_of_Personal_Data-2010.pdf. "Methodology for privacy risk management" available in French at http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf and in English at http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf. "Measures for the privacy Risk treatment" available in French at http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_securite_avance_Mesures.pdf and in English at http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Measures.pdf (last accessed 16.07.2013)..

national legislation in a Member State stipulates that the retained data have to be deleted in the end of the retention period, there are no norms and standards in place regulating how the destruction of data should take place.

The data security principle, requiring that the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed only by specially authorised personnel, has been transposed in diverging ways between the surveyed countries. The **Estonian** law does not require that technical and organisational measures are taken in order to ensure that data can be accessed only by specially authorised personnel.

3.3 Norms and standards on the security measures for retained data

The **United Kingdom** Information Commissioner's Office has made extensive reference to the use of ISO 27001. In respect of encryption, the Information Commissioner has noted that "Since encryption standards are always evolving, it is recommended that data controllers ensure that any solution which is implemented, meets the current standard such as the recommended FIPS 140-2 (cryptographic modules, software and hardware) and FIPS – 197. Encryption products certified via CESG's CPA or CAPS schemes to at least FOUNDATION grade would also meet the current standard"[48].

In **Austria** the Federal Minister of Transport, Innovation and Technology adopted a regulation on security measures concerning retention and other processing of data for crime prevention purposes, which entered into force on April 1, 2012[49]. Sec 3 TKG-DSVO provides for the establishment of a Centralized Unit (DLS), which serves as an electronic inbox system for the safe processing of requests and information regarding traffic data, location data and retained data. Both requesting authority and provider are assigned to a unique inbox, to which the requested data are transported in an encrypted form. Every access is assigned a unique ID to ensure traceability. Only authorised entities, as specified in Sec 14 TKG-DSVO have access to these inboxes. Authentication and identification is performed through an advanced electronic signature (Sec 13 TKG-DSVO).

Sec 7 TKG-DSVO further requires audit-proof logging of every access to retained data and strict adherence to the dual control principle. Data transmission via the DLS and logging of the access is not legally required in "cases of a general danger", § 3 TKG-DSVO. An Annex to the TKG-DSVO specifies the technical implementation of requests for retained data under Sec 94 (4) TKG 2003 („*Technische Richtlinie zur CSV-Datei für die Beantwortung von Auskunftsbegehren gemäß § 94 Abs 4 TKG 2003 – EP020*").

Summary of findings

The United Kingdom and Austria have made specific references to standards and encryption mechanisms for the retention of user data. However, *it became obvious from the study that there is no homogeneity in the technical ways in which the storage of retained data takes place.*

3.4 Transfer of retained data to law enforcement authorities and relevant norms and standards

In **Spain**, the Prime Minister's Office (Ministerio de la Presidencia) has issued a data delivery protocol, which is contained in Order PRE/199/2013.[50] Specific security measures applicable to the

[48] See above, footnote. 39. UK ICO, Our approach to encryption.
[49] See above, footnote 41. Austrian Data Security Regulation, Datensicherheitsverordnung, TKG-DSVO.
[50] Order PRE/199/2013 of 29 January which defines the delivery format of data retained by operators of electronic communications services or of public communications networks to authorized agents. [Orden PRE/199/2013, de 29 de

transfer of retained data can be found in Annex II of the Order. The Order provides that retained data should be transferred only in electronic copy. Further technical details of the electronic format to be used can be found in the 100-pages long Annex I. The format that is contained in the Order is compliant with ETSI standards. In particular the Order states that it takes into account the handover requirements from ETSI TS 102 656. Providers can ask the Homeland Security Department of State (Ministerio de Interior) for a specific data exchange framework, presumably as an out-of-the-box product ready to comply with the PRE/199/2013 protocol.[51]

With regard to the time within which the retained data should be delivered to the competent authorities, the requesting authority (Court of Justice or National Security Agency) shall provide the specific term within retained data should be delivered, in view of the intrinsic nature and the circumstances involved in the legal proceeding. In case no specific term is provided by the requesting authority, then data should be transferred as soon as possible and in any event within 72 hours counted from 8:00 a.m. of the first labour day after the request has been received by the Provider. [52]

In **Estonia**, neither the Electronic Communications Act nor the Regulation by the Minister of Economic Affairs and Communications prescribe any specific requirements for the format of the retained data transferred to law enforcement authorities. Section 112 of the Estonian Electronic Communications Act regulates the obligation to provide information. It stipulates that if the relevant agency or authority submits a request, a communications undertaking is required to provide the information at the earliest opportunity, but not later than ten hours after receiving an urgent request or within ten working days after receipt of the request if the request is not urgent, and if adherence to the specified terms is possible based on the substance of the request. The request can be submitted in writing or by electronic means. Requests concerning certain data may also be submitted in oral form confirming the request with a password. Access to the data may be ensured, on the basis of a written contract, also by way of continuous electronic connection. Furthermore, a communications undertaking providing mobile telephone services is required to provide a surveillance agency and security authority and the Police and Border Guard Board on the bases provided for in the Police and Border Guard Act with real time identification of the location of the terminal equipment used in the mobile telephone network. Access to this data must be ensured on the basis of a written contract and by way of continuous electronic connection.

In **Sweden** neither the Electronic Communications Act nor the Ordinance stipulate any specific requirements concerning the format of data that have to be transferred to the competent authorities. However, both law enforcement authorities and providers of electronic communications have discussed a common interface for the transfer of retained data. The Swedish IT and Telecom Industries[53], an industry organisation, led the development of a standard which is based on the ETSI standard TS 102 657. The Swedish implementation of ETSI TS 102 657 was issued in August 2012 as a national technical specification by the Informations Tekniska Standardiseringen (ITS), which is one of the main standardisation bodies in Sweden, appointed by the Government[54]. The Swedish standard is called ITS 27 and concerns an "interface for the request and disclosure of traffic data for law

enero, por la que se define el formato de entrega de los datos conservados por los operadores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a los agentes facultados], available only in Spanish at: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2013-1591 (last accessed 16.07.2013)..

[51] Dedicated website at the `ministry of the Interior, available in Spanish at http://www.interior.gob.es/conservacion-de-datos-93/solicitud-de-archivos-de-implementacion-2018?locale=es (last accessed 16.07.2013).

[52] Article 7 of the Spanish Data Retention Act (Organic Law 25/2007), see above footnote 24.

[53] More information about the work is available in Swedish at http://www.pts.se/sv/Bransch/Internet/Integritet/Regler/Trafikdatalagring/PTS-arbete-med-trafikdatalagring/Andra-organisationer/ (last accessed 16.07.2013).

