Privacy Rules, A Steeple Chase For Systems Architects

John Borking Wassenaar The Netherlands[1]
E-mail: jborking@xs4all.nl

Abstract. Building privacy rules set down in the Directives 95/46/EC and 2002/58/EC into information systems for protecting personal data poses a great challenge for the architects. Especially in Internet applications that carry personal data worldwide around and the fact, that it generates traceable traffic in the network create legal questions about how to protect personal data without violating the privacy laws in different legal regimes. Architectures and subsequently software applications must have built-in privacy protection features to ward off privacy intrusion risks and legal liabilities. At least 20 legal privacy principles architects and developers should take into consideration. Under EU privacy legislation in case of unlawful processing of personal data, the data subject can always hold the controller responsible and most likely under product liability rules the architect and developer of the privacy infringing information system.

1 Introduction

At present, data protection is very much centered around the legal and administrative sphere, with management having to spend a lot of time on the (policy) preparation and monitoring. Under a lot of pressure already, management can better devote this time to other activities. If the protection of personal data could be automated more than has been the case so far: this would free up time for the primary processes for which management is responsible and it would better enforce data protection. Information and communication technology (ICT) could play a significant role in guaranteeing the protection of personal data. Besides organizational measures such as separation of duties and data handling procedures, technology can also be deployed to protect personal data. Over the last twelve years architects and developers have proven that Privacy-Enhancing Technologies' (PET) can protect personal data adequately in conformity with privacy legislation worldwide. The term 'Privacy-Enhancing Technologies' (PET) is used to define all the technical controls that can be used to protect personal data. This concept also includes the design of the information systems architecture.

Within Europe the Directives 95/46/EC and 2002/58/EC and national data protection acts defines the rights and duties of all the relevant organizations and people with respect to the processing of personal data. 'Processing' includes the entire life cycle

[1] Drs John Borking is director of Borking Consultancy and was a privacy commissioner, vice president and board member of the Dutch Data Protection Authority from 1-1-1994 till 1-1-2006

from collection and registration through to destruction. The Data Protection Act also defines a number of basic privacy principles.

Currently there are at least six different legal system in the world and the rigor with which privacy rules are applied and enforced differ from nation to nation. Worldwide has been recognized that privacy principles at least comprise the following four principles or rules.

A. Principle of existence of privacy

A data subject possesses an identity and other pertinent and variable information that this person may consider to belong to his or her privacy domain. This collection of information is called *personal data.*

B. Principle of withholding

The data subject has the right and should be equipped with the ability to withhold some or all of his personal data to other persons and organizations at this person's private choice.

C. Principle of trusted usage

The person or organization that receives the personal data and stores it is called *the controller or collector*. This *collector* of information has the obligation to keep to the constraints on dissemination and processing of personal data as either stated in the EC privacy directives, or when such piece of law doesn't exist according to the privacy preferences of the data subject. Furthermore, this collector has the obligation to inform the person involved of its possession of personal data and to provide the opportunity for change. If so permitted, the *collector* may copy the personal data to one or more *processors* for further processing.

D. Principle of controlled dissemination

The data subject has the right to disclose some or all of his or her personal data to other persons and organizations, the collectors of the personal data, at this data subject's own choice. This data subject may issue constraints on the dissemination of the personal data to one or more processors for further processing of this data and has the right to change the personal data, to extend and restrict it, to withdraw this information and to change the constraints.

A major step towards privacy protection in Europe was the adoption of 1981 Convention 108 of the Council of Europe. Today, informational privacy protection for individuals is articulated through different European Union Directives like 95/46/EC (Data Protection Directive, hereafter DPD), 1999 Digital Signature Directive 99/93/EC and the Directive 2002/58/EC (Directive on Privacy and Electronic Communications, hereafter DPEC). The EU Commission always sees the directives 95/46/EC and 2002/58/EC as one piece of legislation for the protection of privacy online and offline. This kind of legislation defines a set of rights concerning personal data accruing to individuals irrespective of sector of

application, and creates obligations concerning the processing of data by third parties .

