View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by JRC Publications Repository

EU Privacy seals project

Challenges and Possible Scope of an EU Privacy Seal Scheme

Final Report Study Deliverable 3.4

Authors
Paul De Hert,
Vagelis Papakonstantinou
Rowena Rodrigues
David Barnard-Wills,
David Wright,
Luca Remotti
Tonia Damvakeraki

Editors
Laurent Beslay, EC JRC–IPSC
Nicolas Dubois, EC DG JUST

2014

Report EUR 26699 EN

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Laurent Beslay
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 361, 21027 Ispra (VA), Italy
E-mail: laurent.beslay@jrc.ec.europa.eu
Tel.: +39 0332 78 6556
Fax: +39 0332 78 9392

https://ec.europa.eu/jrc/en/institutes/ipsc
https://ec.europa.eu/jrc

Legal Notice
Neither the European Commission nor any person acting on behalf of the Commission
is responsible for the use which might be made of this publication.

Europe Direct is a service to help you find answers to your questions about the European Union
Freephone number (*): 00 800 6 7 8 9 10 11
(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

A great deal of additional information on the European Union is available on the Internet.
It can be accessed through the Europa server http://europa.eu/.

JRC90543

EUR 26699 EN

ISBN 978-92-79-38672-5

ISSN 1831-9424

doi:10.2788/85717

Luxembourg: Publications Office of the European Union, 2014

© European Union, 2014

Reproduction is authorised provided the source is acknowledged.

Printed in Italy

The Institute for the Protection and Security of the Citizen of the Joint Research Centre (JRC), in collaboration with the Directorate-General for Justice (DG JUST), has launched a project on EU privacy Seals in April 2013. The project aims at identifying procedures and mechanisms necessary for the successful launch of an European-wide certification scheme, (e.g. EU privacy seals) regarding the privacy compliance of processes, technologies, products and services.

In the frame of this project, the JRC has commissioned under Service Contract Number 258065, a study to a consortium comprising Trilateral Research & Consulting, Vrije Universiteit Brussel and Intrasoft International S.A. Divided in five steps, the objective of the study is to analyse the scientific and organisational success factors for which it will be appropriate and feasible to launch such a European wide privacy certification scheme.

In order to provide advices and guidance on how successfully achieve the goals envisaged by the overall study, the JRC has set up a steering group composed by representatives from other DGs[1], the LIBE committee secretariat of the European Parliament, ENISA. This report constitutes the third deliverable of the study.

The authors of this report are:

- Paul De Hert, Vrije Universiteit Brussel
- Vagelis Papakonstantinou, Vrije Universiteit Brussel
- Rowena Rodrigues, Associate Partner, Trilateral Research
- David Barnard-Wills, Associate Partner, Trilateral Research
- David Wright, Managing Partner, Trilateral Research
- Luca Remotti, Intrasoft International S.A
- Tonia Damvakeraki, Intrasoft International S.A

In addition, the report has benefited from comments and suggestions made by the members of the study Advisory Board, comprising:

- Kirsten Bock, Office of the Data Protection and Freedom of Information Commissioner of Schleswig-Holstein, Germany
- Kostas Rossoglou, Senior Legal Officer, BEUC, Brussels
- Douwe Korff, Professor of International Law, London Metropolitan University.

Responsible Administrator
Laurent Beslay
Digital Citizen Security unit
European Commission, DG Joint Research Centre
Directorate G - Institute for the Protection and Security of the Citizen
Unit G06 - Digital Citizen Security
TP 361
Via Enrico Fermi 2749
21027 Ispra (VA), ITALY
Tel: +39 0332 78 6556
Fax: +39 0332 78 9392

[1] DG Communications Networks, Content and Technology (CONNECT), DG Enterprise and Industry (ENTR), DG for Health & Consumers (SANCO)

Contents

List of tables

1 INTRODUCTION

The introduction of a widely used and effective EU privacy seal scheme constitutes a self-evident, but nevertheless to-date unattained objective. This is focus of this report: the challenges of implementing such a scheme and its possible scope.

Task 1 of the Study on EU Privacy Seals (Inventory and Analysis of Privacy Seal Schemes) coherently and comparably summarised the operating particulars of 25 privacy, data protection and security certification schemes. Task 2 (Comparison with other EU certification schemes) identified and analysed the success factors of EU certification schemes in select fields unrelated to privacy that benefit from strong, long-existing and well-established EU-level certification. The fields of study included network and information security, general product compliance, the environment, financial auditing and accounting, entertainment, the food industry and the telecommunications sectors. This task (i.e., Task 3) and this report return the focus to privacy and data protection, and present further groundwork to feed into Task 4 of the Study (Proposals and evaluation of options for an EU-wide privacy seals scheme). Where relevant, we use the research results and analyses of Tasks 1 and 2.

The *EC DG JUST Final Report on New Challenges to Data Protection* discusses privacy seals and maintains that they are a low-tech solution to protect data.[2] In 2010, the European Commission set out its intent to explore the possible creation of EU certification schemes (e.g., "privacy seals") for "privacy-compliant" processes, technologies, products and services. This report follows the mandate specified in the Tender Specifications. First, it assesses the gaps in current privacy seal sector. Next, it highlights the advantages of, priorities for and possible scope of an EU privacy seal scheme. Four case studies (CCTV systems, cloud services, smart metering systems and biometric systems) illustrate the possible scope of an EU privacy seal scheme and demonstrate whether an EU privacy seals scheme would bring any added value to privacy and data protection.

2 OBJECTIVES

The two key objectives of this report are:

1. To assess the gaps in current privacy seal policies and determine how an EU privacy seal can fix them;
2. To describe in detail the possible scope of an EU privacy certification scheme with the help of four case studies in relation to CCTV systems, international transfers, smart metering and biometric systems.

3 METHODOLOGY

[2] European Commission, Directorate-General Justice, Freedom and Security, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*, Final Report, 20 Jan 2010.
http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

This task uses the findings and analyses of Tasks 1 (Inventory and Analysis of Privacy Seal Schemes) and 2 (Comparison with other EU certification schemes) of the Study on EU Privacy Seals.

This task primarily used two main methods: literature review and development of detailed case studies. The literature review examined the results of Task 1 and 2 of the Study and reviewed policy, academic, industry and other relevant publications. The literature review directly contributed to the sections on gaps in current EU privacy seal schemes, the advantages of an EU privacy seal and the key priorities.

Four illustrative case studies support the analysis of Task 3 and show the possible scope of an EU privacy seal: CCTV systems, international transfers (cloud services), smart metering and biometric systems. Their choice is based on time-relevance: they are among the most critical issues for data protection, and all show privacy and data protection sensitivity. All four cases raise various privacy and data protection concerns and have attracted considerable public, academic and regulatory attention. The detailed case study methodology is outlined in Section 5.3.1. The consortium liaised with identified experts in developing the case studies. The case studies each take a divergent approach in determining the type of certification that would be suitable, its potential scope and the challenges it would have to address.

Finally, the report presents the lessons learned and draws conclusions, following a comparative analysis of the findings in the preceding chapters.

A necessary clarification at this point refers to the applicable regulatory framework. While the Data Protection Directive 95/46/EC[3] constitutes the common European legal basis for data protection, we will also refer to the proposed General Data Protection Regulation as adopted by the European Commission[4] and the report of the Rapporteur on the Regulation released after the LIBE Committee vote, in early November 2013 - referred to in this document as the Draft European Parliament Legislative Resolution on GDPR)[5]. None of the EU institutions, as of writing, are bound by the latter but we refer to this version as relevant to the discussion.

4 GAPS IN CURRENT PRIVACY SEAL SCHEMES

[3] European Parliament and the Council, Directive 95/46/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, *OJ L* 281, 23 Nov 1995, pp. 0031-0050.

[4] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, Brussels, 25 Jan 2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[5] European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), A7-0402/2013, 21 Nov 2013. Note: On 12 March 2014, the European Parliament approved this version by voting in plenary with 621 votes in favour, 10 against and 22 abstentions for the Regulation and 371 votes in favour, 276 against and 30 abstentions for the Directive).

This section identifies and analyses gaps in privacy seal schemes operating predominantly in the EU, with some reference, where applicable, to schemes based outside the EU.

Task 1 identified problems and challenges in relation to existing privacy seals.[6] Task 2 outlined the success factors of and challenges faced by sectoral certification schemes, and presented some lessons (i.e., requirements) for EU privacy seals. Based on these, we will try to determine the gaps in privacy seal schemes operating within the EU. To bolster the analysis, we will refer to relevant academic literature, official documents and reports on privacy certification and seals. Where applicable, we refer to the provisions in the EU data protection reform package.

In this section, 'privacy seal operators' denotes the legal persons organising and executing the scheme; 'addressees' denotes the natural and legal persons to whom the scheme is addressed, for instance, end users viewing the seal on the website of providers or individuals observing the seal on products. 'Participants' refers to legal persons certified by operators and awarded the privacy seal.

We now examine the gaps in greater depth and analyse why they occur and how they could be addressed.

4.1 LACK OF A WARRANTED LEVEL OF PROTECTION FOR PERSONAL DATA

The adequate level of data protection in the EU is set by EU law. The basic text of reference is the EU Data Protection Directive, Article 16 of the Treaty on the Functioning of the European Union (TFEU) and, in the electronic communications sector, the ePrivacy Directive currently in its third version.[7] Case law from the Court of Justice, whenever available, is also applicable. The work performed by the Article 29 Data Protection Working Party and the European Data Protection Supervisor (at an admittedly less binding level) can also be considered. Altogether, the above form basis of the protection afforded to individuals with regard to any personal data processing performed within the EU. Consequently, it is at least this level of protection that any privacy seals scheme operating within the EU should warrant for its addressees to be considered successful.

The ability of privacy seal providers to warrant a sufficient level of data protection involves at least two elements: first, demonstrating publicly (transparently) the relevant scheme requirements or criteria for evaluating participants; second, demonstrating that such criteria are instrumental and effective in achieving the level of data protection prescribed by EU law.

However, data protection laws and regulations across the EU are many in number and, at times, somewhat abstract in nature or on the contrary very prescriptive regarding particular issues. Identifying the applicable ones each time and making them concrete for the purposes of specific personal data processing requires considerable effort, resources and expertise.

[6] Rodrigues, Rowena, David Barnard-Wills, David Wright, Paul De Hert and Vagelis Papakonstantinou, *Inventory and Analysis of Privacy Certification Schemes: Final Report Study Deliverable 1.4*, Publications Office of the European Union, Luxembourg, 2013.

[7] Security-related processing is regulated by the Data Protection Framework Decision, given that privacy seals exclusively refer to private parties' processing, its provisions are not expected to be applicable with regard to this report. Council of the European Union, Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJ L* 350, 30 Dec 2008, pp 60-71.

Regular update initiatives have to be undertaken, given the pace of change in the applicable rules. Operators therefore have to be very careful while constructing their scheme criteria and requirements. Even after doing so, given that no formal ratification system exists in EU law, they might still be uncertain about whether they have met the required standard.

The results of Task 1 show that existing operators in most cases publish scheme requirements or criteria governing the seal programme on their website. This is a sound policy that serves their business purposes (participants are able to discern compliance requirements for applying and acquiring a seal) and public awareness purposes (i.e., addressees can examine the requirements or criteria a seal represents). Nevertheless, such publication does not necessarily mean effectiveness. The posting of the requirements or criteria on the operator's website does not guarantee or mean an adequate level of privacy and data protection. This can only be evaluated, preferably by an expert independent third party (e.g. a data protection authority that possesses both the institutional warranties and possibly the necessary knowledge to execute this task).

Although we refer to privacy seals schemes run by data protection authorities (DPAs), no DPA (apart from the French Commission nationale de l'informatique et des libertés (CNIL) which certifies auditors) has certified any privacy seal scheme or any third party as warranting an adequate level of privacy and data protection or, in other words, that a scheme operator sufficiently applies the national and EU data protection provisions in its sector of operation. In this context, the analysis of schemes in Task 1 identified several difficulties in the scheme criteria of various scheme operators.

Admittedly, no formal legislative mandate exists in EU law either for DPAs to certify privacy seal schemes or for operators to submit their scheme criteria or requirements to DPAs to be certified. This gap is addressed in the proposed General Data Protection Regulation (Article 39) and should be an essential part of any EU privacy seal scheme – the certifiers may need to be certified to become trustworthy for their participants and their addressees.

4.2 LACK OF USER AWARENESS OF SCHEMES

A key success factor for a privacy certification scheme is user awareness; seal programmes must be widely recognised and acknowledged by public to secure maximum use by their addressees. A seal that is little known to the public may not add much value either to its participants or to its operators; though, if a product or service achieves compliance through certification, much is gained even if people are not aware of the scheme (e.g. the scheme participant gains in reducing its risks).

Within the EU, a successful scheme would need to achieve cross-border user awareness. One factor contributing to user awareness is the implementation of adequate marketing strategies to achieve user trust (elaborated in section 4.3). In addition, data subjects must be aware of seal programmes.

User awareness, in particular when aimed at a sector-specific seal scheme, is not easily measurable. Unlike participants' awareness, which can be inferred from the number of participants enrolled in the scheme, the level of penetration of a scheme in relation to addressees does not have a concrete metric (unless specialised market research is available). From this point of view, an accurate picture of user awareness, achieved by the privacy seal schemes in operation, is not easy to establish. However, from the cumulative findings of Task

1 (such as number of participants, years in operation, relevant mentions and references in other sources such as the press of the Internet), it appears to be relatively low.[8]

Some features of existing privacy schemes appear to contribute to low user awareness of the schemes. One major problem is the multiplication and fragmentation of efforts. To date, most efforts aim at certifying online sellers and service providers; however, this is done mostly at the very broad international, or primarily local, national level. In some cases several schemes compete in the same market sector. Currently, no true EU effort is evident.

Another problem is the apparent failure of many of the analysed schemes to place addressees at the centre of attention. Existing privacy seal schemes are more participant than addressee-centric. This can be inferred from the schemes' websites; information there is predominantly addressed to participants, for instance, specifying procedures and rules of certification. Very little information is targeted at addressees (for instance, easily accessible redress mechanisms, simplified information on the scheme, promotional material and, more importantly, local contact details). The language of the relevant websites is also important; a true EU effort would need to include if not all, a substantial number of the EU languages (or the more prominent, widely used ones such as English, German and French), so that scheme-related information is more equally and universally accessible to addressees. Unless concentrated efforts to raise awareness are made both at the EU and national level, seals and schemes will only be of marginal use to experts and experienced users, and will fail to serve the wider, general population.

4.3 LACK OF USER TRUST AND CONFIDENCE IN SCHEMES

Contemporary privacy schemes appear to score low with regard to user trust and confidence, though some of them expressly state this to be their objective. Even the more successful privacy seal schemes (in terms of participation) based outside the EU have failed, so far, to convince the wider, international public of their usefulness. The situation in the EU is no better; the limited public attention and use that privacy seal schemes have attracted so far is an indicator that trust, at a more effective level, is yet to be gained.

However, trust and confidence are difficult values to measure. Unless dedicated consumer or data subject surveys provide relevant assistance, we can only make assumptions about the factors that might generate public trust and confidence in a privacy seals scheme. However, based on the extensive research of this Study, we can conclude that some of these factors include: a strong and established presence in the market, transparent and constantly updated evaluation procedures, an effective redress mechanism (that proves its worth in cases of infringements) and a strong communication strategy.[9] Privacy schemes operated on a for-profit basis must find a means of addressing concerns about conflicts of interest (i.e. whether they bend the rules to accommodate their own vested, or subscribers' interests). In any case, Task 1 was not able to identify any existing scheme operating within the EU that fulfils the all

[8] Rodrigues et al, *Inventory,* op. cit., 2013, chapter 6.3.6; Rodrigues, Rowena, David Wright and Kush Wadhwa, "Developing a privacy seal scheme (that works)" *International Data Privacy Law*, Vol. 3, Issue 2, 2013, pp. 100-116, [p.107]; European Consumer Centre Denmark, "E-Commerce Trustmarks in Europe - an overview and comparison of Trustmarks in the European Union, Iceland and Norway", *Report,* 18 March 2010, 4.2.

[9] See also, Bock, Kirsten, "EuroPriSe Trust Certification: An approach to strengthen user confidence through privacy certification", *Datenschutz und Datensicherheit,* Vol. 1, 2008, p. 3.

above conditions and therefore, at least demonstrably, enjoys a high level of public trust, at EU or Member State level.

The failure of privacy seals schemes to achieve public trust is particularly noteworthy given the otherwise favourable conditions in their respective markets. Though individuals customarily rate the lack of trust high on their list of e-commerce deterrents, current privacy seals schemes have failed to effectively address this issue. This constitutes an important lost opportunity both for privacy seals operators and privacy and personal data protection.

4.4 LACK OF INCENTIVES FOR USE AND IMPLEMENTATION OF SCHEMES

Another issue affecting the effectiveness of privacy seals schemes is the lack of adequate incentives offered to the participants of the scheme.[10] Incentives are a crucial component of a certification system, given the significant difficulties and burdens that might fall upon an entity that applies for certification. The effort required and the monetary cost for acquiring and maintaining the certification can only be offset by real and useful advantages that the certification will offer to successful applicants. Research in Task 1 shows there are very few incentives to enrol in privacy seal programmes.

Privacy seal incentives could fall under two broad categories: first, a certified organisation would gain a ***compliance*** advantage, in knowing that it fulfils its privacy and data protection obligations; and second, and more important from the participants' point of view, a certified organisation would gain a ***competitive*** advantage in the market (i.e. the certification might generate consumer trust in the organisation and boost sales or help retain existing customers. However, existing privacy seal schemes do not provide the above two incentives at an optimal level for aspiring participants.

Compliance is not warranted for certified participants carrying the certification, even when all relevant conditions are met and processing standards are kept high, because the certifiers are themselves not certified. Consequently, participants can only hope that their certifying organisation did a good job in interpreting and implementing privacy and data protection provisions relating to their specific sector and processing activity. Only one of our analysed privacy seal scheme, CNIL Label, is (as of writing) operated by a national data protection authority;[11] only in the case of this scheme, participants compliance with their national law can be said to have been thoroughly assessed. However, national schemes would be more compliant with the law of a specific Member State (i.e., its own data protection act) and not to the law of other Member States that might vary. Privacy seal operators within the EU, even with the best intentions and efforts, will have to wait for a complaint to arise and be adjudicated by the competent authorities before they are certain of the adequacy of their legal work – a far from reassuring factor for organisations considering whether it is worth to subscribe to such a scheme.

[10] For a useful list of incentives for private and public sector certification (in a non-privacy related field) see ENISA, *Security certification practice in the EU, Information Security Management Systems – A case study*, Report, October 2013, pp.18-19, 21.

[11] The EuroPriSe seal and certification scheme was transferred to EuroPriSe GmbH as of 1 January 2014. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), "EuroPriSe 2.0 – Continuation of the European Privacy Seal (EuroPriSe) by EuroPriSe GmbH – Extended range of certifications", 14 Nov 2013. https://www.european-privacy-seal.eu/ws/EPS-en/Press-releases

The sales incentive of existing privacy seals programmes is also uncertain. This is due to the impacts of fragmentation and duplication evident in contemporary privacy seals schemes. Another factor is the national nature of such schemes. A national scheme participant may advertise and intend to capitalise on its privacy seal, but once it attempts to exit the boundaries of the Member State in question, its certification might not be recognised, accepted or even applicable.

The above lack of incentives is evident in the generally low level of penetration of the privacy seal schemes in their respective market within the EU.[12] In very few cases has the number of scheme participants (see Task 1 report)[13] reached more than a couple of thousand organisations – with a significant number of schemes limited to no more than a few dozen certifications. Such numbers could generally be considered as inadequate, given that the market to which such schemes are usually addressed at (e.g. the e-commerce market) involves sellers in thousands in each Member State (and in millions for some Member States). Consequently, till adequate incentives are provided for a larger number of organisations to participate in a privacy seal scheme, such schemes will only enjoy marginal acceptance; this offers little support to advance data protection.

The proposed General Data Protection Regulation (2012 draft) did not explicitly provide any assistance in terms of the above discussed incentives. Article 39 (1) of this draft sees the role of data protection certification mechanisms as contributing "to the proper application of this Regulation". The Draft European Parliament Legislative Resolution on GDPR, on the other hand, is more explicit in Article 39 (1a), and sets the scope of certification: to certify that the processing of personal data is performed in compliance with this Regulation. This seems to grant a more solid ground for participants in such a scheme to claim that their personal data processing adheres to the applicable data protection provisions but may lead to more costly compliance verification programmes and a double layer of supervision and enforcement.

4.5 DECEPTIVE POTENTIAL OF SCHEMES

Privacy seal schemes have a certain potential to deceive their addressees. This is a risk that all certification schemes encounter.[14] Addressees, specifically, a large number of Internet users, rarely take the time (or have the expertise) to study in detail a certification scheme's rules and regulations and reasonably understand what exactly a particular scheme certifies.[15] There is often a substantial difference between an addressee's perception of the scheme and its actual operation.[16] This understanding sometimes only comes about when a right is infringed or a complaint is made. This is a risk particularly relevant to privacy certification schemes. Privacy is a concept that is approached differently in different societies (even amongst EU Member States) and protected differently in different legal systems. Schemes essentially promising its protection run a significant risk of not meeting public expectations despite their best, lawful, efforts.

[12] This, however, appears to be a general trend within the EU and not privacy-specific. See, for instance, ENISA, *Security certification practice in the EU, Information Security Management Systems – A case study*, Report, October 2013, p. 25.
[13] Rodrigues et al, *Inventory*, op. cit., 2013.
[14] ENISA, *Security certification*, op. cit., 2013, p. 10, expanding also on the issue of "adverse selection".
[15] See also European Consumer Centres Network (ECC-Net), "Can I trust the trustmark?" *Trustmarks Report 2013*, October 2013, p. 56.
[16] See also Rodrigues et al, "Developing a Privacy Seal", op. cit., 2013, p. 107.

Although relevant public surveys that would help determine public expectations of a privacy seal scheme are still missing; a privacy seal might be perceived by the public as presenting a series of characteristics: an adequate level of protection of the right to privacy (and data protection, if within the EU) as laid down by the applicable legislation, a monitoring mechanism to enforce application to participants and minimise misuse of the seal by unauthorised parties (see section 4.10), an effective redress system for violation of scheme rules, and in some cases, regulatory control of all the above and the scheme operators. These expectations are supported by the general characteristics of any certification scheme, such as those outlined in Task 2; some of which have long become embedded in the public expectations in relation to the different sectors.

However, as shown in Task 1, it is not uncommon that existing privacy certification schemes do not meet some or even all of the listed public expectations. Despite their being termed 'privacy seal' schemes, many analysed schemes vary substantially in the manner they perceive, execute their role and even interpret the notions of privacy and data protection. Approaches differ from strict implementations developed by EU data protection authorities to schemes that are customised to cater to the needs of their subscribers (participants). The fact that the relevant seals are widely used over the Internet, where consumers may or may not make the distinction between seals originating from different regions and/or organisations (and signifying different things), only increases their deceptive potential.

The divergent approaches adopted by existing privacy schemes within and out with the EU inevitably, accentuates a deceptive potential that is otherwise inherent in other certification schemes as well. The lack of harmonisation, common rules and regulation, even within the EU, means that very different rules and regulations (or standards) form the basis of a privacy seal. When individuals actually inquire about what any given scheme can 'actually do' to assist them in protecting their privacy and personal data, it may lead to public disillusionment and eventually, loss of public trust. Such loss of trust will ultimately impact the privacy seals cause as a whole; this is because they share common name (i.e. privacy seal), even though their underlying basis (rules, regulations or standards) differ. Public criticism of any one of them could affect the reputation of all.

4.6 SCHEMES JUSTIFYING INCREASED COLLECTION AND USE OF PERSONAL DATA

Any privacy certification scheme could be perceived as self-serving, in the sense that, once acquired, a privacy seal might justify the collection and use of personal data by a participant. This despite the fact that privacy seals do not legitimise the collection and use of personal data by any, successful, participant. In the EU, data controllers may process data only and to the extent that is lawfully permitted and proportionate to their legitimate purposes.[17] Privacy certification, whatever its basis, should not mean that we do not stop to question whether the certified entity is allowed to collect and process personal information in the first place.

The schemes analysed in Task 1 do not address this aspect. Participants are usually not asked to perform a legal due diligence or an impact assessment on whether their processing *per se* is legitimate, prior to it being analysed under the seal scheme's requirements. The focus is

[17] As per Articles 6 and 7 of the EU Data Protection Directive.

placed on processes and technicalities, rather than on the actual legitimacy of the underlying personal data processing (excepting for instance, as found in the case of the EuroPriSe Criteria Set 2, 2.1 Legitimacy) This is an unavoidable gap, given that many of the schemes are based outside the EU, and even the privacy schemes within the EU are not monitored by any independent third party (e.g. a regulatory authority). This means that a scheme's requirements or criteria, with very few exceptions, are not tested against the general EU data protection law requirements for proportionality and necessity of the processing. Most of the analysed schemes do not make any distinctions between the different types of scheme participants (i.e. different types of data controllers and the types of processing).

Unregulated and unmonitored privacy schemes, could, therefore lead to increased collection and use of personal data.[18] Successful participants may feel justified in their processing practices, without inquiring whether their processing itself is lawful or not. Addressees may feel compelled to leave unchallenged any request for personal information by data controllers carrying a privacy seal. If privacy seals continue to be left outside the scope of any regulatory oversight (see section 4.8), they risk developing into a self-justifying data collection and use mechanism that would harm the very privacy and data protection purposes they mostly pledge to serve.

4.7 ENFORCEMENT ISSUES

Enforcement is an integral part of any successful certification scheme. Unless privacy certification scheme operators can demonstrate that vigilant and efficient monitoring mechanisms exist and are willing to take enforcement actions, their schemes may lose the element of trust.[19] This is especially important, as it is largely private, for-profit organisations (including membership organisations) that operate privacy certification schemes without any formal, state oversight. The operators must be able to demonstrate how they will, if required, take enforcement actions against their own clients. In addition, outside the EU, no formal comprehensive privacy or data protection legislation exists, that would assist them in this element of their work.

An efficient enforcement mechanism is composed of at least two elements. First, a permanent monitoring mechanism, and, second, an effective redress mechanism that would include the use of penalties. A permanent monitoring mechanism would ensure that scheme participants do not infringe the scheme's rules and regulations. Checks would be run on a regular, periodic basis, and not only at the time of application and renewal. This would ensure that third party misuse does not endanger the scheme's good standing. An effective redress mechanism must give complainants an easy and accessible way to file their complaints. In cases of infringements, a scheme operator must be able to impose penalties that would need to be more severe than (often, temporary) suspension from the scheme (such as monetary penalties, reference of the matter to the competent regulatory authorities etc.).

Most of the privacy seal schemes analysed in Task 1, scored rather poorly with regard to enforcement.[20] A number of difficulties have been noted and are well documented in the case of certain non-EU schemes which are best known to the public. Even EU-based schemes do

[18] A point also made by Rodrigues et al, "Developing a Privacy Seal", op. cit., 2013, p. 108.
[19] Ibid, p. 108.
[20] See Rodrigues et al, *Inventory and Analysis*, op. cit., 2013, pp. 86-89.

not seem to have adequately covered all the enforcement components, i.e., monitoring and redress mechanisms. Addresses may, therefore, be inclined to perceive schemes as rather weak, ineffectual and unable to impose an adequate level of privacy or data protection their participants.

4.8 LACK OF REGULATORY OVERSIGHT

An important shortcoming of existing privacy seals schemes is the lack of regulatory oversight.[21] Regulatory oversight is important from several perspectives: it ratifies and confirms, the legality of the rules applicable in context of a specific seal scheme; it monitors its continued operation, therefore guarantees that there are no slippages in what is certified and what is signified, and, it ultimately controls the certification process. Regulatory oversight and proper articulation of this oversight in the regulatory framework is therefore, a crucial factor.

National data protection authorities, however, who might be the most logical entities to provide regulatory oversight currently have no such role to play. This is because current privacy seals operate in a largely self-regulatory environment. Neither the EU Data Protection Directive nor data protection acts of Member States (other than France and Schleswig-Holstein), to our knowledge formally adopt the notion of privacy or data protection seals. DPAs could take the initiative (as in Germany, France, and UK in the future) based on their broad mission to monitor data protection implementation within their jurisdictions.