[54] Information Technical Standards [InformationsTekniskaStandardiseringen], http://www.its.se/ (last accessed 16.07.2013).

enforcement purposes".[55] In this sense, electronic transfer is the chosen option. Standard ITS 27 is being defined as "an application guide describing interface and procedures for the transfer of information between databases, through an automatic electronic interface, where the request for and disclosure of traffic data for law enforcement purposes is approved by the operator's staff". The standard distinguishes between mandatory, conditional or optional traffic data, and also includes a reference to the appropriate data fields in the Data Retention Directive. The standard includes a process of requests (*beställningar*) and answers (*svar*) via a pre-defined interface. The idea is to ensure security and authenticity through asymmetric encryption with private and public keys, thereby being able to work without written signatures on paper documents. Each order should contain mandatory fields, e.g. which authority is requesting the data and when. In addition, a unique reference number will link the request to the answer, and subsequently to the official decision by the authority allowing access to the data. The data is sent to the authority via a TCP/IP interface, using ASN.1 or XML as a data format. Though the standard is not mandatory as such, its support by the main industry organisation in the electronic communications sector should lead to its implementation on a large scale. With regard to the time period, within which the retain data have to be delivered to the requesting competent authorities, Chapter 6 Section 16 of the Swedish Electronic Communications Act stipulates that the provider of electronic communications shall run its operations in a way that allows data to be handed over without any delay. If necessary, requests by authorities for access to retained data must also be dealt with by the provider outside of regular office hours. The Government Bill implementing the Directive discussed that a transfer should take place as soon as the data is available. This implies that a transfer might take places on several occasions. The Government emphasised in this regard the importance for law enforcement agencies to be able to access the data as soon as possible[56].

In the **United Kingdom**, the Data Retention Regulations do not specify any particular format for the transfer of data. As mentioned in the previous section, the United Kingdom Information Commissioner's Office has made extensive reference to the use of ISO 27001 and has recommended that "data controllers ensure that any solution which is implemented, meets the current standard such as the recommended FIPS 140-2 (cryptographic modules, software and hardware) and FIPS – 197. Encryption products certified via CESG's CPA or CAPS schemes to at least FOUNDATION grade would also meet the current standard"[57]. With regard to the time, the Data Retention Regulations require that data must be retained in such a manner that it can be supplied "without undue delay in response to requests" (Regulation 8). No specific time is given. However, the Code of Practice on the Acquisition of Communications Data[58] provides in paragraph 3.56 for urgent requests to be made to a communications service provider (either orally or in writing) in cases where the provision of data within a maximum period of 48 hours would "directly assist the prevention or detection of the commission of a serious crime, … the making of arrests or the seizure of illicit material". In other cases the Code of Practice indicates that data should be supplied within 10 working days. Reports by the Interception of Communications Commissioner indicated that a growing number of police forces are introducing automated platforms for use in making requests for access to communications data.

[55] ITS 27 on "interface for the request and disclosure of traffic data for law enforcement purposes", available in Swedish at http://www.its.se/ITS/ss6363x/Report-ITS27-Ed1.pdf (last accessed 16.07.2013).
[56] Swedish Government Bill implementing the Directive [Lagringavtrafikuppgifterförbrottsbekämpandeändamål - genomförandeavdirektiv 2006/24/EG Prop. 2010/11:46], p. 51, available in Swedish at http://www.regeringen.se/sb/d/13654/a/157433 (last accessed 16.07.2013).
[57] See above footnote 39.
[58] Code of Practice on the Acquisition of Communications Data, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97961/code-of-practice-acquisition.pdf (last accessed 16.07.2013).

During the implementation of the Data Retention Directive in **Austria**, there was extensive discussion on the technical realisation of the process. Two options were discussed: on the one hand, the common S/MIME standard which would allow the exchange of information regarding retained data via encrypted email (using transit encryption) and on the other hand, a centralized unit, interface for the transfer of retained data, (*Zentrale Durchlaufstelle - DLS*). Austria decided in favour of the DLS, taking into account the advantages and disadvantages of both options especially in respect of (i) identification and authentication, (ii) encryption (data), (iii) encryption (access), (iv) logging, (v) workflow information request and (vi) reception of data. Each of these criteria was examined under the following four criteria: implementation effort, maintenance, usage and security. The outcome of the analysis showed that DLS was in all respects more favourable.[59] As the DLS represents a technical novelty, there have been no reliable statistics on costs to refer to, and the considerations regarding the expected costs are therefore based on assumptions. The technical specifications regarding the transmission of retained data to law enforcement and security authorities are laid down in an Annex to the TKG-DSVO, which is a regulation on security measures concerning retention and other processing of data for crime prevention purposes[60]. Due to the substantial expenditure associated with it, ETSI and ISO standards do not apply. With regard to the request for and transmission of retained data, Sec 94 (4) TKG 2003 stipulates a centralized unit, interface for the transfer of retained users data, (*Zentrale Durchlaufstelle - DLS*), which shall ensure the highest level of data security possible. The details of the technical processing within this unit are specified in Sec 8 et sq TKG-DSVO which provides for the transmission of the encrypted data via a centralized unit (DLS). As to the file format, the "Comma-Separated Value (CSV)" applies. Details regarding the technical realization are stipulated in the Annex to TKG-DSVO. The data are transmitted in electronic, encrypted format through a secured inbox system (= DLS), described in the previous section. As mentioned in the previous section, encryption at transmission level related to encryption on the itinerary that is based on https. An Annex to the TKG-DSVO specifies the technical implementation of requests for retained data under Sec 94 (4) TKG 2003[61]. Sec 102b (2) TKG 2003 stipulates that the provider shall run its operations in a way that allows data to be handed over without any delay.

In **France** the applicable regulation does not request that the retained data shall be transferred in a specific format. The applicable regulation does not provide for a specific time period for the law enforcement authorities to get access to the retained data. According to the provisions of Article R.10-19 of the CPEC, the electronic communications operators and the persons whose activity is to provide access to online public communication services shall transfer the data requested without any delay.

Summary of findings

The transfer of retained data to law enforcement authorities has been regulated more extensively by the Member States with regard to the technical specifications that had to be followed. In **Spain**, the electronic format to be used for the transmission of data to the competent authorities has to be compliant with ETSI standards and it takes into account the handover requirements from ETSI TS 102

[59] Ludwig Boltzmann Institut Für Menschenrechte (BIM), Datensicherheit TKG Novelle 2010, Studie: Datensicherheit in der TKG Novelle zur Umsetzung der Vorratsdatenspeicherung in Österreich, Wien, 14.06.2011, p. 62, available at http://bim.lbg.ac.at/files/sites/bim/BIM%20Studie%20Datensicherheit%20TKG%20Novelle%202010_final_online-Publikation.pdf (last accessed 16.07.2013)..

