enisa
European Network and Information Security Agency

Study on data collection and storage in the EU

[Deliverable – 2012-02-08]

Contributors to this report

Contractor data, if the production of the report has been subcontracted.

Authors:

- Eleni Kosta, Jos Dumortier & Hans Graux of time.lex CVBA

ENISA project management:

- Rodica Tirtea, Demosthenes Ikonomou

Other ENISA staff involved in the project:

- Giorgos Dimitriou, Stefan Schiffner

Agreements or Acknowledgements

The authors would like to thank the respondents to the survey for their collaboration. Their appreciation is also extended to the members of the FP7 ICR project ABC4Trust for their support in this activity and especially Dr. Harald Zwingelberg and Prof. Kai Rannenberg.

About ENISA

The European Network and Information Security Agency (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.

Contact details

For contacting ENISA or for general enquiries on this topic, please use the following details:

- E-mail: sta@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

For questions related to this project, please use the following details:

- E-mail: sta@enisa.europa.eu

Contents

List of Tables and Figures

1 Executive Summary

The overall objective of the *Study on data collection and storage in the EU* is to serve as a starting point for a pan-European view on the rules relating to the collection and storage of personal data in the European Union and on their implementation in Member States legislation. This is realised via the examination of the *principle of minimal disclosure* (which is also known as the data minimisation principle) and the *duration of the storage of personal* data (which is also known as conservation principle). Both these principles are examined as integral parts of the principle of proportionality, which is fundamental in the European privacy and data protection legal framework.

The European Commission's 2010 Digital Agenda has set high the importance of the principle of "privacy by design", along with the issues that need to be examined in order to develop a comprehensive and coherent approach on data protection. Given the clear contrast between the importance of the *privacy by design principle* on the one hand and the reality of *lax data protection practices* with many online service providers on the other hand, the aim of this study is to conduct an analysis of the relevant legal framework of European Member States on the *principle of minimal disclosure* and the *minimum duration of the storage of personal* data.

The study is not intended to go too deep into the details of the legal complexities of the data protection legislation. It rather focuses on a limited number of relevant use cases and tries to find out how the aforementioned principles are expressed in concrete legal or regulatory provisions applicable to these cases, and how they are observed in practice. The examined use cases focus on the registration to online social networking sites, on online ticket booking in the transportation sector and the collection of customer data and retention of traffic data in the telecommunications sector. Via these use cases, the principle of *minimal disclosure* (when collecting personal data) and the principle *of minimal storage period* (when storing data) is operationalized.

In order to realise this goal, this study offers first a *general introduction* to the principle of minimal disclosure and minimal data storage periods, to establish the backdrop against which this study was conducted, and to set out the major questions examined through the study. As a second step the principle of minimal disclosure is examined in relation to the deployment of *eID cards*, as a first practical illustration of how technological design choices can impact the proportionate or disproportionate disclosure of personal data; the Belgian and German eID card projects are provided as illustrations of this topic. Next, the *three case studies* – focusing on social networking, transportation sector and telecommunications sector – are presented. Through these three real life use cases, this study examines how the collection and storage of personal data is realised in practice, and what the current impact on privacy protection is. A short discussion follows on the *current perspectives* relating to the collection and storage of personal data through data anonymisation and the (im)possibility of re-identification, or through the right to be forgotten.

Finally, this study ends with a *concluding section* and the drafting of *recommendations* to support minimal data disclosure and to encourage minimal data storage periods. Although the types of personal data that should be collected and processed for a specific processing operation, as well as their storage period, should be determined on a case-by-case basis,

depending on the context and the circumstances relating to the processing, it would be helpful for data controllers to have some general guidance on how to collect and process personal data. To this end, the study concludes with some recommendations

- to the national Data Protection Authorities that they should provide clear guidelines to data controllers;
- to the Article 29 Data Protection Working Party, the European Data Protection Supervisor and ENISA that they should do the same for specific areas of processing of personal data with pan-European impact;
- to the Data Protection Authorities that they should aim to improve user awareness relating to the rights stemming from the data protection legislation and on the possibilities offered to users by the legal system to exercise these rights, including by complaining in cases of excessive collection and storage of personal data, and
- to the Member States that they should identify and eliminate conflicting regulatory provisions relating to the collection and storage of persona data.

2 Introduction

2.1.1 Objectives and scope of the study

The European Commission in its Digital Agenda for Europe[1], one of the flagship initiatives of the Europe 2020 Strategy, identified and outlined policies and actions in order to maximize the benefits of Information and Communication Technologies (ICT). In this context, specific actions are proposed as part of the modernization of the European personal data protection regulatory framework in order "to make it more coherent and legally certain"[2]. Key Action 4 is specifically dedicated to the "review of the European data protection regulatory framework with a view to enhancing individuals' confidence and strengthening their rights"[3].

The Communication on a comprehensive approach on personal data protection in the European Union has identified the enhancement of the control of the citizens over their personal data as a key objective of the comprehensive approach on data protection in the general frame of the strengthening of the rights of the individuals. In this context, the European Commission committed to examine ways of "strengthening the principle of data minimisation; improving the modalities for the actual exercise of the rights of access, rectification, erasure or blocking of data (e.g., by introducing deadlines for responding to individuals' requests, by allowing the exercise of rights by electronic means or by providing that right of access should be ensured free of charge as a principle); clarifying the so-called 'right to be forgotten', i.e. the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person's consent and when he or she withdraws consent or when the storage period has expired"[4].

The European Commission adopted in January 2012[5] a proposal for a regulation on data protection that will replace the existing Data Protection Directive. The proposal for the new Regulation contains specific provisions relevant to the collection and storage of personal data.

Parallel to these developments at European Commission level, ENISA launched in its 2010 Work Programme a new area of work[6] on **"***Trust and Privacy in the Future Internet*". In its 2011 Work Programme[7], ENISA included a work stream entitled 'ENISA as promoter of privacy

---

[1] *European Commission, A Digital Agenda for Europe, COM(2010)245, 19.05.2010, available at: http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf (last accessed on 04.10.2011).*

[2] *Idem, Other Actions, after Key Actions 6 & 7.*

[3] *Idem, Key Action 4.*

[4] *European Commission, A comprehensive approach on personal data protection in the European Union, Communication COM(2010) 609, 04 November, 2010, p. 9, available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (last accessed on 04.10.2011).*

[5] *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) 11 final, 25 January 2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed on 07.02.2012)*

[6] *ENISA Work Program 2010, available online at: http://www.enisa.europa.eu/media/key-documents/enisa-work-programme-2010 , p. 36 (last accessed on 25.01.2012) .*

[7] *ENISA Work Programme 2011, available online at: http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011 (last accessed on 25.01.2012).*

& trust', with activities on 'Deploying privacy & trust in operational environment' (WPK 3.2 in WP 2011).

In 2010, ENISA conducted a "survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments"[8], and prepared a report on "Privacy, Accountability and Trust – Challenges and Opportunities"[9].[10] The two aforementioned documents revealed that the majority of online service providers surveyed by ENISA collect personal data of users, and almost half of them consider user personal data as a commercial asset. More than half of the surveyed providers were found to be tracking user's behaviour in order to profile them, with a considerable number of them storing tracking records indefinitely.

In all these policy initiatives the "privacy by design principle" plays a prominent role. The "privacy by design" principle is understood as meaning that "privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal".[11] This principle has been promoted as a fundamental tool for ensuring trust and security through the Digital Agenda for Europe: "The right to privacy and to the protection of personal data are fundamental rights in the EU which must be – also online - effectively enforced using the widest range of means: from the wide application of the principle of "Privacy by Design" in the relevant ICT technologies, to dissuasive sanctions wherever necessary."[12]

Recently, the European Commission discussed the "privacy by design" principle in the frame of the upcoming review of the European Data Protection Directive along with the issues that need to be examined in order to develop a "comprehensive and coherent approach guaranteeing that the fundamental right to data protection for individuals is fully respected within the EU and beyond"[13]. The European Commission admitted that "the 'Privacy by Design' principle could play an important role in [ensuring compliance with data protection rules], including in ensuring data security"[14], and announced its intention to examine possibilities for the concrete legislative implementation of the principle.

Given the clear contrast between the importance of the *privacy by design principle* on the one hand and the reality of *lax data protection practices* with online service providers on the other hand, ENISA was prompted to consider conducting an analysis of the relevant legal framework of EU Member States (MS) and has therefore commissioned the present report. In it, the

---

[8] *ENISA, Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments, 31.01.2011, available online at www.enisa.europa.eu/act/it/library/deliverables/survey-pat/at_download/fullReport (last accessed on 04.10.2011).*

[9] *ENISA, Privacy, Accountability and Trust – Challenges and Opportunities, 18.02.2011, available online at: www.enisa.europa.eu/act/it/library/deliverables/pat-study/at_download/fullReport (last accessed on 04.10.2011).*

[10] *Both of these documents were officially published in the beginning of 2011.*

[11] *European Commission, Communication from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions "A Digital Agenda for Europe" COM(2010) 245, 19 May 2010, p. 17 (fn. 21).*

[12] *idem, p. 17.*

[13] *idem, p. 4.*

[14] *European Commission, Communication from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions "A comprehensive approach on personal data protection in the European Union" COM(2010) 609 final, 04 November 2010, p. 12.*

authors examine the *principle of minimal disclosure* (which is also known as the data minimisation principle) and the *duration of the storage of personal* data (which is also known as conservation principle). Both these principles are examined as integral parts of the principle of proportionality, which is fundamental in the European privacy and data protection legal framework. The proportionality principle can be construed in a very broad way and comprises also other aspects relating to the processing of personal data, such as the provision of access to the stored data to specific entities or the further communication of the data to third parties. As an exhaustive examination of the full range of rules that are covered under the proportionality principle would be practically impossible, ENISA chose to focus on the two aforementioned crucial aspects of the proportionality principle, i.e. the principle of minimal disclosure and the duration of the storage of personal data.

The document is not intended to go too deep into the details of the legal complexities of the data protection legislation and it should not result in a general, abstract and high-level explanation of the European regulatory framework on the protection of personal data. It will rather focus on a limited number of relevant use cases and try to find out how the aforementioned principles are expressed in concrete legal or regulatory provisions applicable to these cases, and how they are observed in practice. In this way, the principle of minimal disclosure (when collecting personal data) and the principle of minimal storage period (when storing data) will be operationalized. Therefore the study focuses on a limited number of relevant use cases or scenarios and illustrates how the aforementioned principles are expressed in concrete legal or regulatory provisions applicable to these use cases.

2.1.2 Methodology of the study

In order to collect up-to-date and high quality information from all 27 Member States within the specified timeframe, the team needed access to local expertise, via contact persons who would already be familiar with the intricacies of the problem and its application in practice. To meet this requirement, a methodology was used that has been successfully employed by the team in a number of recent studies carried out for the European Commission and ENISA in the field of ICT policy.

The main characteristics of this methodology are as follows:

- data is collected via an established network of national correspondents (one correspondent per Member State). This guarantees that the final report will be based on a complete collection of country reports including information from *all* Member States;
- initially, one model country report is drafted along with a model questionnaire. Both of these are submitted for feedback and approval by ENISA. Thereafter, the national correspondents are requested to strictly follow the outline of the model report in responding to the questionnaire.

2.1.3 Limitations

The objective of this study is to obtain a practical insight into the current impact of these principles, based on real-life scenarios. We therefore address actual case studies in this

report, with the goal of gaining practical and reasonably representative knowledge on the current policy situation in Europe, but we do not provide a complete view for this area.

2.1.4 Audience

The current study should be a good starting point for a pan-European view on the rules relating to the collection and storage of personal data and the way how they are actually implemented in Member States legislation.

A more general audience can develop understanding of concepts and reach interesting findings, while specialized audiences can find a good starting point for future studies.

2.1.5 Structure of the study

With regard to structure, this document is made up of five major sections:

- General introduction to the principle of minimal disclosure and minimal data storage periods, to establish the backdrop against which this study was conducted, and to set out the major questions examined through the study.
- The principle of minimal disclosure and the deployment of eID cards, as a first practical illustration of how technological design choices can impact the proportionate or disproportionate disclosure of personal data; the Belgian and German eID card projects are provided as illustrations of this topic.
- Case studies: social networking, transportation sector and telecommunications sector. Through these three real life use cases, we will examine to what extent minimal data disclosure principles are observed in practice, and what the current impact on privacy protection is.
- Current perspectives on the implementation of the principle of minimal disclosure through data anonymisation and the (im)possibility of re-identification, or through the right to be forgotten.
- Conclusions and final recommendations to support minimal data disclosure and to encourage minimal data storage periods.

3 Data collection and storage of personal data

3.1 The seven laws of identity and the principle of minimal disclosure

One of the most poignant statements of the principle of minimal disclosure was provided by Kim Cameron, through his frequently quoted seven Laws of Identity.[15] Through these Laws, Cameron specified seven essential rules that explain the successes and failures of digital identity systems. One of these laws is the principle of minimal disclosure, which can be summarised as stipulating that "the solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution"[16]. According to the principle of minimal disclosure, when building a system that employs personal data, it should be taken into account that there is always a risk that the system may be breached, in order to minimise the possible damage arising from an eventual breach.[17] Thus, data minimisation is presented as a design principle that minimises risk to data subjects, and which therefore improves the protection of their privacy.

3.2 Data collection and storage of personal data in the European Union

The Data Protection Directive refers to basic principles for the processing of personal data, commonly known as *data protection principles*. These principles are implemented through obligations that data controllers should comply with in order to protect the data they hold, reflecting both their interests and those of the data subjects.[18] The collection and processing of personal data has to be carried out in compliance to the data protection principles, as they are specified in Article 6 of the Data Protection Directive[19]. In *relation to the principle of minimal disclosure and to the duration of the minimum storage of personal data*, the Data Protection Directive stipulates that personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"[20] and they must be "kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed".[21] In practice these principles implement the concept of the aforementioned *principle of minimal disclosure* in a binding legal text, and they will be referred to interchangeably throughout this report.

In principle, the data controller decides both on the types and amount of data that should be collected, processed and possibly further processed, as well as on the minimum period during which the data can be stored. These decisions will (or should) be based on *the proportionality principle* and after carrying out a 'balance test' between the various interests at stake, for

---

[15] *Cameron Kim, The Laws of Identity, available online at http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (last accessed on 21.06.2011).*
[16] *idem.*
[17] *idem.*
[18] *Walden Ian., "Data Protection", in Reed Chris, Angel John,* Computer Law*, 5th edition, Oxford University Press, 2003, p. 432.*
[19] *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] OJ L281/31.*
[20] *Article 6(1)(c) Data Protection Directive.*
[21] *Article 6(1)(e) Data Protection Directive.*

instance the protection of the individual and the commercial profit of the service provider. At least in theory, the data controller does not have full autonomy in making this decision: the data controller will need to be able to justify why certain data was collected and/or retained for processing, when requested by the relevant Data Protection Authority or by the data subject himself when exercising his rights. If the data controller cannot provide an adequate justification, then the processing of personal data will be in violation of applicable data protection rules, and might therefore result in the liability of the data controller. Thus, the Data Protection Directive provides a theoretical incentive to data controllers to conduct this assessment responsibly.

The importance of the *principles* of data minimisation and of conservation, which are in practice specific aspects of the proportionality principle, has been demonstrated in a recent Eurobarometer survey on the attitudes on data protection and electronic identity in the European Union.[22] According to the survey, 43% of Internet users say they have been asked for more personal information than necessary when they proposed to obtain access to or use an online service and 70% of Europeans are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected. Moreover, 75% of Europeans want to delete personal information on a website whenever they decide to do so.[23] However, the 2010 Annual Report published by the Irish Data Protection Commissioner presents a different picture, by examining the actual complaints registered with the Commissioner (rather than measuring consumer opinion, as the Eurobarometer does). When looking at these complaints, only 0.64% of the total complaints received by the Commissioner refer to the requesting of excessive data, while a greater concern is expressed in relation to the disclosure of personal data, as this represented the third highest category of complaint – making up 10.47% of total complaints.[24] Thus, the stated consumer concern does not appear to be reflected in consumer protest. That actions of individuals not always reflect their privacy concerns (although in a different context, i.e. that of a commercial transaction) was also found in an ENISA study on the economics of privacy[25].

