Collection and Storage of Personal Data: A Critical View on Current Practices in the Transportation Sector

Eleni Kosta[1], Hans Graux[2], and Jos Dumortier[2]

[1] TILT-Tilburg University, Tilburg, The Netherlands / time.lex law offices, Brussels, Belgium
e.kosta@tilburguniversity.edu, eleni.kosta@timelex.eu
[2] ICRI-KU Leuven, Leuven, Belgium / time.lex law offices, Brussels, Belgium
{hans.graux,jos.dumortier}@law.kuleuven.be/timelex.eu

Abstract. This paper is based on a 2011 ENISA study that aimed at the analysis of two core principles that can be considered as key manifestations of privacy by design: on the one hand the *principle of minimal disclosure* (which is also known as the data minimisation principle), and on the other the *duration of the storage of personal data* (which is also known as conservation principle). It focuses on the data collected for two specific application areas: online ticket booking and purchasing, and the collection and exchange of so-called Passenger Name Record (PNR) data in the European air travel sector and it provides a summary of its findings in relation to the transportation sector across the EU Member States. The analysis shows that it is worrisome to observe that so many systems deployed in real life do not follow a privacy by design approach, and insufficiently consider the data minimisation and data conservation principles. There is a need for these principles to be strengthened in practice, through legislation and governance mechanisms that favour privacy by design, including a clear assessment of privacy impacts and the identification of more privacy conscious implementation alternatives, in order to ensure that the personal data of European citizens is proactively protected, instead of having to modify operational systems only after privacy problems come to light.

1 Introduction

The European legislative approach to protecting personal data against abuses is based on a number of core principles. Most of these primarily target human behaviour, by specifying what persons can and cannot do with personal data. However, because of the strong role that modern technologies play in enabling the processing of personal data – collecting, analysing and disseminating it – the realisation has grown that the design of information processing systems themselves should be impacted by data protection concerns as well. Technology should become a tool that prevents data protection abuses, instead of enabling them. The clearest manifestation of this shift in focus is the so-called "privacy by design" principle.

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

B. Preneel and D. Ikonomou (Eds.): APF 2012, LNCS 8319, pp. 157–176, 2014.

early design stage to their deployment, use and ultimate disposal".[1] This principle has been promoted as a fundamental tool for ensuring trust and security in European public policy, including notably through the recent 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."[2]

Recently, the European Commission discussed the "privacy by design" principle in the frame of the current review of the European Data Protection Directive, with a view of explicitly codifying the principle into European data protection rules, 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"[3]. 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"[4], and announced its intention to examine possibilities for the concrete legislative implementation of the principle.

While the importance of the *privacy by design* principle as a way of protecting personal data is becoming clearer every day, it is much less clear to what extent the principle is observed in practice. This is especially true in the world of online service providers, where unbridled and excessive data processing is easy, cheap, and relatively risk free. To examine this tension, ENISA recently commissioned an analysis of two core principles that can be considered as key manifestations of privacy by design: on the one hand the *principle of minimal disclosure* (which is also known as the data minimisation principle), and on the other the *duration of the storage of personal data* (which is also known as conservation principle).

The study, entitled the "Study on data collection and storage in the EU"[5] was not intended as a theoretical legal study that identified and analysed national legislation, but instead focused on a limited number of relevant use cases, attempting to discover if and how the aforementioned principles were expressed in concrete legal or regulatory provisions applicable to these cases, and how they were observed in practice. To achieve this objective, the study collected detailed legal information from expert correspondents in all 27 Member States, who were also asked to identify and analyse

[1] 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).

[2] Idem, p. 17.

[3] Idem, p. 4.

[4] 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.

[5] See: `http://www.enisa.europa.eu/act/it/library/deliverables/data-collection/at_download/fullReport`

three real life examples of use cases in their own country, covering three different sectors: social networking, transportation, and electronic communication.

This paper is based on the ENISA study, and provides a summary of its findings in relation to the transportation sector. In the sections below, we will first provide an overview of the European regulatory backdrop of the data minimisation and conservation principles, and then assess how these principles are being observed in the transportation sector across the EU. This will be done based on the data collected through the aforementioned study for two specific application areas: online ticket booking and purchasing, and the collection and exchange of so-called Passenger Name Record (PNR) data in the European air travel sector. Finally, we will present our conclusions on the current implementation of these principles in the transportation sector.

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.[6] 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[7]. In relation to the principles of *minimal disclosure* and 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"[8] 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".[9] In practice these rules implement the concept of the aforementioned *principle of minimal disclosure* in a binding legal text, and they will be referred to interchangeably throughout this paper.