[60] See above footnote 41.

[61] An Annex to the TKG-DSVO on the technical implementation of requests for retained data under Sec 94 (4) TKG 2003 („*Technische Richtlinie zur CSV-Datei für die Beantwortung von Auskunftsbegehren gemäß § 94 Abs 4 TKG 2003 – EP020*"), available at https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007596 (last accessed 16.07.2013).

656. In **Sweden** law enforcement authorities and providers of electronic communications have discussed a common interface for the transfer of retained user's data. The Swedish IT and Telecom Industries, an industry organisation, led the development of a standard which is based on the ETSI standard TS 102 657. To the contrary, **Austria** decided that due to the substantial expenditures associated with it, ETSI and ISO standards do not apply, and Austria developed a centralized unit, an interface for the transfer of retained data that is based on "Comma-Separated Value (CSV)".

Article 8 of the Data Retention Directive stipulates that the retained data have to be transmitted to the competent authorities "**without undue delay**". The survey revealed that the Member States interpret the term "without undue delay" in diverging ways, as some countries do not provide for an explanation of how the term should be interpreted, while others define specific time periods within the data have to be transmitted to the competent authorities. **Sweden**, **France** and **Austria**, for instance, require the data to be handed over without any delay. In **Spain** the requesting authority (Court of Justice or National Security Agency) shall provide the specific time period within which the retained data should be delivered, taking into account their nature and the circumstances relating to the specific case. In case no specific term is provided by the requesting authority, then data should be transferred as soon as possible and in any event within 72 hours counted upon 8:00 a.m. of the first working day where request has been received by the Provider. The **Estonian** law requires that the data have to be provided opportunity, but not later than ten hours after receiving an urgent request or within ten working days after receipt of the request if the request is not urgent. In the **United Kingdom** although no specific time period is provided for in the law transposing the Data Retention Directive, the Code of Practice on the Acquisition of Communications Data provides that data for urgent requests have to be provided within a maximum period of 48 hours. In other cases the Code of Practice indicates that data should be supplied within 10 working days.

3.5 Supervisory authority for the monitoring of the application of the data security principles

In **Spain** Article 8.4 of the Data Retention Act provides that the Spanish Data Protection Authority[62] shall have jurisdiction on operators failing to abide by the security measures applicable to retained data. The Spanish Data Protection Authority has jurisdiction on breaches occurring in the handling of retained data. Nevertheless, the Spanish Telecommunications Act[63] states in Article 53 o) and z) that the Spanish Telecommunications Authority (NRA)[64] has jurisdiction over operators failing to retain data at all. Presumably there is no overlap between the two, since there is a difference between failing to provide enough security to collected data and failing to provide the means to collect those data -at all- in the first place. The Spanish Data Protection Authority is clearly the competent body in the first scenario, for as long as a breach of security measures is concerned, whereas the Spanish Telecommunications Authority has a jurisdiction of a more abstract nature, and might eventually withdraw administrative permits to the telecom companies who are not complying with regulatory requisites.

[62] Spanish Data Protection Authority [Agencia Española de Protección de Datos, available at http://www.agpd.es/ (last accessed 16.07.2013).
[63] Spanish Telecommunications Act, Act 32/2003 (Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones), available online at http://www.cmt.es/ver-documento?&articleId=09002719800ABD97. Unofficial translation of some of the provisions of the Act is available in English at: http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/Ley_32-2003_LGT.pdf (last accessed 16.07.2013).
[64] Telecommunications Market Commission [Comisión Nacional del Mercado de las Telecomunicaciones], available at http://www.cmt.es (last accessed 16.07.2013)..

In **Estonia**, the Technical Surveillance Authority is the central supervisory authority with regard to data retention. In addition, the Ministry of Economic Affairs and Communications may also monitor the compliance of relevant regulations in accordance with the limits of their competence. The Technical Surveillance Authority, which is an independent authority under the Ministry of Economic Affairs and Communications, is the competent supervisory authority with regard to electronic communications in general (NRA). The Minister of Economic Affairs and Communications is responsible for establishing procedures relating to retained data, log files, applications, and requests. These procedures cover preservation, delivery to the Technical Surveillance Authority, deletion and destruction.

In **Sweden**, Sections 37 onwards of the Electronic Communications Ordinance[65] appoints the Swedish Post and Telecom Authority (PTS) as the responsible supervisory authority with regard to data retention. PTS had been the supervisory authority for electronic communications in general (NRA), so its competency was simply widened to include data retention as well. The Swedish Post and Telecom Authority (PTS) is the competent supervisory authority with regard to electronic communications in general, including competition aspects on the electronic communications market, and security of electronic information processes. Though the Swedish Post and Telecom Authority (PTS) has to consult with the Swedish Data Inspection Board (*Datainspektionen*) and the Swedish National Police Board (*Rikspolisstyrelsen*) with regard to regulations to be adopted, PTS is the central supervisory authority with regard to data retention.

In the **United Kingdom**, Regulation 6(2) of the Data Retention Regulations provides that it is the duty of the Information Commissioner, who has supervisory responsibility for general data protection legislation, to monitor the application of the Regulations to ensure compliance by providers and others with the Regulations. Also relevant in this context is the activity of the Interception of Communications Commissioner. Established under the Regulation of Investigatory Powers Act, this official has oversight of the activities of law enforcement agencies and other statutory bodies in the exercise of powers conferred on them under legislation to seek access to communications data held by communication service providers. The Interception of Communications Commissioner has no direct powers of intervention, but submits an annual report to Parliament. Responsibility for monitoring the operation of the data retention regime lies also with the Interception of Communications Commissioner.[66] The Office of Communications (OFCOM) is the regulatory body with responsibility for the electronic communications sector. It has concurrent responsibility with the Information Commissioner for the operation of the Privacy in Electronic Communications Directive and Regulations. A memorandum of understanding has been signed between the Information Commissioner and OFCOM under which it is agreed that primacy will be given to the Information Commissioner in respect of the operation of this legislation.