There may be a need in particular cases to specify the principles of data minimisation and of conservation, either in a legal provision, or via an opinion of the Data Protection Authority or in another way, such as via the request for specific authorisation by a competent entity, for instance in order to acquire the authorisation for secondary processing of personal data. In Sweden, for example, the Swedish Data Inspection Board has issued several decisions where companies were ordered to delete or anonymise personal data before the time when they generally used to delete or anonymise them. The Swedish Data Inspection Board published for example specific decisions on the deletion of data by the Postal Office[26], by travel agents[27], in

[22] *Eurobarometer, Attitudes on Data Protection and Electronic Identity in the European Union, Special Eurobarometer 359, available online at http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (last accessed on 16.12.2011).*
[23] *Idem, p. 6.*
[24] *http://www.dataprotection.ie/documents/annualreports/2010AR.pdf (last accessed on 18.12.2011).*
[25] *ENISA, Study on Monetizing Privacy. An Economic Model for Pricing Personal Information, To be publish at on 2012 on ENISA web page: http://www.enisa.europa.eu/act/it/library .*
[26] *http://www.datainspektionen.se/press/nyhetsarkiv/2008/posten-lagrar-personuppgifter-onodigt-lange/ (last accessed on 16.12.2011).*
[27] *http://www.datainspektionen.se/press/nyhetsarkiv/2009/charterbolagen-lagrar-kunduppgifter-och-resehistorik-for-lange (last accessed on 16.12.2011).*

the context of video surveillance in grocery stores[28]. The Swedish Data Inspection Board has also published a decision on the storage of customer data by the Swedish train company SJ, which is analysed in detail below in section 5.2.

Indications on acceptable storage periods are sometimes also provided through indirectly related legislation. According to the Dutch Act on Personal Data Protection[29], any automated processing of personal data has to be notified to the Dutch Data Protection Authority. As notifying every automated processing of personal data would be excessive at times, the Dutch legislator provided for various exemptions from the notification obligation. To this end, the so-called Exemption Decree[30] lays down certain categories of data processing which are unlikely to infringe the fundamental rights and freedoms of the data subject and which are therefore exempted from the notification requirement referred to in the Data Protection Act. This Exemption Decree provides an indication of a reasonable storage period for certain personal data. For instance data of customers and suppliers and entities that have a similar role, such as retailers and their standard clients, libraries and readers etc must be deleted two years after the carrying out of the relevant transaction.[31]

3.3 Data collection and storage of personal data beyond the EU

As the collection and storage of personal data is an issue that goes beyond the borders of the European Union, this section will focus on these issues in three countries, the U.S.A., Canada and Australia, , which are useful for conducting legal and policy comparative analysis. The study of the U.S.A. was chosen, as the U.S.A. is a country of economic importance as a trade partner of Europe and as the primary country in which innovative ICT services involving the processing of personal data (including data of European citizens) are established. Canada is highly relevant as a country in the same economic sphere as the U.S.A., the legal framework of which is more closely aligned to the European data protection approach. This is also witnessed by the decision of the European Commission that Canada ensures an adequate level of protection of personal data.[32] Finally, Australia is the sole Asian-Pacific country to have received an adequacy decision from the European Commission.[33].

3.3.1 Data collection and storage of personal data in the USA

Privacy and issues relating to the processing of personally identifiable information (PII) in the USA are regulated in a different way compared to the European Union. The collection, use or disclosure of personal data is not governed by a general privacy law, but privacy regulation is rather influenced by market powers and is defined in sectorial laws and through self-regulatory initiatives. In general, the US privacy legislation and the relevant business practices are not based on the principle that companies have to collect as little information as possible,

[28] http://www.datainspektionen.se/Documents/beslut/2011-06-20-lidl.pdf *(last accessed on 16.12.2011).*
[29] *Wet bescherming persoonsgegevens (WBP), 06.07.2000 (O.J. 302/2000); see* http://wetten.overheid.nl/BWBR0011468 *(last accessed on 20.12.2011).*
[30] *Vrijstellingsbesluit WBP,* http://www.cbpweb.nl/hvb_website_1.0/vwc11.htm *(last accessed on 16.12.2011).*
[31] *idem.*
[32] http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm#countries *(last accessed on 25.01.2012).*
[33] http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm#countries *(last accessed on 25.01.2012).*

but sometimes they are based on exactly the opposite logic, that systems should be made in such a way that they collect and process as much information as possible.[34]

Only a few provisions enforcing the minimal disclosure principle exist in the US privacy legislation. The most prominent example of a rule requiring that only personal information that is relevant to the purpose pursued should be processed exists in the US Privacy Act of 1974[35], which regulates how federal government agencies treat citizen personal information. More specifically, Section 552a(e)(1) stipulates that "[e]ach agency that maintains a system of records shall [..] maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency […][36].

Sector specific privacy legislation only exceptionally limits the amounts of personal information that are collected and processed by private entities. Such limitations exist for instance in the Cable TV Privacy Act and the Children's Online Privacy Protection Rule.

The Cable TV Privacy Act[37] provides that "a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned"[38], thus offering the subscriber the full control on the processing of his personal information. The Children's Online Privacy Protection Rule[39] contains section 312.7 entitled 'Prohibition against conditioning a child's participation on collection of personal information', which rules that "[a]n operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity"[40]. Although the Rule does not specify what information can be collected, it requires a proportionality test to be carried out in order to decide whether the requested information is reasonably necessary for the participation of the child in an activity, as described above.

Similar to the lack of a general provision regulating the amount of personal information that can be collected and processed, the US privacy legislation does not in principle restrict the ability of commercial entities to retain personal information of citizens according to their wishes. Although in some instances there is a requirement that data should be kept for a specific period of time, there is not subsequent requirement that these data should be deleted after this period elapses. For instance, the US Communications Act contains a specific provision on the retention period of telephone toll records, as well as on specific types of personal information that can be stored, stating that "[e]ach carrier that offers or bills toll telephone service shall retain for a period of 18 months such records as are necessary to provide the following billing information about telephone toll calls: the name, address, and

---

[34] *Hoofnagle Chris, Country Study B.1 – United States of America, in Korff Douwe, 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, p. 24, 2010 available online at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf (last accessed on 25.01.2012).*

[35] *Public law no 93-579, 5 USC §552a.*

[36] *Public law no 93-579, 5 USC §552a(e)(1).*

[37] *47 USC §551.*

[38] *47 USC §551(b)(1).*

[39] *16 CFR Part 312.*

[40] *16 CFR Part 312.7.*

telephone number of the caller, telephone number called, date, time and length of the call […]"[41]. However, it does not require the deletion of the data after the 18-month period.

Nevertheless, there are a few legal provisions in the US privacy legislation that actually provide for the deletion of personal information after a given period of time. One prominent example can be found in the Cable TV Privacy Act that contains a specific provision on the destruction of personally identifiable information by the cable operator: "A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information […]"[42]. Another example can be found in the US Video Privacy Protection Act of 1988, which was adopted as a reaction to the disclosure in a newspaper of the video rental records of Mr Robert Bork, who was nominated as candidate for the Supreme Court. The Act contains a specific provision on the destruction of old records requiring that personally identifiable information should be destroyed "as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information […]"[43]. The Fair Credit Reporting Act does not allow consumer reporting agencies to make any consumer report containing specific consumer information after a period of seven years.[44] However the is no actual obligation for them to delete the data, which they usually not do in practice.[45]

In general, the US privacy legislation does not contain a general rule limiting potential excessive collection and storage of personally identifiable information from private entities. Sector specific legislation exists in specific areas implementing the principle of minimal disclosure, as in the case of Cable TV Privacy Act and the Children's Online Privacy Protection Rule, as well as regulating the maximum storage period of personal information, as for instance in the Cable TV Privacy Act and the US Video Privacy Protection Act of 1988. The provisions remain however exceptional and do not set a general rule towards the protection of the privacy of individuals.

3.3.2 Data collection and storage of personal data in Canada

Privacy legislation at federal level in Canada is encompassed in two pieces of privacy legislation, the Privacy Act[46] and the Personal Information Protection and Electronic Documents Act (PIPEDA)[47]. The Canadian Privacy Act applies to government institutions and regulates the collection and processing of personal information[48] of individuals by these

[41] *47 CFR §42.6.*
[42] *47 USC §551(e).*
[43] *18 USC § 2710(e).*
[44] *15 USC § 1681c(a).*
[45] *Hoofnagle Chris, Country Study B.1 – United States of America, in Korff Douwe, 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, 2010, p. 29, available online at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf (last accessed on 25.01.2012).*
[46] *R.S.C., 1985, c. P-21.*
[47] *S.C. 2000, c. 5.*
[48] *The term personal information is defined in a different way in the two Acts, yet with no big differences in its substance: The Privacy Act includes a list of examples of information that could be considered as personal and defines personal information as*

institutions.[49] The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) establishes rules for private sector organisations on "the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances"[50]. Both Acts contain rules on the collection and storage of personal information, which will be presented below.

With regard to the collection of personal information, the Canadian Privacy Act establishes the rule that government institutions shall not collect personal information "unless it relates directly to an operating program or activity of the institution".[51] Similarly the Canadian Personal Information Protection and Electronic Documents Act allows organisations to collect, use or disclose personal information "only for purposes that a reasonable person would consider appropriate in the circumstances"[52]. Schedule 1 of PIPEDA contains a number of principles set out in the national standard of Canada entitled 'Model code for the protection of personal information'[53]. Clause 4.4 contains the limiting collection principle, which requires organisations to collect only personal information that is necessary for the purposes identified by them. Clause 4.4.1 specified that both the type and the amount of collected personal information should be limited to what is necessary for the fulfilment of the identified purpose. The types of information collected should be specified in the information-handling policies and practices of the organisations.[54] The rules contained in PIPEDA bear great resemblance to the data minimisation principle, as contained in the European Data Protection Directive.

With regard to the storage of personal information, the Canadian Privacy Act contains the general rule that "[p]ersonal information that has been used by a government institution for an administrative purpose shall be retained by the institution for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it

---

"information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing, (a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual, (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations, (f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual […]" (Art. 3). In the frame of the Personal Information Protection and Electronic Documents Act, personal information is defined in a more concise way as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization" (Art. 2).

[49] *Article 2 Canadian Privacy Act.*

[50] *Article 3 Canadian Personal Information Protection and Electronic Documents Act.*

[51] *Article 4 Canadian Privacy Act.*

[52] *Article 5(3) Canadian Personal Information Protection and Electronic Documents Act.*

[53] *CAN/CSA-Q830-96.*

[54] *Clause 4.4.1 Schedule 1 Canadian Personal Information Protection and Electronic Documents Act.*

relates has a reasonable opportunity to obtain access to the information"[55]. In general government institutions shall "dispose of personal information under the control of the institution in accordance with the regulations and in accordance with any directives or guidelines issued by the designated minister in relation to the disposal of that information"[56]. The Privacy Regulations, which are an Annex to the Privacy Act, specify further the rules on the storage of personal information. A government institution that has used personal information for an administrative purpose has to retain it for "**at least two years** following the last time the personal information was used for an administrative purpose unless the individual consents to its disposal […] and where a request for access to the information has been received, [the institution has to retain the information] until such time as the individual has had the opportunity to exercise all his rights under the Act"[57] (emphasis added). When a request for access to personal information has been submitted by an individual, then a copy of every request received and a record of any information disclosed based on that request shall be retained for **at least two years** from the date when the request was received by the institution.[58]

The fifth principle of Schedule 1 of PIPEDA focuses on the limitation on the use, disclosure and retention of personal information. Personal information shall be retained only as long as necessary for the fulfilment of the purposes for which they were collected.[59] The organisations should set out guidelines and implement specific procedures relating to the retention of personal information specifying the minimum and maximum retention periods.[60] However, when an organisation has personal information, to which individuals may make a request for access, it has to retain the information for as long as necessary in order to allow the individual to make use of any rights he has.[61] When the personal information is no longer required for the fulfilment of the identified purposes, it should be destroyed, erased, or made anonymous. Relevant guidelines and implementation procedures should be developed by organisations on the destruction of personal information.[62]

The federal privacy legislation in Canada safeguards a high level of protection of the individuals with regard to the collection, use and disclosure of personal information both by government organisation and by private ones. The rules of the PIPEDA safeguard the same level of protection as the European Data Protection Directive in relation to the collection and storage of personal data and the rules contained in the two documents are comparable. In order to safeguard the respect of these principles (on the collection limitation and on the retention and destruction of personal information) PIPEDA requires that organisations should develop guidelines and should also implement specific procedures on these issues, so that their practices can be easily auditable and that the individuals are sufficiently informed.

[55] *Article 6(1) Canadian Privacy Act.*
[56] *Article 6(3) Canadian Privacy Act.*
[57] *Article 4(1) Canadian Privacy Regulations.*
[58] *Article 7 Canadian Privacy Regulations.*
[59] *Clause 4.5 Schedule 1 Canadian Personal Information Protection and Electronic Documents Act.*
[60] *Clause 4.5.2 Schedule 1 Canadian Personal Information Protection and Electronic Documents Act.*
[61] *Article 8(8) Canadian Personal Information Protection and Electronic Documents Act.*
[62] *Clause 4.5.3 Schedule 1 Canadian Personal Information Protection and Electronic Documents Act.*

3.3.3 Data collection and storage of personal data in Australia

The privacy regulation in Australia is regulated via the Federal Privacy Act 1988, as well as via eight state and territory privacy laws.[63] The Federal Privacy Act[64] contains a list of information privacy principles that bear great resemblance to the data protection principles that are included in the European Data Protection Directive.

The first information privacy principle of the Australian Privacy Act 1988 'Manner and purpose of personal information' established the rule of data minimisation stating that "Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless […] (b) the collection of the information is necessary for or directly related to that purpose. […]".[65] The personal information[66] that is collected has thus to be relevant to the purposes for which the processing is taking place and this principle is in practice enacting the principle of minimal disclosure.

The Information Privacy Principles of the Australian Privacy Act 1988 do not contain any specific provision requiring the deletion of personal data when they are no longer necessary for the purpose for which they were collected. However, Section 18F contains a specific rule on the deletion of information from credit information files, requiring that "A credit reporting agency must delete from an individual's credit information file maintained by the credit reporting agency [specific types of] personal information […] within 1 month after the end of the maximum permissible period for the keeping of personal information of that kind."[67]

[63] *Australian Capital Territory, Northern Territory, New South Wales, Queensland, South Australia, Tasmania, Victoria and Western Australia.*
[64] *http://www.comlaw.gov.au/Series/C2004A03712 (last accessed on 24.01.2012).*
[65] *Section 14, Principle 1 Australian Privacy Act 1988.*
[66] *Section 6 Australian Privacy Act 1988 defines personal information as "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion".*
[67] *Section 18F(1) Australian Privacy Act 1988.*

4 Data collection and storage of personal data in relation to the deployment of eID cards

An illustrative example of how the principle of minimal disclosure is applied in practice in a diverging way is the deployment of the electronic identity (eID) card in various European Member States and the different approaches that have been adopted. Below, the Belgian and the German eID card will be examined under the light of the data they reveal when the citizen makes use of his eID card.