3. Different Levels of Personal Data

The fact that within Internet applications personal data will be carried around and traceable traffic data will be generated in the network is relevant to what the data protection legislation considers as personal data[2]. Personal data means any piece of information regarding an identified or identifiable natural person. Whether data can be qualified as 'personal data' depends on a number of elements of which, within the scope of this essay, 'identification' is the only significant element. According to Article 2 of the EU Directive 95/46/EC, a natural person can be identified 'directly or indirectly'. Direct identification requires basic details collected in PII. PII is name, address, a personal number, a widely known pseudo-identity, a biometric characteristic such as a fingerprint, etc. Indirect identification requires other unique characteristics or attributes or a combination of both, to provide for sufficiently identifying information .
Non-identification is assumed if the amount and the nature of the indirectly identifying data are such that identification of the individual is only possible with the application of disproportionate effort[3]. Whether we can talk of disproportionate effort depends, on the one hand, on the nature of the data and the size of the population; and on the other hand, the resources of time and money one is willing to spend in order to be able to identify the person [3]. Internet identifiers such as an IP address, browsing activities of a user, session login data and the listing of web sites visited by an Internet user are classified as personal data .
In order to create maximum privacy protection within the Internet environment in a business to consumer (B2C) communication personal data needs to be divided into three categories:

Level 1: 'Deal Closing Information'.
This set of PII is transferred when direct communication between data subject and company is needed. Level 1 PII may contain items like: Name and Address information, telephone number and e-mail address. It is irrelevant whether one uses a real identity or a pseudo-identity. The sole use one can make of this data is when the flow of communication between the data subject and the company/ organization have created the desired result and direct human contact between the data subject and the management of the company is needed. For this reason this type of PII is sometimes referred to as 'contact information'.

---

[2] See Article 2 of EU Directive 95/46/EC (DPD); 'personal data' are defined in for instance Article 1 of the UK Data Protection Act 1998. There is a lot of confusion about what is considered as identification and verification

[3] See Recital 26 of the EU Directive 95/46/EC. When processing takes place without any personal data the DPD is not applicable See also recital 20 of the Directive 2002/58/EC

Level 2: All others items of personal data except data belonging to level 3.
Level 3: Special categories of personal data as defined in Directive 96/46/EC Article 8 paragraph 1. Level 3 personal data are only to be processed under the conditions specified in Article 8 paragraph 2 through 7.

Level 4. A special category of personal data is the traffic data created when moving around in cyberspace. As long as this data is directly or indirectly generating information about the user, this data is considered as personal data. In the design of Internet applications this data must be made unlinkable to a person by means of secure communication and/or encryption [17][18].

4. Liability

Architects and developers build information systems and Internet applications. In the case of unlawful processing of personal data, the EU system of law is that the data subject always can hold the controller responsible. A controller can't defer this responsibility to a third party developer, even if this developer has deviated from the agreed design. Liability actions between the controller and the third party developer are civil or common law actions that may be based on malpractice and/or product liability but privacy violations have to be dealt within the scope of the privacy legislation.

The Privacy Commissioners have taken the position [4] that developers should take into consideration at an early stage of the design, the implications of the use of Internet applications for the privacy of individuals [5].
There are various ways in which privacy and related interests can be threatened. Related interests denote interests that privacy helps to promote and which help to promote privacy like autonomy, integrity and dignity of an individual. Hence controllers should ensure that Internet applications should keep control over the PII and the design should give maximum of transparency and other proper means to protect the privacy of the users. A privacy threat analysis is a sine qua non [6]. These threats have to be countered and neutralized in the design of the information system and Internet application .

5. Privacy principles for consideration by Architects

The four *Global Privacy Principles* as described here above can be elaborated in the direction of information processing, to produce rules that will govern the rules for the handling of personal data in more detail, for example as it applies in the European Union. These will be qualified as *Privacy Facilitation Principles*, These rights facilitate the ability to keep control over the personal data by the person behind it, notably in the light of the available technology. The aim of this elaboration is to facilitate the ability to keep control over the personal data by the person behind it, notably in the light of the available technology. The

elaboration provides also a handle on when privacy protection is sufficiently well addressed.
There are nine privacy principles incorporated into the DPD and DPEC. The DPEC has moreover four extra requirements. The principles are collations of articles from the DPD and DPEC that are frequently applied together [7].

1. *Intention and Notification* - The processing of personal data must be reported in advance to the Data Protection Authority or a privacy officer (where applicable), unless the processing system in question has been exempted from notification.