This means that the existing privacy seals schemes remain, relatively, unregulated. Because they have no place in the formal data protection edifice, they operate largely informally, demonstrating, in effect, good intentions (or, for the same purposes, lack of a wilful act or gross negligence), rather than concrete compliance to the law. The lack of regulatory oversight, in particular, deprives them of the formal endorsement that is indispensable to gain trust, both from participants and addressees.

The proposed General Data Protection Regulation generally leaves the issue of regulatory oversight open; Article 39 (2) explicitly recognises the role of certification and privacy and data protection seals and grants the Commission the right to issue delegated acts to regulate the criteria and requirements for the data protection certification mechanisms or conditions for granting and withdrawal. It does not, however, detail the role of the DPAs as regards formal regulatory oversight over schemes operating in their jurisdiction. Oversight is an important principle that should be specified in the text of the Regulation.

4.9 LACK OF HARMONISATION AND COMMON STANDARDS

There is a lack of harmonisation and common standards for privacy seal schemes.[22] This could be expected in the case of non-EU schemes, where different laws and standards might apply and there is no comprehensive privacy and data protection legislation that can be used as a common basis. Within the EU, given the EU Data Protection Directive, one would expect a greater if not certain basic level of harmonisation; i.e. that schemes based in the EU would apply common standards across market sectors, contributing to the Single Market. The results

[21] Rodrigues et al, "Developing a Privacy Seal", op. cit., 2013, p. 108.
[22] Rodrigues et al, "Developing a Privacy Seal", op. cit., 2013, p. 109.

of Task 1 show a different picture.[23] EU privacy schemes apply different rules and warrant different levels of privacy and data protection, even within the same market sectors. The same applies to their redress and enforcement mechanisms. Similarly, technical standards, wherever applicable, are developed and applied by separate operators within their individual schemes, with limited attention to their interoperability and establishment of common grounds.

The above are particularly problematic within the privacy certification field. Participants may be tempted to shop in the certification market for the most flexible and accommodating operator. Addressees, on the other hand, may find it difficult to understand that schemes, bearing similar names and operating within the same market sectors, apply substantially different standards. Operators suffer from multiplication of efforts and uncertainty that their scheme implementation effectively supports the protection of privacy and personal data (in a manner better than their competitors). In addition, lack of common standards offers very little to the cause of the Single Market. Existing privacy schemes, even those based in the EU need to apply cross-sector harmonised rules and standards, in order to fully develop their potential as a simplified and immediate instrument to protect individual privacy.

4.10 THIRD PARTY MISUSE

Closely connected to the lack of efficient enforcement mechanisms (section 4.7) is the risk of third party misuse of a privacy seal.[24] Third parties may use privacy seals in an unauthorised manner – for example, by affixing seal on website without being actually certified by the scheme. This will deceive potential website users and other relying parties into believing that they adhere to the scheme's rules and regulations. This risk is evidently greater for the more well-known and established schemes (it is the more prominent seals that run the risk of being misused due to their wide appeal). This requires the implementation of an efficient surveillance mechanism that can identify such cases and counter their effects.[25]

Weak surveillance and enforcement facilitate potential misuse, fraud and adversely affect a scheme's credibility. Privacy seal schemes and regulators should take measures to deter and act against misuse and eliminate such risks (this is currently lacking in existing schemes).

4.11 CONFLICTS OF INTEREST

[23] See also European Consumer Centre Denmark, "E-commerce Trustmarks", op. cit., 2010.

[24] Task 1 identified such cases in relation to the following seals: CNIL label, PrivacyMark, TRUSTe, Verified by Visa. Rodrigues et al, *Inventory*, op. cit., 2013, p. 53.

[25] The Directive on Unfair Commercial Practices 2005/29/EC (which strengthens the rights of consumers) blacklists certain trust marks and code of conduct related activities such as: claiming to be a signatory to a code of conduct when the trader is not; displaying a trust mark, quality mark or equivalent without having obtained the necessary authorisation; claiming that a code of conduct has an endorsement from a public or other body which it does not have; claiming that a trader (including his commercial practices) or a product has been approved, endorsed or authorised by a public or private body when he/it has not or making such a claim without complying with the terms of the approval, endorsement or authorisation. The Misleading and Comparative Advertising Directive (2006/114/EC) covers business-to-business misleading advertising and comparative advertising which may harm a competitor but where there is no direct consumer detriment (e.g. denigration).

Certification schemes must be able to demonstrate a certain level of credibility and neutrality. This is particularly true of schemes run by private, for-profit operators; they need to be able to demonstrate that they would not bend their rules to accommodate the needs of their clients (i.e. the scheme's participants).[26] Another concern identified in Task 1 was how some schemes act as a front or means for an organisation to build and develop its profile and other supplementary activities (e.g., consulting). These conflicts of interest are detrimental to privacy and data protection in general, and privacy seal schemes in particular. Unless operators are able alleviate conflict of interest concerns, schemes risk losing, or not being able to maintain their long-term credibility.

Privacy seal schemes within the EU are distinguished between private and public authority (such as those operated by DPAs). The private schemes may be operated by for-profit entities and also by not-for-profit organisations (such as the Market Research Society, the ESRB and Euro-Label). The risk of a conflict of interest runs deeper in for-profit organisations and where their revenues are proportional to the number of certified entities. Even though no scheme operator within the EU has been charged of bending its rules in favour of its clients, the above distinctions are complex, and require careful study of each scheme's organisational details. A conflict of interest that is proved in the case of one scheme would detrimentally affect the reputation of all other schemes, particularly if the public is not able to distinguish between the different scheme operators. Some sort of common organisational structure or regulatory oversight might address this problem and create the necessary conditions for public trust and wider implementation.

4.12 TRANSITORY NATURE OF SCHEMES

Another major problem with privacy seals is their often short-lived nature. Connolly's report identifies several examples of privacy seal certification schemes that have ceased to exist, for instance, the privacy-specific BBB Online Privacy Seal, the Australian eTick, controlscan, enshrine, web trader, trust UK, and safetrade.[27] Research in Task 1 explicitly showed that some schemes such as i-Privacy (Australia), Portugal's PACE, PrivacyBot, and TrustUK, mentioned in the tender call were not available anymore. i-Privacy (Australia) and PrivacyBot's websites are currently not available. Data is not available for PACE other than a mention on the Caslon Analytics Trust marks directory.[28] A fluctuating privacy seals market contributes to the scepticism expressed of seals as an effective privacy and data protection mechanism.

Given the effort and resources required for the development and operation of a privacy seals scheme, if applicable, the relevant legislative framework for privacy certification should remain relatively stable. This will give operators sufficient time to develop their programmes and market them sufficiently, and also learn from their experiences. A legal framework that constantly changes, or, even worse, a 'vulnerable' legal framework with uncertain provisions will not be able to effectively contribute to the development of privacy seal programmes. An example to illustrate how legal changes affect schemes is the European Privacy Trustmark whose implementation has been postponed in view of EU data protection reform process.[29]

[26] Rodrigues et al, "Developing a Privacy Seal", op. cit., 2013, p. 109.
[27] Connolly, Chris, 'Trustmark Schemes Struggle to Protect Privacy 2008', *Galexia*, Version 1.0, 26 Sept 2008. http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/
[28] Caslon Analytics, "Trust marks". http://www.caslon.com.au/trustmarksprofile2.htm
[29] Confirmed via personal communication from a European Privacy Association team member to the study team.

Existing privacy seals may therefore, seem justifiably operating in a largely self-regulatory environment and performing a secondary role in privacy and data protection. The final wording of the General Data Protection Regulation will impact them in different ways: it might increase their business, it might make them more competitive, or it might even lose them business (for example if DPAs take on the role of granting privacy seals and outsource work to their own approved evaluators). There is a long list of privacy certification programme components left to be regulated by Commission delegated (Article 39 (2)) or implementing (Article 39 (3)) acts in the proposed General Data Protection Regulation of 2012. While this ensures flexibility, it also simultaneously extends the period of legal uncertainty for scheme operators. The Draft European Parliament Legislative Resolution on GDPR, in contrast, expressly specifies a model (which might be detrimental to some of the existing operators' interests) and to some extent lifts the uncertainty. At this stage, we do not endorse this model; we will examine it further in Task 4 (analysis of options).

5 THE ADVANTAGES, PRIORITIES AND SCOPE OF AN EU PRIVACY SEAL SCHEME

The aforementioned difficulties (problems evident in current schemes) do not mean that a privacy seal is not a useful or desirable mechanism to advance privacy and personal data protection interests. Privacy seals continue to be a flexible and easy mechanism to demonstrate privacy and data protection compliance, particularly in terms how they can make difficult privacy and data protection issues easily understandable to the general public.[30] However, to be effective, privacy seal schemes (and other stakeholders) must address the previously outlined challenges.

Given the transborder character of personal data processing, and the regulatory environment, regardless whether under the EU Data Protection Directive or the General Data Protection Regulation regime, it is crucial to have an EU-level scheme. Fragmentation and multiplication of efforts offers little to data subjects and data controllers alike. An EU level system could offer a harmonised and uniform standard of data protection. The proposed General Data Protection Regulation acknowledges in Article 39. This understanding came at the end of a long elaboration process. In 2010, the *EC DG JUST Final Report on New Challenges to Data Protection* discussed privacy seals and maintained that they are a low-tech but effective solution to protect data.[31] Accordingly, in 2010 the European Commission set out its intent to explore the possible creation of EU certification schemes (e.g. 'privacy seals') for 'privacy-compliant' processes, technologies, products and services. This would not only give an orientation to the individual as a user of such technologies, products and services, but would also be relevant in relation to the responsibility of data controllers: opting for certified

[30] Particularly in the online environment (see, for instance, on website privacy statements, "website privacy statements are frequently a legal requirement and can help to answer the questions of interested individuals, but as a communication tool with the vast majority they are nearly worthless. Because customers are wary about privacy, finding ways to communicate relevant elements of privacy policies effectively will be a key element in building trust and relationships". The Economist, *Privacy uncovered; Can private life exist in the Digital Age? A report from the Economist Intelligence Unit*, 2013, p.17).

[31] European Commission, DG Freedom and Security, *Comparative study*, op. cit., 2010.

technologies, products or services could help to prove that the controller has fulfilled its obligations.[32]

First, this section focuses on the advantages of and priorities for an EU privacy seal scheme. Four case studies illustrate the possible scope of an EU privacy seal scheme: CCTV systems, international transfers (cloud services), smart metering and biometric systems.

5.1 ADVANTAGES OF AN EU PRIVACY SEAL SCHEME

This section elaborates the advantages of introducing an EU privacy seal scheme (as compared to national privacy seal schemes). The advantages are drawn from the analysis in Task 1 (Inventory and analysis of privacy seal schemes) and Task 2 (Study and comparison with EU non-privacy related certification schemes).

To resolve identified problems of existing schemes

Existing privacy seals schemes operators had to develop and implement their schemes in a fragmented, self-regulatory, rather disorganised, resource-constrained environment. Though many of them have been around for a long time, they have not been able to address many of the concerns expressed and challenges that affect them. This is aggravated by the lack of common standards that form their basis. These schemes lack formal acknowledgement and regulatory oversight. An EU level scheme will need to be able to address these and some of the other problems identified in the previous section. There are various forms this scheme could take; these will be examined further in Task 4.

To enhance accountability, transparency and public awareness

Accountability is a basic principle in the proposed General Data Protection Regulation, especially as existing notification system will be abolished. The introduction of this principle is the culmination of 20 years' experience on data protection oversight and control in the EU. Mechanisms that have become obsolete due to technological developments (such as the notification system) are being abandoned in favour of broader and less bureaucratic approaches that afford data controllers with the necessary flexibility to improve data protection compliance. An EU privacy seals scheme can substantially contribute to this objective. Privacy and data protection rules and regulations are, admittedly, complex and, being general in nature, need to be made concrete in each personal data processing instance. This is by no means an easy or straightforward task. A certification scheme that could be sector-specific for all processing within the EU would provide data controllers with more concrete rules and procedures for their processing, thus assisting them, enhancing compliance and enabling them to be accountable for their processing. In this manner, legal certainty in an otherwise complex legal field would be enhanced, both from the controllers' and the data subjects' point of view.

[32] European Commission, Communication from the Commission to the European Parliament, the Council, the 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, Brussels, 4 Nov 2010. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

Transparency, a requirement under the proposed General Data Protection Regulation, would benefit from an EU privacy certification scheme. A typical certification scheme, as demonstrated in Tasks 1 and 2, must publicise its requirements, criteria, evaluation and audit results (in full or short form), enforcement and redress mechanisms and actions, and the names and status of its participants, thus helping participants to be transparent about their data protection practices. Due to the abolition of the notification system, data subjects will have no way of knowing the particulars of data processing that do not present a high level of risk (i.e., processing that does not require prior notifications or impact assessments, under the proposed Regulation). However, it is such personal data processing that covers most of the processing conducted in typical, daily lives. An EU scheme would be able to provide accessible information to data subjects (or other relying parties). This will enhance transparency.

An EU privacy seal scheme will improve public awareness of privacy and data protection. This is an important result of a successful certification scheme. Once it attains critical mass, it would be able to achieve this objective. However, we recognise that this will mean significant investment in resources to publicise and build the credibility of the scheme. The European nature of the scheme should make it more relevant to the cause of the Single Market. Data subjects in the EU would also find it easier to identify a single scheme or seal that signifies adherence to EU privacy and data protection law (even if implemented in different sectors), rather than a multitude of schemes and seals.

To reduce fragmentation and duplication of efforts

An EU privacy seals scheme could eliminate concerns of fragmentation, duplication of efforts and waste of resources. As demonstrated in section 4, existing privacy seals are fragmented, and duplicate effort. There are a multitude of seals, developed mostly locally in certain Member States often addressed to the same sector (e.g. e-commerce). This is problematic; connected, inter alia, to the lack of harmonisation and common standards and resulting in a lack of a warranted level of personal data protection. An EU privacy seal would resolve such issues. By developing a common, harmonised umbrella framework for the EU, the scheme would achieve a substantial economy of resources.

5.2 SCOPE – KEY PRIORITIES

For an EU privacy seal scheme to be effective, it must have a clear defined purpose and objectives. To determine these, we need to understand the key priorities that the scheme must address. Based on our research, we outline the following key priorities for an EU privacy certification scheme.

5.2.1 Appropriate level of privacy and data protection for individuals

An EU privacy seal scheme must be able to guarantee an adequate level of privacy and personal data protection. The scheme operator must be able to determine how privacy and data protection provisions apply and must be protected in different sectors.

This is not an easy task, given the breadth of the applicable regulatory framework (EU Data Protection Directive, national data protection acts, case law and soft law (e.g. Article 29 Data Protection Working Party and European Data Protection Supervisor (EDPS) opinions). The scheme operators need to demonstrate a sound knowledge of the framework and a deep and

practical understanding of the particular needs and technical aspects of different sectors. This is why a certify-the-certifier approach might be useful. The effective consolidation of the EU privacy and data protection regulatory framework by the scheme operator into its requirements should ideally be verified by an expert, independent third party.

5.2.2 Enhancing the internal market dimension

An EU privacy seal scheme would essentially constitute an instrument aimed at strengthening public trust and facilitating data controller compliance and accountability. The EU Data Protection Directive aimed at lifting commercial barriers that the exchange of personal information would pose to the internal market.[33]

An EU privacy seal's scheme's founding rules and regulations should ideally lie in EU law (the General Data Protection Regulation, if adopted, and any secondary legislation such as Commission delegated acts, decisions of national DPAs, relevant case law etc.). Its certifying authorities, whether state or (outsourced) private parties, would be EU based. Its technical requirements could impose EU residence, location or business (for instance, the location of basic data processing machinery, the establishment of fully accountable data controllers, a one-stop-shop supervisory authority to address all issues, marketing to EU consumers), in order to warrant transparency and accountability. Such a scheme could constitute a valuable data protection standard that would not only enhance intra-EU personal data processing but could also demonstrate to third countries the level of privacy and data protection attainable under such a scheme. This would certainly further the cause of the Internal Market. A common legal basis, in the form of a Regulation, would mean common rules among all Member States. This would enhance the sustainability of privacy seal schemes and also strengthen intra-EU personal data processing. EU privacy certification could constitute a global standard as to level of protection afforded by similar schemes. The Internal Market dimension of relevant EU legislation would therefore once again be strengthened.

5.2.3 Standardised approach for the EU

Whatever the model of an EU privacy seals scheme, a standardised approach is best to eliminate fragmentation. It should be possible to get certified in the EU on fulfilment of prescribed criteria regardless of which Member State the application is made. The certification must be valid and recognisable throughout the EU. An EU privacy seal applicable in Member States would mean that participants established and certified in one Member State could use it in other Member States.

Standardisation could operate at two levels with regard to an EU privacy seal scheme: at the first level, common criteria and procedures must be set that are applicable to all Member States. The scheme must have a common title and graphic seal (if relevant) across the EU. Successful applicants must be able to display the seal on their products or services. There must be a common privacy seal programme that outlines the specific process (fees, application, evaluation, certification, audits, renewal, and redress mechanisms) of the scheme. A single title and visual identity for the scheme across the EU is crucial as this would make the scheme more identifiable and appealing to relying parties.

[33] See Article 1 and Preamble (3).

A standardised EU approach should help eliminate forum shopping (i.e. participants applying to countries with less rigorous standards, certification or audit processes). The EU privacy seal must provide addressees across the EU with uniform rights, as feasible. Scheme participants might be established in one Member State while addressees may be based in another. The EU privacy seals scheme must outline a standardised approach to resolving complaints and settling disputes (i.e. who will have the competence to address these in a timely and efficient manner; also addressees must not be burdened further).

Regardless of the difficulties of implementation, particularly with regard to mutual recognition of schemes and an effective redress mechanism for cross-border cases, harmonisation and standardisation is a crucial component of an effective EU privacy seal scheme.

5.2.4 Specificity of scheme and detailed guidance

An EU privacy seal scheme would need to address sector-specific privacy and data protection requirements. It would need to provide detailed guidance to its participants in different sectors on how to comply with their privacy and data protection obligations. The correct interpretation of generic, abstract and even dispersed privacy and data protection provisions in relation to different sectors and technologies is a difficult task. Data controllers may not have the capacity and knowledge to perform this task themselves. To this end, sectoral self- and co-regulation (e.g. some form of industry self-certification or DPA-supported certification) may be necessary in some industry sectors.

Different sectors (and even technologies within sectors) have different requirements and face different privacy and data protection problems, as the case studies analysed next will demonstrate. Concrete guidelines based on the specificities and needs of each sector will help achieve compliance, accountability and transparency.[34]

While an EU privacy seal scheme might need to address each sector differently, it does not necessarily mean that different sectors will need to have different seals. On the contrary, the use of multiple titles and visual identities would result in greater public confusion and hinder widespread awareness and use of the scheme. As shown in Task 2, and the lessons learnt from other EU sectoral certification schemes, a single, uniform and easily identifiable seal could be used on products and services conforming to the scheme's requirements, which might vary depending on the sectoral needs.

5.2.5 Flexibility and adaptability

An EU privacy seals scheme must be flexible and adaptable. The need for sector-specificity does not translate into rigidity and retracted, high-level management. The processing of personal data is connected to some of the most advanced and fast-paced fields of human progress. There is a blurring of divisions between sectors as new developments occur and technologies advance. People's expectations and needs in relation to privacy, change over time. This is why flexibility and adaptability are crucial in developing an effective and relevant privacy seals scheme.

[34] See Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, WP 173, Adopted on 13 July 2010.

The scheme must have co-operation mechanisms that enable it to address the need for flexibility and adaptability (e.g. between the scheme operator and industry). As this is an ongoing requirement; one-off efforts to release sector-specific rules, even if successful, are bound to become outdated and obsolete in a relatively short period of time. Periodical reviews of scheme rules are necessary to keep it relevant. Even with the best intentions and efforts of the scheme rule drafters, adjustments will be needed after the scheme's pilot stages.

One means of addressing these needs (flexibility and adaptability) is to establish a permanent review mechanism to evaluate the scheme. The review mechanism must apply the principles of participation and transparency. Involving and getting views of different stakeholders will ensure the scheme stays relevant and gains wider acceptability. Transparency will help achieve public trust. All the work leading up the drafting of the scheme's rules and regulations, and the scheme review ought to be public and accessible to any interested party.

The model outlined in the Draft European Parliament Legislative Resolution on GDPR is general; this may be to achieve the purposes of flexibility and adaptability (see Article 39). DPAs, who are to award "European Data Protection Seal", presumably have no means of knowing (and thus drafting) rules that are adaptable enough for each processing sector and following its implementation closely, to update appropriately, them. The Commission is empowered to issue delegated acts with the relevant details, but these may come too late – and, at any event, the Commission may face challenges, like the DPAs, in knowing and following the processing particulars of each separate sector. Less assistance as to the need for flexibility and adaptability is evident in the text of the proposed General Data Protection Regulation adopted in 2012. A successful EU privacy certification scheme should incorporate these, and therefore they must be visible at the highest possible level. The same applies to the establishment of a permanent drafting and review mechanism, for each separate sector where certification will be available; this will ensure flexibility and adaptability for the sector concerned.

5.2.6 Transparency and accountability

Transparency and accountability are the two main advantages of implementing an EU privacy seal scheme. With regard to transparency,[35] it is important that the scheme (to gain public trust and therefore wide use) adopt transparent processes both in relation to its rules and regulations, and in relation to its evaluation processes and results. The principle of transparency requires a participatory and open process for all stakeholders. Transparency must be adopted through the publication of the relevant evaluation results; this would include not only the list of successful participants but also cases of serious infringements and the operators' responses to them.

Accountability would be enhanced through the introduction of an EU privacy seal scheme, because controllers would have a certification system tailored to their particular processing instances, against which are able to evaluate their practices.[36] However, a certification system does not operate in void; it is based on the assumption that participants have the will to conform to its rules and regulations and that they will continue to do so for as long as they carry the relevant seal. Consequently, the principle of accountability is paramount to the success of this scheme; participants must be aware that, despite evaluation and follow-up

[35] See also Bock, "EuroPriSe Trust Certification", op. cit., 2008, p. 5.
[36] See also Article 29 WP, Opinion 3/2010, op. cit., 2010.

audits, they are ultimately responsible for applying the scheme's rules to their processing practices.

Enforcement[37] is critical to the success of an EU privacy seals scheme – it is the point where the principles of transparency and accountability meet. In cases of confirmed infringements, scheme operators should not only hold the infringer liable and impose relevant penalties, but also announce the findings and make their decision public. As shown in Task 1 and also identified in section 4.7, many existing privacy seal schemes suffer from enforcement weaknesses. The lax response to scheme rule infringements has led to loss of public trust. Such a case would be catastrophic for an EU privacy seals scheme, especially if it will be overseen by regulatory agencies (DPAs). A relaxed approach to infringers would endanger both the scheme and the concerned DPA's public credibility. A firm and transparent reaction[38] would convince addressees that the scheme is performing its declared task - providing them with a means of quickly and easily distinguishing between the entities that respect their privacy and personal data and those that do not.

The principles of transparency and accountability should be embedded in any model of an EU privacy seal scheme, whatever its final form.

5.2.7 Scheme sustainability

An EU privacy seal scheme needs to be self-sustainable, but not for-profit. A number of reasons and the lessons learnt from existing privacy seal and sectoral certification schemes support this conclusion. First, a scheme that is not supported by the industry it is addressed to, may not be a scheme worth maintaining. An EU privacy seal scheme would enhance transaction potential for sellers and service providers and facilitate their privacy compliance. Consumers would benefit (from informed choice and an accessible redress system). If these substantial benefits are not enough, or implemented in a convincing way through an EU privacy seal scheme, participants may not be prepared to pay for it and such a scheme would then be ineffective. Because it is a scheme aimed at the industry, industry must show an active interest in it. In this context, it is possible that industry associations would be interested in supporting a certification scheme pertaining to their members' activities; this option could prove beneficial from other points of view (for instance, addressees and users' awareness).

Second, the scheme (or, for the same purposes, any certification scheme) must demonstrate its financial independence. A solely government-funded scheme might lack the incentive to serve its participants better by constantly improving, adapting its rules and technical details to address evolving and new concerns. On the other hand, a scheme that intends to profit from its participants' risks alienating its addressees; even if it is well-established and has the best of intentions and practices.

Third, the maintenance an EU privacy seals scheme will be an expensive and resource-intensive effort. The setting up of the scheme, rules, determining technical standards for each sector, regular updates, evaluation of participants, monitoring and enforcement requires significant all require resources (financial, time or other). Any money made from the scheme

[37] What is meant by enforcement varies significantly depending on whether the scheme operator is a public authority with administrative powers, private company, industry association or non-governmental organisation.
[38] See also ECC-Net, Can I trust, op. cit., 2013, p. 56, where blacklisting is also listed among enforcement solutions.

would necessarily need to be re-invested in itself to strengthen it and ensure its continued relevance and success. To maintain credibility, it would be useful for the scheme to be transparent about its financial aspects, to the extent that is possible. The scheme operator, if not a data protection authority, evaluators or auditors (whether internal or outsourced), the fees charged, all need to demonstrate a balance between self-sustainability and an unwillingness to pursue profit to the detriment of data subject interests. Whatever the final form of the General Data Protection Regulation, the need of an EU privacy seal scheme to be self-sustainable without becoming a profit mechanism should be guaranteed.

5.2.8 Public awareness and trust

An important priority for an EU privacy seals scheme that is also crucial to its survival and success in the market, is the achievement of public awareness and trust.[39] Wide public use of a certification scheme constitutes a self-fulfilling promise for its success; the more people use it (both participants and addressees), the more it becomes established in the relevant market, gaining public trust and leading to greater participation in it. Existing privacy seal schemes, as shown in Task 1, are not optimised for public awareness and trust.

It is difficult to narrow down all the means through which public awareness and trust are achieved as they often relate to social, political and market factors that are not only indistinguishable, but may vary among Member States. One factor that would contribute to public awareness and trust is the consistent, diligent and transparent use of the certification scheme. Public awareness would be better served if the scheme is widely publicised after launch and through a sustained campaign at regular points in its life cycle.

Public awareness and trust would probably be unspoken priorities, at least from a legal point of view, in the sense that there might be little meaning in including relevant provisions in an EU privacy seals legal mandate. Any such reference could only be interpreted, at best, as general guidance and declaration of intentions, without however leading to any concrete legal rights or obligations. This is why this priority is listed last in the catalogue of priorities for an EU privacy seal scheme; if attained, however, it will constitute a fundamental assurance for the scheme's longevity and effectiveness in fulfilling its purposes.

5.3 CASE STUDIES

This section presents case studies to illustrate the possible scope of an EU privacy seal scheme in the following four areas: CCTV systems, international transfers (cloud services), smart metering and biometric systems.

The four case studies illustrate how an EU privacy seal scheme might work in practice, along the lines discussed before. Each case study refers to a sector that is expansively processes personal data and triggers numerous debates in terms of privacy and data protection. For instance, CCTV raises concerns of unauthorised surveillance, facilitating identification, data use, the retention and sharing of personal data. International transfers (cloud services) introduce new critical challenges to the EU data protection system, by way of circumventing its adequacy criterion when it comes to transfers of personal data to third countries. The risks include privacy and confidentiality risks, storage on remote computers, and lack of security of

[39] Rodrigues, Rowena, David Wright and Kush Wadhwa, "Developing a privacy seal scheme (that works)" *International Data Privacy Law*, Vol. 3, Issue 2, 2013, p.102; ECC-Net, Can I trust, op. cit., 2013, p. 54.

the processing. The privacy and data protection concerns prompted by smart metering include the ability to facilitate the collection of massive amounts of data, data mining and energy-consumption-based personal and household profiling.[40] Biometrics raise concerns such as unauthorised collection, use and sharing of data, unnecessary collection and retention, facilitating identification (particularly across databases) and surveillance uses, unauthorised disclosure and function creep. An effective privacy seal scheme in each of these sectors might help resolve some of these concerns.