The data controller generally 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 instance the protection of the individual and the commercial profit of the service provider. At least in theory, the data controller does

---

[6] Walden Ian., "Data Protection", in Reed Chris, Angel John, *Computer Law*, 5th edition, Oxford University Press, 2003, p. 432.

[7] 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.

[8] Article 6(1)(c) Data Protection Directive.

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

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.[10] 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.[11] 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.[12] Thus, the stated consumer concern does not appear to be reflected in consumer protest. The same observation was made in an ENISA study on the economics of privacy[13].

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

[10] 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)

[11] Idem, p. 6.

[12] http://www.dataprotection.ie/documents/annualreports/2010AR.pdf (last accessed on 18.12.2011)

[13] ENISA, Study on Monetizing Privacy. An Economic Model for Pricing Personal Information To be publish at the beginning on 2012 on ENISA web page: http://www.enisa.europa.eu/act/it/library

decisions on the deletion of data by the Postal Office[14], by travel agents[15], in the context of video surveillance in grocery stores[16]. 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 3.1.

Indications on acceptable storage periods are sometimes also provided through indirectly related legislation. According to the Dutch Act on Personal Data Protection[17], 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[18] 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.[19]

3 The Collection and Storage of Personal Data in the Transportation Sector: From Principle to Practice

3.1 Online Booking and Purchasing of Tickets

The booking and 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 ENISA study examined the purchasing of a ticket online from a private or public transportation company in each of the twenty seven European Member States. Seventeen railway company cases were identified, along with three bus company cases, three airline companies, two online travel agencies, a ferries company

[14] http://www.datainspektionen.se/press/nyhetsarkiv/2008/posten-lagrar-personuppgifter-onodigt-lange/ (last accessed on 16.12.2011)

[15] http://www.datainspektionen.se/press/nyhetsarkiv/2009/charterbolagen-lagrar-kunduppgifter-och-resehistorik-for-lange (last accessed on 16.12.2011)

[16] http://www.datainspektionen.se/Documents/beslut/2011-06-20-lidl.pdf (last accessed on 16.12.2011)

[17] Wet bescherming persoonsgegevens (WBP), 06.07.2000 (O.J. 302/2000); see http://wetten.overheid.nl/BWBR0011468 (last accessed on 20.12.2011)

[18] Vrijstellingsbesluit WBP, http://www.cbpweb.nl/hvb_website_1.0/vwc11.htm (last accessed on 16.12.2011)

[19] Idem.

and finally a ski ticket purchasing process. 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 (Figure 1). 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 also e.g. belong to the person that realised the purchasing. Sixteen of the surveyed companies required a fixed or mobile phone number, while ten of them asked for a postal address.

Interestingly, six of the surveyed companies required an identity card or passport number. These six companies did not belong to the same category of transportation companies, but offered 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 were 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 was 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 were required by various transportation companies for the booking of a ticket online revealed 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 (e.g. to conduct market research into key consumer profiles), this cannot be justified under the principle of data minimisation which stipulates that only the necessary information should be collected and stored.

The study also examined the options that transportation companies (either private or public ones) offered to their customers with regard to the processing of customer data for the sending of information and for marketing purposes (Figure 2). The majority of transportation companies processed 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 was a tick-box already pre-checked, which the users would have to uncheck if they did not wish to receive such information.

In some other cases, information about the processing of the personal data of the customers was contained in the privacy statement or the Terms and Conditions of the website. The users were 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 could 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.