4.1 The Belgian eID card

The Belgian eID card holds three private keys[68], information about the eID card (SHA-1 hash of citizen photo, eID card chip number, card number, the card's validity begin and end date, card delivery municipality and document type), the address of the citizen, as well as a number of personal data of the card holder: the identity file contains the first and last name of the citizen, their gender, national registry number, nationality, location of birth, noble status, special status.[69] It should be noted that the National Registry Number acts as a single unique identifier within the Belgian governmental system and it is used by all governmental agencies to identify the citizens, with only a few exceptions.[70]

The Belgian eID card traditionally belongs to the first generation of eIDs and has implemented an "all or nothing" model. This means that the citizen, when he/she wishes to use his/her eID card, has to disclose all the personal data that are stored in his card and does not have the opportunity to choose which types of personal data he/she would like to disclose. Moreover, there are no special access control mechanisms in place to protect unauthorised reading of the information that is stored in the address and identity files. This means that anybody who get physical access to the card can read all the information using standard software tools that are provided by the government.[71] It should be clarified that only if the identity file is read from the eID card, or if the eID card is used to sign or authenticate information, the receiver of the identity file or authentication certificate or non-repudiation certificate gets evidence on the gender and birth date of the cardholder.[72]

In Belgium, more precise rules on the practical application of the principle of minimal disclosure have been developed in the context of eGovernment, for example with regard to the processing of data extracted from the National Register. Any access to the National Register, in the sense of any "network connection" established using the National Registry Number, which is also stored in the Belgian eID card, has to receive prior authorisation from

---

[68] *The first (basic) private key is used for the management of the card and is used in order to provide proof to external applications regarding the authenticity of the card. The second key is used to identify/authenticate the card holder, while the third key is used for the production of qualified electronic signatures.*

[69] *Van Alsenoy Brendan & De Cock Danny, Due processing of personal data in eGovernment? A case study of the Belgian electronic identity card, Datenschutz und Datensicherheit 3/2008, p. 178.*

[70] *Coudert Fanny, Kindt Els and Van Alsenoy Brendan (2011) Contribution to the Review and update of country Chapter 'Kingdom of Belgium', in Privacy International, the Electronic Privacy Information Center (EPIC), available online at https://www.privacyinternational.org/article/belgium-privacy-profile (last accessed 05.10.2011).*

[71] *Van Alsenoy Brendan & De Cock Danny, Due processing of personal data in eGovernment? A case study of the Belgian electronic identity card, Datenschutz und Datensicherheit 3/2008, p. 178 (179).*

[72] *Clarification provided verbally by Dr. Danny De Cock.*

the Belgian Privacy Commission.[73] Similarly, the use of the number itself (even in isolation of the National Register) by private sector parties is not permitted without specific authorisations, for data protection reasons: a generic use of the identification number would make it unacceptably easy to link databases of Belgian citizens together. This leads to a somewhat counterintuitive situation: the National Register Number is not technologically protected against access and even provided by default with any use of the eID card, due to the "all or nothing" model. However, its subsequent use by the recipient is not permitted unless he/she has an appropriate authorisation. The Belgian eID card is thus an example of an identification solution where the existing strict privacy protection rules have not been reflected in design choices, thus facilitating the needless disclosure of personal data.

4.2 The German eID card

In comparison to the Belgian eID card, the German eID project is significantly more recent, and its design more closely reflects the current state of the art with respect to data protection. Germany started issuing eID cards since the 1st of November 2010. The card is equipped with a contactless chip which allows the card to be used for eGovernment purposes, as well as for the production of qualified electronic signatures.[74] The eID card contains in principle the personal data of the citizen that are also visible on the card, such as the name, last name, doctor title, address, data of birth, place of birth etc.[75] The German eID card has been built respecting the principle of minimal disclosure and the system allows the user to select the data fields of the eID card to which access will be granted.[76] The data that can be transmitted electronically are the following: first and last name (religious name or stage name and/or doctor title, if applicable), date and place of birth, address, document type, age verification, residence verification and restricted verification.[77] The last three are specific functions introduced in the card in order to ensure full respect of the principle of minimal disclosure. For instance, the age verification function ensures that when a certain age is required for the delivery of a service, then the service provider will only get verification whether the card holder has reached the required age, without transmitting his/her exact age.[78]

---

[73] *Van Alsenoy Brendan & De Cock Danny, Due processing of personal data in eGovernment? A case study of the Belgian electronic identity card, Datenschutz und Datensicherheit 3/2008, p. 178 (181). More information on the sectoral committee of the National Register can be found at http://www.privacycommission.be/en/sectoral_committees/national_register/ (last accessed on 05.10.2011).*

[74] *Braun Werner, Arendt Dirk, AusweisApp and the eID Service/Server – Online Identification finally more secure, in Norbert Pohlmann, Helmut Reimer, Wolfgang Schneider (Eds.), ISSE 2010 Securing Electronic Business Processes: highlights of the Information Security Solutions Europe 2010 Conference, Viewweg+Teubner Verlag, 2011, p. 374*

[75] *Fromm Jens, Hoepner Petra, The new Greman eID card, in Walter Fumy, Manfred Paeschke (eds.), Handbook of eID Security, Publicis, 2011, p. 154 (155).*

[76] *Margraf Marian, The new German ID card, in Norbert Pohlmann, Helmut Reimer, Wolfgang Schneider (Eds.), ISSE 2010 Securing Electronic Business Processes: highlights of the Information Security Solutions Europe 2010 Conference, Viewweg+Teubner Verlag, 2011, p. 367; Braun Werner, Arendt Dirk, AusweisApp and the eID Service/Server – Online Identification finally more secure, in Norbert Pohlmann, Helmut Reimer, Wolfgang Schneider (Eds.), ISSE 2010 Securing Electronic Business Processes: highlights of the Information Security Solutions Europe 2010 Conference, Viewweg+Teubner Verlag, 2011, p. 374 (376).*

[77] *Fromm Jens, Hoepner Petra, The new Greman eID card, in Walter Fumy, Manfred Paeschke (eds.), Handbook of eID Security, Publicis, 2011, p. 154 (155).*

[78] *idem, p. 156.*

In addition, the use of the eID is allowed based on card-verifiable certificates (CV certificates), which are verified by the contactless chip that is stored on the eID. These certificates contain the name of the institution that owns the certificate and wishes to have access to the eID data, the expiration date of the certificate, as well as fine-grained information about the categories of data that the service provider is allowed to access.[79] These certificates are issued by the Issuing Office of Certificates (*Vergabstelle für Berechtigungsyertifikate* – VfB). The use of the certificates enforces in practice the principle of minimal disclosure as the service provider only gets access to data that are necessary for the purpose he wishes to achieve. For instance "service providers who only need to verify whether a customer is above a certain age, will only obtain access rights to a binary inquiry function exactly for this purpose (age verification)"[80].

4.3 Challenges relating to data collection and the storage of personal data

The principle of data minimisation and the duration of the storage of personal data are laid down in the Data Protection Directive and apply to every collection and processing of personal data. However, the aforementioned examples have illustrated that in particular cases, both in the private and the public sector, there may be a need for specification of these aspects that can be realised in various ways.

Specifically, the examples show that the design choices made when creating identification systems have a strong impact on the allocation of risks and responsibilities. In the Belgian example, the "all-or-nothing" approach means that every use of the eID card results in all personal data of the card holder being shared. This places the responsibility for complying with data protection rules entirely with the recipient of the data, who will need to assess which data he/she actually needs, and for how long he/she will retain it. Inversely, it increases the risk of non-compliance to the card holder, who cannot manage his data in a fine-grained manner, and who will have to accept that any use of the card results in the disclosure of personal data that the recipient may not need, including the relatively sensitive unique identification number. In the more state-of-the-art German example on the other hand, the card holder has more control over his personal data, which reduces both the risk of inappropriate disclosure and the effort of compliance for the data recipient (who will not necessarily need to filter out the unnecessary surplus data). Of course, the German eID project is still relatively recent, and it will thus need to be assessed in the future whether these more fine-grained data control options are realistically usable for card holders: privacy by design is only effective if end users are capable and willing to use the provided design features.

[79] *Margraf Marian, The new German ID card, in Norbert Pohlmann, Helmut Reimer, Wolfgang Schneider (Eds.), ISSE 2010 Securing Electronic Business Processes: highlights of the Information Security Solutions Europe 2010 Conference, Viewweg+Teubner Verlag, 2011, p. 367 (369).*

[80] *idem.*

5 Case studies

5.1 The collection and storage of personal data in social networking: registration to online social networking sites

The emergence of a new generation of participatory and collaborative network technologies that provide individuals with a platform for sophisticated online (or mobile) social interaction is already a reality. Social networking sites count a growing population of users, who share common interests, have common goals or strive for a usable tool to communicate with people they already know or with people that are complete strangers to them. Boyd and Ellison define social network sites as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site"[81]. Social networking sites are very popular among adolescents and young people, but, depending on their focus are also widespread among users of an older age.

The ease with which users reveal personal information in social networking sites, as well as the simultaneous lack of awareness and understanding regarding the threats and dangers lurking in such disclosure of personal information, alarmed International and European agencies, data protection and privacy advisory bodies. The European Network and Information Security Agency (ENISA) published position papers providing information on security issues relating to social networking services and giving recommendations regarding their use[82]. The International Working Group on Data Protection in Telecommunications (IWGDPT) adopted a report and guidance on Social Network Services, commonly known as "Rome Memorandum"[83]. The Working Group made recommendations for regulators, providers of social networking services and users, in an attempt to raise awareness on privacy issues in social networking services. The Rome Memorandum was followed by a Resolution on Privacy Protection in Social Network Services that was adopted by the 30th International Conference of Data Protection and Privacy Commissioners in 2008, which also contained recommendations for users and providers of social networking services[84]. In response to the heated debate on the protection of the privacy of the European users of social networking sites, the Article 29 Data Protection Working Party[85] adopted in June 2009 an opinion on social

---

[81] *Boyd dana & Ellison Nicole, Social Networks Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 2007, article 11.*

[82] *ENISA, Security Issues and Recommendations for Online Social Networks,14.11.2007., available online at http://www.enisa.europa.eu/act/it/past-work-areas/social-networks/security-issues-and-recommendations-for-online-social-networks (last accessed on 25.01.2012).*

[83] *International Working Group on Data Protection in Telecommunications (IWGDPT), Report and guidance on Social Network Services ("Rome Memorandum"),2008.,, available online at http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group (last accessed on 25.01.2012).*

[84] *Data Protection and Privacy Commissioners, Resolution on Privacy Protection in Social Network Services, 30th International Conference of Data Protection ad Privacy Commissioners, October 2008, available online at http://www.lda.brandenburg.de/sixcms/media.php/3509/resolution_social_networks_en.pdf (last accessed on 25.01.2012).*

[85] *Under Article 29 of the Data Protection Directive, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data is established, made up of the Data Protection Commissioners from the Member States together*

networking sites, in which it included, among others, key recommendations on the obligations of providers of social networking sites, so that they comply with the European regulatory framework on the protection of personal data[86].

At the same time, the users of such sites and platforms are usually revealing a lot of personal information already when registering at the social networking site, before even revealing any information to other users. The significance of the collection and processing of personal data by social networking service providers already at the registration phase of the users, has also been confirmed by the Latvian Data State Inspectorate in its 2011 recommendation on "Personal data processing in online social networking sites"[87]. According to the recommendation, the data subjects before registering at any online social networking site should obtain information on several issues, among which whether the information required for registering at the site is not too excessive.[88]

For the needs of this study national correspondents from the twenty-seven European Member States were requested to examine one social networking site that had a specific link to their Member State, such as one where the social networking service provider is established in their Member State, and examine the registration procedure to that site in relation to the principle of data minimisation. Before moving into the analysis of the surveyed social networking sites, we are going to examine the registration procedure followed by two popular social networks, Facebook and Google+, as an initial registration of the practices and challenges encountered on such sites.

5.1.1 Facebook, Google+ and the Safe Harbour Principles

Facebook counts more than 800 million active users[89], while Google recently entered the field of social networking by launching its own platform, Google+, which is currently functioning in beta mode.

As the service providers for these two social networking sites are established in the US, their use presents a specific data protection compliance challenges, due to the fact that personal data of the end users are moved to a destination outside of the EU, and therefore possibly outside of the effective reach of European data protection rules. According to the European Data Protection Directive, the transfer of personal data to a third country is allowed, without prejudice to specific exceptions foreseen in Article 26 of the Directive, when the third country in question ensures an adequate level of protection of the data.[90] Soon after the entering into force of the Data Protection Directive, the privacy and data protection regulatory framework in the United States was assessed by the European Commission as being a somewhat complex fabric of sectoral regulation, at both federal and state level, combined with industry self-

with a representative of the European Commission. The Working Party is independent and acts in an advisory capacity. The Working Party seeks to harmonize the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics.

[86] *Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, WP 163 (12.06.2009).*

[87] *Latvian Data State Inspectorate, Recommendation on "Personal data processing in online social networking sites, available online only in Latvian at http://www.dvi.gov.lv/files/rekomendacija_soc.pdf (last accessed 18.12.2011).*

[88] *Idem.*

[89] *As of 14.12.2011.*

[90] *Article 25 Data Protection Directive.*

regulation.[91] As such, this fabric did not comply with the more all-encompassing requirements of European data protection principles. However, the European Commission recognised that the Safe Harbor Privacy Principles, which are issued by the Department of Commerce of the United States, provide adequate protection for the purposes of personal data transfers from the European Union. [92] Therefore, when U.S. organisation chooses to voluntarily adhere to the Safe Harbor Privacy Principles, the transfers of personal data from the European Union to that organisation are deemed to provide adequate level of protection for the processing of the personal data.[93] Both Facebook[94] and Google[95] have adhered to the US-EU Safe Harbour Privacy Principles, thus allowing the transfer of personal data to their US based sites (i.e. allowing them to process personal data in relation to EU based end users).

The Safe Harbor Privacy Principles are the following: notice, choice, onward transfer, access, security, data integrity and enforcement. The data integrity privacy principle requires that the personal information must be relevant for the purposes for which it is to be used, realising in practice the data minimisation principle. However, none of these principles refers to the obligation of the organisations to delete the data after a specific period of time, when the purpose is completed for which the data were collected. Thus, the data minimisation principle is only present in a very high level and embryonic form.

In order for a user to register with Facebook they have to reveal their first and last name, their e-mail address (and choose a password), their gender and their date of birth. In order to justify the request for the date of birth Facebook informs the users that: *"Facebook requires all users to provide their real date of birth to encourage authenticity and provide only age-appropriate access to content. You will be able to hide this information from your profile if you wish, and its use is governed by the Facebook Privacy Policy"*[96].

However, the registration process of Facebook requires also the gender of the user that is not essentially necessary for the purposes of social networking. The same information could, however, be relevant in the context of another social networking site, aiming for instance at single mothers. Besides the information collected via the registration to the site, Facebook collects, processes and retains for a long period of time much more personal information from the users profiles, their interactions in the site, and their behaviour on other websites. This situation motivated the advocacy group Europe v. Facebook to file 22 privacy related complaints[97] with the Irish Data Protection Commissioner, who carried out an official audit on Facebook[98]. The complaint was filed in Ireland because, according to Facebook's Statement of Rights and Responsibilities, residents outside the United States and Canada enter into a

---

[91] *Article 29 Data Protection Working Party, Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, WP 15 (26.01.1999).*
[92] http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm *(last accessed on 07.02.2012).*
[93] *On the adherence of Facebook to the Safe Harbor Privacy Principles, see Kuczerawy, Aleksandra, "Facebook and its EU users - applicability of the EU data protection law to US based SNS", in M. Bezzi et al. (Eds.): Privacy and Identity, IFIP AICT 320, 2010, pp. 75–85.*
[94] http://www.facebook.com/safeharbor.php *(last accessed on 25.01.2012).*
[95] http://www.google.com/privacy/privacy-policy.html *(last accessed on 25.01.2012).*
[96] *Pop-up window when the user clicks on the question "why do I need to provide my date of birth?" when registering.*
[97] http://europe-v-facebook.org/EN/Complaints/complaints.html *(last accessed on 17.12.2011).*
[98] *The report of the Data Protection Audit of Facebook Ireland was published on the 21st of December 2011 and is available online at* http://dataprotection.ie/viewdoc.asp?DocID=1182&m=f *(last accessed on 07.02.2012).*

contract with Facebook Ireland Ltd.[99] As Facebook Ireland Ltd is a data controller established in Ireland, they are subject to the Irish legislation, and consequently the Irish Data Protection Commissioner has jurisdiction in relation to Facebook Ireland Ltd's use of personal data belonging to data subjects that are not residents or do not have their principal place of business in the USA and Canada. The complaints filed by Europe v. Facebook refer, among others, to the collection and processing of personal data that are excessive to the purposes, as well as to the long (or even indefinite) storage periods of personal data of users and it is claimed to constitute violations of the data minimisation and the conservation principles.