2. *Transparency* - The person involved must aware of who is processing his personal data and for what purpose. Thus any collection of personal data implies prior supply of certain information to the individual concerned. Two situations may be distinguished: (i) the personal data are collected from the data subject, and (ii) the personal data are collected in another manner.

    a. In the case of situation (i), the data subject must be provided with at least the following information before the data are collected: - the identity of the controller (which includes the name as well as the physical and electronic address); and - the intended purpose(s) of the processing. It also has to be determined whether further information (e.g. the recipients of the data, whether replies to the questions are obligatory[4] and the possible consequences of failure to reply, and the existence of the right of access to and the right to rectify the data) has to be provided to guarantee fair processing.
    b. In case of situation (ii) the data subject must get information at the latest at the moment where personal data are recorded or first disclosed to a third party. It should be noted that the requirement to provide information does not apply where it would be impossible or would involve a disproportionate effort, or if recording or disclosure of data is expressly laid down by law.

    Moreover the DPD requires that the information about the identity of the controller, the purpose of the processing etc. be provided to the user at registration (or at another early stage of the application at issue). Any other information required by law (e.g. that a disclosure of personal data to third parties is foreseen) has to be provided in a comprehensible form.

[4]Obligatory information is information that is necessary to carry out the requested service. All other information qualifies as “optional”. It should be noted that the fact that someone does not provide such optional information couldn’t count against him in any way.

3. *Legitimate Ground for Processing* - The processing of personal data must be based on a foundation referred to in national legislation, such as consent, contract, legal obligation, justified interest and such like. For special data, such as health, stricter limits prevail. The DPD explicitly lists the cases in which personal data may be processed. This means that for each processing of personal data – collection, recording, storage, adaptation, alteration, retrieval, consultation, disclosure, dissemination, etc. - the controller has to verify if the processing falls under one of the criteria for making data processing legitimate.
4. *Finality and purpose limitation principle* - This principle rules the collection of data. Personal data may only be collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. In other words, in lack of a legitimate basis for processing personal data it may not be collected/processed and the individual concerned must remain anonymous. Users have to be aware that they have the right to object to processing of their personal data for the purposes of direct marketing. Actually, the law protects them to an even further extent: they must opt-in to processing for such purposes; otherwise their personal data may not be used. If the use of direct marketing techniques is foreseen, the possibility to opt-in should be offered during registration. A "just-in-time-click-through agreement" can be used for final acceptance of such use [8].
5. *Data Quality* - The personal data must be correct, accurate, sufficient, to the point and not excessive in relation to the purpose in question. Also the following issues have to be taken into account: 1.authorization inspection for data input; 2.storage terms; 3.periodical clearing; 4. information on the disclosure of corrected data to third parties to whom these data have been previously disclosed; and 5.final inspection of automated decisions (Article 15 of the Directive 95/46/EC).
6. *Data subject's rights* - The data subjects involved have the right to access and to correct their data as well as the right to object. The right of access to and the right to rectify the data is for guaranteeing fair processing Under Article 14(a) of the DPD a data subject has the right to object, on compelling and legitimate grounds relating to his particular situation, to the processing of data relating to him. This right to object must at least cover the cases where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority and where processing is necessary for the purposes of the legitimate interests pursued by the controller[5]. A special legal regime applies to the processing of personal data for the purposes of direct marketing, and in particular to unsolicited commercial communications sent electronically such as "spam'. Of course, adequate security measures should be taken in order to guarantee that only the data subject has on-line access to information concerning him.

[5] See Article 7(e) and (f) of the Directive 95/46/EC

In order to be able to exercise their rights, users must know what rights they have and understand them. The interface should provide obvious tools for exercising the data subject's rights.

7. *Security* - Providing appropriate security for personal data held within ICT-systems is one of the cornerstones of the DPD. Measures of technical and organizational nature suitable and proportional to the sensitivity of the personal data and the nature of possible risks have to be taken to avoid potential harm should the PII be misused or disclosed in an unauthorized matter.
8. *Processing by a processor* - If processing is outsourced to a processor (acting on behalf of the controller), it must be ensured that a contract (or another legal act) in writing (or another equivalent form) must be concluded between the two parties, binding the processor to the controller and stipulating, in particular, that:

   (i) The processor shall only act on instructions from the controller; and

   (ii) The obligations concerning security) shall also be applicable and binding on the processor irrespective of the country in which the data processing is taking place.