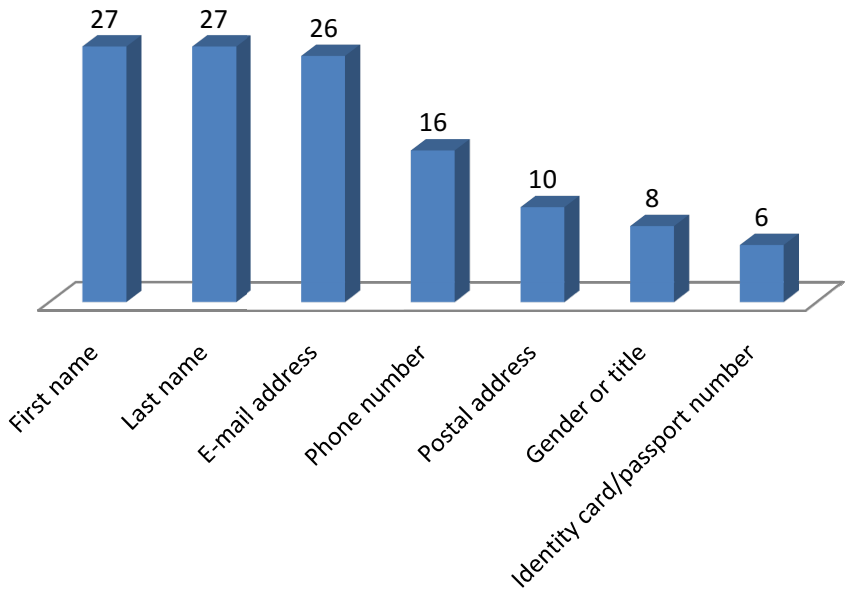

Fig. 1. Types of personal data collected when booking the ticket online in 27 MS

Only one surveyed company collected personal data from its customers only in order to process purchasing requests without collecting data for any other marketing purposes. To the contrary, another surveyed company (Malta), which by default implemented a right to sell or otherwise communicate the contact details of an individual to third parties for marketing purposes, did 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 mentioned 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 did not offer any kind of option and did 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.

The ENISA study showed that 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, were 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.

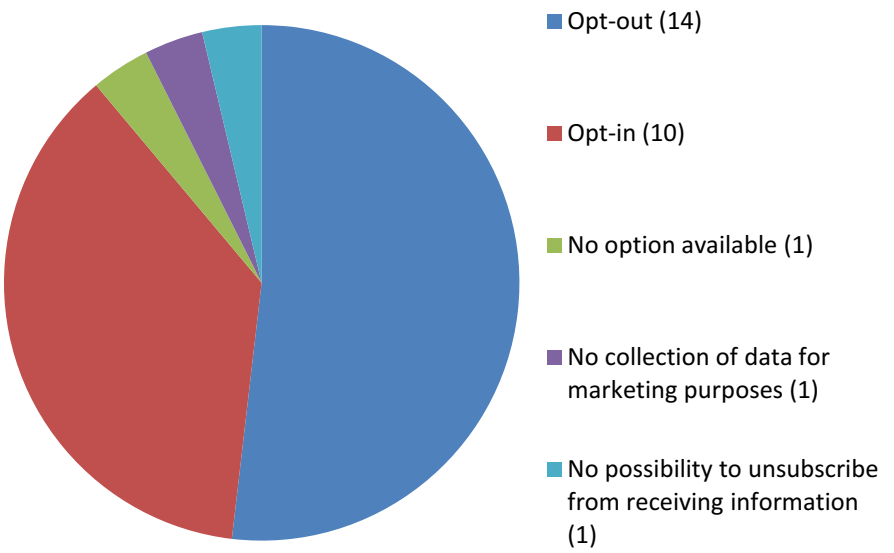

Fig. 2. Options offered by transportation companies to customers regarding the sending of information by the company in the future based on the data they collect on them

The 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.[20] 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.

[20] 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[21] (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[22]. 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.[23] This means that the citizen, when he wishes to use his elD, 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.[24]

3.2 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 (following the booking/purchasing process as described in section 3.1 directly above) 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, the name of the bank issuing the card is also required.

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, which require the user to reveal a number of personal information when purchasing the card online. Users tend to reveal a large amount 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. However, the unique number that is stored on the card allows for

[21] http://www.b-rail.be (NMBS/SNCB) (last accessed on 25.01.2012)

[22] http://mobile.b-rail.be/en/Novelties/Use-your-Belgian-e-ID-as-ticket (last accessed on 25.01.2012)

[23] 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.

[24] http://www.privacycommission.be/nl/docs/Commission/2010/aanbeveling_01_2010.pdf (last accessed on 25.01.2012)

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 bank account information and their personal identification number. The card scheme foresees the possibility for travellers to get an anonymous travel card, but at a higher cost. This approach, in which privacy protection is essentially treated as a common barter, has created a heated debate in Denmark. In this section some further prominent examples will be presented in greater detail, along with the challenges they pose to the principle of minimal disclosure.

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 for a card online, their telephone number and email address also have to 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.[25]

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.

The data are stored for a period of **eight weeks**, a time period that was agreed in consultation with the Information Commissioner's Office (the UK data protection authority), when the card was first implemented in 2003.[26] The data are then anonymised and 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.[27]

The details of debit or credit cards that are used to buy Oyster products are retained for a maximum period of 18 months.[28] When a user is issued a penalty fare notice or

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

[26] Idem.

[27] Idem.

[28] Idem.

prosecuted for fare evasion, their personal details and relevant journey and transaction history will be retained for a longer period, which is not specified.[29]

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.

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[30] for ticketing systems, which was updated in 2010,[31] 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.

---

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

[30] 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.

[31] 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.

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 in practice only allows the loading of single tickets.

The study showed that 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 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 made 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 particular interest. 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.