At the same time, intense debates are taking place in Germany concerning social networking sites, such as Facebook or Google+, with regard to the processing of personal data of the users and the storage period of the collected data. The Independent Centre for Privacy Protection (*Unabhängiges Leistungszentrum Datenschutz*-ULD) in Schleswig-Holstein has been very active in enforcing data protection issues, in particular against Facebook.[100]

In order for a user to create a Google+ account, they need to create a general Google account.[101] For this, they need to reveal their first and last name, their birthday and their gender. Their Gmail e-mail address will function as a username. When a user has already a Google account, Google already knows their name, last name and e-mail address. In order to create a Google+ account, they still need to reveal their gender and birthdate, which according to Google will not be visible to others. Similar to the practice of Facebook, Google informs the prospective users of Google+ that: "*When you sign up for Google+, we'll ask you to provide your birthday so that we can provide you with features like age-appropriate settings when you use Google services. If you already have a birthday associated with your Google account, you won't be prompted to enter your birthday*."[102] Optionally, the user is also asked to upload a picture already at the registration phase. Moreover, there is a pre-checked box stating that "Google may use my information to personalize content and ads on non-Google web sites", which the user can uncheck, if they do not wish to receive such information. Several issues are interesting to be noted during the registration to Google+. When the user adds a different name during this registration, their name will automatically be updated in other Google products. Moreover, the user is informed in small letters that their profile and +1's[103] appear publicly in search, on ads, and across the web. Upon clicking on the question mark that is placed next to the aforementioned statement in small letters, the user is redirected to a page that explains what are +1 annotations on the web[104] and where there is a further link on how to delete a +1. After entering all this information, the users are requested

---

[99] *Article 18(1) of Facebook's Statement of Rights and Responsibilities: "If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to "us," "we," and "our" mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate.", available online at http://www.facebook.com/legal/terms (last accessed on 17.12.2011).*

[100] *https://www.datenschutzzentrum.de/facebook/ (last accessed on 25.01.2012).*

[101] *Situation as of December 2011.*

[102] *https://support.google.com/plus/bin/answer.py?hl=en&p=birthday&answer=1350405 (last accessed on 25.01.2012).*

[103] *+1 is a button that can be used for instance when the user wants to recommend pages on the web, Google ads or a Google search result.*

[104] *https://support.google.com/plus/bin/static.py?hl=en&guide=1207011&page=guide.cs&answer=1186915 (last accessed on 25.01.2012).*

to link their Google+ account with their Picasa Web Albums. If they do not accept to this linking, they are not allowed to create a Google+ account.

5.1.2 Surveyed social networking sites and the collection and storage of personal data

Having the example of popular US-based social networking sites in mind, this study similarly examined randomly twenty-seven social networking sites, the providers of which are established or operating in each of the European Union Member States, or which specifically target end users in the Member States. The surveyed social networking sites cover a broad range of focus. The majority of them aim at the communication between friends, (ex-)colleagues and/or (ex-)classmates, and people sharing common interests. Several of them have a very special target audience, ranging from bringing together people with common religious beliefs, people interested in dating or for cross-border workers between two specific European countries. Table 1 provides an overview of the distribution of the surveyed social networking sites based on their target audience.

Friends	Bulgaria Estonia Hungary Latvia Lithuania Netherlands Poland Spain United Kingdom
Ex-school friends, classmates, or colleagues	Czech Republic France Malta
People with common interests	Finland Italy Romania Slovakia Slovenia Sweden
For country nationals, diaspora and people interested in the country	Austria Cyprus Ireland Portugal
Common religious beliefs	Greece
Sharing reviews on local shops, restaurants etc.	Belgium
Cross border workers	Luxembourg
Dating	Denmark
Business and career	Germany

Table 1. Focus of surveyed social networking sites

The data that the user is expected to reveal in order to register to the social networking sites vary significantly. Only three of the surveyed social networking sites (Belgium, Czech Republic and Slovenia) require only the e-mail address of the user. Three other social networking sites (Italy, Cyprus and Luxembourg) require in addition the full name of the user. Seventeen sites ask for the data of birth or the age of the user, while fourteen of them require the user to reveal their gender. In some cases the registration procedure requires an extensive list of personal information of the user, such in the case of a social networking site aiming at the

country nationals (Austria), which requires the first and last name of the user, their e-mail address, their province, gender, date of birth, postal code and city. Similarly three popular social networking site for friends in Bulgaria, Estonia and Poland respectively require besides the e-mail address of the prospective user, their name and last name, their date of birth, gender and location. In the case of the Estonian site, the user is also required to provide a photo.

Similarly a social networking site for young adults who want to network, post pictures, publish blogs and share their views on various issues of interest in Finland requires the same information (name, data of birth, gender, e-mail address, picture), but not their location, while a social networking site for Irish people abroad and in Ireland, as well as a site for friends in Latvia and a site for ex-school friends in Malta, require their full name, e-mail address, date of birth and gender. In these cases the required information and especially the request for the date of birth and the gender, seems excessive and not in line with the data minimisation principle.

On the other hand, when the social networking site is dedicated to a purpose that justifies the collection of specific data, the collection of the data is in line with the data minimisation principle. For instance, a social networking site in Denmark aiming at people interested in dating, requires only the regional residents and the date of birth of the user in order to complete the registration. While the date of birth could be considered as excessive in other contexts, in this case it can be argued that it is relevant to the purpose that is pursued by the social networking site, striving for instance to ensure that no children are allowed to create a profile at such a site. For social networking sites that aim at enhancing contact between ex-classmates or ex-colleagues information is sometimes required at the registration phase on the organisation they worked at or on the school they attended and the time period when this took place (such as in the case of the French surveyed social networking site). In this case it can definitely be argued that there is no need for the user to reveal this information at the time of registration to the site, but they should be allowed to reveal it later when creating their profile.

Social networking sites take different approaches with regard to the data they collect about non-registered users. Six of the surveyed social networking sites do not allow any access to non-registered users, while another six of them they do not collect any data on non-registered users. The rest of the sites collect information about the language preference of the users, their location, their browser or their IP addresses, usually by storing a cookie on the terminal equipment of the users.

The majority of social networking sites do not inform their users about the storage period of their personal data. Usually at most a reference to the general principle that data will be deleted (or anonymised) when they are no longer necessary for the purposes for which they were collected or for which they are further processed. In the personal data policy of its website, one of the surveyed social networking sites (Luxembourg) informed its users that ‘personal data are stored until being deleted’. Only one of the surveyed social networking sites (Lithuania) informed its users clearly on its storage and retention policy: the Lithuanian social networking site aiming at friends, informed its users that the maximum period of

storage of personal data is six months after a user terminates his registration, while the data of inactive users are automatically deleted if they do not use the website for three years.

The Latvian Data State Inspectorate adopted in 2011 a recommendation on "Personal data processing in online social networking sites"[105]. The Data State Inspectorate recommended that data subjects, before registering at any online social networking site, should obtain information on the following issues:

a) who is a service provided, what is the purpose of the service and what are the service provider's policy in relation to protection of privacy;
b) whether the information required for registering at the site is not too excessive;
c) whether there is information on persons who will have access to the user's profile;
d) what are the possibilities to delete personal data from the profile and what is the term for storage of the data;
e) whether the service provider offers a possibility to choose a higher personal data protection level in the social networking site and whether it is explained how to do this.[106]

The respect to the data minimisation and the conservation principles is promoted as essential in the Latvian recommendation for the legitimate collection, processing and storing of personal data in online social networking sites.

5.2 The collection and storage of personal data in the transportation sector: the example of online ticket booking

5.2.1 Online purchasing of tickets

The purchasing of tickets for public or private transportation is an everyday activity that can be carried out by natural persons either online or offline. The procedures established in various Member States for the booking of the ticket, as well as for its actual payment, differ significantly depending on the type of the means of transportation. The national correspondents were asked to describe the purchasing of a ticket online from a private or public transportation company in each of the twenty seven European Member States. The correspondents were urged to preferably analyse a travel agency or a bus or train company, as airline companies are subject to additional requirements relating to the collection of PNR data of their customer (see below section 5.2.4). Seventeen correspondents chose to study a railway company, three a bus company, another three focused on an airline company established in a European Member State, two described the purchasing of a ticket online via a travel agency, one via a ferries company and finally one analysed the purchasing of a ski ticket, operated by the owner of the ski resort. The reason for this last choice is because the major public transportation service providers do not offer an e-ticketing service in the specific country (Slovenia) and the chosen case was deemed as an adequate example of an e-ticketing

[105] *As noted through the Lativan report; the original recommendation is available online only in Latvian at http://www.dvi.gov.lv/files/rekomendacija_soc.pdf (last accessed 18.12.2011).*
[106] *Idem.*

service. All but one surveyed transportation companies offer also alternative ways of purchasing tickets, i.e. by telephone or in person at the offices of the company.

The booking of a ticket online from a transportation company gave the opportunity to examine the obligatory types of personal data of the customers that were collected for the completion of the booking in relation to the principle of data minimisation and to examine whether transportation companies carry out excessive collection of personal data during the booking process. All transportation companies required the first and last name of the passenger and all but one required a valid e-mail address. The e-mail address did not need to belong to the passenger, but could even be the one of the person that realised the purchasing. Sixteen of the surveyed companies require a fixed or mobile phone number, while ten of them ask a postal address.

It is interesting to note that six of the surveyed companies require an identity card or passport number. These companies do not belong to the same category of transportation companies, but they offer various types of tickets online, i.e. railway tickets, bus tickets and ferries tickets. Depending on the surveyed transportation company several other types of data are required for the booking of a ticket online, such as the gender or the title of the passenger, date of birth, nationality etc. Additional information on the passenger is sometimes required in order to justify discounts (for instance age of the passenger for youth or senior ticket). The fragmentation on the types of data that are required by various transportation companies for the booking of a ticket online reveals a challenge for the principle of minimal disclosure. Although the transportation companies may wish to collect as much personal data about their customers as possible, this cannot be justified under the principle of data minimisation which stipulates that only the necessary information should be collected and stored.

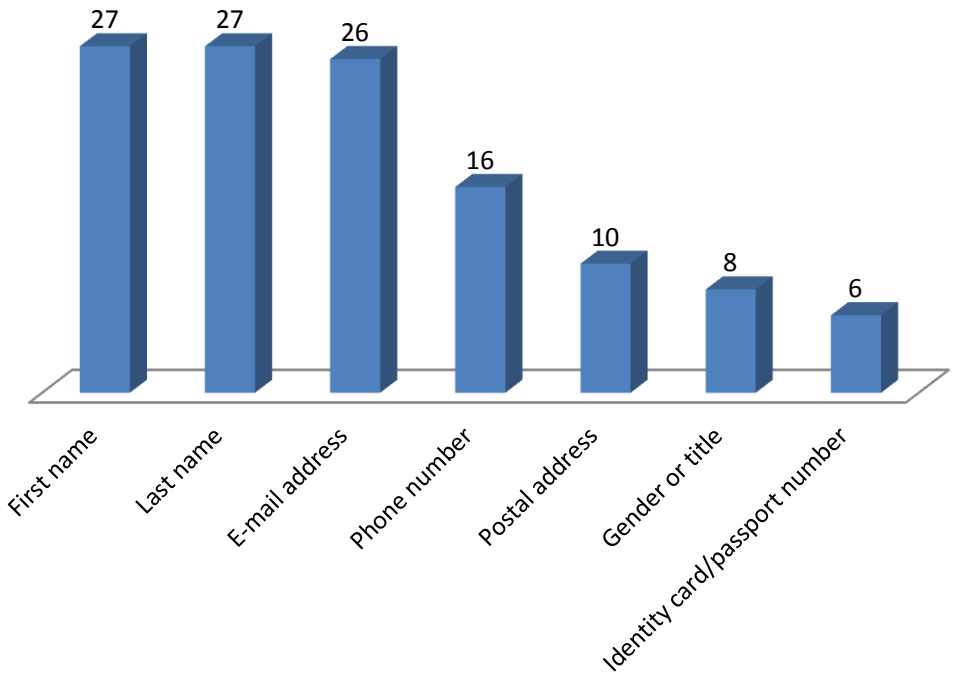

Figure 1. Types of personal data collected when booking the ticket online in 27 MS

The survey that was carried out among the 27 European Member States examined the options that transportation companies (either private or public ones) offer to their customers with regard to the processing of customer data for the sending of information and for marketing purposes. The majority of transportation companies process as a default the personal data of their customers for the sending of information about their products and services as well as for marketing purposes. In several websites there is a tick-box already checked, which the users have to uncheck if they do not wish to receive such information.

In some other cases, the information about the processing of the personal data of the customers is contained in the privacy statement or the Terms and Conditions of the website. The users are given the opportunity to refuse the processing of their information for such purposes via sending an e-mail to a dedicated e-mail address or via configuring the relevant option in their account on the website. In almost one third of the surveyed companies the users are given the opportunity to consent to the processing of their data in order to receive promotions and news of the company or for marketing purposes by ticking a checkbox. In two of the surveyed companies the fact that data can be used for marketing purposed only after the explicit consent of the user, is mentioned in the privacy policy. In these cases, the users have to explicitly give such permissions via their account.

One surveyed company collects personal data from its customers only in order to process purchasing requests and it does not collect data for any other marketing purposes. To the contrary, another surveyed company (Malta), which by default may sell or otherwise communicate the contact details of an individual to third parties for marketing purposes, does not even allow the users to unsubscribe or refuse the processing of their data for specific purposes. Specifically, the privacy notice of the transportation company mentions that “We also reserve the right to send all customers of our service email communications from time to time regarding updates and changes to our goods and services, new links to our website and any technical, administrative or legal notices important to our website, our products and services that we consider essential. **Customers are not able to unsubscribe from these notices**.” (emphasis added). Finally, one of the surveyed companies does not offer any kind of option and does not inform its users with regard to the processing of their data for marketing purposes and for the sending of promotions and news of the company.