9. *Transfer of personal data outside the EU* - In principle, the transfer of personal data to a country outside the EU is permitted only if that country offers adequate protection. Personal data may flow freely between all the 25 Member States of the EU and the three European Economic Area (EEA) states (Norway, Lichtenstein and Iceland). In addition, the Commission may, by means of a decision, determine that a third country ensures an adequate level of protection. The effect of such a decision is that personal data can flow from the 25 EU Member States plus EEA to that third country without any further safeguard being necessary. The Commission has so far recognized Switzerland, Canada, Argentina, Guernsey, Isle of Man, the US Department of Commerce's Safe harbor Privacy Principles, and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection as providing adequate protection.

10. *Four Requirements Resulting from the Directive 2002/58/EC*

a. Confidentiality of Communications

Ex Article 5 of this Directive the confidentiality of communications by means of public communications network and publicly available electronic communication services (and the actual traffic data) is ensured through national legislation in a way analogous to the centuries-old secrecy of correspondence. In particular, listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned and except when legally authorized to do so is prohibited. However, legal authorization for the

monitoring of electronic communications is possible when it constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the communications system.

b. Traffic Data

Article 6 requires that traffic data (i.e. any data processed for the purpose of the conveyance of a communication) relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed but such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

c. Location Data

Article 9 defines location data as data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user. Such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service.

Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

d. Unsolicited Communication

Article 13 makes clear that the use of electronic mail for the purposes of direct marketing is only allowed in respect of subscribers who have given their prior consent (opt-in). As an exception on this general rule, it remains possible for merchants to send electronic mail to their own customers for direct marketing of similar products or services provided that customers *clearly and distinctly* are given the opportunity to object. Other types of unsolicited communications (than electronic mail – for instance, SMS) for purposes of direct marketing are subject either to an opt-in or opt-out system (at the discretion of the Member States). [19]

6. A Privacy Architecture for Internet applications

6.2 Anonymity

In order to warrant privacy protection the first principle is that the design must start from maximum privacy. This means that interactions are *a priori* anonymous or pseudonymous. Privacy and anonymity is also ensured with respect to system operators, although anonymity revocation might be needed for resolving disputes and supporting law enforcement. Data should be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which they were collected/processed [9].

Therefore the possibility of identification of the data subject, i.e. linking personal data with an individual should be removed as long as it is not longer indispensable. This may be achieved through anonymization or pseudonomyzation of personal data.

Data that is no longer needed for the purpose(s) for which it was collected/ processed should be erased; for certain categories of data, such as traffic data, this requirement is specified in Article 6 of Directive 2002/58/EC.

Furthermore users should be aware about the planned retention period of their data. They should be provided with this information prior to giving their consent for the processing[6]. After the expiration of the retention period the personal data is either deleted or made anonymous and users must be aware of this fact. Therefore, it is necessary to inform users when their personal data is deleted or anonymized upon the expiry of the retention period.

Article 17 paragraph 1 of the DPD on the protection of individuals with regard to the processing of personal data and the free movement of such data regulates components like anonymity and pseudonymity and further the security functions of the ISA and the PII. Article 17 of the DPD requires data controllers to implement 'appropriate technical and organizational measures' to protect personal data. Recital 46, in explaining the meaning of Article 17, highlights the requirement that these measures should be taken 'both at the time of the design of the processing system and at the time of the processing itself'. Thus indicating that security and data protection cannot simply be bolted onto data systems, but must be built into them. Although this provision mainly concerns data security, it is generally intended as a safeguard against other forms of unlawful processing. Based on article 17 of DPD the concept of Privacy Enhancing Technologies (PET) has been developed in 1994 by the Dutch data Protection Authority [3] and fully applied in the design of the Privacy Incorporated software agent (PISA) [10].

---

[6]Some national privacy laws provide that this information need not be provided if personal data is collected for purely research or statistical purposes.

6.2 Consent

Apart from the fact that the starting point for designing information systems and Internet applications should be anonymity and pseudonymity, consent management is the most important. It should be kept in mind that, according to the DPD, a data subject's consent means "any freely given specific and informed indication by which the data subject signifies his agreement to personal data relating to him being processed". The data subject must be given the opportunity to give his consent in a clear, unambiguous way. Many national privacy laws use other adjectives describing consent: "freely", "specific", "informed", "unambiguously" and "explicit". Interface elements for making privacy decisions (such as giving consent) should be prominent and obvious.