In **Austria**, data retention generally falls within the responsibility of the Federal Minister of Transport, Innovation and Technology. By implementing Article 9 of the Directive, Sec 102c para 1 TKG 2003 appoints the Austrian Data Protection Commission (DSK)[67] as the responsible supervisory authority.[68] The DSK is not obliged to perform regular monitoring of the providers. As of today, no such monitoring has been performed. It is therefore currently unclear whether the providers comply with their obligations regarding security measures for retained data. On October 16, 2012 (infringement proceeding C-614/10), the European Court of Justice condemned Austria for infringing

[65] *See above, footnote 32.*
[66] UK Interception of Communications Commissioner, http://www.iocco-uk.info (last accessed 16.07.2013).
[67] Austrian Data Protection Aithority [Datenschutzkommission – DSK], http://www.dsk.gv.at (last accessed 16.07.2013).
[68] Austrian Telecommunications Act [TKG 2003] is available in German at https://www.rtr.at/?id=2545 and in English via https://www.rtr.at/en/tk/TKG2003 (last accessed 16.07.2013).

Article 28 (1) and (2) of the Data Protection Directive by failing to ensure sufficient independence of the DSK. As a consequence Sec 38 para 2 DSG 2000 has been amended. The amendment entered into force on May 1, 2013, guaranteeing the independence of the DSK also from the Austrian government. The Federal Minister of Transport, Innovation and Technology is the responsible authority for the technical realization of the secured inbox system (DLS) for the transfer of retained data, as described in section 3.4 above.

In **France** the CNIL, the French data protection authority, is appointed as the supervisory authority for any data processing within the scope of the Data Retention Directive. The French National Commission for Information Technology and Civil Liberties (CNIL) is the competent supervisory authority with regard to data protection in general, including the electronic communications market, and security of electronic information processes. The French Regulation Authority of Posts and Electronic Communications (ARCEP) liaises with the CNIL on all issues related to data protection in the telecom industry. ARCEP appointed a dedicated Data Protection Officer (*Correspondant Informatique et Libertés*) in 2011 to liaise with CNIL.

Summary of findings

Article 9 of the Data Retention Directive stipulates that Member States "shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data", clarifying that these can be the same as the national Data Protection Authorities. The surveyed Member States have chosen either the Data Protection Authority (DPA) or the National Regulatory Authority (NRA) for electronic communications as the authority that would be responsible for the monitoring of the application of the data security principles for the retained data. Even in cases when several authorities area partly involved in the monitoring, there is one authority that has the primacy as a supervisory authority with regard to data retention. More specifically **Spain**, **Austria**, **France** and the **United Kingdom** have designated their Data Protection Authorities as the Article 9 authorities of the Data Retention Directive. **Estonia** and **Sweden** have designated their respective electronic communications NRAs as the authorities that would be responsible for monitoring the application of data security principles for retained data.

3.6 Audits

In **Spain** Article 96 of Royal Decree 1720/2007 foresees that an internal or external audit shall be carried out at least every two years to verify compliance with security measures that are taken for retained data. Security audits can be performed by own personnel of the company or by third-parties. However there is no specific provision as to who shall qualify for performing such audits. Industry standards shall apply in that concern. In order to ensure independence and objectiveness, third party audits are clearly more reliable.

In **Estonia**, under subsection 87^2 (5) of the Electronic Communications Act, the Technical Surveillance Authority is entitled to require a communications undertaking to provide information needed to assess the security and integrity of their communications services and networks, including security policies. The Authority can also order a security audit to be carried out by a qualified independent body or a competent state authority (i.e. a third party) and make the results available to the Technical Surveillance Authority. To our best knowledge there is no established practice regarding such security audits and the relevant procedure will be determined case-by-case.

In **Sweden** PTS can execute audits based on their general responsibility for security measures within the electronic communications sectors. Audits can be conducted without any suspicions of misconduct. In addition, providers are obliged to report integrity incidents (*integritetsincidenter*) to PTS. Integrity incidents are incidents that lead to accidental or unlawful loss or change, or unlawful

disclosure of or access to data, both during processing or retention. In general, all incidents should be reported to both PTS and the concerned users. In addition, the providers have to keep a log file on integrity incidents. PTS is currently developing an e-service for the reports.[69]

In **Austria**, in principle, the Data Protection Authority would be the competent authority for audits. However, such audits have not yet taken place.

In the **United Kingdom** the Information Commissioner can conduct audits of any data controller's activities with the controller's consent. Mandatory audits may be carried out in the case of some public sector data controllers although the Information Commissioner has indicated that these will only take place where the controller has first been asked to consent to an audit. The Information Commissioner also has power to conduct audits in respect of the data breach notification requirements introduced under the Privacy and Electronic Communications Directive and Regulations. Audit powers also extend to measures taken by communications service providers to ensure the overall security of their networks. Agencies responsible for activities in respect of the Data Retention Regulations are obliged to report any errors to the Interception of Communications Commissioner. The Commissioner also conducts a rolling programme of inspections of law enforcement agencies and communications service providers and in some cases publishes a report on his findings.

Summary of findings

The Member States surveyed have different approaches with regard to the conducting of audits relating to the correct implementation of the data security principles, namely external with support of private bodies or internal with support of public bodies as DPAs or NRAs. The **Spanish** legislation provides that an internal or external audit shall be carried out at least every two years in order to verify compliance with the security measures that are taken for retained data. In the rest of the surveyed countries the supervisory authority has the right to carry out audits based on their general competencies. The possibility of the national data protection authorities or the NRAs carrying out audits to ensure compliance to the general data protection or electronic communications legislation is not presented in detail in this study (as it is outside of the scope of this study).

3.7 Costs of implementing data security measures

The survey showed that there is no concrete information available about the cost regarding specifically the maintaining and developing of security measures. The information about general costs does not allow for an estimation of what would be the specific financial costs for the providers incurred from the implementation of the data security principles, as foreseen in Article 7 of the Data Retention Directive.

In **Spain**, Section 2 in Annex II of Order PRE/199/2013, provides that the costs arising from the implementation of data retention infrastructure shall be borne by the operator. There are no industry average costs or any estimates. In **Estonia** there are no specific estimates on costs regarding the maintaining and developing of security measures. It is stipulated that the cost of the audit shall be covered by the communications undertaking. According to Subsection 111^1 (10) of the Electronic Communications Act the expenses related to the preserving or processing of data shall not be compensated to communications undertakings, but the costs related to transmission of messages and provision of information shall be compensated to the communications undertaking out of the state budget through the budget of the ministry in the area of government to which the surveillance

[69] Read more in Swedish at http://www.pts.se/sv/Bransch/Internet/Integritet/Regler/Rapportera-integritetsincidenter/ (last accessed 16.07.2013).

agency or security authority belongs, as provided in Subsection 114 (4). Such costs shall be compensated for in accordance with the contract entered into between the surveillance agency or security authority and the communications undertaking. The explanatory memorandum of the Estonian Electronic Communications Act discloses that the costs of appropriate hardware and software used for *transmission of messages* to a central surveillance device, which ensures the preservation of independent log files concerning the actions performed by means of the central surveillance device, and their maintenance are covered from the state budget through the budget of Ministry of Economic Affairs and Communications. The explanatory memorandum gives the following estimates for such reimbursement, only for years 2007 – 2010: 2007 – 10 million EEK (EUR 639,146), 2008 – 15 million EEK (EUR 958,719), according to the state budget strategy of the Ministry of Economic Affairs and Communications, the estimates for these costs for years 2007 – 2010 were 10 million EEK (EUR 639,146) per year.