The Brussels MoBIB Card. In 2008, the Brussels public transportation company[32], launched the 'MoBIB' card.[33] 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 printed on the card.[34]

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.[35]

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.[36]

The Brussels public transportation company mentions in the terms of use of the MoBIB card that the data will be stored for limited periods of time as necessary for the specific foreseen processing. No exact storage period is however specified.[37] The Belgian Privacy Commission has advised in its recommendation 01/2010 that the data

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

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

[34] 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)

[35] 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)

[36] 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, 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)

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

that are collected for travel ticket administration should be deleted at the latest after six months.[38] 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 after the time when the customer has returned the card.[39]

The Prague 'Opencard'. In 2008 the Prague City Hall launched an electronic card 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.[40] 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.[41] 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 age-related discounts.[42]

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 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.

---

[38] 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)

[39] 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)

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

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

[42] Idem.

Dutch OV-Chipcard. The OV-chipcard has recently been introduced in the Netherlands, as a smart card with a built-in chip for public transportation. There are currently three types of OV-chipcards: a personalised one, which mainly aims at season ticket holders; a disposable card which can be used for a certain period of time; and an 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[43] were storing personal data for a longer period than was necessary. The transportation companies modified the **storage period** of the personal data[44] 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.[45] The Commission imposed an order for incremental penalty payments if the companies do not comply with the order.

3.3 Airline Companies and PNR Data

Concept and Legal Background. The purchasing of airplane tickets, either online or offline, especially for flights into the U.S. (or even Canada or Australia) requires the revealing of a large number of personal information of the user. The most well known example of such a data transfer mechanism is the so-called Passenger Name Record (PNR) data. PNR data[46] is information that is provided by passengers and is collected by carriers for enabling reservations and carrying out the check-in process.[47]

---

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

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

[45] 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)

[46] 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.

[47] 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)

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.[48]

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)[49] 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[50]. 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[51] 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"[52]. 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

---

[48] Idem. See below Section 3.3.2 for the detailed list of PNR data in the context of the EU-US PNR draft agreement.

[49] 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.

[50] 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.

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

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

the Data Protection Directive[53]. 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)[54], 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 Homeland Security.[55] 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.[56]

---

[53] 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.

[54] 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.

[55] 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.

[56] 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).

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 suspected of any wrongdoings. 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 their trip. The list of data was considered as excessive and 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".[57] As for the processing of sensitive data, the EDPS recommended that airline carriers should not transfer any sensitive data to the DHS.[58]

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[59] for a period of 30 days after

[57] 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.

[58] Idem.

[59] 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).

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.[60] The Article 29 Data Protection Working Party considers the retention period of five years as disproportionate.[61]

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.[62] 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 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"[63] allows room for broad interpretation.

4 Conclusions

As shown by the examples above, new technologies can greatly improve the efficiency, user friendliness and security of transportation systems. However, from a data protection perspective it is worrisome to observe that so many systems deployed in real life do not follow a privacy by design approach, and insufficiently consider the data minimisation and data conservation principles. This can be seen in online ticket purchasing systems, where data collection practices vary quite widely between the

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

[61] 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.

[62] "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.

[63] Article 6(e) Data Protection Directive.

countries, despite the fact that data needs behind these services are relatively homogeneous. This would seem to indicate that these systems are designed without systematically considering how data collection can be minimized. This can also be seen in the mechanisms for obtaining the consent of data subjects, particularly for direct marketing purposes, where communication towards data subjects is often ambiguous and clearly slanted towards facilitating data collection and data processing, rather than towards protecting the privacy of the users of such services.

Similar observations can be made with respect to travel cards and PNR data. A commonly recurring trend appears to be that such technologies are developed and deployed with optimal usability and usefulness in mind, but without duly considering data protection implications. Only after these concerns are brought to light – either by data protection authorities, court cases or consumer complains – are the systems reviewed and updated to improve privacy friendliness. In some cases – PNR data being a prime example, as are several travel card deployments – no conclusive answer to privacy questions has been found yet, and existing practices still fail to appropriately observe the data minimisation and conservation principles.

Globally, the examples illustrate that there is a need for these principles to be strengthened in practice, through legislation and governance mechanisms that favour privacy by design, including a clear assessment of privacy impacts and the identification of more privacy conscious implementation alternatives, in order to ensure that the personal data of European citizens is proactively protected, instead of having to modify operational systems only after privacy problems come to light. Hopefully, the ongoing revision of the Data Protection Directive and its future successor will take some steps in that direction.

Acknowledgments. The authors would like to acknowledge the kind contributions and keen insights offered by ENISA in the course of conducting the Study on data collection and storage in the EU, including notably Dr. Rodica Tirtea, Dr. Demosthenes Ikonomou and their team, as well as the national correspondents who provided extensive information on the legal systems and administrative practices in their countries for the study.