5.3.1 Methodology

There were five key steps in the development of the case studies:[41]

- *Initial literature review*: This helped determine the state of the art in the area, specifically the needs and requirements for certification. We identified and provided a summary of the 'problem' of privacy in this context.
- *Initial contact with experts:* This helped obtain necessary information and set the scene for the case studies.
- *Brainstorming:* The partners used this technique to elaborate the content of each case study. The process generated more than one potential use of privacy certification in these contexts; however, the partners selected an appropriate and illustrative case for further detail.
- *Development of case study:* This involved the research and actual writing of the case study based on the points outlined below (i-xviii).
- *Validation and finalisation:* This encompasses further liaison with appropriate experts (such as those specified in each case study) for validation and finalisation of the case study. The case studies will be shared and discussed at the Task 5 workshop in Brussels, held on 8 April 2014.

Each of the case studies focuses on the following aspects:

Understanding the problem of privacy in the context

i. **Definition and explanation of the context**: This defines and scopes the field of examination for the case study and explains its context – i.e., its broader operating environment.
ii. **Risks and mitigation measures**: This identifies the specific privacy and data protection risks (such as unauthorised surveillance, facilitating identification, data use, retention and sharing of personal data, security of data) in relation to each case study and how these are generally mitigated.
iii. **Applicable legislation and standards**: This identifies the legislation (EU and, where possible, a few Member States) applicable to the case study with a particular focus on privacy and data protection. Where relevant, it identifies industry or technical standards.
iv. **Good practices**: Some of case studies already use some sort of certification – we identify these and other good practices that privacy certification for this sector must take into account. These include Privacy Enhancing Technologies

[40] Doward, Jamie, "Energy smart meters are a threat to privacy, says watchdog", *The Observer*, 1 July 2012. http://www.guardian.co.uk/environment/2012/jul/01/household-energy-trackers-threat-privacy
[41] This methodology elaborates more comprehensively the methodology proposed in the Tender document.

(PETs), privacy by design as advocated by the proposed General Data Protection Regulation, and products that follow the specifications of these technologies.

v. **Need for privacy certification**: This outlines why privacy certification is relevant to the case study.

vi. **Potential barriers to certification**: This identifies potential barriers to certification in relation to the individual context of the case study.

Certification approach and methodology

vii. **Scope and limitations of privacy certification**: This outlines the scope and limitations of privacy certification in relation to the case study. It shows how far privacy certification can go to protect privacy and personal data.

viii. **Target of certification:** For each case study, we identity the target of certification and the rationale. To whom or what should the certification best be aimed? A technology, process, product, service or organisation?

ix. **Beneficiaries:** This identifies who would benefit from privacy certification in relation to the case study.

x. **Harmonisation and common standards**: This explores whether harmonisation and common standards are possible. What would need to be done in terms of harmonisation and development of common standards? Who might be the bodies we need to bring on board to achieve this objective?

xi. **Policy requirements:** This identifies the policy requirements for privacy certification in relation to the case study. What are the policy actions that would be applicable and required to be taken to support the scheme?

xii. **Regulatory requirements:** This identifies the regulatory requirements for privacy certification. Would there be a need for additional legislative measures? Is the current framework sufficient? What happens in cases of cross border effects?

xiii. **Technical requirements:** This identifies the technical requirements for privacy certification in relation to the case study. It presents some general recommendations in relation to some core aspects of operating the schemes.

xiv. **Market requirements**: This identifies the market requirements for privacy certification in relation to the case study.

xv. **Roles and actions of stakeholders:** This identifies the roles and actions of different stakeholders such as the European Commission, national policy-makers, regulatory authorities, standards organisations, seal issuers, seal subscribers, third parties, privacy organisations, and end users.

xvi. **Responsibility and accountability (compliance and oversight) mechanisms:** This identifies who might be responsible for administering and overseeing the scheme. Who would be responsible for the enforcement of the scheme?

xvii. **Sustainability**: Sustainability is an important element of a successful privacy certification scheme. We identify how the scheme might sustain itself or the additional resources needed to achieve this.

xviii. **Evaluation and conclusion**: Based on the above analysis, we make a broader evaluation of privacy certification in relation to the case study.

5.3.2 CCTV systems

This case study benefitted from input from the UK Information Commissioner's Office (ICO),[42] CNIL (the French Data Protection Authority)[43] and the CCTV User Group[44].

5.3.2.1 Definition and explanation of the context

Closed Circuit Television Cameras (CCTV) are "a situational measure that enables a locale to be kept under surveillance remotely".[45] CCTV has become highly pervasive and is now a highly normalised form of surveillance in Europe, specifically in countries such as the UK, stated to have "set the pace in CCTV deployment"[46]. A report on *Surveillance, fighting crime and violence* suggests that "although the presence of video surveillance cameras in public places is a common occurrence throughout Europe, these systems differ in a number of respects, making a precise definition very difficult."[47] In the UK, the term 'CCTV' is used to refer to these systems; in Europe the term 'video surveillance' is more commonly used.

According to the European Committee for Electrotechnical Standardization (CENELEC), a CCTV surveillance system is "a system consisting of camera equipment, monitoring and associated equipment for transmission and controlling purposes, which may be necessary for the surveillance of a defined security zone".[48] CCTV is means of "providing images from a television camera for viewing on a monitor via a private transmission system".[49] Any number of cameras and monitors may be used in a CCTV surveillance installation (dependent on the combination of control and display equipment and the operator's ability to manage the system).

A CCTV system may be used on an ad hoc basis to monitor a specific event or people, or on a more permanent basis for more routine and continuous monitoring of events and people. CCTV systems may be used overtly or covertly for a variety for purposes ranging from national security, public safety, deterring crime, general surveillance of people, asset protection, employee surveillance, patient monitoring, traffic monitoring. The different types of CCTV cameras include: dome cameras (common indoor cameras mounted on the ceiling with covered lenses to shield direction of filming), box cameras (mounted to wall or vertical

[42] Contributions from Jonathan Bamford (Head of Strategic Liaison), Steve Wood (Head of Policy Delivery), Jo Pedder (responsible for currently reviewing the CCTV Code of Practice along with Richard Sissons) and Gemma Farmer (Senior Policy Officer) of the ICO.
[43] Please note, CNIL views expressed in this case study are the position of the CNIL's technical services and do not bind the Board of Commissioners of the French DPA.
[44] For an overview of the aims and objectives of the group see CCTV User Group, "Aims and Objectives". https://www.cctvusergroup.com/art.php?art=9. The group (of over 400) is largely made up of organisational members responsible for CCTV systems and includes local Authorities operating public area CCTV Systems, police forces within the UK, universities, hospitals, health trusts, housing associations and passenger transport.
[45] Gill, Martin & Angela Spriggs, *Home Office Research Study 292: Assessing the Impact of CCTV*, Home Office Research, Development and Statistics Directorate, February 2005.
[46] Wright, David (ed.), *Surveillance, fighting crime and violence*, Deliverable D1.1. A report of the IRISS consortium to the European Commission, December 2012, pp. 71-156 [p. 7]. http://irissproject.eu/wp-content/uploads/2012/02/IRISS_D1_MASTER_DOCUMENT_17Dec20121.pdf. See also http://www.urbaneye.net/
[47] Ibid.
[48] European Committee for Electrotechnical Standardization (CENELEC), EN 50132-7 Alarm systems - CCTV surveillance systems for use in security applications Part 7: Application guidelines, ICS 13.320, June 1996.
[49] Ibid.

area ideal for viewing long distances), infra-red cameras (suited for low lighting conditions), bullet cameras (inconspicuous but not covert devices for shorter distance filming), covert cameras (which come in range of shapes and sizes and may be illegal to use in some jurisdictions), wireless cameras, and pan-tilt-zoom (PTZ) cameras (that permit live control of the camera).[50] There are different types and levels of CCTV systems – some more basic and others more advanced. Advanced CCTV systems include "the capability to automatically analyse irregular events within a video stream, an intruder crossing a line or other Intelligent Video Analytics (IVA) algorithms".[51] Professor William Webster[52] presents the following typology of CCTV systems:[53]

Type	Features
Interactive or smart	Computerisation of CCTV processes so that live surveillance is also determined by computer-based algorithms and profiles.
Proactive	Live surveillance from a dedicated control room with recording, storage and playback facilities. Allows for an immediate response to incidents as they occur.
Reactive	Recording, storage and playback facilities. Provides access to footage of incidents after the event has occurred.
Non-active	No monitoring, storage or playback facilities. Acts as a visual deterrent by using fake 'cameras' to create the illusion of surveillance.

Table 1 Typology of CCTV systems

This table illustrates the levels of complexity in the nature of these systems.

5.3.2.2 Risks and mitigation measures

CCTV presents a number of privacy and data protection risks. The following table presents some of the CCTV-related risks, their consequent effects and lists some of the possible or commonly adopted mitigation measures.

Risk	Effect	Mitigation measures
Placement of CCTV camera	Loss of privacy and anonymity[54], capture of personal data, changes in behaviour.	Placement only in places where there is no reasonable expectation of privacy. Notice of CCTV used by installing signs detailing the scheme and its purpose, along with a contact telephone number.

[50] Aventura Technologies, "Camera Tutorial". http://www.aventuracctv.com/PDF/Aventura_Camera_Tutorial.pdf

[51] Katz, Hagai, "Access Denied". http://www.magal-s3.com/contentManagment/uploadedFiles/In_the_Press/Airports_World_-Access_denied_AW6.pdf

[52] Professor William Webster is the Director of the Public Service Management MBA and BA (Hons) Public Management & Administration programmes at the University of Stirling. He is a recognised expert on Closed Circuit Television (CCTV) surveillance cameras and Interactive Digital Television (iDTV) and the Chair of the Living in Surveillance Societies (LiSS) COST Action IS0807 (2009-13).

[53] Webster, C. William R., "CCTV Policy in the UK: Reconsidering the Evidence Base", *Surveillance & Society*, Vol. 6, No. 1, 2009, pp. 10-22.

[54] Goold, Benjamin, "CCTV and Human Rights" in European Forum for Urban Security (ed.), *Citizens, Cities and Video Surveillance, Towards a democratic and responsible use of CCTV*, June 2010, pp. 27-36, p. 29.

		Regulation restricting placement.
Heightened observation and identification of individuals and groups. Recording more than necessary.	Loss of anonymity, chilling effects on free expression, movement and association	Face blurring. Privacy zone blanking/scene blurring.[55] Encrypting data for persons not being tracked or involved in a particular incident.[56] Regulatory measures.
Unauthorised (data capture) filming and use of information	Loss of privacy; no meaningful opportunity to withhold consent to having an image captured, stored, used or shared.	Face blurring. Privacy zone blanking. Encrypting data for persons not being tracked or involved in a particular incident. Regulatory measures.
Sharing of CCTV images and data	Loss of privacy. Loss of control over personal data. Increased risk of compromise of personal data.	Redaction of data[57] Purpose limitation policy. Maintenance of records of data sharing. Mandating approval for sharing. Regulatory measures.
Uncontrolled (unlimited) and unlawful retention of CCTV records/data	Threat to personal data, loss of privacy and security	Clear and explicit retention policies. Regular destruction of data. Regulatory measures.
Inappropriate access to CCTV systems and logs, data breaches and misuse	Threat to personal data, loss of privacy and security	Limiting access to authorised users. Strict access control procedures and policies. Password protection. Rules of behaviour. Regulatory measures.
Low levels of security, security vulnerabilities for CCTV systems	Threat to personal data, loss of privacy and security	Encryption Use of trusted middleware agents such as Discrete Box. Security policies. Security audits. Regulatory measures.
Lack of privacy, data protection measures and policies	Loss of privacy, Compromise of personal data	Privacy impact assessments, implementation of data protection measures. PETs.
Targeted surveillance[58]	Discrimination,	Privacy impact assessment.

[55] Neustaedter, C., S. Greenberg, M. Boyle, "Blur filtration fails to preserve privacy for homebased video conferencing", *ACM Transactions on Computer Human Interactions,* Volume 13, Number 1, March 2006, pp. 1-36.

[56]Department of Homeland Security, *CCTV: Developing Privacy Best Practices*, Report on the DHS Privacy Office Public Workshop, 17-18 Dec. 2007.
http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf

[57] Chen, D., Y. Chang, R. Yan, & J. Yang, "Tools for protecting the privacy of specific individuals in video", *EURASIP Journal on Applied Signal Processing*, Volume 2007, Issue 1, 2007, pp. 107-107.

[58] Goold, B., *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*, Oxford University Press, Oxford, 2004.

	Chilling effects	Clear CCTV use policies. Standards and Codes of Conduct. Regulatory measures.
Use and expansion of system's use beyond indicated use[59]	Wider surveillance. Abuse of powers. Unlawful retention, sharing, data breaches.	Privacy impact assessment Standards and Codes of Conduct Audit and reviews. Regulatory measures.
Lack of a properly justified and proportionate approach to establishing CCTV schemes	Patchwork of systems Confusion about scope of CCTV operation and impacts	Clearly articulated policy. Regulation of CCTV implementation.

Table 2 Risks, effects and mitigation measures of CCTV systems

The UK Information Commissioner's Office (ICO) highlights that there are three important aspects of CCTV risks[60]: their universality, context and the potential for their aggravation. While the risks associated with CCTV might be universal, they increase in the following conditions: where the recording is carried out using more sophisticated technologies or used in conjunction with other technologies (e.g. combining thermal imaging, audio recording, zooming possibilities); and, where the recording is more intrusive or includes sensitive images. The use of CCTV in different contexts is also relevant to the nature of risks; the place at which a CCTV is used pose different sorts of risks. For example, installing CCTV in school or parking area to deal with vandalism at night and installing CCTV in a changing room or school toilet to deal with bullying or criminal damage to fittings by students pose different risks and may have varying privacy and data protection impacts. Finally, CCTV risks may be aggravated when the technology is used for purposes other than its original intended one. Here, the ICO cites the example of how Automatic Number Plate Recognition (ANPR) originally used to monitor unregistered vehicles is now extensively used for other purposes, e.g., to locate vehicles (and their owners) that might appear on police databases; and, how private car parking operators are collecting large amounts of ANPR 'read' data to enforce parking restrictions in private car parks such as supermarkets and often retaining this data indefinitely.

5.3.2.3 Applicable legislation and standards

This section discusses the applicable privacy and data protection related legislative and other compliance standards applicable to CCTV systems in the EU.

The Charter of Fundamental Rights of the EU consolidates fundamental rights protected in the EU. Proclaimed in 2000, the Charter is legally binding on the EU with the entry into force of the Treaty of Lisbon, in December 2009.[61] Article 7 (respect for private and family life) states that everyone has the right to respect for his or her private and family life, home and

[59] The UK ICO suggests that complaints to its office show that citizens are less supportive of cameras being used for wider commercial purposes such as car parking, marketing and promotion, or income generation.

[60] Other broader general risks, that the UK ICO highlights, are: poor image quality; the technical difficulties and cost of police retrieval of digital images from a wide variety of incompatible systems; technical and organisational barriers to organisations sharing images, for example between police and prosecutors; and the criminal justice system being unable to use CCTV footage as evidence.

[61] European Parliament, the Council and the Commission, Charter of Fundamental Rights of the European Union, *Official Journal of the European Union*, C 83/391, 30 March 2010. The Charter specifies rights and freedoms under six titles: dignity, freedoms, equality, solidarity, citizens' rights, and justice.

communications. According to Article 8 (protection of personal data), everyone has the right to the protection of personal data concerning him or her; such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with Article 8 rules is subject to control by an independent authority.

The next important piece of legislation is the EU Data Protection Directive 95/46/EC.[62] CCTV images are personal data.[63] Article 6 of the Directive sets out the data protection principles in relation to personal data: fair and lawful processing, purpose limitation, data adequacy, accuracy of data, time limitation). Other significant elements are: data subject's right of access to data (Article 12a), integrity of data (Article 12b), automated decision making (Article 15), security of data (Article 17) and conditions of transfer of data to third countries (Chapter IV). These would all apply to CCTV data controllers and processors. However, we must note the limitation of the applicability of the Directive. Recital 16 of the Directive expressly states that "the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law".[64] The Directive also excludes from its scope the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic.[65]

Each EU Member State has its own national privacy and data protection legislation that impacts CCTV (and also the potential scope of privacy certification connected to it). In France, for example, video surveillance is governed by the legal guidelines and security planning act (LOPS, 21 January 1995), Decree n° 96-926 of 17 October 1996 and the decree on its enforcement (22 October 1996); and Loi n° 2011-267 du 14 Mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.[66] The latter empowers the CNIL to oversee all videosurveillance systems installed on the public highway.[67] The following table illustrates the regulatory regime applicable to CCTV in Spain:[68]

Table 1 – Legal regulation of CCTV in Spain.

Regulation	Purpose	Scope
LO 4/1997	To regulate the use of video cameras in public spaces by the Spanish Police Forces	Public
RD 596/1999	To give effect to the regulations of the Organic law	Public
LO 15/1999	On the protection of personal data	Public and private
I 1/2006 (DPA)	On the treatment of personal data linked to surveillance through camera systems or video surveillance	Private

[62] European Parliament and the Council, Directive 95/46/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, *OJ L* 281, 23 Nov 1995, pp. 0031-0050.
[63] Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, Adopted on 20 June 2007, 01248/07/EN, WP 136.
[64] Directive 95/46/EC.
[65] Recital 12, Directive 95/46/EC.
[66] JORF n°0062, 15 March 2011, p. 4582.
[67] Commission nationale de l'information et des libertés (CNIL), *Vidéosurveillance / vidéoprotection: les bonnes pratiques pour des systèmes plus respectueux de la vie privée*, Press communication, June 2012.
[68] Agustina, J.R., & Gemma Galdon Clavell, "The impact of CCTV on fundamental rights and crime prevention strategies: The case of the Catalan Control Commission of Video surveillance Devices", *Computer Law & Security Review*, Volume 27, 2011, pp. 168-174.

Table 3 Legal regulation of CCTV in Spain

In the UK, the Data Protection Act 1998, Human Rights Act 1998 and the Freedom of Information Act regulate the use of CCTV. Data subjects have a right to see what information is held, including CCTV images, or images which give away personal information (e.g. car number plate). The Data Protection Act sets rules which CCTV operators must follow when they gather, store and release CCTV images of individuals. The Information Commissioner (ICO) can enforce these rules. The ICO has issued a CCTV Code of Practice.[69] Law enforcement covert surveillance activities are covered by a separate Act - the Regulation of Investigatory Powers Act (RIPA) 2000 and the Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2000.[70] The Protection of Freedoms Act 2012 regulates 'surveillance camera systems' which includes CCTV and ANPR systems. The Act prescribes the appointment and role of the Surveillance Camera Commissioner whose responsibilities include promoting and encouraging compliance with the surveillance camera code of practice amongst users; reviewing how the code is working; and providing advice about the code (which may include, for example, advice to users of surveillance systems, members of the public, and Ministers as necessary). The Private Security Industry Act 2001 applies in relation to requirements to have a public space surveillance licence; under this legislation the Security Industry Authority licenses individuals working within the security industry including those monitoring CCTV.

The Article 29 Data Protection Working Party adopted *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance.*[71] This document aimed at drawing attention to the wide scope of criteria for the assessment of lawfulness and appropriateness of installing video surveillance systems.

Article 8 of the European Convention on Human Rights (ECHR)[72] applies in cases where CCTV systems are used by public authorities and their agencies. Article 8 deals with the right to respect for private and family life. It states:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The European Court of Human Rights deliberated upon the use of CCTV by public authorities in *Peck v the United Kingdom* (publication of CCTV images of a person wielding knife in

[69] ICO, *CCTV Code of Practice*, 2008.
http://www.ico.org.uk/Global/faqs/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx

[70] For a more comprehensive listing of national laws impacting CCTV in the EU Member States see Lim, Laurent, "The legal framework of video surveillance in Europe", in European Forum for Urban Security (ed.), *Citizens, Cities and Video Surveillance: Towards a democratic and responsible use of CCTV,* June 2010, pp.81-98.

[71] Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 11750/02/EN, WP 89, 11 Feb 2004.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf

[72] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13, Rome, 4 Nov 1950.
http://www.echr.coe.int/Documents/Convention_ENG.pdf

street)[73]. The Court held that the publication of the images by the public authority constituted a serious interference with the individual's right to respect for private life. The only limitation of the ECHR is that it is a 'closed' instrument that does not permit the participation of non-European and non-member States."[74]

The Convention for the Protection of Individuals with regard to automatic processing of personal data (or Convention 108), aims to secure in each contracting State "for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him".[75] The main objective of the Convention is to strengthen data protection, i.e. the legal protection of individuals with regard to automatic processing of personal information relating to them."[76] As opposed to the ECHR, the Convention protects certain individual rights regardless of frontiers.

The Council of Europe's Parliamentary Assembly adopted a Resolution on Video Surveillance in public areas in 2008[77] calling upon the Council of Europe member states to:

- apply the guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance adopted by the Council of Europe's European Committee on Legal Co-operation (CDCJ) in May 2003 and to ensure that they are adhered to as systematically as possible;
- lay down by law technical restrictions for installation limits of the equipment with reference to each place under surveillance;
- define privacy zones to be excluded from video surveillance by law, imposing the use of specialised software;
- provide in their legislation for the practice of encoding video data;
- provide access to a legal remedy in cases of alleged abuse related to video surveillance.

A paper commissioned by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), criticises the ability of the law in Europe to regulate CCTV terming the relevant regulatory instruments "patchy in their scope and application".[78] It further highlights differences in regulatory practices across the Member States of Europe in relation to installation requirements, powers of inspection etc. It also highlights the failure of law and codes in controlling breaches.

There is also one European Standard that deals specifically with CCTV surveillance systems - *European Standard EN 50132-1:2010 Alarm systems - CCTV surveillance systems for use in security applications.*[79] This Standard applies to CCTV systems for surveillance of private

[73] (2003) 36 *EHRR* 41.
[74] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Explanatory Report. http://conventions.coe.int/Treaty/en/Reports/Html/108.htm
[75] Council of the European Union, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108, Strasbourg, 28 Jan 1981. The convention entered into force on 1 October 1985.
[76] Ibid.
[77] Council of Europe Parliamentary Assembly, Video Surveillance in Public Areas, Resolution 1604 (2008). http://assembly.coe.int/ASP/Doc/XrefViewPDF.asp?FileID=17633&Language=en
[78] Norris, Clive, *A Review of the Increased Use of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe*, Civil Liberties, Justice and Home Affairs Committee (LIBE), European Parliament, April 2009. [p.16]
[79] CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. CENELEC

and public areas and intends to assist CCTV companies, manufacturers, system integrators, installers, consultants, owners, users, insurers and law enforcement in achieving a complete and accurate specification of the surveillance system. This standard specifies the minimum performance and functional requirements for CCTV surveillance systems installed for security applications.[80] It does not include requirements for design, planning, installation, testing, operation or maintenance.[81] While this Standard excludes installation of remotely monitored detector activated CCTV systems, it applies to CCTV systems sharing means of detection, triggering, interconnection, control, communication and power supplies with other applications. Part 1 of the Standard specifies the system requirements, Part 5-1 focus on 'Video transmission – General Video Transmission Performance Requirements', Part 5-2 on IP Video Transmission Protocols, Part 5-3 on Video transmission – Analog and Digital Video Transmission and Part 7 on Application guidelines. The System Requirements (*EN 50132-1:2010 Part 1)* specify four grades of security and state that the protection of a CCTV system depends on the integrity of the system and on integrity of data which must be maintained. The integrity of data has three elements:

- Data identification (exact identification of a source of data, time, date, etc.),
- Data authentication (preventing from modifications, deleting, or adding data), and
- Data security (preventing from unauthorized data access).[82]

Other privacy, data protection-related provisions of the Standard relate to: user choice in relation to scope of time and source of exported or copied video, verification of integrity of images and other data, metadata and their identity, encryption to prevent unauthorised previews of data, method of secure copying and exporting of data, adequate methods of controlled access to data with respect to the level of authorisation, privacy masking, and documentation of compliance with local privacy and other legislation.

At the national level, in the UK, the British Standards Institution (BSI) has standards aimed at supplementing the Data Protection Act, 1998 (DPA), the Human Rights Act, 1998 and the Freedom of Information Act 2000 – these provide recommendations for the operation and management of CCTV and assist owners of CCTV schemes to follow best practices in obtaining reliable information that may be used as evidence.[83] The current standards include:

- BS 7958:2009 *Closed-circuit television (CCTV), Management and operation, Code of practice*.[84]
- BS 8418:2010 *Installation and remote monitoring of detector-activated CCTV systems, Code of practice*.[85]

---

members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the UK.

[80] CENELEC, "*European Standard EN 50132-1:2010 Alarm systems - CCTV surveillance systems for use in security applications",* 2010.
http://www.cenelec.eu/dyn/www/f?p=104:110:730415270979609::::FSP_PROJECT,FSP_LANG_ID:2485,25

[81] Ibid.

[82] CENELAC, *European Standard*, op. cit., 2010.

[83] BSI, "CCTV". http://shop.bsigroup.com/Browse-By-Subject/Security/Electronic-Security-Systems/CCTV/

[84] BSI, *BS 7958:2009 Closed circuit television (CCTV), Management and operation, Code of practice,* BSI, London, 30 Sept 2009. BS 7958 provides recommendations for the operation and management of CCTV within a controlled environment. It applies where data that might be offered as evidence is received, stored, reviewed or analysed. It also applies to the monitoring of traffic regulations. BS 7958 applies to CCTV schemes used in public places. BS 7958 provides recommendations on best practice to assist users in obtaining reliable information that can be used as evidence.

5.3.2.4 Certification-related good practices

There are a number of certification and privacy-related good practices in relation to CCTV.

The EDPS Video-surveillance Guidelines

The *EDPS Video-surveillance Guidelines*,[86] offer practical guidance to EU institutions and bodies operating video surveillance[87] equipment on how to comply with the Regulation 45/2001[88] and use video surveillance responsibly with effective safeguards. The Guidelines set out the principles for evaluating the need for video surveillance and provide guidance on how to conduct it in a way which minimises impact on privacy and other fundamental rights. While the Guidelines focus on video surveillance for typical security purposes (including access control), they are also applicable to: more complex or more specific security operations, video surveillance used during internal investigations (whether or not related to security) and, video surveillance used for any other purpose. The Guidelines emphasise carrying out a privacy and data protection impact assessment before installing and implementing video surveillance systems "whenever this adds value to the Institution's compliance efforts".[89] They focus on the following aspects:

- Assessment of potential benefits and impact of system before use (purpose, lawfulness, necessity, efficiency, intrusiveness, detrimental effects, security)
- Selecting, siting and configuration of the video surveillance system (to minimise negative impact on privacy and fundamental rights)
- Retention of recordings
- Access to images
- Security measures to protect data
- Transfers and disclosures
- Provision of information to the public
- Fulfilment of access requests
- Accountability (ensuring, verifying and demonstrating good administration)
- Outsourcing and third parties

The Guidelines are not definitive statements of law, but according to the EDPS, compliance with them will be taken into account during enforcement proceedings.

---

[85] BSI, *Installation and remote monitoring of detector-activated CCTV systems, Code of practice*, BSI, London, 31 July 2010. BS 8418 defines the code of good practice for the design, installation, commissioning, operation and remote monitoring of detector-activated closed-circuit television (CCTV) systems

[86] European Data Protection Supervisor (EDPS), *The EDPS Video-surveillance Guidelines*, Brussels, 17 March 2010. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

[87] Defined as "the monitoring of a specific area, event, activity, or person by means of an electronic device or system for visual monitoring" and typically representing CCTV systems.

[88] European Parliament and the Council, Regulation 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *OJ L* 8, 12 Jan 2001, [p. 1].

[89] EDPS, *The EDPS Video-surveillance Guidelines*, op. cit., 2010.

European Forum for Urban Security Charter for a democratic use of video-surveillance

The *Charter for a democratic use of video-surveillance*[90] aims at providing citizens with guarantees regarding the use of CCTV systems. The Charter governs the design, operation and subsequent development of public video surveillance systems (i.e. those operated by public authorities, national, regional or local) and are amenable to extension to private video surveillance systems, especially when their use and their data might be made available to public authorities. Signatories commit to a set of self-imposed rules outlined in the Charter. The seven fundamental principles of the Charter are: legality, necessity, proportionality, transparency, accountability, independent oversight, and citizen participation. The Charter also contains illustrations of appropriate CCTV signage (that could be applied across the EU).