In **Sweden** there are no specific estimates on costs regarding the security measures but both the Government Bill[70] implementing the Data Retention Directive and a report by the relevant industry organisation contain estimates for the general costs, which include costs on security. In December 2010, the Swedish Government estimated the costs for storage, which included costs for technical and organisational security measures, to amount to around 100 million SEK for the industry. In addition, the costs to identify and store the data were estimated at 100 million SEK for the entire industry, which leads to a total of 200 million SEK. The Government pointed out that many providers already had sufficient security measures in place, which implied less additional cost. In January 2011, the Swedish IT and telecom industries estimated the general costs of data retention to amount to 1140 million SEK for adaptation of the providers' systems and 76 million SEK for the storage of the data. The report did not specify how much refers to costs for security.[71]

In the **United Kingdom**, the explanatory Memorandum attached to the 2009 Regulations[72] indicates that all costs incurred by communications service providers in complying with requests for data made under the Regulations will be met by the government. Costs were estimated at £30.35 million in respect of start up costs with annual operational costs of £2.21 million.

In **Austria**, as the Austrian DLS system represents a technical novelty, there have been no reliable statistics on costs to refer to and the considerations regarding the expected costs are therefore based on assumptions. Sec 102a para 6 TKG 2003 stipulates that small providers, who are not liable for contributions in terms of Sec 34 Komm-Austria-Gesetz (KOG), are not obliged to retain data. KOG defines the 'small providers' and the conditions under which providers are liable for contributions to financing of the telecommunications sector using the result of calculations on the basis of the ratio of the (domestic) revenues incurred by each provider and the total sectorial revenues respectively.[73] All other providers that are not considered "small providers" have to implement the aforementioned storage and security measures. Costs will be reimbursed in the

[70] Prop. 2010/11:46, page 63-64, *Lagringavtrafikuppgifterförbrottsbekämpandeändamål - genomförandeavdirektiv 2006/24/EG*, available in Swedish at http://www.regeringen.se/sb/d/13654/a/157433

[71] Read more in Swedish at http://www.itotelekomforetagen.se/fakta-och-debatt/rapporter_1/kostnader-for-inforandet-av-trafikdatalagringsdirektivet.

[72] Available from < http://www.legislation.gov.uk/uksi/2009/859/contents/made

[73] The Federal Ministry for Transport, Innovation and Technology provides a list of all providers falling under Sec 102 para 6 TKG: http://www.bmvit.gv.at/telekommunikation/Internet/downloads/vorratsdaten.pdf , whereas a list of all providers is available by the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) under https://www.rtr.at/de/tk/ListeAGGTK (the one named in the latter but not in the first are "small providers").

amount of 80% pursuant to Sec 94 para 1 TKG 2003. The details are laid down in a regulation adopted by the Minister of Transport, Innovation and Technology.[74]

In 2011, the Government Bill[75] (explanatory notes) anticipated costs regarding the development of the *storage infrastructure* at some EUR 15 Million (based on surveys addressed to the providers). The running costs were estimated by the Ministry of Justice at EUR 3 Mio a year. These estimates also included the costs for the DLS, amounting to EUR 500,000 (development costs) and EUR 7000 (monthly operating costs). The Federal Minister of Transport, Innovation and Technology issued a regulation containing details as to the compensation of the investment costs.[76]

In **France** there is no information specifically related to the costs of maintaining and developing security measures in relation to the retained data. However, the French regulation provides specific information in relation to the compensation of the extra costs borne by the operators requested by the judicial authorities to provide retained data. According to Article R.10-13-IV of the CPEC, the specific and identifiable extra costs borne by the operators requested by the judiciary authorities to provide data related to the categories mentioned in the present article are compensated according to the terms of Article R213-1 of the Criminal Procedure Code. According to the latter, the rates related to the expenses corresponding to the provision of retained data in accordance with Article L34-1 of the CPEC are fixed in an order of the Minister of Economy, Finances and Industry and Minister for Justice. Such order shall differentiate the rates applicable depending on the category of data and the services requested, taking into consideration, if necessary, the extra costs specific and identifiable borne by the operators requested by the judiciary authorities to provide such data. Article A43-9 of the Criminal Procedure Code provides that the requisitions issued to obtain the production and the provision of data mentioned in Article R.10-13-IV of the CPEC give rise to the reimbursement of the electronic communications operators. They shall present all invoices and appropriate justifications. For each of the services stated in a given requisition, the rates (all taxes excluded) detailed in the schedules attached to such Articles will apply. The abovementioned Article then provides a list of the rates applicable depending on the category of data requested and the services requested to the mobile phone operators and fixed-line operators.[77]

[74] "Überwachungskostenverordnung – ÜKVO, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003507.
[75] http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_01074/index.shtml.
[76] Investitionskostenersatzverordnung – IKEV, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007762.
[77] http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=787679C659070FBD6CE2E20E9E87CD91.tpdjo08v_2?idArticle=LEGIARTI000025580096&cidTexte=LEGITEXT000006071154&dateTexte=20120419.

4 Review of state-of-the-art security measures

In this section we present the analysis of existing technical measures (ETSI TR 102 661) [2] and we analyse the existing published opinions mentioned in Section 2.3.3 and how are they covered by ETSI TR.

4.1 Proposed legal formulations from the perspective of technical protective measures

Directive 2006/24/EC Article 7 formulates requirements for the protection and security of data retained in accordance with this directive.

We recommend modifying the text of item (b) of Article 7 for a better definition of the protective measures. As can be seen in the justification below, such changes will cover more situations with adequate protective measures.

Original text, alignment (b) of DRD *Article 7. Data protection and data security*	Proposed text
"(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction,	*"(b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or **deliberate**(*1) unlawful destruction,*
accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;"	*accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;* ***The technical measures will include encryption and authentication by state-of-the-art cryptographic techniques.** (*2)"*

Justification:

(*1) The technical measures against accidental destruction, loss, alteration ... are very different from the technical measures against deliberate destruction, alteration, etc. Therefore we propose to add "deliberate."

(*2) addition in order to specify a minimum level of appropriate technical measures.

4.2 Analysis of ETSI TR 102 661

This section provides comments and suggestions. It also identifies few contexts in which improvements could be made and as such proposals are made. Overall, the document has a very good structure, and is very readable. Note that the document seems to be mostly concentrated on the secure communication of data, rather than secure storage (& deletion).

Note that when we talk here about authentication, we are referring to "data authentication," i.e. mechanisms that also protect the integrity of the data.

Detailed comments on ETSI TR 102 661 main body

Comments on the cryptographic terminology being used in the ETSI document.

1. The document uses "certificates" as synonyms to "cryptographic keys". For example, on page 7, line -3 and line -5: "if all certificates are revealed to an attacker".
2. Originally, the term "certificate" was used only in relation to public keys. Hence, the phrase "if all certificates are revealed" can be understood by some readers as referring to public-key certificates only. However, the property "forward secrecy", which is discussed here, is related to the situation where an attacker gets access to all public and all (long-term) secret

and private keys. We recommend to stay closer to the definition given in the Handbook of Applied Cryptography[78]:

> Definition 12.16: A protocol is said to have *perfect forward secrecy* if compromise of long-term keys does not compromise past session keys.

3. The document writes that the integrity of data can be protected "by using hashing algorithms," (page 20, line -9, and line -2, page 21, line 4). This formulation could create the impression that digital signatures are added solely to acquire non-repudiations, and that if only integrity protection is required, it suffices to add hashes. Similarly, Page 30, 3rd row of the table: "hashing as SHA-1 or HMAC".
   The integrity of data can be protected by using a MAC algorithm or a digital signature. A MAC algorithm usually offers better performance. There are two popular constructions for MAC algorithms: CBC-MAC and its variants on one side, and HMAC on the other side. CBC-MAC is based on a block cipher. HMAC is based on a hash algorithm, e.g. HMAC-SHA-1 uses the hash algorithm SHA-1 in a special mode to achieve integrity protection.
   We recommend to replace "by using hashing algorithms" by "by using MAC algorithms" and to explain e.g. in Annex D that a MAC algorithm can be based on a hash function. Alternatively, since the concept of authenticated encryption is getting more and more acceptance, it might be better to restructure Section 7.6 and Section 7.7 more fundamentally.

Page 8, line 19: "recognized certificate". Since this concept is not widely known, we recommend to add a clarification and reference.

Page 21, line 11: "The CSP may choose to validate the certificate as well". We recommend writing: "The CSP SHOULD validate the certificate".

Page 24, item k): "Log entries of the log files should be encrypted in a way as for assuring their confidentiality and integrity". Encryption by itself does not assure integrity. We recommend writing: "Log entries of the log files should be encrypted to assure their confidentiality and authenticated to assure their integrity". This recommendation may become obsolete if authenticated encryption is described in Section 7.6 and 7.7.

Page 24, item s): "Encryption and signature keys is recommended to be protected …" This should probably read: "Decryption and signature keys …", since both decryption keys and signature keys need to be kept secret and authenticated, while encryption keys are public keys, which need to be authenticated only.

Page 38, Annex D: we would of course prefer that this annex refers to the report on algorithms and key lengths.

Proposal for new sections to replace Section 7.6 and Section 7.7

Like in the rest of the document, Section 7.7 also states that hash functions can be used to protect integrity, which is not 100% correct. Since the current trend in cryptology is to use authenticated encryption[79] instead of separate encryption and authentication, we propose to merge the texts on

[78] Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, 2001 (fifth edition), available at: http://cacr.uwaterloo.ca/hac/ (last accessed 16.07.2013).

[79] A definition of authenticated encryption can be found in Wikipedia: http://en.wikipedia.org/wiki/Authenticated_encryption

confidentiality and integrity of data (while keeping the text on the system integrity in a separate section).

Below we give a proposal, which is strongly based on the texts from the ETSI report. Note that besides the merge, we also propose changes to the parts of the text dealing with signatures and integrity protection.

"*7.6 Confidentiality and Integrity of Data*

The privacy and integrity of sensitive information for each different LI/DR session should be protected during transmission or storage, by using appropriate cryptographic mechanisms. This can be achieved by using a method for authenticated encryption, or by using separate encryption and authentication methods. In the latter case, special care needs to be taken that no undesirable interactions between the two operations take place.

Only standardized and well-known techniques are recommended to be used, such as the Advanced Encryption Standard (AES) in Galois Counter Mode (GCM). The key length of the related cryptographic keys should provide adequate protection from exhaustive attacks. The related cryptographic keys should be securely managed during their generation, use, storage and destruction.

7.6.1 Confidentiality and integrity of stored data

LI case:

The LI session execution data and the LI-related log data are recommended to be encrypted and authenticated during their storage, either in isolated log servers or within other CSP devices (e.g. the mediation device, the AAA server, the network or data link layer elements, etc.). The secure logging clause (clause 7.10) analyses the measures for fulfilling this security requirement. In effect, only authorized users should be able to see this information in decrypted form. It is recommended that it is made impossible for anyone other than authorized users to have access to decrypted information through the ports of the system. Moreover, the system should assure that the deletion of information is done in a secure way, without prejudice to the auditing activity established in clause 7.10 and according to the deletion requirements that are set in clause 7.11.

DR case:

DR data that are stored within storage devices require high protection in terms of confidentiality and authentication. Hence it is recommended that the DR retained telecommunication data, the DR session execution data and the DR-related log data (for definition analysis see clause 5) that the CSP network produces and stores, are kept encrypted during their entire retention period within storage devices. Moreover, any system that is used for the storage of the DR data should protect the integrity of data (see Annex D). It is recommended that key management procedures are also taken into consideration. Each encryption key should have a retention period equal to the retention period of the stored data that the key is encrypting and then it should be removed together with the corresponding data. Secure removal and deletion of information should follow the requirements described in clause 7.11. General requirements for the LI/DR-related log data, log files and their encryption needs, are given in clause 7.10 while Annex B proposes a solution for secure management of the log events.