It is crucial that users understand when they are entering into a contract for goods or services and the implications of that contract.[7] They should also be aware of and understand the special cases where their personal data may be processed without their consent (without a contract).
Thus three aspects to be taken into account concerning consent. First the data subject must freely express (without being put under pressure) his or her wishes. If there is no free will then any consent given will be void. Secondly the consent must be aimed at a specified purpose of processing and specific data. A general-purpose consent is not acceptable under the DPD. Thirdly the consent must be free of a double meaning, clear and certain. With regard to PISA an affirmative answer can be given to the legal question whether such an agent [1] can give unambiguous consent required by the law for legitimate processing of the PII on behalf of the user.

Bygrave [2] points out that if the consent is carried out via electronic agents that such consent will only be valid if it manifests itself in accordance with the DPD requirements. After consultation of the European Commission concerning the PISA project the legal position is that the instructions to the agent should be very specific and time bound. This requirement can be met if a specific one-time task intelligent software agent with a pseudo-identity is generated or created for only one specific transaction or piece of work carrying around no more personal data than strictly necessary. This specific task agent will be proof of the required unambiguous consent for that transaction or imposed piece of work only.

More complicated is the fact that the DPD prohibits the processing of sensitive or special categories of data[8] like data revealing race or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sexual life. This ban on processing those data is lifted when processing occurs after explicit consent of the data subject. The required consent may be given in such an

[7] This requirement follows not only from the data protection legislation, but also above all from the series of EU and national consumer protection measures, as well as the Directive 2000/31/EC on electronic commerce.

[8] See article 8 – 95/46/EC

electronic form combined with a biometric string of the user that the non repudiation and explicitness is beyond doubt, provided that an accompanying timestamp with the instruction of explicit consent from the user is recent, i.e. not older than 24 hours. Article 8 paragraph 2 defines exemptions to the prohibition like situations in which data are processed for medical care. By way of an example, the French data protection law requires "express consent" for the processing of sensitive data, and that has been interpreted as requiring that the consent be expressed in writing. The French Commission Nationale de l'Information et des Libertes (CNIL) accepted that, with regard to processing of sensitive data on the Internet, one might substitute a "double click" for this consent (i.e. one "click" to confirm that one is aware of the proposed processing, and a further one to "expressly" consent to it).

6.3 Translation of privacy rules into the design / legal instantion

In order to assure a system design against privacy risks as discovered in the privacy threat analysis[9], the privacy law rules must have a strong influence on the design forcing the system designer to obligatory represent the data protection rights and duties into the system. The legal instantiation procedure works as follows:

First the core text of the DPD and DPEC is selected and analyzed, then the rules and exceptions to the rules are extracted and broken down into sentences, like "individuals, have to be informed about processing of their data; have the right to consult the data; to request corrections and to object to processing in certain circumstances". Then the source of the broken down text is registered, for example recital 25 and articles 10 and 11 of the DPD. The next step is the abstraction to generate general concepts formed by extracting common features for specific instances. The activity of rule abstraction is the substitution of a rule with super classes or super properties of these rules and an abstracted term that can substitute the terms that are the sub classes or terms that are with sub properties. For example white can be abstracted into "color" at a lower level and into object description at a higher level. Legal experts are consulted for the relevant legal terms and the legal notes corresponding to these terms. The whole process ends in to lexon engineering. After the breakdown simple sentences representing elementary facts must be produced. The criterion to use for an "elementary fact" is that it cannot be split into smaller constituent parts. The sentences should correspond to a simple "subject-verb-object" structure. Facts represented by such a structure resemble a lexon, but not yet in a formalized form that is needed for the privacy ontology engineering.[10][11].

---

[9] J.J.Borking, The status of Privacy Enhancing Technologies in Certification and Security in E-Services..(E.Nardelli et all, eds) Boston 2003 p.215-221

[10] The described methodology in a nutshell is the PRIME OCM (ontology capture methodology) December 2005. See also STAR lab report 2005-3 of the Free University of Brus-