Privacy impact assessments

Privacy impact assessment or PIA is a "methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders for taking remedial actions as necessary in order to avoid or minimise negative impacts".[91] Public bodies conduct PIAs on CCTV systems. The following UK examples illustrate this: the Sedgemoor District Council CCTV Impact Assessment (UK)[92], the Impact Assessment on the Urban Traffic Management and Control (UTMC) CCTV and ANPR System (UK).[93]

CCTV installer certification

The National Standards Authority of Ireland (NSAI), the official standards body operating under the National Standards Authority of Ireland Act (1996)[94] offers a certification scheme for CCTV installers, based on the EN 50132 series of Standards (European Standards for CCTV systems). The assessment procedure involves a physical inspection of selected installations. The NSAI examines: contractual requirements, training records, calibration, risk assessment, national wiring regulations, and manufacturers' documentation. After an assessment is successfully completed, NSAI issues the CCTV installer with a certificate confirming that the company satisfies all requirements of the NSAI document, and Inspection Criteria for Assessment of CCTV Installers.[95]

[90] EFUS, Charter for a democratic use of video-surveillance, 28 May 2010, http://www.cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Charta/CCTV_Charter_EN.pdf
[91] Wright, David and Paul De Hert, "Introduction to Privacy Impact Assessment," in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment,* Springer, pp. 3-32, [p. 5].
[92] Donbavand, Barry, *Sedgemoor District Council CCTV Impact Assessment S.4 ICO COP*, 28 Feb 2013 http://www.sedgemoor.gov.uk/CHttpHandler.ashx?id=12244&p=0
[93] Buckinghamshire County Council (UK), *Privacy Impact Assessment on the UTMC CCTV and ANPR System: Summary Report*, http://democracy.buckscc.gov.uk/documents/s20018/PT14.11%20PIA%20Report.pdf
[94] The NSAI is accountable to the Irish Minister of Jobs, Enterprise and Innovation and is the national certification authority for the CE Marking.
[95] NSAI, "CCTV Certification". http://www.nsai.ie/Our-Services/Certification/Product-Certification/Product-Certificaton-for-Security-Systems/IS-EN-5013---CCTV-Certification.aspx

CCTV Guidance from data protection authorities

Some DPAs such as the UK ICO have a CCTV Code of Practice.[96] The objective of the ICO Code is to ensure that operators of CCTV adopt good practice standards.[97] More specifically, the Code is designed to:

- help ensure that those capturing images of individuals comply with the Data Protection Act 1998;
- mean that the images that are captured are usable; and
- reassure those whose images are being captured.

The CCTV Code of Practice provides good practice advice for those (i.e. businesses and organisations who routinely capture images of individuals on their CCTV equipment) involved in operating CCTV and other devices which view or record images of individuals. The Code sets out the recommendations on how the legal requirements of the Data Protection Act 1998 can be met. The Code covers the use of CCTV and other systems which capture images of identifiable individuals or information relating to individuals for any of the following purposes:

- Seeing what an individual is doing, for example monitoring them in a shop or walking down the street.
- Potentially taking some action in relation to an individual, for example handing the images over to the police to investigate a crime.
- Using the images of an individual in some way that will affect their privacy, for example passing images on to a TV company.[98]

The Code does not cover covert surveillance activities of the law enforcement community,[99] conventional cameras (not CCTV) used by the news media or for artistic purposes, and the use of dummy or non-operational cameras. The Code makes many recommendations some of which include:

- Conducting an impact assessment to determine whether CCTV is justified and how it should be operated in practice.
- Consideration of wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life)
- Establishing who has responsibility for the control of the images
- Regular reviews of whether the use of CCTV continues to be justified.
- Annual renewal of notification
- Exceptional use of CCTV in environments where there is a heightened expectation of privacy
- Recorded material should be stored in a way that maintains the integrity of the image.
- Viewing of live images on monitors should usually be restricted to the operator
- Controlled and consistent disclosure of images from the CCTV system
- Retention should reflect the organisation's own purposes for recording images.

[96] ICO, ICO, *CCTV Code of Practice*, 2008. http://www.ico.org.uk/Global/faqs/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx

[97] Ibid.

[98] ICO, *CCTV Code of Practice*, op. cit., 2008.

[99] These are governed by the Regulation of Investigatory Powers Act (RIPA) 2000 and the Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2000.

- Use of signs – clear, visible, readable and prominently placed at the entrance to the CCTV zone.

CNIL has an agreement between the CNIL and main stakeholders and guidelines for employers using CCTV.

Surveillance Camera Code of Practice (UK)

This code of practice[100] issued by the UK Home Office provides guidance on the appropriate and effective use of surveillance camera systems[101] by relevant authorities (as defined by Section 33 of the Protection of Freedoms Act 2012) in England and Wales who must have regard to the code when exercising any functions to which the code relates. Other operators and users of surveillance camera systems in England and Wales are encouraged to adopt the code voluntarily (they are however not bound by any duty to do so). The purpose of the code is to "ensure that individuals and wider communities have confidence that surveillance cameras are deployed to protect and support them, rather than spy on them".[102] The code applies to the use of surveillance camera systems operating in public places in England and Wales, regardless of whether there is any live viewing, or recording of images or information or associated data. The code does not cover covert surveillance by public authorities; this is regulated by the Regulation of Investigatory Powers Act 2000. The Code states "A relevant authority must follow a duty to have regard to the guidance in this code when, in exercising any of its functions, it considers that the future deployment or continued deployment of surveillance camera systems to observe public places may be appropriate."[103] The Code provides 12 guiding principles for systems operators.

At this juncture, we must note that CCTV related codes of conduct have been criticised as being "mere box ticking exercises".[104] Privacy certification would have to go beyond and address that concern or it will fail to be effective as a privacy-enhancing or personal data protection measure.

CCTV National Standards Forum (UK)

The CCTV National Standards Forum is a newly formed organisation aimed at providing a source of independent and expert advice to the government, regulators and a wide variety of stakeholders on issues that relate to the deployment of CCTV, both in the public and private sectors in the UK.[105] The Forum's membership includes representatives from the Security Institute, Association of Train Operating Companies (ATOC), Association of Chief Police

[100] Home Office, Surveillance Camera Code of Practice Pursuant to Section 29 of the Protection of Freedoms Act 2012.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf
[101] Surveillance camera systems has the meaning given by Section 29(6) of the Protection of Freedoms Act 2012 and is taken to include: (a) closed circuit television or automatic number plate recognition systems; (b) any other systems for recording or viewing visual images for surveillance purposes; (c) any systems for storing, receiving, transmitting, processing or checking the images or information obtained by (a) or (b); (d) any other systems associated with, or otherwise connected with (a), (b) or (c).
[102] Home Office, Surveillance Camera Code, op. cit., 2012.
[103] Ibid.
[104] No CCTV. http://www.no-cctv.org.uk/news.asp
[105] CCTV National Standards Forum. http://www.cnsf.co.uk/

Officers (ACPO), Public CCTV Managers Association (PCMA), the Association of Security Consultants (ASC), retail, health and educational establishments. According to its website, it "seeks to develop a set of standards, guidelines and processes built on the principles of 'best practice'" by reviewing existing guidance and procedures that focus on management, training and technical standards across both the public and private sectors and identifying a coherent and structured model, built on sound professional principles, for the deployment of CCTV systems.[106]

5.3.2.5 Need for privacy certification

There are some reservations about whether there is a need for privacy certification for CCTV systems at all.[107] This section discusses why privacy certification might be relevant for CCTV systems.

To ensure effective control of CCTV systems and reduce regulatory burden

Privacy certification might present one means of controlling CCTV systems and the organisations developing and using them, more effectively. Despite the majority of the privacy and data protection risks in relation to CCTV being generally well known and documented, concerns and challenges remain. CNIL reports that it received 363 complaints in relation to CCTV or video surveillance.[108] Privacy certification might help alleviate some of the concerns that the complaints bring up and reduce the burden on the regulators by providing data subjects with an alternative forum for complaints redress (e.g. for instance by directing these to the certification scheme operator).

To make the design and implementation of CCTV systems more transparent

Certifying CCTV systems might make their design more transparent. We could also argue that it might make the whole process of their implementation more transparent (if privacy certification can check how the system is used, how personal and sensitive personal data is shared and the impacts it has on data subjects). It could serve as an additional check to make CCTV manufacturers, installers, owners and users more attentive and responsive to privacy and data protection concerns. More vitally, privacy certification might help support regulatory and industry efforts to facilitate more responsible and societally grounded CCTV practices. Information displayed in a seal (if implemented in this manner) might help end users make an easy assessment of how their data is used, shared and secured.

To drive up and incentivise privacy and data protection standards

Privacy certification could be one way of driving up privacy and data protection standards (a view also expressed by the UK ICO). Privacy certification would not only lead to the reinforcement of existing privacy good practices and standards, it would also open up the possibility of new and improved standards. Organisations that wish to set themselves apart from their competitors could use privacy certification to their (commercial, competitive and reputational) advantage – an EU privacy certification scheme might provide them with an easy, accessible and universal means of demonstrating privacy compliance. As the UK ICO

[106] CCTV National Standards Forum. http://www.cnsf.co.uk/
[107] CNIL expressed such a reservation.
[108] CNIL, "Videosurveillance". http://www.cnil.fr/les-themes/videosurveillance/

points out, "there is also the possibility of driving up standards by creating a market for services that offer accredited CCTV systems, if those who buy the services stipulate the certification as part of the procurement".[109]

To support privacy and data protection compliance

Privacy certification of CCTV systems could help support privacy and data protection compliance. One industry expert explicitly states "even when privacy protection methods are mandated, compliance and enforcement are still open to question", and suggests that "a potential solution is certification and registration of systems…"[110] Privacy certification could help CCTV scheme owners and implementers comply with privacy and data protection requirements and ensure that their systems meet accepted standards.

To boost privacy and data protection practice visibility for subjects of CCTV surveillance

Currently, good practice dictates that the use of CCTV cameras must be communicated to the public. However, CCTV warning signs are not uniformly used or highly efficient in communicating to individuals the true nature of the surveillance (for instance the type of camera; some notably have more privacy invasive potential than others), how their images may be used or shared, for how long data may be retained, who to contact in case of concerns, and what law or Code of practice applies. Consequently, there is no quick and easy means of allaying the privacy and data protection concerns of the subjects of CCTV surveillance. CCTV privacy certification might be an easy means for CCTV manufacturers and other entities such as users to show privacy and data protection compliance. Further, it might provide affected parties with a more user-friendly complaints redress mechanism and opportunities.

While these may be relevant generally to privacy certification for CCTV, an EU privacy certification scheme is specifically relevant to help further the cause of the Internal Market. It is also relevant due to the large cross-border movement of people within the Union. It might enable individuals to know that no matter where they reside in the Union, their privacy and personal data will be adequately protected to a high standard. However, as CNIL points out, despite certification, a product or service could be misused and risks could continue; there are also the difficulties involved in subsequent monitoring (especially in the European context).

5.3.2.6 Potential barriers to certification

We can identify the following potential barriers to EU privacy certification for CCTV systems.

National considerations and distinctions in policy, regulation and implementation of CCTV

One of the biggest barriers might be that the use (and regulation) of CCTV is highly contextual and localised. As a report on *Surveillance, fighting crime and violence* suggests, *"*CCTV has diffused in different ways in different policy environments and social settings

[109] ICO, Response to CCTV privacy certification questionnaire, Study on EU Privacy Seals, 13 Nov 2013.
[110] Senior, Andrew, "Privacy protection in a Video Surveillance System", in Andrew Senior (ed.), *Protecting Privacy in Video Surveillance*, Springer, New York, 2009, p. 39.

and that those settings shape the way CCTV is configured and used. History, culture, legislative legacies, administrative rules and procedures, vested interests, all play a role in shaping the use of such technologies."[111] Thus, there are a number of factors at play in the design and implementation of CCTV systems. These present challenges to privacy certification. Many stakeholders (even in government) are highly sceptical about whether privacy certification schemes are effective at all[112] and this might pose a problem in terms of whether stakeholders see any added value from EU privacy certification for CCTV systems.

Differences in cultural attitudes and threat perceptions

Cultural attitudes to and threat perceptions in relation to CCTV systems are highly divergent across the EU. The final report of the Urbaneye project[113] suggests that "peoples' attitudes towards CCTV were shown to be contingent on local culture and personal values".[114] Some cultures might therefore perceive CCTV systems to be less privacy threatening or as a part of the necessary apparatus of social governance and control; such cultures might not see any value in privacy certification of CCTV systems or see a need to devote resources to it.

Existence of other threats in conjunction with privacy/data protection threats

CCTV systems impact other fundamental rights and civil liberties such as the freedom of expression, movement, association in addition to affecting privacy and personal data protection.[115] This will have an impact on an exclusively 'privacy and data protection approach' to CCTV certification in terms of the added value such a scheme would provide to scheme operators and subscribers However, we recognise that a reduced form of certification is better than none at all.

Resistance and mistrust of the scheme

This is one potentially serious barrier – any resistance or mistrust of the privacy certification scheme from stakeholders (e.g. government, industry, the public) would result in its low uptake, infectiveness and ultimately its failure. While this might seem to be a general barrier

[111] Wright, *Surveillance, fighting crime,* op. cit., 2012, p. 48.
[112] See Moores, Trevor, "Do Consumers Understand the Role of Privacy Seals in E-commerce?" *Communications of the ACM*, Vol. 48, No. 3, March 2005, pp. 86-91; Privacy International, "Response to the European Commission's Communication on the 'Comprehensive Approach on Personal Data Protection in the European Union", January 2011.
http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/pi_en.pdf; LaRose, Robert, and Nora Rifon, "Your privacy is Assured of Being Disturbed: Websites With and Without Privacy Seals", *New Media & Society*, Vol. 8, No. 6, 2006, pp. 1009; Gellman, Robert, "TRUSTe fails to justify its role as privacy arbiter", *Privacy Law and Policy Reporter*, Vol. 7, No. 6, December 2000.
http://www.austlii.edu.au/au/journals/PLPR/2000/53.html.
[113] This comparative research project (2001-2004) analysed the employment of CCTV in public spaces in Europe and aimed at clarifying the European state of affairs in relation to CCTV in Europe (regulation, debate, extent, legality, sophistication, acceptance), assessing how CCTV worked in different national, institutional, social and spatial contexts, and considering the political impacts of CCTV and need for its regulation. The study was undertaken in Austria, Hungary, Germany, Great Britain, Norway, and in parts in Denmark and Spain.
[114] Urbaneye, *On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts*, Final report, Office for Official Publications of the European Communities, Luxembourg, HPSE-CT-2001-00094, [p. 27].
http://cordis.europa.eu/documents/documentlibrary/100123891EN6.pdf
[115] Hier, S. and K. Walby, "Privacy Pragmatism and Streetscape Video Surveillance in Canada," *International Sociology*, Volume 26, No. 6, 2011, pp. 844–861.

to certification, it is highly relevant to the CCTV sector. Resistance to the scheme might stem from past experiences with failed schemes, inability to see or derive added value from the scheme etc. CCTV operators might not be willing to expose the architecture (which often includes the use of fake CCTV cameras) and operational details of their CCTV systems (e.g. permanence of operation etc.). Any attempts to generate transparency in this area will face this problem.

Mistrust of the scheme will develop if the scheme is non-transparent, not run by an independent, established organisation, shows potential certifier bias or has the effect of sanctioning the use of privacy-unfriendly technologies by entities with dubious credentials. A CCTV privacy certification scheme that is mistrusted or actively resisted by its target subscribers will probably fail.

Lack of added value

A privacy certification scheme for CCTV systems must add value to the current privacy and data protection framework applicable to CCTV systems. It must be of such nature that it adds something positive to other established privacy protection mechanisms and measures that apply to CCTV systems. It must bring added value in terms of efforts to comply (i.e. give subscribers a financial, competitive, market or reputational advantage). The privacy certification scheme will have to bring some added value to stakeholders at all levels.

Fast changing nature of the technology

One of the key challenges and potential barriers might be rapid changes, development and innovation in CCTV technologies. If technology changes and the EU privacy certification scheme is not designed to take this into account, it will impact the effectiveness of the scheme. As the ICO points out, these "can overtake any common technical standards, especially if certification takes a long time to be agreed, implemented and approved".[116] A flexible privacy certification approach would, therefore, be crucial.

Lack of regulatory support and a legal compulsion to certify

Lack of policy and regulatory support for an EU privacy certification scheme would hamper its development and sustained existence. Industry might not see the need to subscribe to or support an EU privacy certification scheme in addition to what already exists. The situation might be different if subscribing to the scheme was mandatory or strongly endorsed by law as a good practice compliance measure that might limit liability in cases of complaints or investigation by regulatory authorities.

Competition and conflict with other existing standards

Another important barrier to an EU privacy certification scheme for CCTV might be the existence of competing (and conflicting) standards and schemes. Some of these schemes might be well-established and have the advantage of maturity. Any new EU scheme would have to determine how it related to or the value added that it brought to existing initiatives.

[116] ICO, Response to CCTV privacy certification questionnaire, EU Study on Privacy Seals, 13 Nov 2013.

In addition CNIL suggests two other factors that might act as a barrier or affect EU privacy certification for CCTV:

- the significant number of stakeholders, and
- sufficient and efficient enforcement powers.

5.3.2.7 Scope and limitations of privacy certification

Based on the research conducted and input received from the CCTV User Group and ICO, there seems to be no merit in restricting the scope of certification too strictly. Government, public sector use of CCTV is more well-regulated and enforced than the private sector and domestic environment. CCTV often operates across these domains with public and private sector bodies operating these systems in partnership for various purposes. The scheme would also have to marry appropriately with national practices and additional requirements.[117] This is relevant as it is only extremely limited cases that CCTV may have cross-border or wider international effects; plus, as we have outlined before CCTV is largely subject to national regulation. Operators would also have to see value in having more transparent CCTV.
That said, an EU privacy certification scheme for CCTV would have to be:

- Flexible (to keep pace with evolving technologies, national attitudes to and uses of CCTV),
- Robust enough to promote consistency across the EU, and
- Subject to periodic review and updates.

What is important is that the scheme clearly specifies what it does and does not certify, particularly since CCTV systems present threats and risks beyond those related to privacy and data protection. Additionally, whatever the type of the scheme, it is essential that it clearly outlines the role of each of the stakeholders and their responsibilities.

Based on our research, there are two main options available for an EU privacy certification scheme for CCTV. These are:

- Self-certification by manufacturers, operators based on some core EU privacy, data protection criteria. Surveillance and enforcement by national regulators. Overall oversight and updates of the scheme's criteria by an EU-level body.
- A minimum privacy certification framework in agreement with international and national standardisation bodies and other stakeholders is set at EU level. National data protection authorities have the flexibility to implement privacy certification schemes as they see fit (based on the EU privacy certification framework).[118]

The self-certification option is not warranted due to the nature of the risks and challenges posed by CCTV. The harms posed by CCTV are not simply or always the result of a product rather, a result of its implementation and use. Based on our research in Task 2 (specifically in relation to the CE marking scheme), we think there is larger scope for the scheme to be

[117] ECORYS, *Security Regulation, Conformity Assessment & Certification Final Report – Volume I: Main Report*, European Commission, DG Enterprise & Industry, Brussels, October 2011, p. 19.
[118] Note, the UK ICO points out that CCTV used for law enforcement purposes is outside the scope of community law, and therefore the European Commission/EDPS may have no role in this area.

mistrusted if it is based on self-certification.[119] Therefore, the most relevant option seems to be the second. This is now further elaborated.

5.3.2.8 Target of certification

There are a number of possibilities in terms of what could be the targets of certification. These include: the CCTV technology (the camera and recording technologies, hardware, and software), the CCTV system (the network of surveillance devices), CCTV operators, system installers, entities that sell, own and/or operate the CCTV system (for example, ADT LLC, a security provider that sells video surveillance solutions has a BBB accredited seal[120] and a TRUSTe Certified Privacy Seal)[121].

There are merits and demerits of certification in relation to each of the outlined targets. It would be useful to have new and developing CCTV technologies privacy and data protection-certified before their implementation or market roll-out. This would ensure privacy and data protection risks are addressed early on; that the technology is sufficient, reliable and appropriate to its purposes and give the technology a positive boost in terms of its acceptability and market potential. While certifying at the point of manufacture (technology) might ensure privacy and personal data protection is embedded into the system at an early stage and help address some of the privacy and data protection risks, it is no guarantee that privacy and personal data will be safeguarded during its implementation or that the privacy embedded into the system is not overridden or circumvented.

Certifying CCTV operators, systems installers and integrators is beneficial as it ensures they become aware of laws, accepted standards and codes of conduct, good practices, their roles and responsibilities, incident handling procedures etc. The ICO points out that certification at this level is important as "it is the point at which the privacy risk explicitly arises".[122] CNIL too expresses that the target of certification should ideally be both the product and its use. Certifying products alone will not provide effective guarantees of data protection.

Certification requirements, practicalities and procedures would differ in relation to each of the entities. For instance, as the ICO outlines, "Certification for manufacturers could be more technical and different to the certification required for operators, which may also require auditing of policies and procedures, alongside technical aspect. It could also involve the auditing of privacy impact assessments (PIAs)".[123]

[119] Rodrigues, Rowena, David Barnard-Wills, David Wright, Luca Remotti, Tonia Damvakeraki, Paul De Hert & Vagelis Papakonstantinou, *Task 2: Comparison with other EU certification schemes, D2.4, Final report*, EU Privacy Seals Study, European Commission Joint Research Centre, Institute for Protection and Security of the Citizen, 2013.
[120] Better Business Bureau, "ADT Security Services, Inc." http://www.bbb.org/south-east-florida/business-reviews/burglar-alarms-and-monitoring-systems/adt-security-services-in-boca-raton-fl-30001337#sealclick. Note that the BBB draws attention to a government action involving ADT.
[121] See TRUSTe, "ADT LLC", 11 Jan 2013. http://privacy.truste.com/privacy-seal/ADT-LLC/validation?rid=9e4c2a3a-1a6d-4bb8-baac-d33720fdc07f
[122] ICO, Response to CCTV privacy certification questionnaire, EU Study on Privacy Seals, 13 Nov 2013.
[123] Ibid.

5.3.2.9 Beneficiaries

There are a number of stakeholders that would benefit from EU privacy certification for CCTV systems. The following table outlines the main beneficiaries and the possible benefits that might accrue to them from EU privacy certification.

Beneficiary	Benefit
CCTV system owners and operators	• Prove compliance with EU privacy and data protection law (and national law, if applicable). • Reputational and competitive benefit • Commercial benefit from increased sales.
Regulators	• Able to target their regulatory efforts in areas of higher risk. • Reduction in complaints.
Third parties (law enforcement, government agencies, public authorities)	• Know CCTV images have been collected in accordance with the law; citizens have been informed that they are being recording and why; images will be adequate for purposes etc.
Subjects of CCTV surveillance	• Improved knowledge and ability to assess CCTV surveillance. • Quick and easy assessments about privacy impact of CCTV systems. • Expedient solutions, accessible disputes redress. • Public trust and confidence.

Table 4 Beneficiaries and benefits

5.3.2.10 Harmonisation and common standards

While recognising that different laws and standards govern CCTV in the individual EU Member States, we posit that the core privacy certification criteria be based upon the provisions of the European Data Protection Directive 95/46/EC. Once the General Data Protection Regulation becomes law, its provisions would form the basis of the core criteria. This would set a common harmonised EU standard.

A central body such as the Article 29 Data Protection Working Party could provide opinions or guidance on what might constitute the core criteria and requirements for CCTV systems to be in compliance with the EU law on privacy and data protection. National regulators such as DPAs, surveillance authorities, industry and standardisation bodies could draw up additional standards to supplement the core harmonised standards.

5.3.2.11 Policy requirements

To make the EU privacy scheme to work for CCTV systems, the following policy actions would be necessary:

- Developing appropriate and consistent EU policies on CCTV and its certification while at the same time maintaining local flexibility.
- Incentivising privacy, data protection compliant organisations, products and services.

- Providing policy guidance/policy recommendations on what is and is not acceptable privacy and data protection.
- Integration of resources to operationalise the scheme
- Setting out of core scheme objectives and priorities for the scheme – e.g. to certify compliance of CCTV systems with privacy and data protection obligations and good practice etc.
- Promoting mutual recognition, if applicable.

5.3.2.12 Regulatory requirements

Currently, the core principles could be taken from the European Data Protection Directive 95/46/EC. Subsequently, we expect that the criteria would be based on the General Data Protection Regulation. However, this Regulation would only provide the broad data protection principles and criteria and it might be necessary to put in place additional regulatory measures (e.g. a Directive on privacy and data protection certification in general, or an Opinion on privacy and data protection certification for CCTV systems) if this does not adequately support the existence of a harmonised framework. The Regulation would have to specify who would oversee or guide the scheme at the EU level and how the scheme might work at the national levels.

A Regulation will mean no additional regulatory efforts are required at the Member State level. If this is not the case, additional national level regulation will be necessary to specify the privacy and data protection criteria that CCTV systems must comply with in line with national laws, guidance and good practice norms. The UK ICO particularly highlights, "for certification to be a complete success and a cornerstone of the use of CCTV, it needs to be embedded in the regulatory process either through direct legal requirement or through soft law approaches such as provisions in codes of practice".[124]

5.3.2.13 Technical requirements

The technical requirements of privacy certification depend on the type of scheme that was finalised. This section makes a few general recommendations in relation to some core aspects.

<u>Operation/administration of the scheme</u>

We propose the following scope for the proposed scheme for CCTV:

1. An EU level centralised body such as European Commission sets out the general privacy certification policy for CCTV/video surveillance (national certification schemes must not fall below the level prescribed by the centralised body but could provide additional protection).
2. National regulatory authorities such as DPAs and surveillance commissioners collaboratively finalise a privacy certification scheme as applicable to the country based on the EU privacy certification policy (and taking into account national requirements).

[124] ICO, Response to CCTV privacy certification questionnaire, EU Study on Privacy Seals, 13 Nov 2013.

3. Third parties accredited by the national regulatory authorities evaluate the targets of certification against the standards prescribed by the national data protection authorities.
4. National regulatory authorities carry out routine surveillance, deal with complaints, monitor and enforce any infringements.
5. The EU level policy is evaluated as and when necessitated by major technological or regulatory changes. However, it is best that the policy is evaluated by default every two years.

Scheme criteria and requirements

The privacy certification scheme would be based on EU privacy and data protection law at core level, taking into account national law, where relevant. The criteria must cover: basic privacy and data protection principles (i.e. fair and lawful processing, collection specification and limitation (proportionality), adequacy, accuracy, and appropriate safeguards). The criteria must also take into account: provision of information to data subject, data subjects' rights (access, rectification and notification), technical organisational measures, confidentiality and security of processing, obligation to notify supervisory authority, prior checking etc.

The EDPS Video-Surveillance Guidelines,[125] that offer practical guidance to the European Union institutions and bodies operating video surveillance[126] equipment and the other standards and good practices identified earlier in this section (such as the UK ICO's CCTV Code of Practice[127]) and otherwise (such as EuroPriSe criteria which take into account EU data protection law) could be used to build and develop a new single coherent standard for privacy certification of CCTV systems.

Conditions for award of certification

The main conditions for award of certification could be: compliance with the scheme requirements (criteria), embedding privacy and data protection risk and mitigation measures and having an adequate complaints and dispute redress system.

Certification process

We suggest that the certification process could follow the following steps:

- Application for certification (and payment of fees)
- Evaluation: verification and testing for conformance with set criteria (a comprehensive privacy impact assessment against set criteria)
- Recording of technical documentation specifying conformity.
- Awarding/rejection of certification
- Publication of results (redacted or full).
- Regular audits.

[125] EDPS, *Video surveillance Guidelines,* op. cit., 2010.
[126] Defined as "the monitoring of a specific area, event, activity, or person by means of an electronic device or system for visual monitoring" and typically representing CCTV systems.
[127] ICO, *CCTV Code of Practice*, op. cit., 2008.

In relation to CCTV, we do not see significant added value in the award of a seal; it could be argued that some form of rating might be more useful based on the nature of the privacy harms and the technological capability of the CCTV system.