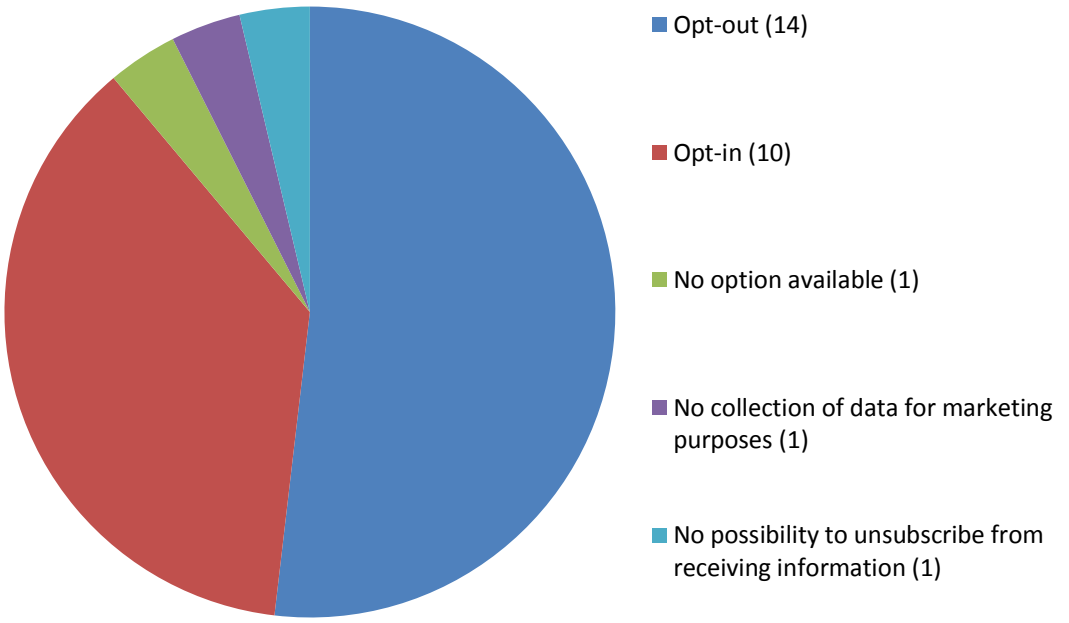

Figure 2. Options offered by transportation companies to customers regarding the sending of information by the company in the future based on the data they collect on them

The lack of specific legislation or policy documents on the collection and storage of personal data in the transportation sector has led to a lack of harmonisation in relation to the storage period of the personal data of the users and the customers. At least four of the surveyed companies (in Greece, Hungary, Romania and Slovakia) did not even have a privacy policy that would inform the users of the types of data that are collected and their storage period, while in the majority of the cases where a privacy policy did exist, the users were informed about the use of cookies on the website, but not about the storage period of their data. In one of the surveyed companies offering online purchasing of bus tickets, the personal data of the passenger, more specifically the first and last name of the passenger, their phone number and birth date, are stored for a maximum period of ten years. It was surprising to note that several of the online transportation companies surveyed did not contain a privacy policy or any kind of document that would inform their users about the processing of their personal data.

The Swedish train company SJ was investigated in 2008 by the Swedish Data Inspection Board as it stored customer data on certain travel cards. SJ was storing personal data on the travel history of the passengers for statistical purposes and for customer complaints. The Swedish Data Inspection Board adopted on 22 December 2008 a decision ordering SJ to anonymise the data relating to travel history 90 days after the departure date at the latest.[107] As highlighted by the Swedish report, in earlier decisions, the DIB had ordered maximum retention periods of 60 days, but in SJ's case the period for customers to reclaim a journey is 3 months, so 90 days were deemed adequate.

[107] *Decision no 711-2008, available in Swedish at http://www.datainspektionen.se/Documents/beslut/2008-12-23-sj.pdf (last accessed 17.12.2011).*

In 2009, the Belgian railway company[108] (Belgium's national railway company) introduced a "ticketless" way of travelling on their railway system, by enabling their customers to link their citizen's National Registry number with the ticket number via their eID card[109]. When travelling, the user will have to show his eID card to the train attendant in order to verify the purchasing of the train ticket. The transfer of personal data in this case is inherently excessive, as the Belgian eID belongs traditionally to the first generation of eIDs and has implemented an "all or nothing" model (see section 4.1 above). This means that the citizen, when he wishes to use his eID, has to disclose all the personal data that are stored in his card and does not have the opportunity to choose which types of personal data he would like to disclose. In this way the citizen reveals an abundance of personal information for the purchasing of the train ticket, which is undoubtedly not necessary for the purpose of purchasing a train ticket and the verification that it has been paid. Such an application puts the respect to the principle of minimal disclosure into question. The Belgian DPA issued a recommendation on transport e-ticketing in 2010, stating that e-ticketing should never allow transportation companies to trace the travel route of individual travellers.[110]

5.2.2 Payment for purchasing on online tickets

The data that are collected either by the transportation company or by an intermediary company that carries out the payment of the ticket are to a large extent common throughout the European Union. For instance for the payment by Visa (or MasterCard or Maestro) the following personal data are required: the card holder's name, the card number, the expiration date of the card and the secure code (CVV2 or CVC2). In Hungary also the name of the bank issuing the card is required.

5.2.3 Electronic ticket cards

The online purchasing of tickets in the transportation sector poses challenges in the way how (and whether) the principle of minimal disclosure is respected in this field. Similar concerns have been raised for the use of electronic travel cards, when purchased online, in which cases the user has to reveal a number of personal information for the purchasing of the card. Users tend to reveal a large number of personal information and leave traces of their location at various time points for the sake of "convenience". The traditional paper ticket used for public means of transportation is gradually being replaced by electronic cards, such as the Oyster card in London or the MoBIB card in Brussels, which allow the user to use the public transportation system in an easy and uninterrupted way. At the same time however, the unique number that is stored on the card allows for the tracking of the location of the user and, when combined with the identification data of the user that may be revealed when the electronic ticket card has been purchased via a credit or debit card, it offers a rich amount of personal information that can be used for user tracking and user profiling. In Denmark, a new national electronic travel card is planned to be launched in 2012. According to information in the press, travellers will have to provide their name, address and e-mail address, but also

[108] http://www.b-rail.be (NMBS/SNCB) (last accessed on 25.01.2012).
[109] http://mobile.b-rail.be/en/Novelties/Use-your-Belgian-e-ID-as-ticket (last accessed on 25.01.2012).
[110] http://www.privacycommission.be/nl/docs/Commission/2010/aanbeveling_01_2010.pdf (last accessed on 25.01.2012).

bank account information and their personal identification number. Travellers will have the possibility to get an anonymous travel card but at a higher cost, which has stimulated a heated debate in Denmark. In this section some prominent examples will be presented and the challenges they pose to the principle of minimal disclosure will be examined.

5.2.3.1 The London Oyster card

The London 'Oyster' card was implemented in 2003 and has been severely criticised over the collection of excessive data of the users, as well as for enabling their tracking and tracing. Transport for London (TfL) collects the following information about the users of the Oyster card: title (Mr/Mrs/Ms/Miss etc), first name, middle initial and surname, address and a password. When a user applies online, their telephone number and email address have to also be supplied. When a user is purchasing the Oyster card using a debit or credit card, the encrypted bank details are stored. When the user is making use of the service for an automatic top-up, then TfL also stores the history of the transactions, including location, date and time. Finally the Oyster ticketing system records the location, date and time an Oyster card was used to validate a journey on TfL's network or on National Rail services where Oyster is accepted.[111] The amount of personal data collected by Transport for London through the Oyster card service has been criticised, especially in relation to children that wish to travel at a discounted rate. They must apply for a photocard ID and provide their name, date of birth, address, school name and telephone number, data that have been deemed as excessive in relation to the purpose of issuing a transportation card, as highlighted in the UK report.

The data are stored for a period of **eight weeks**, a time period that was agreed in consultation with the U.K. Information Commissioner's Office, when the card was first implemented in 2003.[112] The data are then anonymised and are used for research purposes. According to the website of TfL, the Oyster ticketing system is being changed so that it will retain customers' names and contact details for **two years** after the customer last used their card or bought an Oyster product.[113]

The details of debit or credit cards that are used to buy Oyster products are retained for a maximum period of 18 months.[114] When a user is issued a penalty fare notice or is prosecuted for fare evasion, their personal details and relevant journey and transaction history will be retained for a longer period, which is not specified.[115]

According to the UK report, there is an ongoing debate in the United Kingdom about how long TfL should hold the data and to what extent is it acting proportionately when it decides to either comply with data requests from the police or withhold information in order to protect peoples' privacy. This debate has been stimulated by the increasing number of requests for data on Oyster card passenger movements from the Metropolitan Police in connection with criminal investigations.

---

[111] http://www.tfl.gov.uk/termsandconditions/12321.aspx#page-link-what-personal-details-are-held-about-oyster-customers- *(last accessed 05.11.2011).*

[112] *idem.*

[113] *idem.*

[114] *idem.*

[115] http://www.tfl.gov.uk/termsandconditions/12321.aspx#page-link-how-long-does-tfl-keep-oyster-information-- *(last accessed on 05.11.2011).*

5.2.3.2 The Paris Navigo Pass

The adoption of the 'navigo pass' for the Paris region, which is similar to the Oyster card, has been in the centre of similar debates in France. Due to the fact that the user could be banned from the use of the 'navigo pass' in cases of delayed payments, the processing of the personal data of the user in relation to the 'navigo pass' had to be authorised by the French Data Protection Authority, the CNIL. The CNIL issued in 2008 a single authorisation[116] for ticketing systems, which was updated in 2010,[117] covering any kind of data processing in the context of ticketing systems that should comply with a series of guarantees defined by the CNIL. The single license for ticketing systems is directed to those systems that imply the processing of personal data for the following purposes: management, delivery and use of transportation tickets, fraud management, statistical analysis of the use of the network, quality assessment of the functioning of the system. The CNIL specified the types of personal data that should be processed, depending of the type of ticketing, enforcing in this way the principle of data minimisation in the transportation sector.

According to the CNIL authorisation, all customer data are kept for the full duration of the contractual relationship and upon the end of it for two years for commercial and statistical purposes. The validation data that reveal information about the movements of the users, should be anonymised 'shortly'. The anonymisation can take place either by completely removing the card number or the joint date, time and place of the journey, or by applying a cryptographic algorithm (a public 'hash') that is deemed safe to the card number. However, the validation data containing information about the movement of people associated with the card number or subscriber and referring indirectly to the identity of a user, may be retained for forty-eight hours and solely for the fight against technological fraud.

During the 2010 amendments, the CNIL distinguished three types of tickets, depending on the anonymity achieved for the user:
- the nominative ticket, such as the 'navigo pass' in the Paris region,
- the declarative ticket which allows anonymity and cannot be replaced if lost or stolen, and
- the anonymous ticket, which only allows in practice the loading of single tickets.

As noted in the report related to France, some authorities, for financial and practical reasons, do not offer special rates (reduced rates or free) on declarative tickets. The CNIL however considers that software vendors are now developing and maps declarative tickets that would support such solution. The name, first name and photograph of the holder of the pass can be

---

[116] *Single authorisation AU-015 - Decision No. 2011-107 of 28 April 2011 authorizing single implementation of automated processing of personal data relating to the management of ticketing applications by operators and public transport authorities (Autorisation unique n° AU-015 - Délibération n° 2011-107 du 28 avril 2011 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel relatifs à la gestion des applications billettiques par les exploitants et les autorités organisatrices de transport public), available online at http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/136/ (last accessed on 17.12.2011). Single authorisations may be issued by the CNIL in accordance with Article 25II of the French Data Protection Act when the processing of personal data meets a single purpose, relating to categories of the same data and have the same recipients or categories of recipients.*

[117] *In 2010, a working group of the CNIL in collaboration with GART (Grouping of transport authorities) was formed to identify new practices in public transportation (http://www.cnil.fr/dossiers/deplacements-transports/actualites/article/les-systemes-billettiques-evoluent-lautorisation-unique-n15-aussi/, last accessed on 17.12.2011). New practices such as post-payment or access to multiple services with the same media called for additional guidelines, while led the CNIL to amend on 28 April 2011 its single license on three topics: anonymity, media tickets and post-pay.*

scanned on the support (without being integrated into the customer file) and a receipt is issued at the time the ticket is loaded (linking the identity of the holder and number to the declarative password). Such a solution reduces the risk of fraud and helps preserve the anonymity of travel for recipients of social tariffs and the resurfacing of the past in case of loss or theft. The CNIL recommends that special rates are also available on declarative support.

With regard to the principles of data minimisation and data conservation, the amendment to the CNIL authorisation on 'post-payment' is of high importance. Transportation authorities in France are developing public transportation services where the billing is based on the actual journeys conducted and it takes place after the service has been offered. As certain information on the journeys made will be needed for the billing of routes and for the resolving of customer complaints, the CNIL specified that only data that are strictly necessary to calculate the price should be collected. Therefore, the information revealing the place where the ticket has been purchased (the station of validation) is not justified to be processed as it is not necessary for the calculation of the price and it would not be in line with the right of the citizens to come and go anonymously. With regard to the storage period of the processed personal data, the CNIL specified that they may be retained for a period of four months from the date of the events –and not from the moment when the billing takes place. Finally, information on the management of overdue payment should be immediately removed from the black list from the moment the amounts due are paid and by default, within maximum two years from registration.

5.2.3.3 The Brussels MoBIB card

In 2008, the Brussels public transportation company[118], launched the 'MoBIB' card.[119] The MoBIB card is equipped with a Radio Frequency Identification (RFID) chip, on which the name, last name, date of birth and postal code of the user are stored. The information relating to the programme that the user has chosen (10-journeys ticket, 1 day ticket etc) is also stored on the card, along with the information on the last three uses of the card. A photo of the user is also visible on the card.[120]

The Brussels public transportation company claims that the location information of a user is never processed, while such processing only takes place based on encoded or anonymous information. However, the implementation of the MoBIB has been criticised as violating the Belgian legislation on the protection of personal data.[121]

The Belgian Privacy Commission adopted a recommendation in March 2010 in which it pointed out that the direct or indirect processing of personal data of the users in order to trace the route they are following via their electronic ticket is not allowed.[122]

---

[118] http://www.mivb.be (STIB/MIVB) (last accessed on 25.01.2012).

[119] http://www.stib.be/mobib.html?l=en (last accessed on 25.01.2012).

[120] http://www.mivb.be/pointdevue_Standpunt.html?l=nl&news_rid=/STIB-MIVB/INTERNET/ACTUS/2010-05/WEB_Article_1274963883674.xml (last accessed on 05.11.2011).

[121] http://www.brusselnieuws.be/artikel/garandeert-nieuwe-mobib-chipkaart-anonimiteit-van-reiziger http://www.brusselnieuws.be/artikel/liga-mensenrechten-mobib-schendt-het-priv%C3%A9leven (last accessed on 05.11.2011).

[122] Commissie voor de bescherming van de persoonlijke levenssfeer (Belgian Privacy Commission), Aanbeveling nr 01/2010 van 17 maart 2010, Aanbevelling over de na te leven basisbeginselen bij het gebruik van e-ticketing door de openbare

The Brussels public transportation company in the terms of use of the MoBIB card mentions that the data will be stored for limited periods of time that are necessary for the specific processing (that is taking place). No specific storage period is specified.[123] However, the Belgian Privacy Commission in its recommendation 01/2010 has advised that the data that are collected for travel ticket administration should be deleted at the latest after six months.[124] The Belgian Privacy Commission also recommended that the client data of the users should be deleted within 12 months after the last use of the card, or since the time when the customer has returned the card.[125]

5.2.3.4 The Prague 'Opencard'

In 2008 the Prague City Hall launched an electronic card in Prague, called 'Opencard', which can be used for public transportation in Prague, can function as a library card for the municipal Library or as the means for discount programmes, and also includes an application for payment of parking fees.[126] The card can be issued with a monthly, quarterly or annual validity.

For the issuing of an Opencard, a number of personal data of the traveller are processed and stored. The first name, the last name and a photograph of the card holder are printed on the card. According to the Opencard website, these data serve for the verification of the card holder's identity during some operations such as public transport inspections.[127] In addition, the date of birth of the traveller is stored in an encrypted way in the contactless chip of the Opencard. The justification for the processing of this information is that the date of birth is needed when applying for the age-related discount.[128]

Following the introduction and widespread deployment of the Opencard, the Czech Office for Personal Data Protection issued a statement urging the Prague City Hall to offer, besides the traditional Opencard, an anonymous alternative for which no personal data of the traveller need to be processed. The Prague City Hall complied with this request and launched in

---

vervoersmaatschappijen (Recommendation 01/2010 on the fundamental principles that have to be respected during the use of e-ticketing by the public transportation companies) (A-2010-003), 17 March 2010, available online at http://www.privacycommission.be/nl/docs/Commission/2010/aanbeveling_01_2010.pdf (last accessed on 05.11.2011). The Belgian Privacy Commission adopted also in 2009 an Opinion on the application of the Belgian Data Protection Act to the processing of personal data in RFID systems: Commissie voor de bescherming van de persoonlijke levenssfeer (Belgian Privacy Commission), Advies nr 27/2009 van 14 oktober 2009 uit eigen beweging inzake RFID (Opinion 27/2009 relating to RFID) (A/2009/003), 14 October 2009, available online at http://www.privacycommission.be/nl/docs/Commission/2009/advies_27_2009.pdf (last accessed on 05.10.2011).