7.6.2 Confidentiality and integrity of transmitted data

Internal LI/DR interfaces:

1. *Non-disclosure of generated LI intercepted telecommunication information for each target user (target information): Target information, as this is transmitted by the internal CSP nodes (IRI-IIF and CC-IIF nodes), should not be accessible to unauthorized personnel from any operational management station, via management protocols, Command Line Interfaces (CLI) and traces and dumps, and should not be stored in Non-volatile Memory. If the IRI-IIF or CC-IIF device fails or re-boots, all intercepted related information and states should disappear and should not be accessible by any means (TR 102 528 [i.5]).*
2. *Non-disclosure of IRI and CC: Transmission of data and target information through INI2 and INI3 interfaces should be done in a secure manner. The option for the IRI and CC data to be routed through the network independently of other traffic should be available and should be preferred, so that it is possible to forward traffic over secured network links (TR 102 528 [i.5]).*
3. *DR user data are generated within network nodes and stored as DR retained telecommunication data, within internal CSP network elements. These data should be collected by the DR data collection function in a secure manner. Hence, all DR user data should be routed through the CSP internal network independently of other traffic so that it is possible to forward these data over secured network links.*
4. *Integrity: The INI1 interface that is used by the administration function to provision the IRI-IIF and indirectly the CC-IIF with intercept orders, should perform some short of cryptographic message integrity checking. INI2 and*

INI3 interfaces should also be integrity protected, as should the interfaces used for transmitting the collected DR telecommunication data from the point of their origin towards the storing machines.

5. *Stored data: The LI/DR intercepted telecommunication information should be protected by applying encryption and authentication to the internal communication links. This can be done by means of a combined authenticated encryption method, or by separately encrypting and authenticating the data packets.*

External LI/DR interfaces:

1. *The privacy and the integrity of the transmitted data through the external communication interfaces (HI1, HI2 and HI3 for LI) need to be protected through strong encryption and authentication (at least 128 bits). The recommended technology is to use TLS (RFC 2246 [i.3]) for these interfaces. TS 102 232-1 [i.2].*
2. *The privacy and the integrity of the transmitted data through the external communication interfaces (HIA and HIB for DR) is recommended to be protected through strong encryption and authentication (at least 128 bits). More specifically, for the DR interfaces, security methods such as IPSec or TLS are suggested. These security methods can be defined as connection level security methods.*
3. *The LEA entity (an authorized person sending requests for requesting DR data) ensures data integrity protection by computing an electronic signature over the entire set of fields in the request (including the time stamp). The signed hash and the entity's certificate (validating its public key) are sent in the request to the CSP. The CSP should validate the request by verifying the electronic signature of the LEA. The CSP should validate the certificate as well.*
4. *The CSP entity similarly computes a digital signature over the entire response (including the timestamp) and sends to the LEA the signature and its certificate (validating this public key) with the set of fields.*

7.7 System integrity

The integrity of the LI, DR and Log system software, their updates and patches and any other piece of software installed in the LI or the DR system is recommended to be authenticated by means of a digital signature by its manufacturer. The LI/DR system administrator should verify their integrity by checking the validity of the signature.

All digital signatures related to the integrity, after their verification, are recommended to be logged in an updated log file that will also identify the software installed date and time of installation and the identity of the installers. The produced log information should be securely kept according to the requirements mentioned in clause 7.10.

In case any system action is executed within the LI or DR system without taking into consideration the aforementioned measures, an alarm system should notify the LI/DR system administrator and the operation of the LI or the DR system (with all the planned and in progress LI or DR sessions) should be automatically stopped."

Detailed comments on Annex C

In C.1, replace the last but one sentence by: "In order to eliminate such risks, critical data may be encrypted and authenticated."

The system proposed in C.2 has a number of problems.

Firstly, the text states that data cannot be altered after storage, since key values are unknown. Encryption by itself doesn't protect the authenticity of data. Either the system needs to add a separate authentication step by means of an MAC, or the system needs to use authenticated encryption. The first option is better known to industry, while the second option is getting more and more support and will be recommend by several organizations in the near future.

Secondly, the system proposes a hashing process to protect the privacy of investigated cases. This solution will not work in practice, because of the limited entropy of the input of the hash function. For example, assume that an operator has 100 million customers; then an attacker can hash the 100 million phone numbers and check which outcome matches the hash output that he intercepted. Hence each operator should create an asymmetric key pair to be used by the LEAs to encrypt their queries. The used encryption system should be a randomized encryption system, such that an attacker cannot exhaust all the possible plaintext inputs.

Thirdly, the text should not mention RSA explicitly, since there are other asymmetric encryption systems with better security-speed trade-offs.

4.3 Analysis of opinions in the context of ETSI TR

This section presents the results of the analysis of existing published opinions on the security aspects vs. the ETSI TR report.

Art 29 WP, 00068/10/EN, WP 172, Report 01/2010 [4] on the second joint enforcement action makes several recommendations which **are dealt with in an adequate way by ETSI TR 102 661.**

The recommendations of the DATRET Expert Group report DATRET/EXPGRP (2009) 7 –FINAL – 11 10 2010 [6], from page 10, **are dealt with in an adequate way by ETSI TR 102 661.**

The opinion [5] of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC) and the recommendations of this report **are dealt with in an adequate way by ETSI TR 102 661.**

5 Findings and recommendations

Based on the analysis carried out and described in this document we summarize below the findings and the recommendations.

5.1 Concluding remarks

Based on the survey presented in Section 3, all surveyed countries have implemented Article 7 of the Data Retention Directive. However, Spain and Estonia have transposed only three of the data security principles, not providing explicitly for the destruction of data at the end of the retention period, while Sweden and Austria have introduced higher security requirements for retained data compared with regular data kept by providers of electronic communications. Nevertheless, Austria does not explicitly require that the retained data shall be of the same quality and subject to the same security and protection as those data in the network. Moreover it became obvious from the study that there is no homogeneity in the technical ways in which the storage of retained data takes place. The transfer of retained data to law enforcement authorities has been regulated more extensively by the Member States with regard to the technical specifications that had to be followed, as described also in Section 4. In addition, the survey revealed that the Member States interpret the term "without undue delay" in diverse ways, as some countries do not provide for an explanation of how the term should be interpreted, while others define specific time periods within which the data have to be transmitted to the competent authorities. With regard to the supervisory authority that is designated to monitor the application of the data security principles, the study showed that the Member States have chosen either the Data Protection Authority or the National Regulatory Authority. The Member States surveyed have different approaches with regard to the conducting of audits relating to the correct implementation of the data security principles, namely external with support of private bodies or internal with support of public bodies as DPAs or NRAs.

The study showed that there is no information available about the cost regarding specifically the maintaining and developing of security measures. The information about general costs does not allow for an estimation of what would be the specific financial costs for the providers incurred for the implementation of the data security principles, as foreseen in Article 7 of the Data Retention Directive. Estonia has estimated the costs for appropriate hardware and software used for transmission of messages to a central surveillance device, Sweden has an estimation on the costs for storage, which includes costs for technical and organisational security measures, while the United Kingdom and Austria have made an estimation of the total costs incurred by the providers.