Review of the scheme

There must be a review of the privacy certification scheme as a whole at the EU level (at least every two years) as and when necessitated by significant technological developments (e.g. changes to CCTV technology and emergent new harms), changes to data protection law and policy and changing societal expectations and needs. The review must also take into account problems and challenges encountered in the operation and enforcement of the scheme. For this, there has to be a means for the designated EU level body to bring together all the stakeholders of the scheme to share and learn lessons from one another.

Validity of certification

There must be specified period for which the certification will be valid. Given the nature of CCTV systems, and as an effective check, we suggest certification is valid for one year. Annual reviews and audits of CCTV systems would best ensure their continued adherence and conformity with privacy and data protection law. The scheme should specifically encourage participants to notify the certification body when there is a significant change to the certified technology or practice that adversely impacts privacy and data protection and was not within the scope of what was certified earlier. A negative incentive could be provided if participants fail to notify.

Termination and revocation of certification

The privacy certification would terminate normally at the end of validity period, or revocation or suspension of the certification.

Certification could be suspended or revoked on the grounds of non-compliance with criteria and requirements of the Scheme, non-conformance of system, wrongful or deceptive application of certification, breach of code, failure to abide by certification terms and conditions, or non-payment of fees. A continuous breach of the Scheme requirements could lead to a restriction or a prohibition from use or withdrawal from the market.

Renewal of certification

An entity could automatically apply for a renewal of certification on termination. It would however, have to inform the certifying body of any relevant technological or other changes to the system that affect its capacity to meet the certification requirements.

5.3.2.14 Market requirements

For an EU privacy certification scheme to work for CCTV systems, it would require:

- A market demand and support for good quality, privacy and data protection compliant CCTV systems.
- Procurement incentives for privacy and data protection compliant CCTV systems.

5.3.2.15 Roles and actions of stakeholders

The following table illustrates the roles and actions of the different stakeholders:[128]

Stakeholder	Action
European Commission (policy maker)/Designated centralised body	Setting and updating EU framework, minimum standards for schemes. Guidance on best practice. Consultation with international standards organisations. Funding.
National policy makers	Working with DPAs and national standards/accreditation bodies to set priorities for CCTV policy and for privacy certification.
Regulator – DPAs, surveillance commissioners	Operating, monitoring and enforcing scheme. Elaborating standards, certification process. Accrediting third party evaluators. Adjudication of scheme related complaints. Advisory services.
Manufacturers/developers of CCTV systems	Privacy by design. Meeting certification requirements. Privacy impact assessment. Mitigation of risks.
Systems integrators	Privacy by design. Privacy impact assessment. Mitigation of risks.
Systems installers	Privacy impact assessment. Mitigation of risks
Systems owners/operators/users	Procuring certified technologies. Privacy impact assessment. Risk mitigation. Regular reviews. Complaints redress.
Third party evaluators (accredited by national bodies)	Evaluation of CCTV systems. Audits, reviews.
Data Protection Officer	Privacy impact assessment. Expert advice before installation Set up policy for use/monitoring during use. Follow-up of corrective actions.
Industry associations	Guidance, best practice, vigilance
Standards organisations	Supporting, adopting or mutually recognising the EU privacy certification scheme Advisory and partnership role to ensure robustness and validity of the scheme.
Privacy organisations/media/academia	Exposing privacy and data protection threats of CCTV systems. Taking action against errant organisations.

[128] This table benefitted from input from the ICO.

	Advisory/consultative services. Educating the public.
Community	Vigilance. Rejection of non-privacy compliant systems.

Table 5 Roles and actions of CCTV stakeholders

Despite the specification of these roles and actions of the different stakeholders in such manner, these roles and actions are not isolated; rather, they involve collaboration and overlap. The different stakeholders will need to consult with each other (e.g. regulators to consult with industry to be up to date on technological developments that impact the scheme and its effectiveness).

5.3.2.16 Responsibility and oversight mechanisms

At the base level, the manufacturers or the persons directly controlling (owner or operator or body commissioning the use) the CCTV system bear responsibility for ensuring that the CCTV system is at always compliant with the certification criteria. They must be aware of their responsibilities, and be vigilant for any potential privacy or data protection risks, which must be mitigated by appropriate measures (as specified in the criteria or generally accepted as good practice). Periodic reviews of CCTV systems are highly recommended. Third party audits or random audits by data protection authorities might also have a compliance-supporting effect.

At the second level, it is the responsibility of the scheme operator (i.e. the DPA or other national body overseeing the scheme) to ensure that certification is not lightly awarded; that a CCTV system complies with all criteria before it is rewarded with certification. The scheme operator should conduct annual, targeted or random audits on certified entities, to ensure that the certified systems are not in breach of scheme requirements.

The national body is best positioned to take actions to prevent the misuse of the certification based on the law and other national considerations. The national regulators would be responsible for sanctioning infringements and bringing (if relevant) cases to the courts.

5.3.2.17 Sustainability

The EU privacy certification scheme would have to be sustainable to be successful. It would need to have some form of sustained public sponsorship (both at EU and national levels, depending on what form it finally takes). The scheme would need dedicated resources for its administration, enforcement and oversight. This would require actions to be taken at policy and regulatory levels.

In terms of funding, this would need to be sustained yet flexible enough to take into account the need to adapt or revise the scheme's criteria or requirements to address changing privacy needs and technological developments. The funding could come from various sources: government grants, evaluation and certification fees, fines etc.

The following would also boost the scheme's sustainability: wide acceptance and recognition of the scheme across the EU, mutual recognition, public-private collaborations and technical assistance, long term policy commitment and its ability to exclude competing schemes.

Whatever the type of scheme, a full scheme assessment (and a pilot) would be necessary prior to implementation and at regular intervals after implementation.

5.3.2.18 Evaluation and conclusion

CCTV systems are established yet constantly changing technologies. They present a number of privacy and data protection risks and challenges – some of which may or not be resolved by EU privacy certification. Implementing an EU privacy certification scheme for CCTV might help maintain a certain overall harmonised and consistent level and privacy, trust and transparency. It might enable manufacturers or organisations using CCTV systems to demonstrate, as the ICO points out, that they do not view privacy and data protection merely as a regulatory burden or a compliance box, but as part of their organisational governance structure. It might help improve legal certainty in relation to the fulfilment of privacy and data protection obligations and might even mean that EU privacy and data protection standards could be exported and extended more globally. But all this is highly dependent on a highly efficient and contextually flexible privacy certification system.

The difficulty for EU-wide privacy certification of CCTV, is that CCTV systems are largely subject to detailed and diversified national policy, law and practice which impacts their scope, operation and effect. This also has implications for their potential and ability to pose threats to privacy and personal data. CCTV also has impacts beyond privacy and data protection, which must be taken into account by the certification scheme (and this might present a problem in terms of what added value a 'privacy and data protection only' type of certification might offer). Further, the existence of other established measures of evaluating CCTV impacts such as privacy impact assessments also affects the added value privacy certification might bring to this area.

5.3.3 International transfers – cloud computing services

This case study benefitted from input from Daniele Catteddu, Managing Director of the Cloud Security Alliance (CSA) EMEA,[129] from Dimitra Liveri, Marnix Dekker (ENISA Cloud team), Francesco Cardarelli, attorney and IT law expert and Erich Rütsche, Manager Business Development & Relations, IBM Zurich Research Laboratory, Switzerland.

5.3.3.1 Definition and explanation of the context.

The Article 29 Working Party issued an Opinion on Cloud Computing, which also covers international transfers and extensively reviews the issues related to personal data protection and privacy.[130] It states, "Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space".[131] According to the Opinion, cloud computing can generate important economic benefits, because on-demand resources can be configured, expanded and accessed on the Internet quite easily. Cloud computing also brings security

[129] Cloud Security Alliance. https://cloudsecurityalliance.org/
[130] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 01037/12/EN WP 196, 1 July 2012.
[131] Ibid., p. 4.

benefits; enterprises, especially SMEs, may acquire, at a marginal cost, top-class technologies, which would otherwise be unaffordable for them.

The European Commission, in its Communication on 'Unleashing the Potential of Cloud Computing in Europe'[132] highlights that users can take advantage of almost unlimited computing power on demand without the need of major capital investments and can access their data from anywhere with an internet connection. According to the Commission, the defining features of cloud computing are manifold and make a general definition elusive. They include:

- hardware (computers, storage devices) owned by the cloud service provider and not by the user interacting with it via the internet;
- dynamically optimised use of hardware across a network of computers, making the information on the location of the piece of hardware or system irrelevant (and transparent) to the user. The Communication however acknowledges the potentially important bearing on the applicable legal environment;
- cloud providers often move their users' workloads around to optimise the use of available hardware, both as concerns computers or data centres;
- organisations and individuals can access their content, and use their software when and where they need it, e.g. on desktop computers, laptops, tablets and smartphones;
- the remote hardware stores and processes data and makes it available, e.g. through applications (so that a company could use its cloud-based computing in just the same way as consumers already use their webmail accounts).[133]

The Commission points out that consumers use cloud services to store information (e.g. pictures or e-mail) and use software (e.g. social networks, streamed video and music, and games). Organisations, including public administrations, use cloud services to successively replace internally run data centres and information and communication technology (ICT) departments. In that case, personal data are entrusted to cloud providers through contracts and are not anymore directly protected in the direct responsibility of the controllers.

The definition of cloud computing by the US National Institute of Standards and Technology (NIST) states

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). Cloud computing is a disruptive technology that has the potential to enhance collaboration, agility, scaling, and availability, and provides the opportunities for cost reduction through optimized and efficient computing. The cloud model envisages a world where components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down to provide an on-demand utility-like model of allocation and consumption. [134]

A fact sheet, by the Canadian Privacy Commissioner aimed at spreading awareness of cloud data protection issues, indicates that cloud computing delivers computing services over the Internet and allows individual consumers and businesses the use of hardware and software

[132] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529 final, Brussels, 27 Sept 2012.
[133] Ibid.
[134] Mell, Peter, and Tim Grance, *The NIST Definition of Cloud Computing, Version 15,* National Institute of Standards and Technology, Information Technology Laboratory, 10 July 2009. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

managed by third parties at remote locations.[135] The types of services include: online data storage, computer processing power, social networking sites, webmail, and other specialised corporate and user applications. The advantage of the cloud computing model is that it allows access to information and computer resources from anywhere through a network connection. Services include the provision of a shared set of resources.

Cloud services are available through a private cloud, community cloud, public cloud or hybrid cloud. Public cloud services are owned and operated by a cloud service provider and offered over the Internet. The target may be the general public or enterprises. A private cloud offers services only to a specific organisation. It can be operated by the organisation itself or by a third party. The services and the infrastructure can be unbundled, i.e., the service provider can deliver a set of integrated cloud services, or just provide one specific service, which the user can integrate with the cloud services of other providers. In a community cloud, the services are offered to several organisations who are part of a closed group. The infrastructure may be managed internally or outsourced. In a hybrid cloud, different combinations of services, resources and infrastructures are possible.

Service Models

The normal service models identified in cloud computing are:

- **Software as a Service (SaaS)**, which provides an off-the-shelf application with software, operating system, hardware and the network;
- **Platform as a Service (PaaS)**, provides an operating system, hardware, and network where the user/customer will install its own software and applications;
- **Infrastructure as a Service (IaaS)** merely provides hardware and networks, leaving the installation of the operating systems, software and applications to the customer.

Multi-tenancy[136]

A single cloud provider may act as a data processor for many cloud customers and, in turn, may support a very large number of cloud users. This efficient use of computing resources gives rise to many of the cost savings cloud computing can deliver. However, cloud customers may find their data being processed on the same systems as that of other cloud providers' customers.[137] Multi-tenancy implies that multiple users, businesses or individuals, from the same organisation or from different organisations, use the same services and the same computing and storage resources. One of the effects of multi-tenancy is the potential visibility of residual data or traces of operations by other users. It implies the need for policy-driven governance, service levels, segmentation and isolation and enforcement for different users. However, cloud service providers have the advantage of economies of scale, management, and operational efficiency for the multiple tenants. Multi-tenancy can also occur in the case of a single-organisation cloud-service, where a multiplicity of business units, internal services, organisational structures, employees, third party consultants and contractors.

[135] Office of the Privacy Commissioner of Canada, "Fact Sheets: Cloud Computing" October 2011. https://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_02_e.asp
[136] Mell and Grance, *The NIST Definition*, op. cit., 2009.
[137] UK Information Commissioner's Office, *Guidance on the use of cloud computing,* Version: 1.1, 2 Oct 2012. http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

Multi-tenancy poses specific challenges for the protection of personal data and is a potential aggravating factor for personal data risks. These risks (discussed in detail later) relate to the concurrent or sequential usage of the same data processing and storage resources by different users. The cloud provider must have a robust set of safeguards in place to protect against the possibility of one cloud customer gaining access to another's personal data. The cloud provider also needs to ensure that the activities of one cloud customer do not impact those of another.

International transfers

The Article 29 WP Opinion on Cloud Computing[138] emphasises that even though Articles 25 and 26 of Data Protection Directive provide for free flow of personal data to countries located outside the EEA, this is allowed only in the case the recipient or the recipient country have in place an adequate level of data protection. If this level is not granted, the controller or data processors must put in place specific safeguards. The key issue, emphasised by Article 29 WP, is that "cloud computing is most frequently based on a complete lack of any stable location of data within the cloud provider's network".[139] This location can rapidly vary over time with the consequence that cloud user normally does not know where the data are located or transferred. Thus, there are important limitations to the application of the legal instruments governing the protection of personal data transferred via the cloud to third countries outside the EU.

The Article 29 WP opinion underlines that not all possible transfers of personal are compliant with the EU personal data and privacy regulation, since adequacy findings[140], including Safe Harbor, do not cover all possible geographical locations. Transfers to organisations adhering to the principles of Safe Harbor may comply with EU law since these organisations are deemed to provide an adequate level of protection to transferred data.[141] However, the Working Party indicates that self-certification under Safe Harbor may not be deemed sufficient to guarantee the respect of the EU personal data and privacy protection regulations if there are no relevant provisions for enforcement of data protection principles. Organisations transferring data should not merely rely on the statement of the data importer claiming that it has Safe Harbor certification. The cloud client should also verify that the cloud service contracts are compliant with national requirements regarding contractual data processing.

Impact of the geographical dimension

Siani Pearson of the UK Chapter of the Cloud Security Alliance indicates that while cloud computing presents the same privacy issues as other online services, it magnifies existing concerns and creates additional ones due to the geographical dimension.[142] Pearson indicates that cloud services, which operate in multiple jurisdictions, face very different, even contradictory, regulatory approaches creating additional administrative burdens and risks, for example requiring regulatory approval for model contracts. Cloud computing also poses risks

[138] Article 29 WP, *Opinion*, op. cit., 2012.
[139] Ibid. p. 17.
[140] Adequacy findings confirm that a third country ensures an adequate level of protection for personal data by reason of its domestic law or of the international commitments it has entered into.
[141] Note, that currently, German DPAs do not recognize Safe Harbor.
[142] Pearson, Siani, "Data Protection in the Cloud" Cloud Security Alliance. https://chapters.cloudsecurityalliance.org/uk/2012/12/13/data-protection-in-the-cloud/

when the legal requirement for the level of data protection is low, or non-existent, in the country of the cloud provider. Pearson further emphasises that in Europe, data protection is almost always used in the context of privacy.[143] In other geographical areas, and jurisdictions, such as the USA, the focus is more narrowly on security. In Europe, privacy is regarded as a human right, while in the USA, it has been regarded more in terms of avoiding harm to data subjects in specific contexts, such as online contexts, where privacy is about the protection and appropriate use of the personal information of citizens, customers and employees, and meeting their expectations about its use.

The Italian Data Protection Authority issued a document with guidelines on the selection and use of cloud services.[144] It confirms that cloud technology develops at a much quicker pace than legislation. There is, as yet, no updated regulatory framework, to deal with all the innovations introduced by cloud computing, that would protect personal data and privacy. This situation will possibly change with the introduction of the General Data Protection Regulation. One of the key provisions of the Regulation is the obligation of all data controllers to notify data subjects of breaches of personal data.

The Italian DPA document advises, that until more specific domestic and international legislation is passed – that cloud service users, individuals, businesses and public administrations, take special care in assessing the risks of entrusting personal data to cloud service providers.[145] Checks should be made to ensure any personal data uploaded to the cloud is used and stored securely. Small-sized users, individuals and companies, however, may not have the contractual power to negotiate appropriate terms for the management of their cloud-based data. The document also underlines that the Italian personal data code gives the data controller specific power to check whether the data processor (here the cloud service provider) complies with the special personal data processing instructions by the data controller. In other terms, the data controller can issue special instructions concerning personal data to the cloud service provider and is empowered to check if the data processor abides by these instructions.

Concerning the specific issue of international data flows, this also very much depends on the provisions of the applicable national law. Article 25 of the Data Protection Directive states "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection". The current formulation determines, in absence of a new regulation, a country-specific regulation of the issue, and thus a potentially fragmented regulatory scenario; this has an important impact on the use of cloud services. A cloud service user will have to assess where the data they place on the cloud are transferred, processed or stored, which, given the dynamic nature of the cloud may be impossible to determine.

The document produced by the Italian DPA also indicates that the limitations to cross-border data flows also apply to "intra-group" data flows in a multinational setting, which need to be

[143] Ibid.
[144] Garante per la Protezione dei Dati Personali, *Cloud Computing. How to protect your data without falling from a cloud*, Rome, June 2012.
[145] Ibid.

assessed.[146] The Italian DPA indicates that a robust set of binding corporate rules on personal data protection will facilitate compliance with applicable rules and shall be considered in the risk assessment. The burden on the data controller using cloud services is significant, since they have the responsibility of ensuring that technical and organisational measures are in place to minimise any data risks. This concerns not only storage, but also the collection and transmission of data. It is important to emphasise that a data subject has a right to know where the data processor stores, processes and transmits the personal data. Therefore, the data processor entrusting personal data of third parties to a cloud service will have to supervise not only the service provider but also any sub-processor contracted by the service provider.

The privacy sensitivity of data in cloud computing

The privacy and data protection sensitivity of personal data processed and stored in cloud services does not change. What differs is the controls and checks on the responsibility of the data processor to ensure the protection, integrity and safeguards required by personal data protection law. The problem relates to the cloud-specific character of multi-location and continuous dynamic re-location of personal data within the cloud (with some exceptions), which in some cases may be beyond the control of the entity collecting and processing personal data in the first instance.

5.3.3.2 Risks and mitigation measures

This section draws on extensive analyses and papers by several institutions, which have examined the risks and measures in cloud computing and international transfers, for example the ENISA report on cloud computing[147] and the Article 29 Working Party Opinion on Cloud Computing.[148]

The ENISA report on cloud computing examines its benefits, discusses the different aspects related to security in cloud services, and related risks.[149] The main security risks identified include:

- Loss of governance: when using cloud services, the client necessarily hands over control to the Cloud Provider (CP) on a number security-related issues. The necessary governance might not be granted fully by the Service Level Agreements (SLAs), thus leaving a security gap.
- Lock-in: the lack of standardisation can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment. This can introduce a dependency on a particular CP for service provision.
- Isolation failure: multi-tenancy and shared resources are defining characteristics of cloud computing. There is a risk of failure of mechanisms separating storage, memory, routing and even reputation between different tenants.
- Compliance risks: previous certifications acquired by organisations may be no longer valid after migrating to the cloud.
- Management interface compromise: internet-accessible interfaces for customer management can allow access to larger sets of data and resources and cause increased risk.
- Data protection: there are several data protection risks for cloud customers and providers.

[146] Garante per la Protezione dei Dati Personali, *Cloud Computing,* op. cit., June 2012.
[147] European Network and Information Security Agency (ENISA), *Cloud Computing: Benefits, risks and recommendations for information security,* ENISA, 2009.
[148] Article 29 Working Party, op. cit., July 2012.
[149] ENISA, *Cloud computing,* op. cit., 2009.

- Insecure or incomplete data deletion, which has severe personal data protection and privacy implications.
- Malicious insider: Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers.

The ENISA report emphasises that in some cases it is possible for the cloud user to transfer risk to the cloud service provider; however, not all risks can be transferred. If a risk leads to the failure of a business, serious damage to reputation or legal implications, it is difficult for another party to compensate this damage. Cloud users can outsource responsibility, but they cannot outsource accountability.

The following table presents the cloud-related risks, effects and mitigation measures:

Risk	Effect	Mitigation measures
Loss of governance	Incapacity to control the data protection responsibilities	Specific provisions and agreements guaranteeing and precisely determining data protection responsibilities in the cloud system.
Compliance challenges	Incapacity to control the data protection responsibilities	Internal compliance assurance, external compliance certification
Loss of business reputation due to co-tenancy activities	Loss of user confidence in relation to personal data protection	Clear and unambiguous specification of data protection and related responsibilities
Cloud service termination or failure	Loss of control over data once service terminates.	Regulatory provisions on the responsibilities to data subjects and in relation to personal data in case of service termination (closure of business)
Cloud provider acquisition	Loss of control over ownership-related procedures	Internal user agreement on responsibility transfer in case of provider acquisition.
Supply chain failure	Threats to personal data integrity and security	Specific user regulation on the individual responsibilities of the "links" in the cloud chain. Specification of the overall responsibility of the main cloud service provider
Isolation failure	Threats to personal data integrity	A Privacy Impact Assessment (PIA) and implementation of a comprehensive set of technical and procedural measures applicable to the service provider and its sub-contractors.
Cloud provider malicious insider - abuse of high privilege roles	Threats to personal data integrity	Identification of threats through a PIA and implementation of technical, organisational and procedural preventative and remedial measures
Management interface compromise (manipulation, availability of infrastructure)	Threats to personal data integrity	Use of Privacy Impact Assessment results to define the specific technical countermeasures and the procedural elements to impede interface compromise.
Intercepting data in transit	Threats to personal data integrity	PIA, network data protection; use of data encryption systems

Risk	Effect	Mitigation measures
Data leakage on up/download, intra-cloud	Threats to personal data integrity	PIA, network data protection; use of data encryption systems
Insecure or ineffective deletion of data	Threats to personal data integrity	Data deletion procedures, technical solutions (and devices), attribution of data deletion process and control responsibilities.
Undertaking malicious probes or scans	Threats to personal data integrity	PIA for network and mass storage access checks. Technical and procedural protection of networks, network devices and mass storage devices.
Conflicts between customer hardening procedures and cloud environment	Threats to personal data integrity	PIA. Creation of specifications to address the PIA findings and specific procedures and standards to manage procedural interaction between customer hardening procedures and cloud environment service procedures.
Risk from changes of jurisdiction	Regulation compliance failure	Regulatory measures
Privilege escalation	Regulation compliance failure, Threats to personal data integrity.	Technical protection measures, testing, patching, encryption
Social engineering attacks (i.e., impersonation)	Regulation compliance failure, Threats to personal data integrity.	Use of relevant technical and procedural protection measures to prevent social engineering attacks.
Loss or compromise of operational logs	Regulation compliance failure, Threats to personal data integrity.	Technical and procedural protection measures to protect logs against intrusion and monitoring of the operations carried out on logs.
Loss or compromise of security logs (manipulation of forensic investigation)	Regulation compliance failure, Threats to personal data integrity	Technical and procedural protection measures to protect logs against intrusion and monitoring of the operations carried out on logs
Lost, stolen backups	Regulation compliance failure Threats to personal data integrity	Technical and procedural measures to protect the access and the operation of backups. Strict authorisation controls and procedures.
Unauthorised access to premises (including physical access to machines and other facilities)	Regulation compliance failure, Threats to personal data integrity.	Physical and logical control measures to prevent unauthorised access.
Theft of computer equipment	Regulation compliance failure, Threats to personal data integrity	Physical and logical control measures to prevent unauthorised access.

Table 6 Risks, effects and mitigation measures

ENISA's report on Cloud Computing identifies five key legal issues for cloud computing:

- data protection, (a) availability and integrity and (b) minimum standard or guarantee

- confidentiality
- intellectual property
- professional negligence
- outsourcing services and changes in control.[150]

ENISA calls for cloud computing providers to "have highly detailed and product-specific contracts and other agreements and disclosures, and for customers to carefully review these contracts or related documentation. Both parties should also pay close attention to service level agreements (SLAs)".[151] ENISA believes that many legal issues associated with cloud computing are resolved or at least mitigated by SLAs. One of the key points raised is that customers of cloud computing services vary in type (i.e., private, public entities, and individuals); and size (i.e., large corporations, public bodies. SMEs, individuals). These elements affect the contractual negotiating position of customers, which is relevant, since the relationships in cloud services have to rely on contracts and their general terms and conditions – these are often unilaterally drafted by the cloud provider and (more commonly) accepted by the customers without modification or negotiation.

Services provided by cloud service providers commonly include email, messaging, project management, business applications such as payroll, accounts and finance, customer relationship management, sales management, custom application development, custom applications, telemedicine, and customers' billing. Many of these applications are used to process personal data. This data often belongs to a number of data subjects, such as employees, clients, suppliers, patients or business partners.

The Article 29 Working Party indicates that any organisation, business or administration should undertake a comprehensive data risk analysis: [152]

- when placing the data in the cloud
- of the legal risks regarding data protection, which concern mainly security obligations and international transfers, and,
- of processing and transfer of sensitive data via cloud computing.

The Article 29 WP produced a checklist for data protection compliance by cloud clients and cloud providers based on the current legal framework, with some recommendations provided with a view to future developments in the regulatory framework:

1) Controller-processor relationship
   a) The typical relationship makes the client-provider relationship a controller-processor relationship
   b) When the provider re-processes some personal data for its own purposes, it has full (joint) responsibility for the processing and must fulfil all legal obligations (of Directives 95/46/EC and 2002/58/EC)
2) Cloud client's controller responsibility: It has to accept responsibility for abiding by data protection legislation and is subject to all the legal obligations. The client should select a cloud provider that guarantees compliance with EU data protection legislation.
3) Contracts should specify the provisions for subcontractors:
   a) sub-processors may only be commissioned on the basis of a consent

[150] ENISA, *Cloud Computing*, op. cit., 2009.
[151] Ibid, p. 97.
[152] Article 29 Working Party, Opinion, op. cit., July 2012, p. 2.

b) clear duty for the processor to inform the controller of any intended changes in subcontracting. The cloud service provider needs to name all the subcontractors commissioned
c) in case of change of subcontractors the client should have the right to object to such changes or to terminate the contract
d) the contracts between the cloud service provider and the subcontractors should reflect the stipulations of the provider-client contract
e) the client needs to have recourse possibilities in case of contractual breaches by the provider's sub-contractors.

4) Compliance with fundamental data protection principles:
   - Transparency from the cloud service provider to the customer: information about all (data protection) relevant aspects of services; subcontractors; information about technical and organisational measures implemented by the provider;
   - Transparency from the customer to their data subjects
   - Purpose specification and limitation: responsibility for data erasure
   - Data retention
   - Contractual safeguards
5) The contract with the provider (and the ones to be stipulated between provider and sub-contractors) should afford sufficient guarantees in terms of technical security and organizational measures. It should specify:
   a) the client's instructions to the provider including subject and time frame of the service
   b) objective and measurable service levels and the relevant penalties
   c) the security measures to be complied with as a function of the risks of the processing and the nature of the data
6) Access to data: only authorised persons should have access to the data
7) Confidentiality
8) Disclosure of data to third parties
9) Obligations to co-operate: provider is obliged to co-operate with regard to the client's right to monitor processing operations
10) Cross-border data transfers
11) Logging and auditing of processing
12) Technical and organisational measures: measures aimed at ensuring availability, integrity, confidentiality, isolation, intervenability and portability
13) Applicable legislation and standards.

The Article 29 Working Party presents the following list of technical and organisational principles for data protection and data security:[153]

- **Availability**: timely and reliable access to personal data. The significant innovation introduced by the opinion of WP Art 29 is that it addresses the connectivity between the client and cloud service provider[154]
- **Integrity**: the property that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission
- **Confidentiality**
- **Transparency**
- **Isolation** (purpose limitation)
- **Intervenability**: the rights of access, rectification, erasure, blocking and objection
- **Portability**: standard data formats and service interfaces facilitating interoperability and portability between different cloud providers

[153] Article 29 Working Party, Opinion, op. cit., July 2012.
[154] Ibid, p. 14.

- **Accountability**: the ability to establish what an entity did at a certain point in time in the past and how. The ability for the cloud platform to provide reliable monitoring and comprehensive logging mechanisms is of paramount importance in this regard.