[123] http://www.stib.be/utilisation_gebruik.html?l=nl *(last accessed on 05.11.2011).*

[124] *Commissie voor de bescherming van de persoonlijke levenssfeer (Belgian Privacy Commission), Aanbeveling nr 01/2010 van 17 maart 2010, Aanbevelling over de na te leven basisbeginselen bij het gebruik van e-ticketing door de openbare vervoersmaatschappijen (Recommendation 01/2010 on the fundamental principles that have to be respected during the use of e-ticketing by the public transportation companies) (A-2010-003), 17 March 2010, p. 5, available online at http://www.privacycommission.be/nl/docs/Commission/2010/aanbeveling_01_2010.pdf (last accessed on 05.11.2011).*

[125] *Commissie voor de bescherming van de persoonlijke levenssfeer (Belgian Privacy Commission), Aanbeveling nr 01/2010 van 17 maart 2010, Aanbevelling over de na te leven basisbeginselen bij het gebruik van e-ticketing door de openbare vervoersmaatschappijen (Recommendation 01/2010 on the fundamental principles that have to be respected during the use of e-ticketing by the public transportation companies) (A-2010-003), 17 March 2010, p. 6, available online at http://www.privacycommission.be/nl/docs/Commission/2010/aanbeveling_01_2010.pdf (last accessed on 05.11.2011).*

[126] http://opencard.praha.eu/jnp/en/home/index.html *(last accessed on 17.12.2011).*

[127] http://opencard.praha.eu/jnp/en/about/security/index.html *(last accessed on 17.12.2011).*

[128] *Idem.*

December 2011 an anonymous Opencard that does not contain any personal data and is transferable. The anonymous travel cards in Prague were introduced in full respect of the data minimisation principle, allowing citizens to exercise their right to come and go anonymously.

5.2.3.5 Dutch OV-chipcard

The OV-chipcard has been recently introduced in the Netherlands, which is a smart card with a built-in chip for public transportation in the Netherlands. There are currently three types of OV-chipcards: the personalised one, which mainly aims at season ticket holders; the disposable cards which can be used for a certain period of time; and the anonymous one. The Dutch Data Protection Commission carried out an investigation with regard to the processing of personal data relating to the use of student OV-chipcards. The Commission found that four companies[129] were storing personal data for a longer period than was necessary. The transportation companies modified the **storage period** of the personal data[130] they were collecting in relation with the student OV-chipcards in order to be in line with the conservation principle and adopted storage periods mainly varying between 18 and 24 months depending on the purposes.[131] The Commission has imposed an order for incremental penalty payments if the companies do not comply with the order.

5.2.4 Airline companies and PNR data

The purchasing of airplane tickets, either online or offline, especially regarding flights to the U.S. (or even Canada or Australia) requires the revealing of a large number of personal information of the user. The transmission and processing of personal data of passengers, as well as their storage period, is extensive in the context of overhaul airplane journeys, especially as regards Passenger Name Record (PNR) data. PNR data[132] is information that is provided by passengers and is collected by carriers for enabling reservations and carrying out the check-in process.[133] The record that is created on each of the passengers contains data, such as the dates of travel and the travel itinerary, ticket information, contact details, address and phone numbers, the travel agent that was involved in the booking of the ticket, payment information, seat number and baggage information.[134]

---

[129] *The Amsterdam-based transportation company GVB, the Rotterdam-based transportation company RET, the transportation company NS and the cards issuer TLS.*

[130] *http://www.cbpweb.nl/Pages/pb_20110726_OV-chip_LOD.aspx (last accessed on 17.12.2011).*

[131] *http://www.cbpweb.nl/downloads_pb/pb_20110726_OV-chip_LOD_TLS.pdf, http://www.cbpweb.nl/downloads_pb/pb_20110726_OV-chip_LOD_NS.pdf, http://www.cbpweb.nl/downloads_pb/pb_20110726_OV-chip_LOD_RET.pdf, http://www.cbpweb.nl/downloads_pb/pb_20110726_OV-chip_LOD_GVB.pdf (last accessed on 25.01.2012).*

[132] *It should be noted that PNR data are different from Advance Passenger Information (API), which has to be communicated by air carriers at the request of the authorities responsible for carrying out checks on persons at external borders (Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L261/24, 06.08.2004). API data are the biographical information taken from the machine-readable part of a passport and contain the name, place of residence, place of birth and nationality of a person.*

[133] *European Commission, Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM(2010) 492, Brussels, 21.09.2010., p. 3, available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0492:FIN:EN:PDF (last accessed on 07.10.2011).*

[134] *Idem. See below Section 5.2.4.1 for the detailed list of PNR data in the context of the EU-US PNR draft agreement.*

The European Union has signed agreements for the transfer of PNR data with the U.S., Canada and Australia. In 2004, the Council of the European Union adopted a Decision concerning the conclusion of an agreement between the European Community and the United States of America on the processing and transfer of passenger name record (PNR)[135] data by air carriers to the United States Bureau of Customs and Border Protection (CBP) and a Decision was also adopted by the European Commission on the adequate protection of those data[136]. The 2004 PNR agreement of the transfer of personal data of passengers between the European Union and the United States Government foresaw that 34 data elements has to be provided to the US Customs Bureau for each passenger. The European Court of Justice in a judgement adopted in 2006[137] annulled the aforementioned decisions.

The Court ruled that the "transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law"[138]. Although the data have been initially collected for commercial purposes, the Court found that the actual purpose of their transfer falls within a framework established by the public authorities that relates to public security and thus the processing falls outside the scope of protection of the data protection directive. The Court followed the argumentation of the General Advocate and distinguished between the activities of collection of data and the purpose of the (further) processing based on public safety needs, in order to exclude the latter from the scope of application of the data protection directive. The Court judgement can be briefly described as admitting that the data collected for commercial purposes fall within the protective ambit of the Data Protection Directive but when the same data are further transferred for public security reasons, they no longer enjoy the same protection. The Judgment of the European Court of Justice created a substantial *lacuna legis* in the protection of PNR data, raising the general problem of protection of personal data that are not covered by the Data Protection Directive[139]. The European Parliament had raised issues relating to the respect to the proportionality principle, although the Court did not consider this issue.

The European Commission recently proposed a Directive of on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (PNR Directive)[140], as well as a Proposal for a Council decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of

---

[135] *Council of the European Union, Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (2004/496/EC), [2004] OJ L183/83.*

[136] *Commission of the European Communities, Commission Decision of 14 May on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection [2004] OJ 235/ 11.*

[137] *Judgment of the Court of Justice in Joined Cases C-317/04 and C-318/04 (30 May 2006), ECR 2006, p. I-4721.*

[138] *Paragraph 56 of the Judgment of the Court of Justice in Joined Cases C-317/04 and C-318/04 (30 May 2006).*

[139] *See also the analysis made by Hielke Hijmans, in HIJMANS Hielke 'De derde pijler in de praktijk: leven met gebreken Over de uitwisseling van informatie tussen lidstaten'. SEW 2006.91, under chapter 4.1.*

[140] *European Commission, Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, Brussels, 02.02.2011.*

Homeland Security.[141] The Article 29 Data Protection Working Party, as well as the European Data Protection Supervisor, have criticised the European Commission initiatives on PNR data with regard to the list of data that have to be transferred, as well as on the storage period of the PNR data.[142]

5.2.4.1 The principle of data minimisation and PNR data

According to the recent proposal for a Council decision on the transfer of PNR data from the European Union to the United States Department of Homeland Security (DHS), an abundance of personal data of all passengers that are flying to and from the European Union have to be collected irrespective of the fact whether they are suspects. According to the Annex to the agreement, the following nineteen types of data would have to be collected by the airlines companies and be transferred to the DHS: (1) PNR record locator code, (2) date of reservation/issue of ticket, (3) date(s) of intended travel, (4) name(s), (5) available frequent flier and benefit information (i.e., free tickets, upgrades, etc.), (6) other names on PNR, including number of travellers on PNR, (7) all available contact information (including originator information), (8) all available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction), (9) travel itinerary for specific PNR, (10) travel agency/travel agent, (11) code share information, (12) split/divided information, (13) travel status of passenger (including confirmations and check-in status), (14) ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote, (15) all baggage information, (16) seat information, including seat number, (17) general remarks including OSI, SSI and SSR information, (18) any collected Advance Passenger Information System (APIS) information, (19) all historical changes to the PNR listed in numbers 1 to 18.

The European Data Protection Supervisor (EDPS) noted that the aforementioned types of data would be collected and stored not only for passengers, but also for prospective passengers who may cancel in their end their trip. The list of data was considered as excessive and

---

[141] *European Commission, Proposal for a Council decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, COM(2011) 807 final, Brussels, 23.11.2011.*

[142] *European Data Protection Supervisor, Opinion of 09.12.2011 on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security; European Data Protection Supervisor, Opinion of 15.07.2011 on the Proposal for a Council Decision on the conclusion of an Agreement between the EU and Australia on the processing and transfer of PNR data by air carriers to the Australian Customs and Border Protection Service; Article 29 Data Protection Working Party, Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, WP181 (05.04.2011); European Data Protection Supervisor, Opinion of 25.03.2011 on the Proposal for a Directive of the European Parliament and of the Council on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime; Article 29 Data Protection Working Party, Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, WP 178 (12.11.2010); European Data Protection Supervisor, Opinion of 19.10.2010 on the global approach to transfers of PNR data to third countries; European Data Protection Supervisor, Opinion of 20.12.2007 on the Proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes; Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, WP138 (17.08.2007); Article 29 Data Protection Working Party, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, WP78 (13.06.2003).*

disproportionate compared to the purposes pursued via the proposed Council decision. The EDPS proposed limiting the data to the following information: "PNR record locator code, date of reservation, date(s) of intended travel, passenger name, other names on PNR, all travel itinerary, identifiers for free tickets, one-way tickets, ticketing field information, ATFQ (Automatic Ticket Fare Quote) data, ticket number, date of ticket issuance, no show history, number of bags, bag tag numbers, go show information, number of bags on each segment, voluntary/involuntary upgrades, historical changes to PNR data with regard to the aforementioned items".[143] As for the processing of sensitive data, the EDPS recommended that airline carriers should not transfer any sensitive data to the DHS.[144]

5.2.4.2 The maximum period of storage and PNR data

According to the proposal for the PNR Directive of 02.02.2011, the PNR data would have to be retained for a period of 30 days in a database at the Passenger Information Unit[145] for a period of 30 days after their transfer to the Passenger Information Unit of the first Member State on whose territory the international flight is landing or departing. Upon expiry of the period of 30 days after the transfer of the PNR data to the aforementioned Passenger Information Unit the data shall be retained, masked out, at the Passenger Information Unit for a further period of five years.[146] The Article 29 Data Protection Working Party considers the retention period of five years as disproportionate.[147]

The European Commission proposal for a Council decision of 23.11.2011 on the transfer of PRN data from the EU to the US DHS foresees even longer storage period for the PNR data. In accordance with Article 8 of the proposal, DHS retains PNR data in an active database for up to five years. The data will be depersonalised and masked after the initial six months of this period, but the passenger will still be able to be identified. After this five-year period, the PRN data will be transferred to a dormant database for a period of up to ten years. According to the European Data Protection Supervisor, and similar to the position taken by the Article 29 Data Protection Working Party, the maximum retention period of fifteen years that is foreseen in the Proposal is disproportionate and excessive. Rather a retention period of six months is recommended.[148] The position of the EDPS requiring for a retention period of six months instead of the period of fifteen years that is currently proposed illustrates a significant challenge on defining what the appropriate storage and retention period would be for specific types of data. The general data protection principle on the conservation of data stipulating

---

[143] *European Data Protection Supervisor, Opinion of 09.12.2011 on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, p. 5.*

[144] *Idem.*

[145] *A Passenger Information Unit is a single designated unit that should be created in each Member State and will be responsible for handling and protecting the data (if the PNR Directive is adopted).*

[146] *Article 9 of the proposal for a PNR Directive.*

[147] *Article 29 Data Protection Working Party, Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, WP 181 (05.04.2011), p. 6.*

[148] *"The data should therefore be anonymised (irreversibly) or deleted immediately after analysis or after a maximum of 6 months": European Data Protection Supervisor, Opinion of 09.12.2011 on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, p. 5.*

that personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed"[149] allows room for broad interpretation.

5.3 The collection and storage of personal data in the telecommunications sector: collection of customer data and retention of traffic data

Telecommunications companies collect several personal data of their customers during the purchasing of their products, which today can also be realised online. For this third case study, the national correspondents were requested to examine the types of data that are collected by a telecommunications provider when purchasing a product online, as well as to specify the retention practices of the provider for the processing of traffic data. The national correspondents were requested to focus on one of the internet service providers, choosing preferably one that is operating only in their country.

5.3.1 Collection of customer data during registration

The national correspondents were first asked to examine the types of identification data of customers when they are registering online for the purchasing of a product by an internet service provider. One of the surveyed countries does not offer the possibility of buying internet packages online, and therefore was materially unable to provide inputs. The remaining 26 Member States will be examined in the section below.

The analysis of the survey illustrated that in principle seven types of personal data are obligatorily collected when the user is registering online for the purchasing of a product from an internet service provider: full name, e-mail address, phone, address, date of birth, gender and national identification number (depending on the country it can be a social security number, personal identification code, tax registration number etc.). Additional information regarding the installation or delivery address is requested when physical installation or delivery of equipment is required.

It is interesting to see how these data are combined, as illustrated in Table 2. Eight of the surveyed companies require only the full name, the e-mail address and the phone number of the person making the order. Three other companies contain in addition also an obligatory field for the indication of an address. The address of the person making the order is usually required in order to verify that the requested service package can be offered at a specific location. Nine of the surveyed companies collect the national identification number of the prospective customer, while five ask for their date of birth. Finally, three of the companies collect the gender of the customer. It is difficult to justify the collection of national identification number, the date of birth and also the gender of the customer in respect to the data minimisation principle. The fact that some companies are able to carry out the execution of the order by collecting only the name, the e-mail address and the phone number or the address of the customer can be seen as sufficient justification that the collection of any further information should be seen excessive in relation to the data minimisation principle.

[149] *Article 6(e) Data Protection Directive.*

Internet service provider established in country	Obligatory personal data requested when purchasing a product online
Belgium Denmark Hungary Latvia Lithuania Malta Poland Slovakia	Full name E-mail address Phone number
France Ireland Luxembourg	Full name E-mail address Address Phone number
Bulgaria Greece Romania	Full name E-mail address Phone number National identification number
Austria Czech Republic	Full name E-mail Address Phone number Date of birth
Finland Poland	Full name Phone number National identification number
Spain Sweden	Full name Address Phone number National identification number
Estonia	Full name Address National identification number Language preference
Germany	Full name E-mail address Telephone number Date of birth
United Kingdom	Full name E-mail address Address Date of birth Gender
Netherlands	Full name E-mail address Address Telephone number Gender
Italy	Full name E-mail address Phone number National identification number Date of birth Gender
Slovenia[150]	Full name E-mail Address

Table 2. Obligatory personal data requested when purchasing a product online by an internet service provider

The online registration process carried out by surveyed Estonian operator entails secure identification of the customer by using an electronic identity card, a mobile identity or banklinks[151]. In Spain, the company Telefonica offers the possibility to the users to register

[150] *According to the Slovenian national correspondent for this study, none of the major Slovene registered operators offers the possibility of an online purchase of an internet, telephony or television package. The surveyed case study was based on the closest example of such practise: the scope of service, provided by the a Slovenian operator was the preparation of an non-binding offer, based on an online registered request.*

[151] *Banklinks is a service that allows immediate and secure payment for goods bought on the internet in Estonia.*

using their electronic identity card. In Sweden, when the user enters the personal identity number, then their full name is automatically filled out.