In the Privacy Incorporated Software Agent (PISA) project [12] first the worldwide accepted privacy principles as for example known from the Convention 108 of the Council of Europe and the 1980 Organization for Economic Co-operation and Development (OECD) guidelines [13] were determined. At the time of the design of the privacy protecting agent it was decided that a simplification of the DPD was necessary as the developers of PISA weren't able to create lexons and privacy ontologies from the refined legal text of the DPD directly. The simplification was realized through the linking together ('chaining') of selected articles of the DPD that belong to the chosen privacy principles. Take for example the principle of transparency [14] that defines that everyone must be informed about what is done with his/her personal data and that the data subject must also be informed of this as the data subject is mostly not aware of the multitude of parties that take part in the processing nor in the data flows.
This principle is a concatenation of the articles 10 a, b, c, 11 section 1 a, b, c, 11 section 2, 13 section 1 a, c, d, e, f, g, 13 section 2 and several recitals of the DPD. Such a representation clusters the DPD articles into logical components generic enough to encapsulate the general meaning of the articles from which they have been derived.
Some articles of the DPD are not belonging to the domain of privacy principles and do not need to be implemented into PISA or in general into the Information system architecture and Internet application design but play a vital role for explanation and interpretation like articles 2 a till h (definitions), 3 section 1, 3 section 2, 4, section 1 a, b, c, 4 section 2, 5, 9, 15 section 1, etc. and influence indirectly the architecture. Some articles are not relevant for the architecture like the DPD requirements for the supervisory authorities, the legal remedies etc.

After the concatenation of the DPD articles into privacy principles the next step in the PISA project was splitting the principles into the tiny elements. Thus the principles are deconstructed into a set of elements that relate to the articles they have been derived from and emphasize the context and what has to be achieved. For example: 1. *The Principle of Transparency*. In order to realize transparency it is necessary that: 1.1. *Data subject (DS) is aware of transparency opportunities*; Thus when 1.1.1. *Personally Identifiable Information (PII level 1 till 3) collected from DS*; then 1.1.1.1. *Prior to DS PII capture: DS informed of: controller identity (ID) and Purpose Specification (PS)* According to the DPD it is also a must that, prior to DS PII capture 1.1.1.2 *Controller is informed of whether PII contains special categories of data* and *1.1.1.3.whether PII have to be treated accordingly to the sensitivity of these data*. Further more elements have to be formulated around information duties, PII distribution, explicit consent and controller obligations For example 2.1. *A controller must process according to his PS* and according to the finality principle 2.2. *DS being aware of controller PS and the*

---

sels, M.L.Reinberger, P.Spyns, Unsupervised Text Mining for the Learning of DOGMA-Inspired Ontologies

retention period (RP), prior to 2.3. *Being presented with a opt in consent decision for having PII processed*, except where PS is statistical data. Etc.
All privacy principles have been treated in PISA as stated above and subsequently the lexons and the privacy ontologies[11] have been developed as a mechanism to achieve shared understanding, neutralizing the problem of two databases using different identifiers for what is the same concept, such as postal code for achieving that all intelligent software agents act in the same way while transferring privacy preferences and privacy policies. These ontologies with taxonomies and a set of inference rules providing the relational aspects of the taxonomies lead to a simplified but correct conceptual model of the privacy principles and has been build into PISA and used as a backbone in conversations between agents.

6.4. Interaction protocols

The interaction protocols show how the communication among senders and receivers in Internet, for example via software agents, should be organized. The protocols will need to be combined for executing the given tasks. The basic protocols related to the transfer rules and data subject rights are explained below.

The sender of personal identifiable information (PII) must be able to determine whether or not the PII can be sent and for this purpose it needs both information on the agent that would receive the PII and privacy metadata on the PII. From the receiver it needs to know the privacy policy and the metadata of the PII is important because it contains the privacy preferences of the data subject. The sender of the PII must compare the privacy preferences with the privacy policy using the privacy transfer rules as stated hereunder. The privacy transfer rules consist of one or more rules per privacy principle. If the transfer rules are evaluated positively and the PII is sent to the receiver, the metadata on the PII containing the privacy preferences of the data subject must be sent along with the PII. This way the receiver can act as a sender of PII in its turn.
The expressions that are evaluated positively (true) in the processing of the rules result in an agreement for transfer. All parts of all principles must be matched with positive results before information is sent[12].
T = true (positive result)
F = false (negative result)

Transparency
For the principle of transparency it looks as follows:
The data subject can specify in his privacy preferences whether he requests transparency or not (Y/N). The receiver can offer no transparency (N) or the legally required transparency applicable in the EU (Y). If the data subject requests transpar-

[11] http://www-ksl.stanford.edu/kst/what-is-an-ontology.html
[12] M. van Breukelen, A.P. Meyer, A.Ricchi. Privacy Transfer Rules in Deliverable D3 PISA project IST-2000-26038, 1 September 2002

ency the receiver must offer it, otherwise it doesn't matter, thus three out of four possible combinations return a positive result.

t^{pref} / t^{pol}	**N**	**Y**
N	*T*	*T*
Y	*F*	*T*

$$(\neg t^{pref} \wedge \neg t^{pol}) \vee (t^{pref} \wedge t^{pol}) \vee (\neg t^{pref} \wedge t^{pol})$$

Finality

The principle of finality has two aspects: purpose binding and retention period.

Purpose Binding

The data subject can specify in his privacy preferences for what purpose information may be used. The receiver may not use the information for any purpose that is not specified by the data subject. Thus, all the purposes that are specified in the receiver's policy must also be specified in the data subject's preferences.

$P_{pref} = \{p_1, \ldots, p_n\}$, n>0 — data subject's preferences for purposes (required)
$P_{pol} = \{q_1, \ldots, q_m\}$, m>0 — receiver's policy for purposes (provided)

$$\forall_{1 \le i \le n, 1 \le j \le m} q_j \exists p_i : p_i = q_j$$

Retention Period

The data subject can specify a deadline in his privacy preferences by which the information must be deleted (retention period t_{pref}). The receiver's retention period (t_{pol}) must be shorter or equal than what the data subject requests.

$$t_{pref} \geq t_{pol}$$

Legitimate ground of Processing

The data subject can specify in his privacy preferences for what other processing his PII may be used[13]. The receiver may not use the information for any processing that is not specified by the data subject.

$P_{pref} = \{p_1, \ldots, p_n\}$, n>0 — data subject's preferences for processing (required)
$P_{pol} = \{q_1, \ldots, q_m\}$, m>0 — receiver's policy for processing (provided)

$$\forall_{1 \le i \le n, 1 \le j \le m} q_j \exists p_i : p_i = q_j$$

[13] e.g., internal or external marketing, list brokering

7. Privacy Preferences, P3P and Privacy Policies

From a social anthropological perspective, Perri Six has pointed out that every human being has its own privacy preferences that alternate with the situation in which personal data are required [15]. The user should set its own privacy preferences. W3C has developed a tool named: P3P as an easy way to communicate about privacy preferences in a standard machine-readable format. The vocabulary of P3P[14] shows who is collecting data, what data is collected, for what purpose data will be used, what are the opt-in and opt-out alternatives for some data uses, who are the data recipients, to what information does the data controller provide access, what is the data retention period, how will disputes about the policy be resolved and where is the human readable privacy policy. Such a policy (in order to achieve a well-balanced processing policy for personal data and to implement and maintain this properly) must occupy an important place in the management cycle. A privacy policy should be based upon established privacy principles, such as the privacy principles described earlier in this paper and regulatory requirements specific to the region(s) the company is operating in.

The privacy policies and privacy statements the user encounters on the websites within the legal realm of the EU should offer a minimum and non-negotiable level of protection for all individuals falling within its application. In our global Internet the user will be confronted with all kinds of legal regimes that are not on the same level as that of the EU. If user meets lower privacy protection levels than the EU legal regime the website should report to this to the user and request for an explicit consent to transfer personal data. In PISA the agent would report directly to the user if he detected an agent that carried an agent practices statement that wasn't in conformity with the privacy preferences of the user.

The privacy policy built into the ISA has to act according to the level of privacy preferences of the user. The highest possible protection for the user of the agent would mean that all privacy principles would be applicable. For example, the minimum position for transparency would be constant logging of the disclosure of highly sensitive personal data by the ISA and his whereabouts.

Ideally if personal data are transferred to other websites or controllers, than these data must have a marker or tool that prevents unwanted processing like secondary use incompatible with the primary purposes for which data are processed. For example if the privacy preferences state that the other party may use the personal data for a specific purpose and a specific retention time, those data should be automatically deleted accordingly. No reliable technological solution exists yet that gives the sender of data personal control over data once data has been transferred from a him to a receiving website, albeit that ideas are developed that facilitate controlled distribution of digital personal information[16]. In PISA as long as ISAs encounter web sites or security hubs that do not match the privacy preferences of the ISA, the ISA will function either anonymously, under a pseudonym or no contact will be made at all because of privacy or security risks.

---

[14] See http://www.w3.org/p3p/

8. Conclusions

Architects and developers should built-in all discussed privacy protection features to ward off privacy intrusion risks and legal liabilities, expressed in the rules of the Directives 95/46/EC and 2003/58/EC. Furthermore such features are a necessity in the expression of the privacy preferences of the user and also in the receiving of the PII of others and the handling of personal data. The PII of the user and the received PII of others have to be managed and processed according to the law. From a point of view of product liability, the developer is liable for privacy infringing code and from a privacy point of view malfunctioning Internet application and information systems intruding the privacy of others or damaging the privacy of its user that makes the controller accountable.

References

1. J.J. Borking, M. van Eck, P. Siepel, Intelligent Software Agents and Privacy - A&V # 13- The Hague 1999
2. L.A. Bygrave, Electronic Agents and Privacy in International Journal of Law and Information Technology Volume 9 No 3
3. See J.J. Borking, C.D. Raab, Laws, PETs and Other Technologies For Privacy Protection -Journal of Information, Law and Technology (JILT) January 2001C.D.
4. See Common Position on Intelligent Software Agents: adopted by the International Data Commissioners ("Berlin") Working party on 29 April 1999.
5. J.J. Borking, J. Giezen, P. Verhaar, R. Coolen, Methodology of Privacy Threat Analysis, Deliverable 7 of WP 2 of the EU PISA project IST-2000-26038. The Hague 2001
6. J.J.Borking, The status of Privacy Enhancing Technologies in E.Nardelli, S.Posadziejewski, M.Talamo, Certification and Security in E-Services, From E-Government to E-Business, Boston, 2003 ISBN 1-4020-7493-X
7. See www.prime-project.eu.org/ PRIME deliverable 6 - 2005
8. G.W. van Blarkom, J.J.Borking, J.G.E.Olk, Handbook of Privacy and Privacy-Enhancing Technologies, The case of Intelligent Software Agents The Hague 2003 ISBN 90-74087-33-7, The main feature of such "just-in-time-click-through agreements" (JITCTA) is not to provide a large, complex list of service terms (as in a typical on-line user agreement), but instead to confirm understanding or consent on an as-needed basis. The responses made by the user during the JITCTAs can be recorded so a clear and unambiguous record of agreements made by the user is ensured. In order to implement JITCTAs, the software has to recognize when users are about to use a service or feature that requires that they understand and agree to some term or condition.
9. As a reference a paper: J. M. Seigneur and C. D. Jensen, "Trading Privacy for Trust," presented at The Second International Conference on Pervasive Computing, Vienna, Austria, 2004. They also speak about use of pseudonyms
10. The PET concepts of anonymity, pseudonymity, unlinkability and unobservability are also described in ISO 15408 Common Criteria for Technology Security Evaluation.

11. Peter.Spijns, Yan Tang, Giles Hogben, John Borking, PRIME deliverable WP 7.3. Executing the steps results in an ontology according to the DOGMA ontology frame work (STAR lab VUB Brussels)
12. S. Kenny, J. Borking, The Value of Privacy Engineering, in The Journal of Information, Law and Technology (JILT), 2002 (1), http://elj.warwick.ac.uk/jilt/02-1/kenny.html.
13. 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data'
14. The article 29 DPD Working Party states in Privacy on the Internet, an integrated EU approach to Online data protection Working Document 37 Brussels November 2000 how transparency should be applied in on-line systems. For Recommendations for online collection of data see http://www.europa.eu.int/comm/privacy
15. Perri 6 -(2001) '*Can we be persuaded to become PET - lovers?*' to be published by Organization for Economic Co-operation and Development Kathy Cartrysse, Private Computing and Mobile Code Systems-Delft 2005 ISBN-10: 90-90199-53-5
16. S. Kenny, and L. Korba, Applying Digital Rights Management Systems to Privacy Rights Management *Computers&Security,* vol. 21, no. 7, 2002.
17. Stefan Brands, Rethinking public key infrastructures and digital certificates building in privacy Utrecht, 1999 ISBN 90-901-3059-4
18. Kathy Cartrysse, Private Computing and Mobile Code Systems-Delft 2005 ISBN-10: 90-90199-53-5
19. B.W.Schermer, M.Durinck, L.Bijmans, Juridische Aspecten van autonome Systemen (Legal Aspects of Autonomous Systems) The Hague 2005 ISBN 90-76957-15-0