Moreover, cloud providers must provide documentary evidence of appropriate and effective measures that deliver the outcomes of the data protection principles outlined in the previous sections. Procedures, to ensure the identification of all data processing operations, to respond to access requests, the allocation of resources, including the designation of data protection officers responsible for the organisation of data protection compliance, or independent certification procedures, are examples of such measures. Data controllers should ensure they are prepared to demonstrate the setting up of the necessary measures to the competent supervisory authority upon request.

5.3.3.3 Applicable legislation and standards

The Article 29 WP Opinion discusses the issue of the applicability of the Data Protection Directive depending on the location of the data subject, data processor and its subcontractor.[155] The place where the controller is established is relevant to the application of the Data Protection Directive. What is not relevant for the application of the Data Protection Directive is the place of processing of the personal data or the residence of the data subject. This means that the Directive is applicable to a processor established in the EU even if processing is done in a non-EU Member State. The Directive is applicable if the controller is not established in the EU but uses equipment located in the EU for processing of personal data.

The data controller is obliged to provide the data subjects with all the mandatory information related to the data processing. A cloud client must, under the Data Protection Directive, inform their customers about the circumstances of the transfer to the cloud provider, the quality of the cloud provider (i.e., external processor), and the purposes of the transfer.

All the parties involved in the data processing (controllers, processors and data subjects) should understand their rights and obligations relating to the processing of data as defined in the Data Protection Directive. To apply the Data Protection Directive adequately, the confidentiality, availability and integrity of data are key. The Article 29 WP in its Opinion further confirms that:

- The data controller operating in different Member States and processing personal data has to comply with the regulations of each of the States where it operates, thus creating a significant administrative burden for multi-located organisations, which have to comply with multiple regulatory settings.
- In cloud services setting:
    - The cloud client is the data controller and determines the ultimate purpose of the processing; they decide on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organisation.
    - The cloud client must accept and cannot re-distribute the responsibility for abiding by data protection legislation and maintains their responsibility for all legal duties defined in Directive 95/46/EC.

[155] Article 29 Working Party, Opinion, op. cit., July 2012, p. 7.

- Cloud providers are considered processors and have a duty to ensure confidentiality, in relation to the cloud service type (public, private, community or hybrid/IaaS, SaaS or PaaS and the type of service contracted by the client).
- Should the cloud service provider outsource part of the cloud services to subcontractors, they are obliged to notify this to the client, specifying the type of service subcontracted, the characteristics of current or potential sub-contractors and guarantees that these entities offer to the provider of cloud computing services to comply with Directive 95/46/E. All the relevant obligations of the data processing regulation therefore apply to the sub-processors through contracts between the cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider.

The Article 29 WP Opinion also outlines the contractual safeguards of the "controller-processor".[156] Data controllers who contract cloud computing services have to choose a processor who provides sufficient technical and organisational security measures to ensure the compliance with privacy and data protection regulations. The data controller needs to sign a formal contract with the cloud service provider, with a number of a minimum set of requirements, including: the obligation to follow the instructions of the controller, and the implementation of technical and organisational measures to adequately protect personal data. These include the implementation of the following measures: [157]

1. The details on the client instructions of the client to the provider, with particular regard to the applicable SLAs, which need to include objectively measurable indicators, as well as the relevant penalties of financial or other nature in case of non-compliance.
2. Specification of the security measures the cloud service provider must comply with, related to the risks embedded in the processing of personal data and their nature of data to be protected. The contract needs to specify the concrete technical and organisational measures. These are without prejudice to the application of more stringent measures, as required by the client's national regulations.
3. The indication of the subject and timeframe of the cloud service, including the assurance of the secure erasure of the data at the request of the cloud client.
4. The specification of how (personal) data will be returned or destroyed on termination of the service. It must be assured that data are securely and permanently erased at the request of the client.
5. The inclusion of a confidentiality clause binding the cloud service provider and its employees operating on the data and providing that only authorised personnel can access the data.
6. The obligation of the cloud service provider to facilitate the data subject's rights to access, correct or delete their data.
7. The prohibition to the cloud provider to communicate data to third parties, including subcontractors, even if only for preservation purposes, unless explicitly provided for in the contract.
8. The explicit indication that sub-processors may only be commissioned on the basis of consent.
9. The obligation, and responsibility of the cloud service provider to notify the client any breach, which affects the cloud client data.
10. The obligation of the cloud service provider to communicate the list of locations of the data processing.

[156] Article 29 Working Party, Opinion, op. cit., July 2012.
[157] Article 29 Working Party, Opinion, op. cit., July 2012.

11. The controller's rights to verify and monitor the cloud service provider's obligations affecting the processing of personal data.
12. The obligation of the cloud service provider to notify any changes in the cloud service setup and functions.
13. The specification of the procedures to monitor, log and audit the relevant personal data operation performed by the service provider and its subcontractors.
14. The obligation on the cloud service provider to notify the client of any legally binding request for disclosure of personal data by a law enforcement authority, unless otherwise prohibited, for example to preserve the secrecy of a law enforcement investigation.
15. A general obligation on the service provider to assure that its internal organisation, data processing arrangements, and those of the sub-processors, if any, are compliant with applicable national and international legal requirements and regulations.

If the controller infringes personal data-related rights, a data subject suffering damages has the right to compensation. Data processors, such as cloud service providers, are considered controllers and liable for any infringements they are personally involved in.

Even if the agreement between the cloud service provider and the user is based on a standard agreement, the potential imbalance in contractual power between the parties will not be considered a justification for users to accept clauses that do not comply with the applicable data protection law.

5.3.3.4 Certification-related good practices

To date, there are no formally established privacy-specific cloud certification schemes. Some privacy seal schemes such as TRUSTe offer cloud privacy certification as part of their certification services.[158]

There is, however, extensive research and discussion on how to deal with privacy and data protection in cloud computing. The ISO work on 27001 is only indirectly related to personal data protection, as it deals with overall protection of information (information security management). As of writing, the ISO/IEC DIS 27018 "Information technology -Security techniques - Code of practice for PII protection in public cloud acting as PII processors" is under development.[159]

The recommendations stemming from the Article 29 Working Party Opinion are an important contribution that must be considered in privacy certification of cloud services. The Cloud Security Alliance has issued security guidance for critical areas of focus in cloud computing.[160] As cloud computing matures, managing its opportunities and security challenges is crucial to business development. The Guidance proposes actionable, best practice based measures to enable businesses transition to cloud services while mitigating risk. The Guidance is not specifically targeted at privacy and personal data protection, but takes a comprehensive approach.

[158] TRUSTe. http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-cloud
[159] ISO. http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498
[160] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing, version 3.0,* 14 Nov 2011. https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

The CSA identifies a number of issues in relation to the cloud:[161]

- There are huge adaptation issues of cloud clients. In many cases, the lack of data protection compliance is an excuse not to adopt cloud-computing services, since now there are the conditions to clarify the issue.
- There is the issue of complex accountability chains, and the integration of contractual systems to guarantee indirect governance. It is necessary to solve the issues of the responsibility and accountability across the different links, which connect data subjects and their rights, data processors and their duties and their rights in respect to other data processors. In this respect the solution might lie in a (self-) regulatory solution of the chain of responsibility.
- There is a very positive trend towards data protection in cloud computing, and increasing maturity of the market and the users. The users have increasing control over data processes in cloud computing systems.
- The proposed GDPR addresses and solves the issue, specifying who the processor is and who the data controller, and how their roles and responsibilities are defined in the Service Level Agreements (SLAs). At present there are organisations delivering cloud services who had their Binding Corporate Rules (BCRs) certified by DPAs and there will be instruments and actions, which will be implemented by the GDPR. The current institutional action and the different initiatives have educated users to more awareness in the relationship with cloud service providers. Certification of processes is seen as a simplification, which can lead to clarity in a first assessment of basic requisites. There is an increased interest in privacy seals following EuroPriSe. The issue is reaching a critical mass. The value of certifications resides in: the credibility of the scheme's governance, the criteria and the standards underlying the certification process and the market acceptance and recognition of those targeted by the seal and by those who are supposed to adopt it.
- One essential element of a prospective privacy seal is its endorsement. A successful privacy seal requires the endorsement by the regulator. The seal needs to provide an agreed mechanism to allocate responsibility and liabilities along the service provision chain. It should build on a convergence of DPA endorsement and industry self-regulation. It also seems that DPAs in general are not inclined to endorse privacy seals. One critical step is the endorsement by the Article 29 WP and overcoming the current differences between the expectations of the WP and what industry is willing to offer.

These issues should be considered when designing a privacy certification scheme, assessing their applicability and potential impacts, also considering the broader issues beyond the personal data and privacy protection in cloud services.

One important initiative is the CSA Privacy Level Agreement (PLA), an attempt to simplify privacy compliance. [162] The PLA is based on the Consensus Assessment Initiative Questionnaire (CAIQ), matched with the CSA STAR register of security measures. The CSA suggests that DPAs support the PLA as example of good practice in certifying transparency of operations but do not consider it suitable means to ensure regulatory compliance. In any case, there is a general consensus on a minimum set of elements:

[161] Based on interview with the CSA EMEA Managing Director Daniele Catteddu.
[162] Cloud Security Alliance, "Privacy Level Agreement Working Group". https://cloudsecurityalliance.org/research/pla/

- A minimal technical framework
- Soft privacy compliance based on information
- Statement on the quality of technical measures

The Cloud Security Alliance has proposed and made available a set of minimum technical measures for personal data and privacy assurance for cloud services. The PLA has the capability of meeting the needs of the DPAs and of industry, finding a minimum common level of agreement. The CSA STAR solution is optimised and builds on ISO 27001, covering the peculiarities of the cloud model.

According to the CSA, a privacy seal cannot be a product certification, but needs to focus on process certification. A process-related privacy certification would supersede a privacy seal connected to a device. It could also incorporate some form of personal certification, considering that the data controller is aware of how the cloud system operates and can take over responsibility of its compliance. Cloud personal data and privacy security can build on a combination of the approach outlined in the Article 29 WP Opinion and of the proposed GDPR, which are capable of setting compliance levels which can work at a global level.

The areas of critical focus

The thirteen domains, which comprise the remainder of the CSA guidance, highlight areas of concern and address both the strategic and tactical security 'pain points' within a cloud environment and can be applied to any combination of cloud service and deployment model. The domains are divided into two broad categories: governance and operations. The governance domains are broad and address strategic and policy issues within a cloud computing environment, while the operational domains focus on more tactical security concerns and implementation within the architecture.

Governance Domains

- Governance and Enterprise Risk Management
- Legal Issues: Contracts and Electronic Discovery
- Compliance and Audit
- Information Management and Data Security
- Portability and Interoperability

Operational Domains

- Traditional Security, Business Continuity and Disaster Recovery
- Data Centre Operations
- Incident Response, Notification and Remediation
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization
- Security as a Service

5.3.3.5 Need for privacy certification

Even though a privacy seal is not directly mentioned, in general, cloud-related studies and commentaries make several references to certification for cloud services. . The Italian DPA indicates that "Cloud providers could also benefit in terms of opportunities from laying down privacy-friendly contractual clauses and/or relying on prior independent certification of their

compliance with EU personal data protection laws".[163] For instance, it is helpful to check that any non-EU cloud service provider has subjected its security and data processing procedures to specific information systems certification schemes such as those regulated by ISO information security standards.

The CSA guidance refers to the right to audit, which gives the customers: "the ability to audit the cloud provider, which supports traceability and transparency in the frequently evolving environments of cloud computing and regulation. Use a normative specification in the right to audit to ensure mutual understanding of expectations. In time, this right should be supplanted by third-party certifications (e.g., driven by ISO/IEC 27001/27017)".[164] It also encourages customers to "request and acquire business continuity planning and disaster recovery documentation prior to visit, including relevant certifications (e.g., based on ISO, ITIL 42 standards), and audit reports and test protocols".[165] The customer "should review the third party Business Continuity processes and any particular certification. For example, the CSP may adhere and certify against BS 25999, the British Standard for Business Continuity Management (BCM). The customer may wish to review the scope of the certification and documented details of the assessment".[166]

ENISA's report on Cloud Computing recommends that the European Commission should study and clarify, in particular:

- cloud providers' obligation to notify their customers of data security breaches;
- how the liability exemptions for intermediaries arising from the eCommerce Directive Articles 12-15 apply to cloud providers;
- how best to support the creation of minimum data protection standards and privacy certification schemes common across all the member States.[167]

ENISA's document on Critical Cloud Computing, emphasises that:

> There is a lot of information security literature about the importance of auditing and testing systems. Cloud computing providers should schedule frequent audits and tests, by internal testers and auditors, and, when relevant, by external testers and auditors. In discussions about governance, often the need for certification, by independent external auditors is stressed. But it is hard for an external auditor to assess the security of a complex and continuously changing system, by performing an audit once per year. Cloud computing providers and government authorities should have a continuous program of monitoring, audits, tests and exercises in place. Yearly audits by external parties are only a small part of such a program".[168]

ENISA indicates that such audits are often embedded in certification processes. ENISA also emphasises that ICT systems are constantly changing and that this reduces the effect of periodic (yearly) audits and that the complexity of the systems underpinning cloud-computing services makes it very difficult to assess security or resilience. It advises that cloud service providers and government authorities should ensure that there is a continuous programme of

[163] Garante per la Protezione dei Dati Personali, *Cloud Computing*, op. cit., June 2012.
[164] Cloud Security Alliance, Cloud Security Alliance, *Security Guidance*, op. cit., 2011.
[165] Ibid.
[166] Ibid.
[167] ENISA, *Cloud computing*, op. cit., 2009
[168] ENISA, *Critical Cloud Computing, A CIIP perspective on cloud computing services, Version 1.0*, ENISA, December 2012.

audits, tests and exercises, and highlights that external audits are only one part of this programme.

The most comprehensive assessment of third party data protection certifications was, undertaken by Article 29 WP.[169] It indicates that independent verification or certification by a reputable third party could be a credible means for providers to demonstrate their compliance with obligations concerning security in general and data protection in particular. The Article 29 WP indicates the minimum requirements for certification should indicate that data protection controls have been subject to audit or review against a recognised standard meeting the requirements. Potential customers should see if cloud services providers could provide a copy of this third party audit certificate or a copy of the audit report verifying the certification including with respect to the requirements set out in this Opinion. The Opinion, also states:

- Individual audits of data hosted in a multi-party, virtualised server environment may be impractical technically and can in some instances serve to increase risks to those physical and logical network security controls in place. In such cases, a relevant third party audit chosen by the controller may be deemed to satisfy in lieu of an individual controller's right to audit.
- The adoption of privacy-specific standards and certifications is central to the establishment of a trustworthy relationship between cloud providers, controllers and data subjects.
- These standards and certifications should address technical measures (such as localisation of data or encryption) as well as processes within cloud providers' organisation that guarantee data protection (such as access control policies, access control or backups).

In the context of the general policy debate in the EU on cloud computing, on 27 September 2012, the European Commission issued a Communication on "Unleashing the potential of Cloud Computing in Europe", which highlights the key actions of the European strategy on cloud:

- Cutting through the jungle of technical standards so that cloud users get interoperability, data portability and reversibility; necessary standards should be identified by 2013,
- Support for EU-wide certification schemes for trustworthy cloud providers,
- Development of model 'safe and fair' contract terms for cloud computing contracts including Service Level Agreements,
- A European Cloud Partnership with Member States and industry to harness the public sector's buying power (20% of all IT spending) to shape the European cloud market, boost the chances for European cloud providers to grow to achieve a competitive scale, and deliver cheaper and better eGovernment (Press Release, Digital Agenda: New strategy to drive European business and government productivity via cloud computing.

The European Data Protection Supervisor (EDPS), in its Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", issued on 16 November 2012, supports the effort of the Commission to propose a set of standard contractual terms for the provision of cloud computing services that respect data protection requirements.[170] The EDPS underlines that to protect personal data on cloud computing systems, and states it is essential: to agree on model contractual terms and conditions to be included in the cloud computing service offerings; to develop common procurement terms and requirements for the use of the cloud by the public sector, particularly taking account of

[169] Article 29 Working Party, op. cit., July 2012.

[170] EDPS, Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe, Brussels, 16 Nov 2012. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

the sensitivity of data processed; to identify a cross-border approach to international data transfers in the cloud, in particular through standard contractual clauses and developing specific clauses for the transfer from EU processors to processors outside the EU; to apply the principles of privacy by design in the development of technology and of standards; to integrate the principles of personal data protection principles of processing purpose limitations, usage limitations and storage limitations; and enforce the obligation of transparency of personal data processing, based on the complete communication from the cloud service provider to the client and data processor.[171]

The rationale for privacy certification

There are a number of reasons why certification could facilitate the personal data and privacy protection in cloud computing and international transfers. For instance:

1) To facilitate some form of control by data subjects and data processors on data transfers and processing in distributed, multi-located cloud environments...
2) To make the complex and distributed nature of cloud computing systems transparent to users in terms of processes and procedures, clarifying the different elements of the responsibility chain in a cloud computing context, and understanding liability and accountability issues.
3) To provide an independent, and possibly institutionally endorsed certification of cloud operations in relation to personal data and privacy.
4) To drive up and incentivise privacy and data protection standards.
5) To support privacy and data protection compliance.

5.3.3.6 Potential barriers to certification

There are a number of potential barriers to certification in a global context, considering the diffused and distributed nature of cloud computing and the relevance of privacy related issues. From the perspective of data subjects, the absence of a global, formally shared regulation on cloud computing and personal data security might create gaps and uncertainties, creating weak spots in the systems, which can be disrupting to user trust and also to the certainty of compliance with personal data and privacy regulations.

On the other hand, from the perspective of data processors and data controllers a lack of harmonisation of national regulations might also be a potential barriers. The Article 29 WP Opinion emphasises the obligation to abide by the data protection regulation of each and every EU Member State where the data processor processes or transfers data. This might be a serious hampering factor for cloud certification.

The achievement of a common agreed position of national DPAs on an EU privacy certification scheme would eliminate a significant barrier to a general certification, even beyond certification of cloud services.

The consensus between DPAs, European and global stakeholders and industry on the scope of privacy and personal data certification taking into account not only transparency elements but also other regulatory aspects would eliminate an important barrier to the implementation of an EU privacy certification scheme. Further, if the scheme is not embedded in the institutional

[171] Ibid.

setting of privacy governance in Europe and in the industry governance of cloud computing systems this might hamper its effectiveness.

Lastly, setting up a privacy certification scheme requires significant investment from government and industry to effectively deal with the specific and large scale issues related to cloud services and their scope. Only a concerted effort will help eliminate this obstacle implementing it.

5.3.3.7 Scope and limitations of privacy certification

The various cloud computing initiatives and activities (such as that of the CSA, the EDPS, the Article 29 WP, and national DPAs) show that it is also the responsibility of the data processor to contribute to guaranteeing compliance with regulations. At present, there is no way of using certification as a means to transfer responsibilities from one link of the chain to the other in the cloud computing system. We deduce the following basic principles of a certification in cloud computing:

- Institutional endorsement
- Agreement between regulating institutions and the industry
- A focus on processes and not on products
- Trust in the setup of the certification and in the management of the certification, allowing for no gaps in application or transparency
- Cross-border validity and acceptance.

5.3.3.8 Target of certification

The target of certification should be the specific cloud computing system as a whole, and include: its locations, its processes, the involved processors, the hardware and software systems and the places of operations. Cloud computing certification could be based on a traditional certification hierarchy, as established for most certification schemes, including:

- A shared certification process and elements agreed among all the players and institutionally endorsed,
- A certification hierarchy
- Common recognition rules agreed between all the players
- A management system
- Agreed shared operations
- Procedural elements such as audit, expiry, revocation.

It would be useful to base the initial assessment of the first data controller on a PIA-based verification of personal data and privacy issues.

5.3.3.9 Beneficiaries

There following table lists the beneficiaries and benefits of cloud privacy certification.

Beneficiary	Benefit
Cloud computing system providers	• Prove/demonstrate their compliance with EU and national privacy and data protection law. • Reputational and competitive and benefit.

	• Commercial benefit from increased sales. • Reduction of the administrative burden (which occurs due to the need of compliance of operations with different national regulations) and thus avoiding duplication.
Regulators	• Co-operation with industry for a better understanding of the cloud-related privacy and data protection issues. • Agreement with industry on common sets of rules. • Improved targeting of regulatory efforts and risk countermeasures. • Better management of data protection
Data subjects	• Better control over personal data and the processes. • Improved knowledge of personal data processing procedures and of sub-processors.
Cloud clients	• Improved knowledge and control over data processes of personal data collected. • Improved control over the personal data processing chain and the sub-processors.
Service provider associations	• Improved coordination and action from industry side. • Increased negotiation possibility and better integration of institutional, regulatory and operational/technical requirements.

Table 7 Beneficiaries and benefits

5.3.3.10 Harmonisation and common standards

The Article 29 Working Party confirms that, at present, all national regulations on personal data protection would be applicable where the personal data processing is carried out. The current European Data Protection Directive 95/46/EC provisions are also applicable. There are currently standards in development, such as those by the CSA, and ISO standards such as the ISO 27018 but these are not integrated in a wider, EU, and possibly, global regulatory framework

There is also a wide-ranging work concerning risk assessment, technical guidelines and practices. Industry associations, regulators at European and national level are engaged various research and consultative efforts targeted at supporting the protection of personal data in cloud computing systems.

5.3.3.11 Policy requirements

An operational EU privacy certification scheme for cloud services requires:

- An institutional setting, identification of stakeholders, collaborators, the coordination role and an institutional endorsement;

- Communication and information dissemination;
- Creation of a combined industry, regulators and users group (a user platform, possibly) to agree on the different types of requirements and actions;
- Creation of a set of personal data and privacy requirements, derived from the applicable law and their translation into certification criteria and a certification process;
- Definition of an action plan for the implementation of the scheme, identifying players, roles and resources;
- Definition of the target of the scheme, the approach and the benefits, together with the principles of the certification process; and
- Promotion of global applicability and mutual recognition, where applicable.

5.3.3.12 Regulatory requirements

The proper operation of a privacy and data protection scheme for cloud computing services would require overarching and harmonised privacy and data protection regulations applicable to all EU Member States and the main EU partner countries.

5.3.3.13 Technical requirements

The technical requirements of the scheme could follow the recommendations issued so far by institutions, regulators and industry associations. We briefly outline the key elements:

1. Setup of the scheme
    a. Operating principles: objectives, target, compliance approach, beneficiaries, target benefits
    b. Certification criteria: technical, procedural and other.
    c. Certification process: steps of certification, documentary audit, process audit, technical audit, periodic audit.
2. Operation and administration of the scheme
    a. Institutional coverage
    b. Management and operation structure
    c. External audit
3. Review of the scheme
    a. Process
    b. Responsibilities
4. Requirements of the scheme
    a. Formal requirements
    b. Self-certifications
    c. Technical requirements
    d. Audit requirements
5. Certification process
    a. Application
    b. Certification plan
    c. Implementation
    d. Certification costs
    e. Award of certification
6. Validity of the scheme
    a. Duration
    b. Periodical audits

7. Revocation and expiry
    a. Checks and revocation process
    b. Revocation communication
    c. Rejection of revocation
    d. Escalation and appeal
    e. Final decision
8. Renewal of certification

5.3.3.14 Market requirements

An EU privacy and personal data certification scheme needs to assure a certain critical mass aimed at:

- The operational strength of the scheme and its "enabling power" to facilitate the diffusion and effectiveness of the scheme
- Enabling adequate cost coverage.

The market size can be estimated carefully in cooperation with industry bodies and by undertaking a market survey to gather information on the cloud service user market. The market survey should also investigate the propensity to pay for privacy certification by cloud service users.

5.3.3.15 Roles and actions of stakeholders

The following table outlines the roles and actions of the different stakeholders:

Stakeholder	Action
The European Parliament and the Council	Policy support for cloud privacy and data protection certification.
European Commission	Setting and updating the certification framework, minimum standards for schemes. Guidance on best practice. Funding. Possible operation (directly or through an agency).
National regulators and policy makers	Data protection regulation, relevant policy making, including sharing setup and management and oversight of schemes.
National data protection authorities	Development and endorsement of the scheme. Regulatory and operational support to cloud privacy certification. Agreement on common rules. Transparency and compliance endorsement.
Data subjects entrusting personal data to cloud services	Assertion of rights. Vigilance.
Industry associations	Guidance, best practice, vigilance, institutional cooperation.
Cloud service providers	Participation in the scheme.

	Procuring technologies that embed privacy, data protection safeguards as prescribed in scheme requirements and applicable law. Privacy (data protection) Impact Assessment. Mitigation of risks. Regular reviews. Redress of complaints. Development of appropriate SLAs, BCRs and SCCs.
Cloud service technology providers (subcontractors)	Compliance with scheme criteria and requirements Compliance with other obligations, and good practice
Data protection officer of the cloud user	Ensuring internal compliance and meeting of scheme-related obligations. Privacy (data protection) Impact Assessment. Monitoring and review of risks and use of mitigation measures. Expert advice
Standards organisations	Development of standards (particularly specifying technical elements) usable in cloud privacy certification schemes. Advisory and partnership role to ensure robustness and validity of the scheme.
Privacy organisations/media/academia	Overall analysis of developments. Assessment and monitoring. Research into technologies, processes, rules and practices. Raising public awareness of the scheme.

Table 8 Stakeholder roles and actions

5.3.3.16 Responsibility and oversight mechanisms

At the primary level, the user collecting the data and entrusting it to the cloud service is responsible and needs ensure full compliance with the legal requirements at EU level and at the level of each country where the processor operates. The cloud service provider must be aware of its responsibilities and be vigilant for any potential privacy or data protection risks, which must be mitigated by appropriate measures (as specified in the criteria or generally accepted as good practice). The cloud user needs to be aware of:

- The various risks
- The processing sequences
- All the transfers which will be performed, where, the regulations applicable, and
- All the measures to protect the rights of the data subject, for which the cloud user is responsible.

The often limited contractual power of the cloud user is, at present, no dispensation for the overall responsibility (as a controller). The cloud user needs to assess whether a privacy impact assessment might be required and must be aware of all the possible risks personal data face in the cloud. The cloud user must be aware of its responsibilities at all times, and be

vigilant for any potential privacy or data protection risks. It is responsible for all the contractual relationships with the cloud provider.

At the second level, the operator of the privacy certification scheme (i.e. national body, or EU body or agency overseeing the scheme) is responsible for ensuring that certification is based on a sound set of certification criteria and a certification process, which are consistently and rigorously applied, and that a cloud service and its systems comply with all criteria before it is rewarded with certification. The scheme operator is responsible for ensuring, that annual, targeted or random audits are conducted on certified entities, and that the certified systems are not in breach of the scheme requirements. The complexity of this oversight function is related to the structurally global nature of cloud services and international transfers of data. The role of the scheme operator is therefore complex, and underscores different levels: a national level and a supranational level, providing the necessary hierarchical structure to ensure that the scheme is applied consistently on a cross-border basis. The oversight could be entrusted to data protection authorities or similar agencies at national levels, and to the European Data Protection Board (proposed in the GDPR) at the EU level. If the scheme needs to operate at global level, the oversight and governance will become even more complex, requiring a number of multilateral agreements with non-EU countries. The scheme operation requires the precise assignment of responsibilities in operating the scheme, and its enforcement and sanctioning functions.

5.3.3.17 Sustainability

The EU cloud privacy certification scheme would have to be sustainable to be successful. It would need to have some form of sustained public sponsorship (both at EU and national levels, depending on its final form), and institutional endorsement. One of the aspects of sustainability is economic sustainability. This covers:

- The institutional costs of setting up the scheme
- The set-up of the scheme
- The operation of the scheme.

The size of the scheme, in terms of the number of subscribers, is a key to sustainability. Also relevant are: wide acceptance and recognition of the scheme across the EU (and beyond), mutual recognition, public-private collaborations and technical assistance, and long term policy commitment. Whatever the type of scheme or certification, a full cost-benefit analysis would be necessary to better assess and guide the implementation.

5.3.3.18 Evaluation and conclusion

A privacy seal, though complex, might solve some difficulties in managing personal data in the cloud environment.