5.3.2 Storage of personal data by telecommunication operators

According to Article 6(2) ePrivacy Directive[152] traffic data may be retained when they are necessary for billing purposes only up to the end of the period during which the bill may be lawfully challenged or payment pursued. The ePrivacy Directive does not specify the exact period, during which the bill may be challenged or further retained. The Article 29 Data Protection Working Party specified this storage period, suggesting that a "routine storage period for billing [should have the duration of] maximum 3-6 months, with the exception of particular cases of dispute where the data may be processed for a longer period. In addition, only traffic data that are adequate, relevant and non-excessive for billing and interconnection purposes may be processed. Other traffic data must be deleted"[153]. The Article 29 Data Protection Working Party in its opinion specified the maximum time period for the storage of traffic data for billing purposes and at the same time reminded that the principle of minimal disclosure is closely linked to it and should be respected. The Member States have adopted varying practices with regard to the implementation of this storage obligation (see Table 3). The majority of the Member States have literally transposed the provision of the ePrivacy Directive and allow the processing of traffic data necessary for the purpose billing and interconnection payments only up to the end of the period during which the bill may lawfully be challenged or payment pursued, without specifying in their national law how long this period would be.

Providers of publicly available electronic communications services may also process traffic data for the purpose of marketing electronic communications services, as well as for the provision of value-added services, to the extent and for the duration that this is necessary for the service or marketing. This is allowed, provided that the subscriber or the user to whom the data relate has given his consent to the processing of traffic data, which may be withdrawn at any time. The consent has to be 'prior', meaning that it has to be given before the collection and processing of data by the provider for these purposes. Otherwise the data should be anonymised. The German Courts have explicitly ruled that the given consent is not indefinitely valid. The District Court (*Landgericht* - LG) of Berlin ruled for instance that the sending of a commercial e-mail two years after the consent was given could not be based on that consent, as there was no communication between the sender and the recipient during that time[154]. The e-mail address of that individual should have been removed from the company's database.

In the frame of the third case study, the national correspondents were asked to provide information with regard to the processing of traffic data, depending on the purposes they are collected and processed, as described above. The majority of the Member States have literally

---

[152] *European Parliament & the Council of the European Union, Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37, as modified by Directive 2009/136/EC.*

[153] *Article 29 Data Protection Working Party, Opinion 1/2003 on the storage of traffic data for billing purposes, WP69 (29.01.2003).*

[154] *LG Berlin,* Beschluss *vom 2.7.2004 -150653/03 (rechtskraftig), Multimedia und Recht (MMR) 2004, p. 688.*

transposed the provision of the ePrivacy Directive and stipulate that traffic data necessary for the purpose billing and interconnection payments may be processed only up to the end of the period during which the bill may lawfully be challenged or payment pursued, without specifying the duration of this period in their national legislation.

Austria has specified in Article 99 of its Telecommunications Act that the bill has to be challenged within **3 months** at the latest. Similarly, the Finish Act on the Protection of Privacy in Electronic Communications allows the storing of data relating to billing for a **minimum of 3 months** from the due date of the bill or the saving of the identification data, whichever is later. Such data must not, however, be stored beyond the time the debt becomes statute-barred under the Finish Act on statute-barred debt. However, in the case of a dispute over a bill, the data pertaining to that bill must be stored until the matter has been settled or resolved.

In accordance with Article 97 of the German Telecommunications Act traffic data that are necessary for billing and interconnection payments can be stored for a maximum period of **6 months** after the bill has been sent to the customer. The same storage period of 6 months is also foreseen in Article 123 of the Italian Data Protection Code for traffic data processed for billing purposes. A storage period of 6 months is also chosen in Lithuania

The Estonian Electronic Communications Act allows the processing of personal data of subscribers if they are necessary for billing purposes, including for the determination and calculation of interconnection charges. Such data must be deleted or rendered anonymous after **one year** from the day of the payment for the communications services prescribed in the communications services contract or of the payment of the arrears by the subscriber. In Hungary, the providers are allowed to store traffic data when they are necessary for billing and interconnection payments only up to the end of the period during which the bill may lawfully be challenged or payment pursued, namely **one year**. According to Article R10-14 of the French Post and Electronic Communications Code, traffic data cannot be stored for longer than the period needed for the invoicing and payment of the services provided, with a **maximum of one year** since the date of recording.

The Romanian legislation has adopted the longest storage period for traffic data that are necessary for billing and interconnection payments. According to Article 5(2) of the Law no. 506 of 2004 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector such traffic data may be processed up to the end of a period of **3 years** from the due date of the corresponding payment obligation.

According to the general data protection conservation principle data must be "kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed".[155] When interpreting this principle and applying it to the case of traffic data that are collected and processed for billing and interconnection principles (as specified in Article 6(2) of the ePrivacy Directive), some countries consider 3 months as sufficient storage period for traffic data collected for billing and interconnection payments, while others require longer periods, reaching 3 years,

[155] *Article 6(1)(e) Data Protection Directive.*

as in the case of Romania. The choices made by the European Member States on the storage period of the aforementioned traffic data reveals a fragmentation with regard to the necessity for the length of the storage period of the data and a significantly varying approach as far as the conservation and the proportionality principles are concerned.

Country	Maximum storage period for traffic data
Austria	**6 months** for law enforcement purposes. **3 months** for traffic data that are necessary for billing and interconnection payments and related dispute settlement procedures.
Belgium	Traffic data should be retained for **as long as they are necessary** for billing and interconnection payments only up to the end of the period during which the bill may lawfully be challenged (Data Retention Directive still not transposed).
Bulgaria	**One year** for law enforcement purposes
Cyprus	**6 months** for law enforcement purposes Extension for **further 6 month periods** in the event of a declaration of an emergency situation
Czech Republic	Traffic data can be retained **as long as they are necessary** for billing only up to the end of the period during which the bill may be lawfully challenged or payment pursued
Denmark	**One year** for law enforcement purposes
Estonia	Subscriber's personal data for billing the subscriber, including for the determination and calculation of interconnection charges must be deleted or rendered anonymous immediately after **one year** from payment Traffic data retained for security and surveillance purposes must be deleted within **one year** from the date of the communication
Finland	**One year** (in total, not more, not less) for law enforcement purposes Billing-related data must be stored for a **minimum of 3 months** from the due date of the bill or the saving of the identification data or until the dispute over a bill has been settled or resolved. The data must not, however, be stored beyond the time the debt becomes statute-barred under the Finish Act on statute-barred debt
France	Traffic data cannot be stored for longer than the period needed for the invoicing and payment of the services provided, with a maximum of **one year** since the date of recording Traffic data stored for purposes of the security of the network cannot be retained longer than **3 months** Electronic communication operators can further process traffic data to offer their own services or added value services, with the prior consent of the subscriber and **for a limited period of time**, which cannot exceed, in any case, the period needed for the provision or the commercialisation of those services.
Germany	**6 months** after having sent the bill to the customer as long as traffic data are necessary for billing and interconnection payments
Greece	**One year** for law enforcement purposes
Hungary	**One year** for law enforcement purposes **One year** for traffic data when they are necessary for billing and interconnection payments **6 months** for data on unsuccessful call attempts
Ireland	**2 years** for traffic data relating to fixed telephone and mobile telephone communications for law enforcement purposes **One year** for traffic data relating to internet access, internet email and internet telephone communications for law enforcement purposes Traffic data necessary for the purpose of subscriber billing and interconnection payments may be processed **only up to the end** of the period in which the bill may be lawfully challenged and payment pursued or, where such proceedings are brought during that period until those proceedings are finally determined
Italy	**6 months** for billing purposes **2 years** for telephone traffic for law enforcement purposes **1 year** for electronic traffic for law enforcement purposes **30 days** for missed calls for law enforcement purposes Traffic data relating to subscribers and users shall be erased or made anonymous when they are **no longer necessary** for the purpose of transmitting the electronic communication
Latvia	**18 months** period for law enforcement purposes, with the exception of pending data requested by state institutions, as well as data, which is necessary for the provision of further services, payment accounting for services provided, the examination of claims, recovery of payments or ensuring interconnections.

Lithuania	**6 months** **6 months** for law enforcement purposes If the bill is lawfully challenged or the data are necessary for the collection of payment, then traffic data can be stored **as long as it is needed** for dispute resolution.
Luxembourg	**6 months** from the communication date for law enforcement purposes Traffic data that are required for issuing invoices and interconnection payments purposes can be retained **until the end of the period** during which the invoice may lawfully be challenged or until the end of pending lawsuits.
Malta	**6 months** from the communication date for communications data relating to Internet Access and Internet e-mail **One year** from the communication date for communications data concerning fixed network telephony, mobile telephony and Internet telephony Traffic data necessary for the purpose billing and interconnection payments may be processed only up to the **end of the period** during which the bill may lawfully be challenged or payment pursued
Poland	**2 years** for law enforcement purposes
Portugal	**One year** from the date of the communication for law enforcement purposes
Romania	Traffic data necessary for the purposes of subscriber billing and interconnection payments may only be processed up to the end of a period of **3 years** from the due date of the corresponding payment obligation
Slovakia	**6 months** for the internet access, internet communication and telephone through the internet for law enforcement purposes **One year** for other kinds of communication for law enforcement purposes
Slovenia	Traffic data necessary for the purpose billing and interconnection payments may be processed only **up until the eventual claims** fall under the statute of limitations **14 months** for telephone services for law enforcement purposes **8 months** for all other services – internet telephony and internet use for law enforcement purposes
Spain	**One year** from the moment the communication took place for law enforcement purposes
Sweden	Traffic data necessary for the purpose billing and interconnection payments may be processed only up to the **end of the period** during which the bill may lawfully be challenged or payment pursued
The Netherlands	**One year** for fixed and mobile telephony data for law enforcement purposes **6 months** for data with respect to internet access, email through Internet and Internet telephony for law enforcement purposes
U.K.	**One year** from the date of the communication for law enforcement purposes

Table 3. Maximum storage periods in relation to traffic data

The storage period of identification, traffic and location data for law enforcement purposes has been regulated recently at European level by the Data Retention Directive[156], establishing a period between 6 months and two years for the from the date of the communication.[157] The Directive aimed at the harmonisation of the relevant provisions in the Member States concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain identification, traffic and location data, which are generated or processed by them, 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.[158] As illustrated in Table 3, the European Member States have made varying choices as to the retention of identification, traffic and location data for law enforcement choices, within the frame provided by the Data Retention Directive.

[156] *European Parliament & 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] OJ L105/54.*
[157] *Article 6 Data Retention Directive.*
[158] *Article 1(1) Data Retention Directive.*

Sweden has not yet transposed the Data Retention Directive and neither has **Belgium**. Article 126(2) of the Belgian Electronic Communications Act of 13 June 2005 provides for the retention of traffic data for law enforcement purposes for a minimum duration between 12 and 36 months, but this provision still needs to be further implemented by Royal decree. **Germany**, **Romania** and the **Czech Republic** transposed the Data Retention Directive, but their Constitutional Courts annulled specific provisions of the national laws implementing the Data Retention Directive.

Poland has adopted the longest retention period, namely 2 years, followed by **Latvia** that has opted for an 18-month retention period. Nine Member States have chosen an one-year retention period for all types of retained data under the Directive, i.e. Bulgaria, Denmark, Estonia, Finland, France, Greece, Portugal, Spain and the United Kingdom. Cyprus, Luxembourg and Lithuania have provided for a six-month retention period. **Ireland**[159] has differentiated on the retention period between traffic data relating to fixed telephone and mobile telephone communications, which have to be retained for two years, and traffic data relating to internet access, internet email and internet telephone communications which have to be retained for one year. Italy has made the same choice, with the additional provision that data relating to missed calls should be retained for a period of 30 days.

Slovenia has foreseen as 14-month retention period for telephone services and an 8-month period for internet related data. Slovakia has chosen for a retention period of 6 months for data relating to internet access, internet communication and internet telephony and one year for other kinds of communication. Finally Malta has regulated a maximum retention period of 6 months from the communication date for communications data relating to Internet Access and Internet e-mail and a retention period of one year from the communication date for communications data concerning fixed network telephony, mobile telephony and Internet telephony.

The varying storage periods for data that have to be retained under the Data Retention Directive even within the limited frame allowed by the Data Retention Directive, as well as the fact that the higher national courts in several Member States have annulled specific provisions of the national implementations of the Directive, raise questions as to the extent to which it is feasible to balance the storage period that is necessary for the achievement of a specific purpose on the one hand, and the purpose itself on the other. The wide disparities observed in the retention periods mentioned above would suggest that either the data minimisation principle has not been appropriately observed in data retention rules (including at the European level, where the permitted fork of storage timeframes was set), or alternatively that the definition of a specific timeframe at the national level is dictated largely by the (in)efficiency of national law enforcement bodies in conducting investigations that could warrant access to logged communications data. Either way, further harmonisation on this point taking into account the data minimisation principle seems to be advisable.

---

[159] *The Data Retention Directive and the relevant Irish legislation transposing it have been challenged in front of the Irish High Court by the civil and human rights advocacy group Digital Rights Ireland on the basis that it is contrary to the Charter of Fundamental Rights and the European Convention on Human Rights. The Irish Human Rights Commission was also joined as an amicus curiae to the case. The Irish High Court granted the relief for a preliminary ruling to the European Court of Justice.*

6 Current perspectives on the collection and storage of personal data

6.1 Data anonymisation and the possibility of re-identification

The principles of conservation and of data minimisation, which should be treated as specific expressions of the proportionality principle, require that a data controller may process only data that are "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"[160] and they must be "kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed"[161]. There is thus a very close link between the data that are collected, processed and stored for a given period of time on the one hand and the purposes that are to be served by the processing on the other. The aforementioned general principles are established to ensure that the privacy of the citizens is safeguarded and that information about them will not be collected or stored when not necessary for a specific purpose.

When the data are no longer necessary for the purposes for which they were collected or for which they are further processed, they should be deleted or anonymised. However, from a technical point of view, achieving full anonymisation of the data that would not allow the tracing back of the person to whom the data relate is considered as very difficult. Especially when the information is content-rich, then it is very difficult to claim that full anonymisation of the data is achieved, but in most of the cases the data will be anonymised. Pseudonymisation of data that would allow the re-identification of the person to whom the data relate would not be enough to satisfy the conservation principle. On this point, the Article 29 Data Protection Working Party expressed the opinion that "retraceably pseudonymised data may be considered as information on individuals which are indirectly identifiable", as "using a pseudonym means that it is possible to backtrack to the individual".[162] Therefore the collection of excessive information, as well as the excessive storage of information pose intrinsic dangers to the correct application of the conservation principle, as the more data there are collected about a citizen, the more difficult it will be to achieve their full anonymisation. Therefore, deleting the data is a more privacy-friendly solution, which is not, however, always preferable, as this may imply a trade-off of auditability or the data may be important for instance for statistical purposes.