As the cost for creating and maintaining appropriate systems for the storage of the retained data and their transmission to competent authorities is high, it is anticipated that providers will look for outsourcing models for the storage of the retained data, which can potentially take place in third countries outside the EU. In addition, small sized companies may find it financially difficult to implement systems for the storage of retained data and their transmission to competent authorities. At this moment the DRD does not make any differentiation with regard to small-to-medium companies. However, Austria has regulated that small providers, who are not liable for contributions in terms of Sec 34 Komm-Austria-Gesetz - KOG, are not obliged to retain data and consequently are not bound by the obligations arising from the DRD.

Due to the sensitive nature of the data stored and processed in the context of DRD, it would be advisable in the future to complement the legal texts with clear technical guidelines addressing the requirements for data protection. Unfortunately the ETSI TR 102 661 "Security framework in Lawful Interception and Retained Data environment", even if it is comprehensive, was developed after

some of the Member States developed their own specifications, or has been deemed not a preferred choice, such as in the case of Austria.

Even when clear technical specifications are given for the security measures that have to be implemented, it remains necessary **to ensure that the specifications are implemented correctly and updated when required**. This can be achieved by means of regular audits. For example, Spain has foreseen that an internal or external audit shall be carried out at least every two years in order to verify compliance with the security measures that are taken for the retained data. Security audits can be performed by own personnel of the company or by third parties.

We encourage ETSI to review and update the standards referring to the security of data retention systems dedicated to the storage of retained data, as well as on the transfer of the retained data to the competent authorities. ETSI could use the results of ongoing work at ENISA, addressing recommendations in the area of cryptography [11][80], regarding algorithms, key sizes and parameters.

5.2 Recommendations

In case of the Data Retention Directive being revised, we make the following recommendations to European Commission for consideration in the context of the DRD Review process:

- Include clear references to minimum security requirements for personal data protection. State-of-the-art security frameworks have already been developed; changing the security mechanisms is neither easy nor inexpensive, however minimum security requirements should be imposed. For this purpose the ETSI TR 102 661 [2] updated with the proposed changes in this document should be used as a reference[81]; while ENISA's report with recommendations on algorithms, key sizes and parameters should be used as a reference for the cryptographic measures [11].
- It is highly recommended that the following paragraph is included in the legal text: "The technical measures will include encryption and authentication by state-of-the-art cryptographic techniques".
- A clear and realistic threat model should be considered, including also the reference to "deliberate" destruction, loss or alteration, storage, processing, access or disclosure.
- Take into account the recently published measures applicable to the notification of personal data breaches included in the EC regulation (EU) No 611/2013 [10] when specifying the appropriate technical and organisational security protection measures for retained data.
- Taking into account the difficulties of smaller companies in complying with data retention obligations, and considering the possibilities that providers would consider outsourcing models for the storage of the retained data, which can potentially take place in third countries outside the EU, there should be no discrimination regarding the quality of personal data protection but consideration should be taken regarding the costs of implementing the required security measures.
- Take into account the risks inherent in outsourcing the storage of retained data and provide clear rules on whether and, if so, how providers shall be allowed to outsource the storage of retained data.

[80] New ENISA study with recommendations covering cryptographic algorithms and protocols 2013 [11].
[81] At the time this document is finalized, to the best of our knowledge, we assume that ETSI will not review TR 102 661 in the near future; however, we expect ETSI to carry on work in this area.

- Provide clear instructions on the procedures that have to be followed at the end of the retention period, when the data are to be deleted securely. ENISA could support this by preparing guidelines for this purpose.
- Include clear provisions on audits on compliance with the security measures that are taken for the retained data, specifying the time period within which an audit should be carried out and the entity that should be performing the audit (This recommendation is made sharing the opinion of Art 29 WP).
- Harmonise the time period within which the retained data have to be transmitted to the competent authorities.
- Harmonise the sanctions that can be imposed when companies do not comply with the data security principles.

6 Annex I

National correspondents for study on data security principles (Section 3)

COUNTRY	NAME	ORGANISATION
Austria	Max W. Mosing	Gassauer-Fleissner Attorneys At Law
Estonia	Kaupo Lepasepp / Mihkel Miidla	Sorainen law firm
France	Annabelle Richard / Diane Mullenex	Ichay & Mullenex Avocats
Spain	Gabriel Nadal / Isaac Grauer / Carlos Perez	Ecija Abogados
Sweden	Christine Kirchberger	Swedish Law & Informatics Research Institute (IRI)
United Kingdom	Ian Lloyd	Ian Lloyd Legal Services Ltd and University of Southampton

7 Bibliography

[1] European Parliament and the Council of the European Union, "Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC," 2006. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF. [Accessed 16 07 2013].

[2] ETSI, "TR 102 661 Security framework in Lawful Interception and Retained Data environment V1.2.1 (2009-11)," 2009. [Online]. Available: http://www.etsi.org/deliver/etsi_tr/102600_102699/102661/01.02.01_60/tr_102661v010201p.pdf. [Accessed 29 07 2013].

[3] European Commission, "COM(2011) 225, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225," 2011. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PD. [Accessed 16 07 2013].

[4] Article 29 Working Party, "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 ..., WP172," 2010. [Online]. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf. [Accessed 29 07 2013].

[5] EDPS, "Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)," 2011. [Online]. Available: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf.

[6] Data Retention Expert Group, EC DG HOME, "DATRET/EXPGRP (2009) Closer understanding of the term "Data Security" in relation to its application in Directive 2006/24/EC," 2010. [Online]. Available: http://ec.europa.eu/home-affairs/policies/police/docs/DATRET%20EXPGRP%202009%207%20-%20FINAL%20-%2011%2010%202010.pdf. [Accessed 29 07 2013].

[7] European Parliament and the Council of the European Union, "Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 1995. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. [Accessed 16 07 2013].

[8] European Commission, "Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012)," 25 01 2012. [Online]. Available: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. [Accessed 16 07 2013].

[9] Council, "Framework Decision 2008/977/JHA of 27 November 2008, on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters," 2008.

[Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF. [Accessed 23 07 2013].

[10] European Commission, "Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications," 26 06 2013. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF. [Accessed 16 07 2013].

[11] ENISA, "Algorithms, Key Size and Parameters Report - 2013 Recommendations - to be avaliable at -," 10 2013. [Online]. Available: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report. [Accessed 6 11 2013].

[12] ENISA, "Study on the Use of Cryptographic Techniques in Europe," 12 2011. [Online]. Available: http://www.enisa.europa.eu/activities/identity-and-trust/library/the-use-of-cryptographic-techniques-in-europe. [Accessed 16 07 2013].

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
info@enisa.europa.eu
www.enisa.europa.eu