The preliminary conclusions of the Article 29 WP recommendation provide a very interesting basis for safeguards and solutions.[172] The Opinion provides a sound basis for securing the processing of personal data that European Economic Area-based clients submit to cloud providers. The Article 29 WP also highlights some issues to ensure that cloud service providers enhance safeguards, and to assist the cloud industry adopt actions and mechanisms that foster respect for the fundamental rights to privacy and data protection.

[172] Article 29 WP, Opinion, op. cit., July 2012.

We have highlighted various aspects that an EU cloud privacy certification scheme will have to take into consideration. If the scheme is implemented, it needs to be flexible and elaborate enough to take account of the complexity of cloud systems, to cater for the regulatory requirements and to evolve with changes in technology. One difficulty is the intrinsically international character of cloud computing, the uncertainty of its configuration, which is part of its operational and technological strengths. This will not only affect but must also be taken into account in the implementation of any EU-wide cloud privacy certification scheme.

5.3.4 Smart metering systems

This case study was developed in consultation with The European Smart Metering Industry Group (ESMIG), The Future of Privacy Forum and members of the Smart Grid Task Force of the European Commission's Directorate-General for Energy.

5.3.4.1 Definition and explanation of the context

Smart meters are digital versions of traditional mechanical utility meters that include a two-way communication capacity. They are currently most commonly used for electricity metering, but the principles can be applied to other utilities. These meters can transmit information directly from the metered property to the utility company, potentially in near-real time and with a much higher granularity of data (a traditional meter records the amount of electricity or gas used over a time period, and can potentially distinguish between peak and off-peak hours based on a clock). Often, the various smart meters in a neighbourhood form a mesh wireless network with a single collection point, which connects to the operating company over a phone line or the Internet.[173] Smart meters are a component of the Smart Grid, a modernisation of electrical infrastructure, with the intended effects of being more responsive to and better able to manage energy demands, and better able to integrate multiple sources of energy. Smart meters are typically the property of the distribution company, not the recipient householder or business. Distribution companies may be different to the electricity retailer, who bills the recipient.

Smart meters increase the amount of data available on energy consumption in a more granular form. This provides opportunities for managing demand, reducing energy use, and lowering customer bills. However, it also potentially reveals patterns of behaviour within the private space of the home. Collection of smart meter data raises surveillance possibilities with potential impacts on physical safety, reputation and financial status.[174] There is a broad consensus that personal information could be determined from the meter data using relatively unsophisticated hardware and software algorithms. Current smart meters do not typically record the type of appliance being used at a given time; however, this may be statistically discernible from the particular energy use profiles of particular devices (for example, an electric heater uses much more electricity than many other household devices, so could be determined by large spikes in energy use, a refrigerator tends to use power in regular cycles to maintain a constant temperature). The technique of Nonintrusive Appliance Load Monitoring

[173] McDaniel, P., and S. McLaughlin, "Security and Privacy challenges in the smart grid", *Security and Privacy, IEEE*, Vol. 7, No. 3, 1 May 2009.
[174] Ponemon Institute, *Perceptions about Privacy on the Smart Grid*, Nov 2010, p. 1

(NALM) can identify individual appliances by comparison with a library of known patterns.[175]

The potential benefits for consumers from smart meters include detailed feedback on energy use, potential tips for saving energy, and identification of high-usage or even faulty equipment. The first benefit can be realised by the householders themselves through their own energy meter. Users will be able to understand their household or business uses energy, compare this with others, program devices to operate at times of low energy demand, control their expenditure on energy, and take advantage of energy saving plans from their suppliers. Smart devices linked to the smart grid could allow customers to make decisions about heating or other energy use, based upon real-time prices. Smart appliances could be programmed to operate when energy is cheaper (for example, a dishwasher may run during the middle of the night) or alter their manner of operation (a thermostat may decrease the heating by a few degrees when there is peak demand for electricity). Smart metering should also facilitate sources of energy that feed back into the grid (for example domestic solar panels).

The benefits for the electricity retailers and distributors are significant and include more accurate billing (including tiered time of use pricing), managing credit risks, detecting and managing energy theft, and the potential to better manage electricity demand loads across the network. There are also labour cost savings associated with the end of manual meter-reading. Energy supply companies will be able to use the data produced for various research purposes, including testing the efficacy of various demand-reduction initiatives.[176] Depending upon the particular market, the price of wholesale electricity can vary by the hour, half-hour or quarter hour. Retailers would therefore seek to expose customers to more of this variability in order to encourage demand-reducing behaviour (for example more selectivity about when to run particular appliances).[177] The ability to remotely shift customers to pre-payment plans in case of default and the ease of changing account holders offers operational cost savings to utility companies.

The roll out of smart grids is a priority for the European Union. Directive 2009/72/EC provides the common rules for the internal market in electricity.[178] According to it, Member States must conduct an economic assessment of long term costs and benefits of smart metering, and determine which form of intelligent metering is economically reasonable in their country by September 2013. The desired outcome is that 80% of consumers will have smart metering systems in place by 2020. The stated intention is to encourage the active participation of consumers in the energy supply market.

There has been some exploration of certification options in relation to the smart grid in the private sector PrivacySmart, also known as the Smart Grid Privacy Seal, is a for-profit Smart

[175] Samani, Raj, "Addressing security and privacy issues with smart meters", *Grid Insights*, 11 Dec 2012. http://gridinsights.energycentral.com/detail.cfm/detail.cfm/Addressing-security-and-privacy-issues-with-smart-meters?id=71

[176] Lisovich, Michael, A., Stephen B. Wicker, "Privacy concerns in upcoming residential and commercial demand-response systems", *IEEE Proceedings on Power Systems,* Vol.1, No.1, March 2008.

[177] Anderson, Ross and Shailendra Fuloria, "Who controls the off switch?" http://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf

[178] European Parliament and the Council, Directive 2009/72/EC of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, *OJ L* 211/55, 14 Aug 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:0093:EN:PDF

Grid certification scheme operated by TRUSTe in the United States.[179] The scheme focuses relatively narrowly upon third party companies providing services to customers that rely on energy data. It does not attempt to certify the information handling practices of the utility providers themselves, but rather to provide consumers and utilities with additional information on companies emerging to make use of this data. Consumers may wish to share energy consumption data (or some sub-set of information derived from it) with third parties in exchange for a service, and a certification scheme provides some standards for these companies. The rationale for this was that utility companies considered their activities strongly regulated by their relevant sector regulators (at state and federal levels) to the extent that they would not benefit from any additional certification scheme.[180] The scheme has relatively small numbers of participants.

5.3.4.2 Risks and mitigation measures

Privacy and data protection concerns arise from the recording of near-real time data on energy use, transmission of this data to a smart grid through a range of communications technologies, and the ability of the meter to receive communications from the grid, including the potential for remotely issued commands that could alter a consumers energy use.[181] Other than individual householder awareness of their energy use, the potential gains from smart metering (in terms of potential better management of energy use, increasing energy supply resilience) all require the use and transmission of some of the data generated by the meters to various parties outside the household (in some form). For example, the data could provide the capacity to identify and respond to major sources of waste.[182]

Data from smart meters could indicate a household's pattern of living and what people do within their own home, by measuring energy usage in detail over time. For example, this data may reveal the number of occupants in a home (or changes in this number), occupancy and behaviour patterns (such as sleeping times, or time spent outside the house), the presence of alarm systems, expensive electronics, computer hardware such as web servers or particular types of medical equipment. If electric vehicles are also charged through smart meters, then information could be derived about movement habits as well. This data is however limited. The activation of a particular appliance could not be attributed to a particular individual in a multiple-occupancy residence, and the behaviour of somebody who does not interact with metered appliances would also be invisible.

Privacy Risk	Details	Mitigation measures
Compulsory use	Smart meter installation may be mandatory in some countries raising issues of data processed without consent.	Opt-in policies. Minimisation of data collected.
Unauthorised access	Broadly overlaps with security issues. Inadequate information and cyber security measures	Secure transmission of data, including encryption; Tamper-proofing of electricity meters,

[179] PrivacySmart was included in the comparative analysis of privacy seal schemes in Deliverable 1.4 of this study.
[180] Interview with Jules Polonetsky, Future of Privacy Forum, 14 Nov 2013.
[181] Murrill, Brandon, J., Edward C. Liu and Richard M. Thompson II, *Smart Meter Data: Privacy and Security*, Congressional Research Service, 3 Feb 2012.
[182] Fitzgerald, Michael, "Finding and fixing a Home's Power Hogs", *The New York Times*, 27 July 2008. http://www.nytimes.com/2008/07/27/technology/27proto.html

	allow usage data to be intercepted by unauthorised third parties. Researchers have discovered security flaws in smart meters that allow energy consumption data to be accessed by unauthorised third parties, this included missing security features that the manufacturer had stated were implemented.[183]	with tampering detected by the distributor; Security measures on web portals for customer; Password protections on smart meters; Paired meters and displays[184]; Controlled access, limited authorised members of staff; Deletion of records with a short time-frame; Security risk assessments.
Disclosure to third parties (including to government)	Intentional disclosure of customer energy use data to third parties. May be legally mandated or a business decision on the part of the data controller. The number of third parties involved in the processing of personal data may also increase with the smart grid.	Privacy policies; De-identification; Deletion of records with a specified time-frame, when storage is no longer necessary for the stated purposes.
Unintentional disclosure to third parties	Loss of privacy, personal data breach.	Secure transmission of data, including encryption; Tamper-proofing of electricity meters, with tampering detected by the distributor; Security measures on web portals for customer; Paired meters and displays; Controlled access, limited authorised members of staff; Deletion of records with a short time-frame; Security risk assessments.
Errors and inaccurate information	Inaccurate information may be recorded leading to inappropriate billing or decision making.	Error-checking, technical standards, data-subject access
Social sorting and categorisation,	Data from energy use could be used to discriminate between customers, place them into different categories for the purposes of automated decision making. This process may be relatively opaque to the data subject.	Privacy policies, Targeted data collection and retention; De-identification and anonymisation[185]; Deletion of records with a short time-frame.

[183] Carlucclo, Dario. http://events.ccc.de/congress/2011/Fahrplan/events/4754.en.html
[184] Smartmeters, "Smart Meter Privacy and Security", 30 Sept 2013. http://www.smartmeters.vic.gov.au/privacy
[185] De-identification is the removal of personal identifiers (such as names) from data, making it more difficult to link an individual to their data. Anonymisation is the permanent removal of the link between an individual and their data so that the individual cannot be re-identified. Simple methods of anonymisation are challenged by the combination of distinct databases and in practice it is often possible to de-anonymise data sets. Anonymisation is likely to be used for any secondary use of personal data. However this may be problematic, as even anonymised data may raise privacy issues

Aggressively-tiered pricing	Customers may be pressured into paying more for their energy use if they cannot be flexible or respond to price changes/demand balancing	Opt-in policies, customer protection legislation
Personal information used for unwanted marketing	Energy usage data may be used to inform targeted marketing. For example, a suggestion that it is time to replace an inefficient or faulty electrical appliance.	Privacy policies; De-identification, Deletion of records with a short time-frame.
Public revelation of energy use without the users' consent	Some energy reduction schemes suggest comparison between neighbour's energy usage. Energy use data of celebrities or politicians may be considered newsworthy.	Privacy policies; De-identification; Opt-in policies; Deletion of records with a short time-frame.
Inadequate protection of personal information by the utility company	If the utility companies (or other data processors in the smart grid) do not sufficiently protect the personal information that it collects and processes, then this information becomes vulnerable to third party capture and abuse, or public revelation.	Secure transmission of data, including encryption; Security measures on web portals for customer; Password protections on smart meters; Controlled access, limited authorised members of staff; Security risk assessments.
Automated decision-making	Smart meters may be programmed to make automated decisions.	Privacy policies.
Installation without consent/awareness	Smart meters may be mandatory in some jurisdictions, or installed by utility companies without the full understanding of the implications on the part of the customer. Once smart meters are installed, it is highly likely that their software will be upgraded or altered over time, and that this will be possible remotely.	Privacy policies; Opt-in policies.
Interception of wireless communications	Smart meters are likely to use wireless rather than wired communication due to the reduced cost and increase ease of installation.	Encrypted communications; Security risk assessments
Data-mining of information from smart meters in ways that are not currently anticipated	This includes combing energy-use data with new sources of data, or using currently non-existing analysis methods.	Privacy policies, Targeted data collection and retention; Opt-in policies.
Combination of various smart metered utilities	Combination of usage data from electricity, gas, water, and other utilities will provide detailed behavioural information, especially if combined together.	Privacy policies
Combination of smart meter energy use data without other	Utility companies have other significant types of personal	Privacy policies; De-identification; Aggregation;

sources	information (billing information, address).	Opt-in policies.
Fraudulent attribution of energy consumption to other meters	Given the cost of utility bills fraudster may attempt to attribute their own energy consumption to other compromised smart meters.	Secure transmission of data, including encryption; Tamper-proofing of electricity meters, with tampering detected by the distributor.
Injection of false data	If the security of smart meters is compromised, it may be possible to inject false data into the system and provide false patterns of energy use.	Secure transmission of data, including encryption; Tamper-proofing of electricity meters, with tampering detected by the distributor; Security risk assessments.
Real-time remote surveillance of activity	As distinct from inferring behaviour patterns over time, real-time smart meter data would provide information on activities within a building, including the presence or absence of occupants.	Targeted data collection and retention; Security measures on web portals for customers; Controlled access, limited access to authorised members of staff.
Linkage between individuals caused by roaming or portable smart grid appliances	Electrical vehicles or portable devices with recognisable signatures that are used in multiple locations could allow data processors to develop images of the linkages between individuals.	Privacy policies; Opt-in policies.
Altering the software on the smart meters by exploiting the update capacity of the smart meter.	Smart meters might have a remote update capacity to change their software. Hackers could exploit this to compromise the meters and potentially gain access to energy usage data.	Secure transmission of data, including encryption; Password protections on smart meters; Security risk assessments.
Internal privacy within households	Less frequently discussed but still significant. For example, a member of the household or a landlord might be able to check on the behaviour and activities of other members of the household.[186]	The aggregation of energy usage across households could potentially prevent this, but then loses the benefits of understanding household energy use. Access restriction (passwords, for example) would not prevent this, as much as delimit the direction of this potential for internal surveillance, from account holder to other members. Denying detailed information on energy consumption to the household reduces some of the claimed benefits to utility customers.

[186] McKenna, Eoghan, Ian Richardson and Murray Thomson, "Smart meter data: Balancing consumer privacy concerns with legitimate applications", *Energy Policy*, Vol. 1, 1 Feb 2012. pp. 807-814.

Table 9 Risks and mitigation measures

Various privacy enhancing technologies (PETs) have been proposed by researchers to reduce the privacy risks from smart meters whilst still making use of their benefits – including measures to mix power use and add battery power to confuse or misdirect appliance load signature analysis[187] and to allow users to calculate their energy usage, and prove it has been done, without revealing fine-grained usage data.[188] For example, billing data might be provided to the smart meter from the energy supplier, combined with the fine-grained usage data from the house in situ producing detailed cost information, without being transmitted externally, with only the resulting billing information provided to the utility company, along with a zero-knowledge proof that the calculation has been conducted correctly.[189]

Solutions to the privacy and data protection problem ultimately lie with policy rather than privacy enhancing technology. This is based upon the relative ease of determining activity from energy use data, and that these techniques are robust and resilient in the face of limited or distorted data. For example, presence within a building, and sleep/wake cycles can be estimated with high levels of confidence even from low resolution data, and non-invasive appliance load-measuring methodologies are likely to become more sophisticated over time. Techniques such as lowering the resolution of the data may represent a useful component of a policy response (suggesting that a consumer may wish to grant third parties access to usage data at a lower level of resolution that they themselves have access to).[190]

The Privacy Commissioner of Ontario published a guide to embedding privacy by design into smart grids with the Future for Privacy Forum.[191] This guide suggests that the moment during the initial roll-out of smart metering systems is the appropriate time to build privacy protection measures into the systems. The guide recommends:

- Minimal amount of information should be provided to third parties,
- Pseudonomysing identity where possible,
- Third parties should not request information from the utility about a consumer. Customers should retain control over the type of information disclosed by the utility,
- Secure communication channels for the various forms of data transmission,
- Third parties should not correlate data with data obtained from other sources without the consent of the individual.[192]

Related risks from smart metering also include cyber security threats. These may include a variety of forms of exploitation, jamming, spoofing, interference, and modification of data;[193]

---

[187] Kalogridis, G., C. Efthymiou, S.Z. Denic, T.A. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards undetectable load signatures", First IEEE International Conference on Smart Grid Communications, Gathersburg, 2010.

[188] Rial, Alfredo, and George Danezis, "Privacy-Preserving smart metering", *WPES 11 Proceedings of the 10th Annual ACM workshop on Privacy in the Electronic Society*, ACM, New York, 2011.

[189] Jaruwek Marek, Martin John, and Florian Kerschbaum, "Plug in Privacy for Smart Metering Billing" in S. Fischer-Hübner and N. Hopper (eds.), *Privacy Enhancing Technologies: 11th International Symposium*, 2011. http://link.springer.com/chapter/10.1007/978-3-642-22263-4_11#page-2

[190] Lisovitch et al, op. cit., 2008.

[191] Information and Privacy Commissioner, Ontario, Canada and Future of Privacy Forum, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, November 2009. http://www.ipc.on.ca/images/Resources/pbd-smartpriv-smartgrid.pdf

[192] Ibid.

[193] Foley, Mark F., "Data Privacy and Security Issues for Advanced Metering Systems (Part 2)", *Smart Grid News*, 1 Jul 2008.

these may result in privacy and data protection risks, as these attacks often target specific users based on their identities. Cyber security experts have identified the capability to remotely deactivate supply as a key vulnerability of smart grids.[194] The potential to easily monetise identified vulnerabilities makes smart meters attractive targets for criminal hackers. Energy usage, and therefore bills could be modified.[195] In the UK at least, it is the supplier's responsibility to ensure the security of the meter.

5.3.4.3 Applicable legislation and standards

Smart metering infrastructure appears to have government support in several countries. This is based upon the possibility for reducing peak power demand and reducing carbon emissions in supporting of achieving legally binding emissions targets. The legal basis for smart metering in the EU arises from Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (Energy Internal Market Directive); and Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments (Measuring Instrument Directive). The European Union's Third Energy Market Package has resulted in most EU Member states implementing legal frameworks for the installation of smart meters. However, this only requires smart meter roll-out if Member State analysis finds this to be economically viable. This legislation calls for 80% of European electricity consumers have smart meters by 2020. It also mandates that consumers have access to their own energy consumption data at no extra cost.

The Article 29 Working Party concludes that smart metering involves the processing of personal data.[196] This conclusion is based on the association of smart meter data with the account holder, enabling the singling out of one customer from others; that this information will be used to take decisions directly effecting individuals (most obviously for, but not limited to, billing purposes); and that energy reduction goals can only be realised by reducing the energy use of individual consumers, and that these reductions are predicated upon detailed information about energy use.[197] The smart meter privacy impact assessment from the Victoria Department of Primary Industries suggested that regardless of the actual legal status of energy consumption data as personal information or not, treating this data as if it was personal data under the appropriate legal regimes would set a high standard of care commensurate with customer anxieties and potential future use of the data.[198]

The protections for personal data in Directive 95/46/EC apply to personally identifiable smart metering data, meaning that this information can only be processed for specified, legitimate and limited purposes and that consent must be obtained. If a supplier operating in the EU intends to transmit personally identifiable data collected in the EU the limitations on transborder data flows will apply.[199] Smart metering data has relevant applications associated

---

http://www.smartgridnews.com/artman/publish/industry/Data_Privacy_and_Security_Issues_for_Advanced_Metering_Systems_Part_2.html

[194] Anderson and Fuloria, "Who controls the off switch", op. cit.

[195] McDaniel, "Security and Privacy", op. cit., 2009.

[196] Article 29 Data Protection Working Party, *Opinion 12/2011 on smart metering*, WP183, Brussels, 4 April 2011, p.8. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

[197] Ibid.

[198] Lockstep Consulting, *PIA Report: Advanced Metering Infrastructure (AMI), Version 1.2*, Department of Primary Industries, Victoria, Canada. August 2011.

[199] Foley, *Data privacy*, op. cit., 2008.

with regulated functions in the energy supply system, which may provide an exception to restrictions on the processing of personal data under Article 13 of the Directive.[200]

Article 8 of the European Convention on Human Rights would also be applicable (the Dutch senate vote against mandatory smart meter roll-out was based on the plans being seen as violating the Article 8 right to respect for private life).[201]

Specific Member States have applicable legislation. As an example, from March 2013, energy suppliers in the UK cannot collect real-time data and require express permission to collect data more than once a day.[202] Customers should be allowed to opt out of half-hourly collection. It is unclear if local councils or security services should have access to smart meter information. It is likely that the UK will adopt a once-monthly transmission of data unless customers opt-in to provide more granular data in exchange for particular pricing tariffs.[203] Supplier use of customer usage data for marketing purposes requires customer consent. The UK Energy Act 2011 requires suppliers to provide public information on the benefits that accrue to consumers from smart meter roll out, to improve transparency and in recognition that many of the benefits of the scheme accrue to the suppliers.[204] The UK government has encouraged the energy industry to develop a 'privacy charter' to explain customer choices on data use, and to adopt principles of Privacy by Design.[205]

There are several international standards applicable to the security of smart meters, which would be an important part of protecting the privacy of consumers. For example International Standard ISO/IEC 27001 is a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System.

The European Commission has issued three mandates to the European Standardisation Organisations (ESOs) CEN, CENELEC and ETSI to work on standards related to Smart Grids.[206] Mandate M/490 for smart grids developed a first set of smart grid standards and a reference architecture in 2012. An ad hoc group (SGIS) dealing with data security and privacy aspects has been established and has issued a report on a privacy and security approach.[207]

5.3.4.4 Certification-related good practices

The following section sets out existing standards and certification approaches in the field of smart metering and privacy. This includes best practice guidance, standardisation approaches and existing privacy seal schemes.

---

[200] McKenna, "Smart meter data", op. cit., 2012, p. 809.
[201] Ibid.
[202] Consumer Focus, "Consumer Information: Smart meters – what are they and how can I find out more". http://www.consumerfocus.org.uk/get-advice/energy/smart-meters-what-are-they-and-how-can-i-find-out-more/privacy-and-security-issues
[203] Mathieson, S.A., "UK gov's smart meter dream unplugged: a 'Colossal waste of cash': Everything you need to know about the kit that'll know everything about you", *The Register*, 19 July 2013. http://www.theregister.co.uk/2013/07/19/feature_uk_gov_power_meter_plan/
[204] Richards, Patsy, and Mike Fell, "Smart Meters", *House of Commons Library Note*, 20 June 2013.
[205] Ibid, p.10.
[206] Mandate M-441 for Smart Meters; Mandate M-468 for a common charging system for electric cars; and Mandate M-490 for Smart Grids.
[207] CEN, CENELEC, ETSI, *Smart Grid Information Security*, Nov 2012. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_security.pdf

Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart meter systems[208] contains provisions on data protection, privacy and security including guidance to Member States on data protection by design and the application of the data protection principles of Directive 95/46/EC. It recommends that Member States take all necessary measures to impose data anonymisation, provides a template for a Data Protection Impact Assessment to be provided for opinion to the Article 29 Data Protection Working Party. The Recommendation sets out a number of required functions for smart meters, and states that Best Available Techniques (BAT) be determined for each of these functions by Member States in collaboration with industry, the Commission, and other stakeholders. The Recommendation also suggests ISO 27000 certification and the notification of personal data breaches within 24 hours. The Commission is developing a data protection impact assessment template and a set of BAT.[209] The Commission sees data protection impact assessment as a key instrument for accountability of data controllers and a way of improving the decision making and planning practices of personal data processing, including risk management. Best Available Techniques for privacy and data protection include privacy enhancing technologies to mitigate the risks associated with the key functions of smart meters. The Expert Group 2 members will produce a selection of current BAT in 2014.

The Cyber Security Working Group of the US National Institute of Standards and Technology made the following recommendations for best practices in relation to privacy and smart meters:[210]

Conduct pre-installation process and activities for using smart grids technologies with utmost transparency.
Conduct an initial privacy impact assessment before making the decision to deploy or participate in the smart grid. Additional privacy impact assessment should be conducted following significant organisational systems, applications, or legal changes – and particularly following privacy breaches and information security incidents involving personal information, or in addition to an independent audit.
Develop and document privacy policies and practices that are drawn from the full set of OECD privacy principles and other authorities. This should include appointing personnel responsible for privacy policies and ensuring protections are implemented.
Provide regular privacy training and ongoing awareness communications activities to all workers who have access to personal information within the smart grid.
Develop privacy use cases that track data flows containing personal information to address and mitigate common privacy risks that exist for business processes within the smart grid.
Educate consumers and other individuals about the privacy risks with the smart grid and what they can to mitigate these risks.
Share information with other smart grid participants concerning solutions to common privacy-related risks.
Manufacturers and vendors should engineer smart devices to only collect the data necessary for the purposes of the smart grid operations. The defaults for collected data should be established to use and share the data only as necessary to allow the device to function as advertised and for the purpose(s) agreed to by the smart grid customers.
Establish law enforcement access request policies and procedures.

[208] *OJ L* 073, 13 March 2012.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:01:EN:HTML
[209] Response to questions from the European Commission, Directorate General Energy, Smart Grid Task Force.
[210] Smart Grid Interoperability Panel – Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, NIST, August 2010.
http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

Table 10 Recommendations for best practice – privacy and smart meters

Mark Foley, a US lawyer specialising in data protection, security and information management provides another suggested set of best practices. These are:

- Consult with legal counsel to resolve privacy and security issues at the design stage.
- Retain data only for a reasonable period of time related to the purpose for which it is collected.
- Avoid resistance by permitting consumers to turn off or limit detailed data collection especially during early research phases. Make "off" the detailed mode for data transmissions.
- Establish Board of Directors and senior management oversight of data privacy and security practices.
- Design security into every collection, access, and transfer point. Create separate pathways for personally identifiable information. [211]

Energy UK published a set of privacy commitments for smart metering, intended to provide customers with information about information collected from smart meters, how it will be used, and to set out rights and choices.[212] A statement such as this could serve the basis of a certification scheme that guarantees these commitments are observed.

The UK government Smart Energy Code includes the following obligations relating to third party access to data.[213] Third parties must

- Take steps to verify that the request for third party services has come from the individual in question.
- Obtain explicit (opt-in) consent from consumers before requesting data from the data and communications company,
- Provide reminders to consumers about the data that is being collected.[214]

A study on the particular personal information required to achieve the desired benefits of smart metering indicates that less sensitive personal information is required than is commonly assumed, for the purposes of system balancing, demand reduction, feedback, demand response, retail billing, distribution system operation and planning, voltage and power quality, fast demand response, outage detection and fault location, operation nearer to limits, and planning reinforcement.[215]

The European Commission issued a mandate to the European Standards Organisation (CEN) for smart grids standards; the primary objective of this mandate is the interoperability of utility meters, rather than any specific mention of privacy standards.[216] The European Commission set up the Smart Grids Task Force (SGTF) in 2009. As part of the SGTF, Expert Group 1 advises on Smart Grid Standards (including on information security standards),

[211] Foley, *Data privacy*, op. cit., 2008.
[212] Energy UK, "Energy UK's Privacy Commitments for Smart Metering: Version 1.0". http://www.energy-uk.org.uk/publication/finish/37-smart-meters/448-era-privacy-commitments-for-smart-metering.html
[213] Department of Energy and Climate Change, *Smart Metering Implementation Programme: Data Access and Privacy: Government response to consultation*, London, December 2012. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf
[214] Ibid.
[215] McKenna, "Smart meter data", op. cit., 2012.
[216] European Commission Enterprise and Industry Directorate-General, *Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability*, Brussels, 12 March 2009. http://www.cen.eu/cen/Sectors/Sectors/Measurement/Documents/M441.pdf

Expert Group 2 advises on regulatory recommendations for privacy, data protection, and cyber security in the smart grid environment, and Expert Group 3 advises on Regulatory Recommendations for Smart Grid Deployment.