6.2 The right to be forgotten

In recent years, and notably since the increase in popularity of social networking websites, discussions around a 'right to be forgotten' have emerged as a way of empowering European citizens in managing their electronic reputation, and as a tool for reducing some of the undesirable side effects of perpetual online data storage and recollection[163]. This concept

[160] *Article 6(1)(c) Data Protection Directive.*
[161] *Article 6(1)(e) Data Protection Directive.*
[162] *Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, WP 136 (20.06.2007).*
[163] *For a detailed discussion on this topic, see Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, Princeton University Press, 2011.*

itself isn't new, as a '*droit à l'oubli*' already had a basis in jurisprudence in e.g. France and in Belgium, including in non-electronic contexts[164].

A right to be forgotten is also indirectly supported by the current Data Protection Directive. The general proportionality principle already requires that data controllers delete personal data when they are no longer required for the legitimate purposes of data processing. In effect, this obligation establishes a 'passive right to be forgotten', in the form of a justification obligation for data controllers: if they can no longer show a legitimate reason for retaining personal data, then they are required to delete them.

Obviously, such a purely passive mechanism would be unlikely to be very effective as a tool for fighting personal data proliferation, especially due to the flexibility that data controllers have in assessing when retention of personal data still serves a legitimate purpose. For instance, a social network operator might well take the position (whether right or wrong) that retaining all personal data provided by its users for an indefinite period of time is legitimate as it falls within the legitimate purpose of the network's activities.

However, the Data Protection Directive also provides an active enforcement mechanism, as it grants data subjects (such as the users of social networking sites) the right to ask data controllers to indicate which personal data are being processed in relation to them[165], and to demand "the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data"[166]. On the basis of the latter provision, data subjects could already ask for the deletion of personal data, for instance on the basis that they are no longer accurate, or because the data subject withdraws its consent for the processing of its data, or simply because the period of reasonable storage has clearly been exceeded. Collectively, these rights provide data subjects with the right and possibility to expunge undesirable track records, both in an online and offline environment. In this manner, they allow individuals a certain degree of control over data which are processed in violation of the principles of minimal disclosure or minimal retention periods.

None the less, current policy debates have argued in favour of a more prominent and explicit right to be forgotten, and such a right has indeed been included in the current leaked draft Data Protection Regulation. Arguments in favour of this right focus on the changed context of data processing in an online environment, and namely on the fact that removing personal data from one source (e.g. a social network) through the right to erasure will not necessarily result in the removal of *all* online and offline references to that information, including e.g. through other sites which may have copied or archived the information, search engines, and caching services. This is especially relevant for information initially disseminated by minors, who were unable to determine the impact of their choices on their adult lives. The new right to be forgotten would therefore include an obligation for the data controller to ensure that the personal data is removed from any publicly available communication service.

---

[164] *E.g. a ruling from the Court of First Instance of Brussels, of 20 September 2001, ruled that a prisoner's right to be forgotten had been violated by TV reports covering his release and recalling his past crimes to the public, including through the broadcasting of images of his earlier prison break in the '80s. .*

[165] *Article 12(a) Data Protection Directive.*

[166] *Article 12(b) Data Protection Directive.*

It is not clear how such an obligation could be met in practical terms, given the unknown and ever changing number of search engines, archiving services, and content aggregators on the Internet, many or even most of which may not consider themselves subject to European law. In addition, the current provision poses specific questions with regard to censorship and chilling effects: while everyone agrees that certain persons are not entitled to have certain acts be forgotten (e.g. war crimes, fraud committed by politicians while in office, or indeed any personal data in relation to historically important events that would normally be documented and archived for the purposes of accurate journalism or keeping of human history), the definition of such exempted persons, acts and data controllers remains very much open to debate. Finally, there is the more fundamental question of whether the reality of people's inability to remember everything should necessarily be reflected in a more or less equivalent right of other people to have certain information be forgotten. From the perspective of fundamental rights, the enshrining into law of a human biological restriction may not be an optimal road towards societal progress.

Thus, it remains to be seen to what extent a right to be forgotten could be implemented in a way that offers a substantial added value to data protection in comparison to the current provisions of the Data Protection Directive, without harming other and equally important fundamental rights, including the freedom of expression in relation to facts that other persons might prefer to see labelled as forgotten.

7 Conclusions and final recommendations

The collection and storage of personal data in the European Union is governed by the *principles of minimal disclosure (data minimisation principle)* and of the *duration of the minimum storage of personal data (conservation principle)*. These general principles are stipulated in the Data Protection Directive in a broad way and apply to any processing of personal data. The amount of personal data that should be collected and processed for a specific processing operation, as well as their storage period, should thus be determined on a case-by-case basis, depending on the context and the circumstances relating to the processing. Both the amount of data, as well as the storage period, relate closely to the purpose for which they are collected, as it has been illustrated throughout the present report.

It would be however helpful for the data controllers to have some general guidance on how they should implement and observe the principles in specific situations, so that they are assisted in the correct and effective application of the data minimisation and the conservation principles. To this end:

*Recommendation 1. The **national Data Protection Authorities**, preferably acting under the coordination of the **Article 29 Data Protection Working Party**, should provide clear implementation guidelines to data controllers, by balancing the interests at stake in each specific context and technology, taking into account the modalities of the national legislation.*

Recommendation 2. The practical implementations of the principles of data minimisation and of conservation in specific cases by data controllers, should be evaluated (for instance in the form of audits) and clear sanctions and enforcement mechanisms should be available in cases of violations.

As illustrated in this report, such an approach is already reality in some Member States, where the Data Protection Authorities are adopting recommendations or opinions on the collection of personal data and on the specification of their storage period in specific contexts. For instance the French CNIL is keen to specify the amounts of data that should be collected in a specific context and to propose specific time periods for the storing of personal data. This has been for instance the case in the authorisation of the CNIL in the field of biometric applications[167] and in the use of geolocalisation devices in employees' vehicles. In the latter case, the CNIL issued a simplified notification norm, where the CNIL defines the kind of data that can be processed by the employer and the maximum duration of storage (in general 2 months).[168]

The Portuguese National Data Protection Commission (CNPD) published in 2009 an approval of an exemption from the notification obligation for automated treatments for the sole purpose of billing and related contact management with costumers, which is applicable for

---

[167] http://www.cnil.fr/dossiers/identite-numerique/fiches-pratiques/article/biometrie-des-dispositifs-sensibles-soumis-a-autorisation-de-la-cnil/ *(last accessed on 18.12.2011).*

[168] http://www.cnil.fr/vos-responsabilites/declarer-a-la-cnil/declarer-un-fichier/declaration/mon-secteur-dactivite/mon-theme/je-dois-declarer/declaration-selectionnee/dec-mode/DISPLAYSINGLEFICHEDECL/dec-uid/23/ *(last accessed on 18.12.2011).*

the billing and related contact management contacts and for all the market services. This typology of personal data can be stored for **ten years**.[169]

Regardless of the importance of such national initiatives, it is important that the specification of the principles of data minimisation and of conservation for specific data processing operations with pan-European impact is carried out at European level:

*Recommendation 3. At European level, the **Article 29 Data Protection Working Party**, the **European Data Protection Supervisor** and **ENISA** should develop clear guidelines on specific areas of processing of personal data with pan-European impact, and more specifically on the interpretation of the principles of data minimisation and of conservation relating to the collection and storage of personal data in such operations.*

The amounts of personal data and their storage period can be also specified by law in specific cases. For instance in the Czech Republic, there is currently a vivid debate around the minimisation of the scope of personal data disclosed in the Companies Register. An amendment to the Commercial Code that is anticipated to take effect as of the 1st of January 2012 will require that personal birth numbers of statutory bodies, shareholders and other individuals registered in the Companies Register will no longer be publicly accessible in its public section.

However, even statutory obligations may not always be in line with the proportionality element enshrined in the data minimisation and the conservation principles. For instance in Luxembourg the limitation period to initiate lawsuits challenging an invoice is 10 years from the due date according to article 189 of the Luxembourg Commercial Code, regardless the fact that the invoice is paid or not. While this article is still in force, it is no longer consistent with article 5 of the Law of 28 July 2011 regarding the protection of personal data in the context of electronic communications, which does not permit to keep traffic data after 6 months from the payment of the invoice and therefore does not permit to keep the relevant supporting documents in the event that a lawsuit is brought 6 months after the payment of the relevant invoice. Such conflicting regulatory provisions should be identified and eliminated in order to ensure respect to the conservation principle.

*Recommendation 4. Given the fact that the collection and storage of personal data is not always only governed by the data protection legislation, **Member States** should take actions to identify and eliminate conflicting regulatory provisions relating to the collection and storage of personal data.*

Obviously, the impact of national laws may diminish under the influence of updates to the European regulatory framework with respect to data protection. Specifically, the draft Data Protection Regulation would, if approved, fully harmonize national data protection rules, including in relation to these two fundamental principles. It goes without saying then, than European lawmakers need to carefully consider how these principles are codified in future European laws.

[169] http://www.cnpd.pt/bin/decisoes/1999/htm/ise/ise003-99.htm *(last accessed on 18.12.2011).*

*Recommendation 5. The **European Commission** should ensure that any provisions in future European legal instruments in relation to the data minimisation principle and the conservation principle are clear. They should also verify that such provisions can be implemented effectively in real environments. This also implies that any related rules (including the enforcement mechanisms and any related provision or data subject rights) are well aligned with the fundamental principles.*

Finally, European citizens must also be empowered in identifying practices that violate these important principles, and in taking appropriate actions, including by exercising their rights as data subjects towards non-compliant data controllers and by registering complaints with the competent authorities, where applicable. This also implies that data subject awareness is increased, as the first step on this road is ensuring that data subjects know and understand the importance of safeguarding their data against needless disclosure. Such awareness raising actions should foremost be undertaken by Data Protection Authorities, as the entities with the most direct link to their citizens in each Member State.

*Recommendation 6. The **Data Protection Authorities** should aim to improve user awareness relating to their rights stemming from the data protection legislation and on the possibilities offered to them by the legal system to exercise these rights, including by complaining in cases of excessive collection and storage of personal data.*

8 Annex I: National correspondents

COUNTRY	NAME	ORGANISATION
Austria	Prof. Dr. Erich Schweighofer/Walter Hotzendorfer	University of Vienna & Vienna Center for Legal Informatics
Belgium	Prof. Dr. Jos Dumortier	Time.lex law offices
Bulgaria	Desislava Krusteva	Dimitrov, Petrov & Co
Cyprus	Olga Georgiades	Lexact Solutions Ltd
Czech Republic	Lenka Suchankova/Adela Munzbergova	Pierstone s.r.o., advokanti kancelar
Denmark	Prof. Dr. Henrik Udsen	Copenhagen University
Estonia	Mihkel Miidla / Kaupo Lepasepp	Sorainen
Finland	Teemu Rissanen/Tapio Rissanen	Conseils Oy/Euro Conseils SPRL
France	Fanny Coudert	Time.lex law offices
Germany	Prof. Dr. Gerald Spindler	University of Goettingen
Greece	Dr. Eleni Kosta	Time.lex law offices
Hungary	Dr. Zsolt Gyorgy Balogh	University of Pecs Faculty of Law
Ireland	Anna Morgan/Anne Bateman	Philip Lee Solicitors
Italy	Prof. Dr. Giusella Finocchiaro	University of Bologna
Latvia	Andis Burkevics	Sorainen Law Firm
Lithuania	Paulius Galubickas	Sorainen law firm
Luxembourg	Claire Leonelli	Molitor, Avocats a la Cour
Malta	Prof Dr. Joseph A. Cannataci	University of Malta
Poland	Dariusz Adamski	Uniwersytet Wroclawski
Portugal	Pedro Simoes Dias	Fujitsu
Romania	Corina Papuzu	Buzescu Ca
Slovakia	Zuzana Halasova	National Security Authority
Slovenia	Klemen Ticar	Ulcer & Partners Law Firm Ltd
Spain	Cristina de Lorenzo/Ignacio Nunez	Sanchez Pintado & Nunez Asociados
Sweden	Christine Kirchberger	Swedish Law & Informatics Research Institute
The Netherlands	Linda Eijpe	Skoop Advocaten
U.K.	Mark Owen	Harbottle & Lewis

9 Annex II: List of surveyed transportation companies

COUNTRY	TRANSPORTATION COMPANY
Austria	ÖBB-Personenverkehr AG (Austrian Federal Railways)
Belgium	SNCB/NMBS (Société Nationale des Chemins de fer Belges / Nationale Maatschappij der Belgische Spoorwegen)
Bulgaria	Global Biomet EOOD
Cyprus	Cyprus Airways
Czech Republic	České dráhy, a.s. (ČD)
Denmark	DSB
Estonia	Edelaraudtee Aktsiaselts
Finland	VR-Group Ltd
France	Voyages-SNCF.com, S.A.
Germany	Deutsche Bundesbahn AG (German Railway)
Greece	Airtickets.gr (Airtickets Tourist Operations)
Hungary	Weco-Online Kft
Ireland	Irish Rail (also known by the Irish language name, Iarnrod Eireann)
Italy	Ferrovie dello Stato S.p.a.
Latvia	AS Latvijas dzelzceļš
Lithuania	UAB Tolimojo keleivinio transporto kompanija
Luxembourg	LUXAIR S.A., Société Luxembourgeoise de Navigation Aérienne
Malta	Virtu Ferries Ltd.
Poland	PKP Intercity" Spółka Akcyjna
Portugal	CP - Comboios de Portugal, E.P.E.
Romania	Touring Europabus Romania S.R.L.
Slovakia	ZSSK (Železničná spoločnosť Slovensko, a.s.)
Slovenia	Unior d.d. Program Turizem
Spain	RENFE-OPERADORA
Sweden	SJ AB
The Netherlands	NS reizigers BV
U.K.	Easy Jet PLC

10 Annex III: List of surveyed social networking sites

COUNTRY	SOCIAL NETWORKING SITE
Austria	sanktonlein.at
Belgium	www.sayso.be
Bulgaria	www.sibir.bg
Cyprus	www.guide2cyprus.com/myguide2.asp
Czech Republic	www.spoluzaci.cz
Denmark	www.dating.dk
Estonia	www.rate.ee
Finland	www.somia.fi (http://www.irc-galleria.net)
France	copainsdavant.linternaute.com
Germany	www.xing.de
Greece	www.greekcatholics.gr
Hungary	iwiw.hu
Ireland	www.irishabroad.com
Italy	connectu.it
Latvia	www.draugiem.lv
Lithuania	www.one.lt
Luxembourg	www.lesfrontaliers.lu
Malta	www.skolahbieb.com
Poland	nk.pl
Portugal	www.thestartracker.com
Romania	www.tpu.ro
Slovakia	www.azet.sk
Slovenia	izklop.com
Spain	www.tuenti.es
Sweden	dayviews.com
The Netherlands	www.hyves.nl
U.K.	Friendsreunited.com

11 Annex IV: List of surveyed telecommunications companies

COUNTRY	TELECOMMUNICATIONS COMPANY
Austria	UPC
Belgium	Telenet
Bulgaria	Bulgarian Telecommunication Company (BTC) [Българска телекомуникационна компания (БТК)]
Cyprus	Cyprus Telecommunications Authority
Czech Republic	Eri Český bezdrát
Denmark	TDC
Estonia	Elion
Finland	Elisa Communications' (www.elisa.com) consumer market brand Saunalahti (www.saunalahti.fi)
France	Free
Germany	Deutsche Telekom AG
Greece	Hellenic Telecommunications Organization (OTE S.A.) [Οργανισμός Τηλεπικοινωνιών Ελλάδος (OTE)]
Hungary	Magyar Telekom Nyrt.
Ireland	Eircom Limited
Italy	Teletu
Latvia	SIA Lattelecom
Lithuania	TEO LT, AB
Luxembourg	Coditel Sàrl
Malta	Melita plc
Poland	TPSA
Portugal	ZON Multimedia
Romania	Romtelecom
Slovakia	Slovanet
Slovenia	Amis d.o.o.
Spain	TELEFONICA
Sweden	TeliaSonera
The Netherlands	www.xs4all.nl
U.K.	BT

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu