Kirsten Bock

EuroPriSe Trust Certification

An approach to strengthen user confidence through privacy certification

Trust marks are well known arbiters of trust. To be successful, sustainable and trustworthy the underlying certification scheme ought to implement specific requirements including transparent criteria and procedures verifying the actual trustworthiness of the recipient by an independent certification authority. The concept of an explicit trust certification scheme is set forth in this article using the example of EuroPriSe, the European Privacy Seal for IT products and IT-based services.

Introduction

The fast development in the ICT-sector has lead to a confusingly many-faceted market. Consumers as well as professionals face a number of serious problems when using the Internet or when seeking to purchase an IT product or an IT-based service. They could stick with the familiar names and addresses, but often this is not an option and would moreover reduce the number of products or services to choose from. Users have no way of knowing whether a product, service or site is trustworthy and whether it will act as expected. Data greediness and data collecting mania of private and public entities have created concerns causing a lack of trust.[1] Personal data for instance are collected whenever possible, at the cash-counter or on the internet, and often without the knowledge and consent of the person affected. Malicious spyware is hidden on computers and spam is sent ferociously. Companies' possibilities to exchange data for insights into user behaviour are huge. The increasing amount of personal and behavioural data collected and exchanged through ICT is a growing source of user unease additionally fuelled by recent security incidents. Government agencies investigate only a small number of ICT offerings and their interventions seem inapt considering the great number of internationally operated unlawful or even malicious sites and services.[2] Unsurprisingly 64% of respondents of a survey conducted on behalf of the European Commission on data protection are concerned about data protection issues and feel that awareness and information on these topics are not yet satisfactory.[3] Without guidance users would be left on their own. But lack of accountability carries substantial risks. Users tend to take precautions and be reluctant to buy products and services or even join sites. Research on behavioural privacy decisions indicate that consumers have a demand for privacy and privacy indicating trust marks.[4] Yet, it is difficult to identify the balance point between consumer rights to data protection and business' desire to improve sales. Data controllers in private companies for instance believe that legislation cannot cope with the increasing amount of personal information being exchanged.[5] Self-regulatory approaches have been introduced to fill in the gaps. Voluntary privacy certification strives for propagation of trust.

This article elaborates on the requirement for privacy certification and trust marks aiming at the propagation of trust. EuroPriSe will be introduced as an example for a voluntary[6] privacy trust mark based on a privacy certification concept for IT products and IT-based services. It does not consider company audits.[7] The concept of trust and its effects on privacy certification and trust marks will be considered, thereby ensuring a common understanding of trust, certification, and trust marks. Certification by a trusted third party offers an instrument of regulated self-regulation to business to reassure users and gain trustworthiness. I will argue that a certification scheme that aims at propagating user trust must fulfil a specific set of requirements. It ought to implement transparent criteria and procedures verifying the actual trustworthiness of the recipient by an independent certification authority. The experiences gained in EuroPriSe, the European

Ass. iur. Kirsten Bock

is International eGovernment Coordinator and Project Manager of EuroPriSe – European Privacy Seal at the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
E-Mail: kbock@datenschutzzentrum.de

1 Cf. *Verbraucherzentrale Bundesverband*, Modernisierung des Datenschutzes aus Sicht des Verbraucherschutzes, Dud 4/2007, p. 271.

2 Cf. *Schaar*, Modernisierung des Datenschutzes: Ethik in der Informationsgesellschaft, DuD 4/2007, p. 263.

3 "Data Protection in the European Union, Citizens' perceptions" http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf (accessed August 1, 2008).

4 *Tsai/Egelman/Cranor/Acquisti*, The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study, June 2007, http://weis2007.econinfosec.org/papers/57.pdf.

5 Ibid.

6 Legally mandatory certifications as required e.g. for electrical and other safety equipment serve additional legal purposes. They are not subject of this article.

7 For company audit certification cf. *Hammer/Schuler*, pp. 77ff., DuD 2/2007.

Privacy Seal project are used to sketch a model for trust certification.

EuroPriSe

The European Privacy Seal (www.european-privacy-seal.eu) offers voluntary certification[8] to manufacturers and vendors of IT products and IT-based services. Under the scheme, products and services are evaluated in order to check if they can be certified as compliant with European regulations on privacy and data security. It applies a two-step procedure: first, an evaluation of the product or service by accepted legal and IT experts, followed by a cross-checking of the evaluation report by an accredited certification body.

EuroPriSe is a project funded by the European Commission's eTEN programme with 1.2 million Euros and implemented by a consortium of nine organisations[9] under the leadership of the Independent Centre for Privacy Protection Schleswig-Holstein (ULD).

The objective of the initiative started in June 2007 is to foster privacy enhancing technologies by marketing mechanisms with the objective to propagate more and better privacy solutions and thus to enhance consumer protection and to implement the right to informational self-determination.[10] The idea behind a product certification from regulators point of view is to provide an incentive for business to incorporate privacy and data protection into the products and services they offer.[11] A trust mark can be used in marketing distinguishing privacy compliant and privacy enhancing products and services.[12] It makes privacy-friendly IT products and IT-based services visible for business customers and consumers.

The positive experiences and lessons learned from the implementation of a regional privacy seal, the Gütesiegel,[13] in Schleswig-Holstein was a starting point for the implementation of a privacy seal on a European level. The EuroPriSe project currently conducts a market evaluation for the European Privacy Seal. The mid-term findings and experiences provide the background of the following analysis.

Trust Certification

Certificates and trust marks are fairly well known instruments to verify trustworthiness. Especially online-merchants addressing potential customers scatter impressively looking labels over their web site to assert that their site is safe to use and offers considerable quality. These labels claim authority and suggest that the site has been inspected by a certificate-granting organisation. Users and customers usually understand the message and even tend to extend it towards anticipation of general approval.

Trust certifications for Internet web sites have been introduced by non-governmental organisations or companies such as TRUSTe, BBBonline, Trusted Shops or Confianza Online in many countries.[14] Product certification is offered by ULD with the Guetesiegel based on Schleswig-Holstein state law[15] and the European Privacy Seal – EuroPriSe. These so-called trusted third parties issue certificates based on specific procedures and criteria with the common goal to reassure users of trustworthiness. Trust certificates are usually combined with a picture and/or word emblem, the trust mark, to easily distinguish its subject, e.g. the product, service or site, to which it has been awarded.

In the past the main incentive for companies to gain a trust mark through certification has been for marketing and image reasons. Accordingly the effectiveness of a certificate was measured by comparison of certification costs against the increase of revenue. Due to increased demands for compliance attestation in general (e.g., Basel II, Sarbanes-Oxley-Act, quality management), there seems to be an increasing demand of demonstrating privacy compliance. Some EuroPriSe pilot participants have indicated that a rigorous assessment provides additional value through the evaluation process. Ideally, the evaluation process and reports help companies to optimize their products and services development and improves risk management.

Nevertheless, the approach to propagate user trust and secure market share by implementing certification schemes to enable the consumer to distinguish the good from the bad is being questioned in several respects.[16] Shortcomings of existing schemes will be addressed when discussing the single aspects. For the purpose of this discussion and in order to elaborate on the necessary compounds and the requirements for credibility and trustworthiness it is necessary to have a solid understanding of the concept of trust, certification and trust mark to start with.

Trust

Trust is not a trivial matter.[17] Once lost it is hard to regain. Trust is the belief that someone (or an entity) will behave as expected.[18] But behaviour is influenced by factors that might or might not be known; they might be unpredictable and even uncontrollable for the person who trusts. The expectation is created by the information available about the object of trust. Additional information can alter the amount and content of knowledge. As Thomas and Venter[19] point out, trust value can thus be quantified and change positively or negatively depending on the update of knowl-

8 Voluntary privacy certifications meet greater acceptance among manufacturers. Unlike mandatory standards voluntariness allows for a special qualification feasible by criteria compliance. Mandatory certifications tend to settle for criteria based on the least common denominator whereas voluntary certifications can establish good practice standards. Cf. on this IPSE (Initiative on Privacy Standardization in Europe): Final Report, February 2002, http://europa.eu.int/comm/enterprise/ict/policy/standards/ipse_finalreport.pdf.

9 The partners from eight European countries include the data protection authorities from Madrid (Agencia de Protección de Datos de la Communidad de Madrid, APDCM), and France (Commission Nationale de l'Informatique et de Libertés, CNIL), the Austrian Academy of Science, London Metropolitan University from the UK, Borking Consultancy from the Netherlands, Ernst and Young AB from Sweden, TÜV Informationstechnik GmbH from Germany, and VaF s.r.o. from Slovakia.

10 Cf. *Bock*, DuD 2007, 410.

11 See *Bäumler*, Marktwirtschaftlicher Datenschutz, DuD 6/2002, p. 325 ff.

12 Cf. *Bäumler*, Der Konkurrenz einen Schritt voraus, in: Bäumler/von Mutius (ed.), Datenschutz als Wettbewerbsvorteil, Braunschweig/Wiesbaden 2002.

13 Detailed information on the Gütesiegel is available at https://www.datenschutzzentrum.de/guetesiegel/index.htm.

14 http://www.truste.org/; http://www.bbbonline.org/; http://www.trustedshops.de; http://www.confianzaonline.org/.

15 The seal is based on § 4 sect. 2 of the State Data Protection Act of Schleswig-Holstein and regulated by a state ordinance available at https://www.datenschutzzentrum.de/material/recht/guetesiegel-verordnung.htm.

16 Cf. e.g. *Edelman* (2006); BITKOM (2007).

17 The concept of trust has been subject to a number of publications in different academic fields; in the area of ICT mostly with a focus on the application of trust in information security. Cf. for further references *Backhouse/Halperin, A survey on EU Citizen's Trust in ID Systems and Authorities, 2007, pp. 4 ff.*

18 *Swarup/Fábrega*, Trust: Benefits, Models, and Mechanisms. Secure Internet Programming, pp. 3 ff., 1999.

19 Cf. *Thomas/Venter*, Propagating Trust in the Web Service Framework, 2004, pp. 2f.

edge, e.g. by experiences gained in interaction with the trusted entity. Consequently information such as the receipt of a certificate or trust mark can influence the expectation and therewith the amount of trust. Obviously the amount and quality of information can make a difference.

A Definition for Certification and Trust Mark

Definitions suggesting certification to be "the confirmation of certain characteristics of an object, person, or organization […] often, but not always, provided by some form of external review, education, or assessment"[20] lack to acknowledge that the subject of certification can be manifold and does not influence the basic characteristic of certification and should not be included in the definition. Of course certification can focus on objects, persons and organisations, but additionally services and processes in general can be subject of certification. The same is true concerning the procedure of confirmation, the evaluation. Review, education or assessment being examples of evaluation can be formal or informal. Only the issuance by an external authority distinguishes confirmation from certification. Thus, the term "certification" as used in the following is defined as the confirmation of certain characteristics by an external[21] authority. Accordingly, a certificate provides proof in writing, whether on paper or in e-format, about the fact of certification and its validity[22]. A trust mark or seal serves the same purpose providing information on the fact of certification in a condensed form.

Internet trust marks have been discussed in literature occasionally but only with very few attempts to define the term. Rüdiger[23] offers a definition for Internet trust marks (German: Internet-Gütesiegel) specifically with respect to online merchants as recipients. He defines Internet trust marks as word and/or picture emblems that are issued by independent institutions and used by online-merchants to distinguish their website by informing their customers or their potential customers in a condensed form that the recipient has complied with requirements (in the form of codes of conduct, criteria catalogues, norms, guidelines or the like) set out by the issuing institution covering privacy, IT-security and consumer protection. Adopting this approach for diverse targets of evaluation, trust marks can be defined as word and/or picture emblems that are issued after successful certification by the certification authority; and to be more explicit, trust marks are word and/or picture emblems that are issued by external authorities and used by recipients to distinguish a specific target of evaluation by informing the customers or the potential customers and users in a condensed form that the recipient has complied with requirements set out by the issuing authority. Trust marks aim at enabling consumers to easily identify that a certain product or service has undergone certification expressing key messages such as "privacy respecting" or "secure".

Fig. 1 | EuroPriSe mark explanation

Basic Compounds and Principles of Trust Certification

A certification scheme aiming at trust and creditability must incorporate basic compounds and principles. It must determine the responsible authorities, the procedures, formal requirements such as the use of templates, and finally, the content respective the criteria. Basic principles to adhere to are legitimacy, transparency and reviewability. This requires profound and comprehensive documentation of general certification procedures, evaluation reports, criteria as well as information on the certified products and services and the certifying authority.

The key elements to determine are

- the message,
- the general procedures including terms and conditions, and eligible participants,
- the evaluation,
- the evaluators,
- the criteria,
- the certificate and/or the trust mark attached to certification, and
- the authority issuing the certificate.

The Message

As pointed out before, trust is based on and can be altered by information. In order to propagate trust, certificates and trust marks ought to have clear and easy to understand key messages "at first glance".[24] Certification and trust marks work on a basis of layered information, the trust mark carrying information in the most condensed form; it is the top of an iceberg. Its objective is to reassure customers' confidence while keeping him or her clear of in depth information. It carries the basic message "confirmed by an authority"[25], addressing the consumer to "trust because the product has been checked by someone who knows". This information provides only little value if it is not specified. Therefore most trust marks carry additional information such as IT security, secure payment, consumer protection, and privacy and data protection.

Trust marks hide or rather offer an entrance for more in depth information. If displayed on a website the trust mark emblem is linked to further information about the certification and the underlying criteria.

The message determines the whole concept of a certification scheme. It ought to be reflected by the definition of the scope of certification.

European Privacy Seal is based on European Privacy Regulations reflected in the criteria the product or service is evaluated against as well as in the procedure. The evaluation is conducted by experts with legal and technical know-ledge as the criteria require compliance with legal as well as technical requirement.

20 Cf. http://en.wikipedia.org/wiki/Certification.

21 Company internal confirmation does not incorporate adequate authority per se. The term external could be replaced by the term independent. However, whether and under which conditions internal evaluation is independent or might otherwise qualify for certification must remain outside the scope of this article.

22 Confirmation can only be reflected upon a certain point of time and is therefore usually restricted in its validity to a specific time-period.

23 *Rüdiger*, Internet-Gütesiegel in Spanien, DuD 6/2007, p. 3 ff.

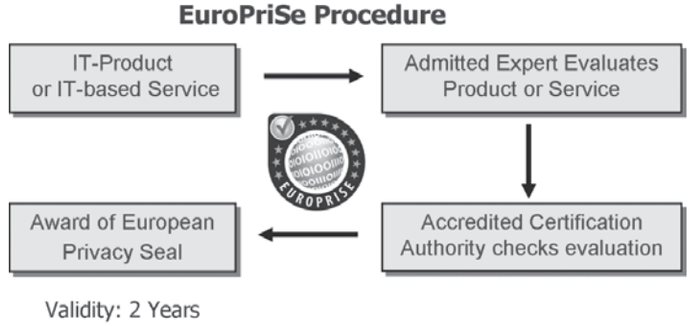
24 Cf. *Verbraucherzentrale Bundesverband e.V.*, Modernisierung des Datenschutzes aus der Sicht des Verbraucherschutzes, DuD 4/2007, p. 274.

25 The CE conformity mark for example only declares conformity with EU-law. It is not considered to be a trust mark because certification by an independent authority is not required. The European Parliament currently discusses a Motion for a Resolution in order to exchange the CE with a „European Consumer Safety Label". The motion is accessible at http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B6-2007-0352&language=EN.

The EuroPriSe trust mark carries the message that the certified product or service is in line with European privacy (regulations). If presented on a website, it must be linked to the EuroPriSe website providing more information on the certificate and the product.[26]

EuroPriSe certifies that an IT product or IT-based service facilitates the use[27] of that product or service in a way compliant with European privacy and data protection regulations. The message implies that the product or service can be easily used in a way that complies with European data protection regulations and that it does not consist of any functions violating these regulations or which are inappropriate in respect of technical security.

Fig. 2 | EuroPriSe Procedure



Certification Procedure

The establishment of certification procedures grants procedural equality. There are many examples describing standardized processes. The procedure should be simple and non-bureaucratic in order to gain acceptance. The relevant international standards on accreditation, certification and evaluation (such as ISO/ICE 1700, EN 45000) have to be recognized as far as relevant for privacy certification. Existing audit schemes recognise private evaluators and independent certification bodies granting a seal in a two-step procedure. Others give certification powers directly to the evaluator.

For IT product certification a quality secured procedure as established for IT-security certification[28] is appropriate. A two-step procedure separates the evaluation of a product and the actual certification. The certification includes a cross-checking in accordance with the four-eye principle. Thus the cross-checking provides an additional assurance of the quality of evaluation and ensures consistent use of criteria among evaluators. It also recognises the rather sensitive nature of the relationship between manufacturer and evaluator: The manufacturer shares confidential information with the evaluator. Consequently, evaluators should not belong to a supervisory body and they should not perform official controlling tasks. It would also contradict the voluntary character of this privacy instrument to determine an official public evaluator.

Most manufacturers seem to give preference to a two-step procedure over a one-step certificate from the evaluator. The granting of a certificate by the evaluator himself is always deemed problematic because the evaluator is paid by the manufacturer. Moreover, if the certifier is an independent body, the procedure is anticipated as unbiased and valued highly implying greater credibility.

EuroPriSe has adopted the quality secured two-step procedure:

Results from the training of EuroPriSe Experts underlined the necessity of a validation level. Training evaluations of experts with considerable experience in IT security and IT law showed considerable difference in evaluation results.[29] Especially in privacy and data protection where only few measurable standards exist and interpretation of the law plays an important role, validation is inevitable to guarantee a consistent level.

Documentation of certification procedures is essential and should be publicly available for reasons of transparency adding greatly to credibility and acceptance. It must include the main steps, guidelines and rules of certification in a general manner. The documentation of procedures must cover the main terms and conditions under which certification is granted covering certification including evaluation and issuance, recertification, investigation and checks, revocation, dispute-settling, and accreditation of evaluators.

In addition to a comprehensive and confidential evaluation report the EuroPriSe procedure requires a public report in which the basic information about the product or service is published and thus facilitates comparability.[30]

In accordance with statements from applicants, the broad acknowledgement of the seal results from this separation in task and the four-eye principle: A private trusted evaluator chosen by the manufacturer and the involvement of a public authority assuring the evaluation quality and providing credibility to the procedure.

When applying for certification, the evaluation report has to be submitted to the certifier for review with respect to methodology, consistency, and completeness. The certifier approves the product as compliant with the regulations of privacy and security (validation) and awards a privacy seal certificate. The validation of the experts' reports includes a completeness check (All relevant criteria evaluated?) and a plausibility check (Product description and experts' opinion reasonable?). Although the certifier will not conduct a second evaluation, specific questions on the product, its intended use and the field of applications may arise during the certification process. These questions have to be answered by the experts and/or the manufacturer. The main task of the certifier is to ensure comparability of all the evaluation results: As data protection regulations often include the weighting of interest (with respect to legal topics) and the decisions on adequacy (of technical security measures), expert's opinions on a specific topic might differ. The certifier will provide guidance in these cases.

26 Cf. for example http://eu.ixquick.com/eng/protect_privacy.html.

27 A product certificate is not a sufficient prerequisite for privacy compliant use. The certificate provides independent proof that the product does deliver the privacy performance defined in the certificate and that it can be used in a privacy compliant way.

28 Cf. Common Criteria 2.3 (ISO/IEC 15408:2005) and its successor Common Criteria 3.1 (not yet an ISO standard) for product certification and ISO 27000 IT Security Management Systems.

29 EuroPriSe training workshops took place in November 2007 and June 2008. From each workshop about 45 training evaluations from ten European Countries (in total) on the same fictitious product have been analysed.

30 EuroPriSe public reports can be accessed at http://www.european-privacy-seal.eu/awarded-seals.

Certification Authority

The acceptance of a certificate depends largely on the credibility of the issuing organisation. It is the true arbiter of trust. Especially consumers seem to trust a certificate in a higher degree if issued by an independent and recognized entity, preferably legally mandated or supervised by a public authority. Independence and knowledge are main requirements for credibility and effectiveness. A certification authority must have the profound knowledge to evaluate and assess the targets of evaluations. It must be capable of detecting and follow up shortcomings and infractions with high probability.[31] Financial independence is a precondition to objectively grant or not grant, or revoke certificates. Reliance on fees for successful certification can seriously endanger the independence of a certification authority.[32] The same applies to membership solutions. Involvement in product or service development excludes independence because a lack of objectivity is anticipated.

Certification bodies may impose the evaluation task to external experts according to the four-eye-principle. Experts must equally prove independence and knowledge. Their tasks and rules of admittance must be described in the documentation of certification procedures.

The EuroPriSe certification is conducted by data protection authorities granting knowledge and ensuring independence from business.

Target of evaluation

Precondition to any successful certification is the exact determination und description of the subject of certification, the target of evaluation (TOE).[33] It is a serious shortcoming of any certification if the TOE remains vague. This can often be observed in web site certification e.g. if the site contains multiple functionalities. Without a clearly identified TOE any evaluation suffers from vagueness in respect to its object and completeness of evaluation cannot be ascertained.

There is a significant difference whether a product, person or organisation, or a process is targeted. Certifications of operational processes, company internal procedures and management systems are generally referred to as audits which require a specific set of criteria and procedures.[34] The same is true for the assessment of a person and its skills, just as it applies to products and product-like services.

The European Privacy Seal is restricted to IT products and services. All IT products and IT based services processing or storing personal data can apply for the European Privacy Seal certificate. Products and services can be small or large in scope. The term „IT product" refers to hardware, software and to automated processes, e.g. to services and commissioned data processing such as the operation of a firewall or the physical destruction of data mediums. Other examples are software for public administrations (resident registers, social welfare, etc.) or administration of health data (remote PACS storage, health information systems, etc.). It can range from local desktop applications to nationwide services or internationally used software. Subject to certification is not only the technical product or service but also and among other aspects its documentation and its possibilities to be configured e.g. adapted to national requirements.

Certification Criteria

The heart of each certification scheme is represented by the certification criteria. They are composed of a set of characteristics to which the product or service is compared with. The set of criteria must cover the key messages comprehensively. The criteria must be publicly available. Otherwise the messages remain an assertion without substance. Procedures must be in place to guarantee consistent application of certification criteria.

EuroPriSe criteria are derived from the European regulations on privacy and data protection. The criteria catalogue is sectioned into four sets: 1. Fundamentals (e.g. purpose, avoidance, transparency), 2. Legitimacy of Data Processing (e.g. legal basis), 3. Technical-Organisational Measures (general, e.g. unauthorised access; Specific, e.g. encryption), 4. Data Subjects' Rights.[35] The basic criteria catalogue is published on the EuroPriSe website.[36]

Validity

In a fast developing ICT market lifetime certification is generally inappropriate and would harm credibility. The validity of the certificate should be determined to a specific time-period.

The European Privacy Seal is valid for two years if the product or service remains unchanged in all privacy relevant matters. After expiration a re-certification procedure is offered. The efforts for re-certification are usually lower depending on the changes in the product or service.

Conclusion

Trust certification and trust marks can be a good instrument to reassure consumers and provide them with information otherwise unavailable. Precondition to achieve consumer trust are a strong trust mark message, a trusted certification authority, a replicable procedure, and transparent criteria. It is important that the trust mark carries a clear message and that the related certification offers the relevant information in order to substantiate the trust marks' claim. Evaluation reports can provide good guidance for consumers in a fast growing IT market to choose a privacy compliant product. Good and comprehensive product documentation enables users to deploy the product or service in a way compliant to data protection regulations.

On this basis the European Privacy Seal offers a trust mark to make good data protection visible and strive for a classic win-win situation, in which business profits from an increase in trust and acceptance of IT and consumers gain from an improvement of privacy and data protection.

31 Cf. *Edelmann*, Adverse Selection in Online „Trust" Certifications, 2006, p. 6, available at http://www.benedelman.org/ (accessed 01/08/2008) who questions the ability of TRUSTe to "detect violations of its rules".

32 *Greenstadt/Smith*, Protecting Personal Information: Obstacles and Directions, 2005, available at http://www.eecs.harvard.edu/~greenie/index.html (accessed 01.08.2008).

33 *Bock/Probst*, European Privacy Seal, in: Expanding the Knowledge Economy: Issues, Application, Case Studies (2007).

34 See for example CEN (European Committee for Standardization): Inventory of Data Protection Auditing Practices, CEN Publication CWA 15262, April 2005, ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15262-00-2005-Apr.pdf (Accessed 12.06.2007). Cf. for requirements *Hammer/Schuler*, Cui bono? – Ziele und Inhalte eines Datenschutz-Zertifikats, pp. 77 ff., DuD 2/2007.

35 For development and interpretation of EuroPriSe-criteria cf. *Meissner*, Zertifizierungskriterien für das europäische Datenschutzgütesiegel EuroPriSe, DuD 9/2008.

36 Available at http://www.european-privacy-seal.eu/criteria.