Expert Group 2 published a recommendation to the Commission on the essential regulatory requirements for data handling, data safety and consumer protection.[217] Recommendations include: considering most smart meter data as personal data; adopting adequate security safeguards to protect this data; incorporation of privacy by design and by default into smart grid methodologies; that each purpose of data collection have its own relevant data retention period and that a single period cannot be adopted; that Member States perform an analysis on the extent to which customer data needs to be retained for electrical grid operation and billing; the principles of minimised data retention, transparency and empowerment of the consumer should apply, and that privacy certification schemes should be encouraged by Member States. The report considers certification primarily in terms of data protection audits and privacy certificates. The report states:

> Achieving privacy certificates can be a large and complex undertaking. It is therefore necessary to formulate requirements with respect to the meaning and contents of the certificate, and to formulate requirements on the expertise of those issuing the certificate. The requirements that the processing of personal data must comply with can be further detailed in a national certification scheme. The requirements for the auditor and the method by which the privacy audit is carried out need to be shown in the accreditation scheme.[218]

The Expert Group recommends that the European Standards Organisations mandate that smart grid products are designed with appropriate levels of security and privacy protection at their core.[219] Finally, the Expert Group report identifies EuroPriSe, as an independent certification of IT products and IT-based services against European data protection regulation, as an example of certification that could be applied to smart metering.

5.3.4.5 Need for privacy certification

Commission Recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU) states:

> For the purpose of optimising transparency and the individual's trust, Member States should encourage use of appropriate privacy certification mechanisms and data protection seals and marks provided by independent parties.[220]

In Opinion 183, the Article 29 Data Protection Working Party noted that the introduction of smart meters marks a shift in the relationship between consumers and energy suppliers. In addition to paying for the supply of electricity or gas, smart meters will now supply these companies with insight into personal routines.[221] Energy consumption and appliance use

[217] Expert Group 2, *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety and Consumer Protection: Recommendation to the European Commission, V1.0*, 5 Dec 2011.
[218] Ibid, p. 41.
[219] Task Force Smart Grids, Expert Group 2, *Regulatory Recommendations for Data Safety, Data Handling and Data Protection*, 16 February 2011. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf
[220] European Commission, Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems, *OJ L* 73/9, Brussels, 13 March 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:EN:PDF
[221] Article 29 Data Protection Working Party, *Opinion 12/2011 on smart metering*, WP183, Brussels, 4 April 2011. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

occupy a complex position with the "moral economy" of households.[222] Energy consumption data should possibly be considered sensitive personal data.[223] Smart meters involve people who have a generally limited engagement with information technology in the area of privacy and data protection. Energy consumption data is desirable data for several types of organisations, including law enforcement agencies, employers marketing agencies, criminals, as summarised in the table below.[224]

Interested Actor	Motivations
Energy customers	Reduce energy costs; reduce energy use; alerting to faulty appliances.
Energy suppliers	Can identify more profitable customers; automate billing and customer switch-over processes; identify energy theft.
Energy network operators	Demand management and balancing, greater information about energy network status
Third-party service providers	Offer services to customers based upon their energy use data.
Law enforcement agencies	Counter terrorism, anti-drug operations, law enforcement.
Employers	Determining presence/absence, determining productivity.
Marketers	Directed advertisement (for repair/upgrade), demographic data.
Criminals	Occupancy patterns in house or neighbourhood to facilitate burglary or other property crime, identify presence of valuable appliances, corporate espionage.
Insurance companies	Determine premiums based upon unfavourable behaviour patterns.
Press	Energy consumption/behaviour of famous/public individuals.
Creditors/financial companies	Behaviour associated with credit risk.

Table 11 Actors and motivations

One potential need for privacy certification arises from relatively strong opposition to the introduction of smart meters and a general lack of positive support for the technology from the public. There are smart meter opposition groups across Europe[225] and several public opinion studies that suggest low enthusiasm for smart meter uptake. A report on privacy in smart grids for the Privacy Commission of Ontario suggests that the relationship between consumers and utility companies is primarily driven by necessity (rather than customer desire or enthusiasm) but that prior to the advent of smart meters had not been an area in which privacy was a significant issue or point of contention.[226] Operators and suppliers face a dilemma if smart meters are required for legal and technical reasons but face public opposition and scepticism.[227]

Navigator consultants conducted a public opinion study on smart metering data access and privacy for the UK Department of Energy & Climate Change using a focus group

[222] Hargreaves, Tom, Michael Nye and Jacquelin Burgess, "Making energy visible: a qualitative field study of how householders interact with feedback from smart energy monitors", *Energy Policy*, Vol. 38, No.10, 1 October 2010, pp. 6111-6119.
[223] McKenna, "Smart meter data", op. cit., 2012.
[224] Lisovich et al, "Privacy concerns", op. cit., 2008, p. 4.
[225] See for example http://www.takebackyourpower.net/directory/europe-uk/
[226] The Future of Privacy Forum and the Information and Privacy Commissioner, Ontario, Canada, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, Toronto, Nov 2009, p. 3. http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf
[227] Jaruwek et al, Plug in Privacy, op. cit., 2011.

methodology.[228] It found that other than billing and costs, understanding of the working of the energy infrastructure and industry was low (including knowledge of how the industry is regulated by Ofgem), and attitudes were characterised by almost universally negative attitudes towards energy suppliers (high prices and profits, overly aggressive sales and marketing tactics). The consequences of personal information falling into the wrong hands were seen as apparent to the participants, with the largest concern being the use of information as leads for marketing. There was also little understanding of smart meters outside of participants who already had one installed. The consultants suggest that activities in the smart meter field should assume no pre-existing background knowledge. The focus group participants were sceptical about the introduction of smart meters based on the reduction in energy use (and therefore energy company profits) and what the resultant "catch" might be. Only a small number of participants questioned the security of smart meters, with concerns being largely pragmatic ("who would pay for the meter?" or "would it lock me into a particular supplier?"). Energy consumption data was not seen as particularly sensitive, however the information appears to increase in sensitivity with the increased granularity of data collection. Participants were unsure why anybody would need detail at highly granular levels, and what the information would be used for. Information provided to consumers about the purposes for which data is used was seen as key to acceptance of smart meters, but there was little confidence in self-regulation or voluntary agreements from suppliers.[229]

In the Netherlands, the roll-out of smart meters faced opposition, with a majority of parliamentarians in 2009 opposing a ministerial intention to make the installation of smart meters compulsory.[230] The opposition was based upon the bill violating citizens' rights to privacy under European law. In Germany, Yello Strom GmbH, an energy supplier, received a Big Brother Award for its plans to implement smart meters in households.[231]

Outside the EU, other jurisdictions are experiencing negative perceptions of smart metering. The Ponemon institute in the USA conducted a public opinion survey for AT&T. The study found a roughly even split between people who thought that smart meters would negatively impact negatively privacy, people who were unsure of the impact, and people who believed it would not have any negative impacts. Concerns about privacy increased with greater levels of knowledge about smart meters.[232] Efforts to de-identify data encouraged support from some consumers. This study asked participants to rank a set of privacy concerns; energy consumption information occupied the middle of the range, considered more private than online search data, but less sensitive than financial and health information. There has been significant opposition to the actual installation of smart meters, which has included protest and direction action. The concerns combine surveillance and privacy concerns with health concerns related to electromagnetic radiation generated by the wireless networks.[233] A Privacy Impact Assessment of Smart Meter systems in Victoria Canada found:

---

[228] Navigator, *Smart Metering – Data Access and Privacy: Public Attitudes Research*, Department of Energy & Climate Change, December 2012.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43045/7227-sm-data-access-privacy-public-att.pdf

[229] Ibid, p.5.

[230] Metering.com, "Smart Meters to not be compulsory in Netherlands", 14 April 2009.
http://www.metering.com/smart-meters-not-to-be-compulsory-in-netherlands/

[231] McKenna, "Smart meter data", op. cit., 2012.

[232] Ponemon Institute, Perceptions, op. cit., 2010.

[233] Regalado, Antonio, "Rage against the Smart Meter" *MIT Technology Review*, 26 April 2012.
https://www.technologyreview.es/printer_friendly_article.aspx?id=40018

> Broader concerns about privacy – most notably openness about use and disclosure and the choices that consumers will have to control secondary usage under a future AMI (advanced metering infrastructure) environment – are not well ingrained across the electricity industry.[234]

The impact assessment report noted that low levels of public communication had resulted in an environment where customers concerns exceeded the risks of privacy invasions, and that a much improved communication programme with the public was necessary. The authors of the report recommend that such a programme focus upon the realities of smart meter data flows, the limited revelation of behavioural patterns and the choices consumers have to control them. They also suggest that future innovation around smart meters that is anticipated by the industry, including the development of new services, may lead to further customer anxieties. Insufficiently informed consumers may be unaware of the possibilities and benefits that might accrue to them.[235]

However, given the relatively early state of smart meter roll-out, the privacy risks and implications are relatively untested at this point. Similarly, the existing practices of utilities companies may not yet adequately cover the privacy and personal information requirements of the data produced by smart meters. Therefore, the ability of utility companies to secure certifications (or not) certification may have an important role in allowing consumers to assess the extent to which utility companies are prepared for processing and protecting smart meter data through their privacy policies and practices. It would be a particularly useful measure during the transition period.

5.3.4.6 Potential barriers to certification

In Deliverable 2.4 of the Study, we identified a number of key challenges for EU-wide certification schemes. Many of these challenges, such as a lack of mutual recognition or EU-wide certification, are relevant to any attempt to establish and maintain a certification scheme for privacy in smart meter applications.[236]

The way that households and individuals interact with the metered utilities affects the dynamics of potential certification options for smart metering. Electricity is seen as "doubly invisible" for affluent consumers, both in that it is invisible and enters the house primarily through hidden wires, but that its use and consumption are often part of inconspicuous and unreflective everyday practices and behaviours.[237] Additionally, in the absence of independent power generation, customers' relationships with utilities companies are often typified by necessity, rather than enthusiasm.

The current role of regulators and attitudes of potential certified entities are potential barriers to certification. Utilities are often relatively strongly regulated sectors of the economy. If the activities of actors in the energy sector are already strongly regulated, then these entities may

[234] Lockstep Consulting, PIA report, op. cit., p. 4.
[235] Wissner, Mathias, "The Smart Grid – A saucerful of secrets?" *Applied Energy*, No. 88, 2011, pp. 2509-2518, [p. 2516].
[236] Rodrigues, Rowena, David Barnard-Wills, David Wright, Luca Remotti, Tonia Damvakeraki, Paul De Hert & Vagelis Papakonstantinou, *Task 2: Comparison with other EU certification schemes, D2.4, Final report*, EU Privacy Seals Study, European Commission Joint Research Centre, Institute for Protection and Security of the Citizen, 2013.
[237] Hargreaves et al, "Making Energy Visible", op. cit., 2010.

see little advantage in participating in a scheme that simply certifies their compliance with existing law.

Liberalised energy markets and unbundling of previously vertically-integrated utilities mean that European energy markets are characterised by a wide range of different types of actors.[238] The US National Institute of Standards and Technology report on Smart Meters states that consumer data in a smart grid is transferred and stored in several locations.[239] This increases the potential for unintended disclosure and unauthorised breach. It also increases the range of entities that might potentially be covered or impacted by a certification scheme for smart grids. These factors call for a careful consideration about which types of organisations that should be the target for certification. The ability to transfer the ownership and control of smart meters between companies (for example, when a customer changes utility provider) also introduces concerns for certification.

5.3.4.7 Scope and limitations of privacy certification

In the following sections, we explore the potential scope and requirements of the application of a hypothetical EU privacy certification scheme for smart meters. We assume that such a scheme works on the basis of an industry-developed standard for smart metering privacy,[240] against which organisations involved in smart metering can be certified, which is endorsed by data protection authorities at the national and European level. This certification would go beyond legal data protection requirements, and could include the conduct of data protection impact assessments as a risk management exercise, and the use of best available techniques for privacy protection.

5.3.4.8 Target of certification

Public privacy concerns about smart meters are based on the potential for previously private activities to be inferred from outside the home by using energy consumption data. Privacy certification schemes should therefore respond to this concern. If certification is intended to respond to potential public unease regarding smart meters, then the scheme should have a public focus. Smart grids may span scan across public and private organisations, in different ways in different Member States, therefore a privacy certification scheme in this sector would need to be applicable to both public and private organisations.

One of the key decisions in smart grid privacy certification is whether to certify devices or organisational practices and processes. Device certification is more suitable for engaging with security related privacy issues, surrounding unauthorised access to personal data. There is ongoing work on security standards for smart grids as part of both the SGTF and CEN standards. If devices are to be certified, then certification should apply to smart meters, and potentially to all devices that can be integrated into a smart grid.[241] However, the previous table of privacy risks includes many elements that are not amenable to device or product certification, but require some form of organisational focus. Additionally, given concerns related to accurate billing and revenue protection, there are existing incentives for smart

[238] Wissner, "The smart grid", op. cit., 2009.
[239] Smart Grid Interoperability Panel, *Guidelines*, op. cit., 2010.
[240] We recognise other approaches might be possible, but this is a good starting point based on the overall purposes of the Study.
[241] Task Force Smart Grids, EG 2, *Regulatory Recommendations*, op. cit., 2011.

metering companies to pay attention to the security of the smart meters as part of a smart grid. There are also information security standards, such as ISO 27000 which can be applied to smart grids. This suggests, therefore, a focus on the processes surrounding the implementation and use of smart grid technologies.

Privacy certification schemes will have little traction on issues of internal privacy within the household, therefore we do not pursue these issues here.

5.3.4.9 Beneficiaries

Concerns about the privacy impacts of smart meters may increase resistance and opposition to their installation and roll-out. Certification that is able to reassure consumers and minimise concerns about privacy and personal information could potentially reduce opposition to the roll-out of smart meters, with the associated benefits that would accrue to the industry. European citizens will receive smart meters for utilities (particularly electricity) over the next decade. Whilst individual opt-outs may be possible, this will become increasingly uncommon with smart meters becoming the norm. Certification may reduce consumer anxiety about smart meters and make consumers more comfortable with their use.

An endorsed standard, written in clear language could provide the consumer with clear information about how they can expect the information from their smart meter to be used and what protection they could expect for that data. The standard would provide clear guidelines to organisations involved in smart grids about how to interpret the relevant data protection legislation in the context of smart grids.

If organisations involved in smart metering subscribe to an endorsed standard then regulatory authorities and privacy advocates gain a potential tool that will help encourage adherence.

5.3.4.10 Harmonisation and common standards

There are divergent legal frameworks for the implementation of smart meters across Europe. The SmartRegions project's European Smart Metering Landscape Report summarises these.[242] Most European Member States have or are about to implement some form of legal framework for the installation of smart meters. The report distinguishes between "dynamic movers" with a clear path towards rollout; "market drivers" proceeding with installation of smart meters without specific legal requirements; "ambiguous movers" where there is a legal framework in place but little active installation of smart meters, potentially due to ambiguity; "waverers" where there is some industry interest in smart metering, but few initiatives have actually started; and finally "laggards" where smart metering is not yet an issue.

The Article 29 Working party stated "there is huge variation in circumstances between member states, ranging from those where rollout is nearly complete following government mandate to those where no meters have been installed."[243] Additionally, there is variation in the level of involvement of DPAs across Member States, and in the nature of the utility

[242] Renner, Stephan, Mihaela Albu, Henk van Elburg, Christoph Heinemann, Artur Lazicki, Lauri Penttinen, Francisco Puente, and Hanne Saele, *European Smart Metering Landscape Report: SmartRegions Deliverable 2.1*, Vienna, Feb 2011. http://www.piio.pl/dok/European_Smart_Metering_Landscape_Report.pdf

[243] Article 29 Data Protection Working Party, *Opinion 12/2011 on smart metering*, WP183, Brussels, 4 April 2011, p. 4. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

markets. The Working Party's Opinion suggests that given this diversity, recommendations could only be general rather than specific.[244]

Energy trading is an increasingly pan-European activity. The European Energy Exchange allows for international trading of electricity, whilst several energy companies operate across different European Member States.[245] The implication of this is that there will be pressures to harmonise standards across the Union. Cooperation between the DPAs of Member States should be encouraged to align the certification requirements to the greatest extent possible.

A regulator-endorsed standard could be harmonised at a number of levels. The absence of harmonisation would be represented by each individual actor establishing their own code of conduct for privacy in smart data (as is the case with current privacy policies). Greater harmonisation could be achieved by certification standards being collaboratively developed by industry organisations at Member State, or for even greater harmonisation, at the European level. These certification standards could be recognised either by national DPAs, or at the European level by the Article 29 Data Protection Working Party or the European Commission. Alternatively, for standards developed at national levels, some form of mutual recognition principle may be appropriate for harmonisation.

5.3.4.11 Policy requirements

The policy requirements for a DPA endorsed privacy and data protection standard are relatively insubstantial. Standards organisations could develop such certification standards in consultation with stakeholders; these could then be endorsed by data protection authorities. DPAs frequently play a role in identifying and promoting best practice in data protection; this activity would clearly fit under this competence. The key policy requirement would be that the entities responsible for recognising the standards would have to agree on the acceptable contents and requirements of such a certification, for it to be recognised. International co-ordination would be beneficial.

The utility industry may require some policy support in developing standards given that the personal information issues that are raised by smart metering are relatively new to this industry and it actors may not as familiar with these issues as other industries (for example, telecommunications) are.[246] It is advisable for proposed standards to be closely linked to the existing best practice guidance issued by a variety of relevant organisations, as summarised in the section on certification-related good practices.

It is policy in some Member States (for example the UK) that new companies should be able to enter the electricity market as electricity suppliers and as meter vendors, therefore the certification scheme should not present an undue burden upon new market entrants that it does not impose upon existing suppliers and vendors. If subscribing to a certification scheme is voluntary, then new entrants could either choose to meet the standard or not.

[244] Ibid.
[245] Wissner, "The smart grid", op. cit., 2009, p. 2509.
[246] Article 29 Data Protection Working Party, *Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force,* 00678/13/EN, WP205, 22 April 2013.

5.3.4.12 Regulatory requirements

Regulation may be required to provide the basis for an EU standard for privacy and data protection in smart metering. Such a certification would be endorsed upon organisations that met this standard. The certification approach could be strengthened at Member State levels by regulation requiring the adopting of such standards, or their submission to DPAs for recognition.

5.3.4.13 Technical requirements

As a primarily textual creation, the technical requirements of an industry-developed then regulator-approved standard are relatively limited. The requirements of the standard could later be incorporated into technical designs for smart metering to facilitate privacy and security by design, data limitation, etc. If the standard includes a commitment to the use of BATs for data protection in smart grids, this would generate further technical requirements.

5.3.4.14 Market requirements

For such a certification scheme to have relevance for commercial actors involved in smart metering, it must either provide a competitive advantage to the actors that adopt the certification over those that do not. It must be able to sufficiently reduce opposition to smart metering in general. These effects depend on attitudes in individual Member States. To the extent that industry-wide agreement is reached on the elements to be certified, the first benefit is reduced and there may be a temptation to free-ride during the development of such a scheme. However, the second benefit may be reinforced by broad industry agreement on the requirements of such a certification.

5.3.4.15 Roles and actions of stakeholders

To be meaningful and acceptable to relevant stakeholders, the process of developing a certification should be a collaborative one that includes stakeholders such as sector regulators and consumer groups. The following table identifies the roles and key actions of various stakeholders in the development of the hypothesised certification approach.

Stakeholder	Role	Action
Industry association	Industry associations bring together representatives of smart metering industries and can identify best practice in both privacy and security.	Propose/collaborate in standard development
Consumer groups	Consumer groups can represent consumer interests and advise industry associations on the information and guarantees customers require	Consult on standard.
Sector regulators	Utility regulators could play an important role in certification.[247]	Consult on standard.
Data protection authorities	The SGTF Expert Group 2 encouraged the involvement of DPAs in the protection of consumer rights in relation to smart grid privacy,	Recognise standards at national level, collaborate at

[247] The Future of Privacy Forum and the Information and Privacy Commissioner, Smart Privacy, op. cit., 2009.

	but recommended that actors in this field be able to demonstrate their own accountability in addition to the requirements of data protection.[248] The report encouraged certification conducted by independent parties.	international/EU level.
International co-ordination of DPAs	Forums for the co-ordination and collaboration of data protection authorities. The key example in the EU is the Article 29 Data Protection Working Party.	Consult on development of standards. Recognise standard at International level
Standardisation organisations	Source of expertise on standards issues, interoperability, security and links to networks of experts.	Critical role in coordinating, developing and promoting standard.
Privacy advocacy organisations	Source of expertise on privacy issues.	Consult on standard.

Table 12 Stakeholders, roles and actions

5.3.4.16 Responsibility and oversight mechanisms

An endorsed standard may require the creation of mechanisms for audit, accountability, and enforcement to certify that organisations are meeting the standard. Regulation might be necessary to allow the recognition of sectoral standards developed by EU-level actors, such as the Article 29 Data Protection Working Party.

5.3.4.17 Sustainability

The direct costs of participation in such a scheme would be relatively low; this is important for sustainability. The approach set out here does not call for new, specific organisations to be set up and maintained over time.

Smart meter technology is still developing, both in spread and in terms of the granularity of data that can be acquired. Smart meter policy will need to integrate future developments in smart housing. Therefore, the standard should be re-evaluated at regular intervals to determine if it was still applicable and relevant in regard of technological developments and a better understanding of the privacy risks of smart metering.

5.3.4.18 Evaluation and conclusion

Smart grid includes several complex privacy and data protection issues that will likely become increasingly relevant with the development of the Internet of things (also known as ubiquitous computing). A privacy seal scheme would ideally be able to anticipate and address these issues.

The concept of an industry developed standard for privacy and data protection in smart metering, which is recognised as meeting certain requirements by regulators would be applicable to the field of smart metering, which is characterised by some level of public

[248] Task Force Smart Grids, EG 2, *Regulatory Recommendations*, op. cit., 2011, p. 5.

concern and a high diversity of actors. The privacy risks are at the institutional level and the proposed certification response is targeted at that level. The approach could be transferable to other domains. It is a lightweight regulatory solution, predicated upon a combination of bottom-up and top-down approaches.

5.3.5 Biometric systems

This case study benefitted from comments from Isabelle Moeller of the Biometrics Institute, London.[249]

5.3.5.1 Definition and explanation of the context

The EU's draft General Data Protection Regulation defines biometric data as "any personal data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data."[250]

Biometric systems are applications of biometric technologies which allow the automatic identification, verification, authentication and/or categorisation of a person.[251] These systems are based upon physical characteristics that are universal (existing in all persons), sufficiently unique (the element is distinctive between persons) and permanent (the property of the biometric element does not change over time).[252] Commonly used biometric elements include fingerprints, iris recognition, retina recognition, face recognition, hand patterns, voice recognition, DNA analysis, signature analysis, gait analysis and keystroke analysis.[253] Biometric technologies therefore make elements of the human body machine-readable.[254]

Recent developments include behavioural biometrics, which use unique features of actions or patterns of actions that individuals perform, either consciously or unconsciously. Examples include blinking pattern, gait, electromagnetic signals from the heart or brain, keystroke dynamics, voice patterns, credit card spending and text style. Particular biometrics often have specific applicability to a particular use case, are most useful in combination with other biometrics. [255]

Biometric systems are increasingly used for authentication, verification and identification purposes and for access control. The cost of biometric technologies has reduced and these technologies are widely deployed. Biometric technologies are attractive for these applications because they offer the possibility of authenticating a user or individual directly, rather than authenticating something they possess or know (for example, a username and password)

[249] http://www.biometricsinstitute.org/. The Biometrics Institute is an international forum (non-profit) whose primary members are government and users of biometric services and products, with other membership categories for vendors.
[250] European Commission, Proposal for a Regulation, op. cit., 2012.
[251] Article 29 Data Protection Working Party, *Working Document on Biometrics*, WP80, Brussels, 1 Aug 2003, p. 3.
[252] In practice these assumptions can break down. For example, some proportion of the population will not have readable fingerprints, and fingerprints can change over subtly over a person's lifetime.
[253] Article 29 WP, Working Document on Biometrics, op. cit., 2003, p. 3.
[254] Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, WP193, Brussels, 27 April 2012, p. 4
[255] ENISA, *ENISA Briefing: Behavioural Biometrics*, Jan 2010.

which could be stolen or shared with another individual.[256] Biometrics are increasingly used in official government issued identification or travel documents and border control, access control and law enforcement are amongst the most common applications of biometric systems. European ePassports contain facial biometric, various national e-ID card of member states make use of facial and fingerprint biometrics, and the EU has developed the European Visa Information System (EU-VIS) and European Biometric Matching Systems (BMS).[257]

As a case study for EU privacy certification schemes, biometric systems have a number of relevant characteristics. Firstly, biometric systems pose particular sets of privacy risks. Secondly, 'biometric systems' encompasses a wide and varied range of technologies, from different manufacturers, across different applications and use-cases. Thirdly, biometric systems are themselves complex and largely opaque to the individual end users whose biometric information is being processed. Finally, there are already existing certification initiatives for biometrics in relation to technological standards, interoperability and security, into which a privacy certification could potentially be integrated.

5.3.5.2 Risks and mitigation measures

According to the Article 29 Data Protection Working Party, "The risks which are presented by biometrics derive from the very nature of the biometric data used in the processing."[258] A 2008 report for the European Commission Joint Research Centre (JRC) examined the challenges to security and privacy arising from large-scale biometric systems. The report states:

> Without alignment on credible ways to address privacy and security concerns in biometric information systems, and without legal and technical conformity of such systems with privacy laws within Europe and around the world, the benefits of such systems could be minor. Even more seriously, it can be assumed that under those circumstances market acceptance and trust of large-scale biometric systems will be hindered.[259]

Risks arise from the growing number of purposes for using biometrics, the increased quality of biometric reference data, interconnectivity with third party databases, database ownership, the types of organisations that are data controllers, and from international data exchange.[260]

Biometric technologies are not 100% accurate. Common measures of the accuracy of a biometric systems are the false reject rate and the false accept rate. The false accept rate is the probability that a biometric system will incorrectly identify an individual, or will accept an imposter. These are invalid inputs that are accepted as valid by the system. The false reject rate is the opposing error of this where valid inputs are treated as invalid, for example when an individual is not matched to his or her own biometric template.[261] The error rates for biometric technologies are not always clear and available. This has implications for attempts

[256] Bolle, Ruud M., Jonathan H. Connell & Nalini K. Ratha, "Biometric Perils and Patches", *Pattern Recognition*, Vol. 35, 2002, pp. 2727-2738.
[257] European Commission, "Visa Information System". http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm
[258] Article 29 WP, *Opinion 3/2012*, op. cit., 2012, p. 5.
[259] Goldstein, James, Rina Angeletti, Manfred Holzbach, Daniel Konrad, Max Snijder & Pawel Rotter, *Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats*, European Commission Joint Research Centre, Seville, Oct 2008, p. 75. http://www.a-sit.at/pdfs/biometrics_report.pdf
[260] Ibid., p.73.
[261] Article 29 WP, Opinion 3/2012, op. cit., 2012, p. 6.

to challenge the assertions of biometric systems when errors occur, and for data protection requirements that personal data stored and processed be accurate. The accuracy of biometric systems is also related to the population size. Identification of false accept and reject rates and population size for a particular technology may comprise an important part of the certification of the accuracy of biometric technologies as a means of increasing the transparency of associated processing of personal data.

There may be non-privacy risks associated with the use of biometric technology, for example, a poorly configured method of taking biometric measurements may be physically harmful to the individual. This case study does not explore these risks in detail, but as most biometric systems involve electronic technologies (and in some cases medical imaging technologies) then relevant safety standards will apply.

The following table collates the privacy risks associated with biometric technologies and discusses some of the associated methods for mitigating or managing these risks:

Privacy risks	Details	Mitigation measures
Identification without consent	Some biometric technologies can collect a biometric profile without an individual data subject giving consent (although they may legally require consent) This is a particular issue with unobtrusive technologies (see below), DNA profiling (where it is difficult to avoid leaving DNA samples) and some behavioural biometrics.	Consent processes, legal protections, signage. Identification without consent can be mitigated by storing the biometric template under user control (for example, on a smart card), rather than in a centralised database controlled by the technology operator.
Mandatory use	Some biometric technologies (particularly in security applications) are mandatory, and consent cannot meaningfully be sought from the data subject.	Minimise the use of such applications.
Identification without knowledge	Biometric characteristics are not secret and can often be obtained covertly without the knowledge of the individual. Biometrics are often exposed in public situations with relatively little control over this exposure. For example, a fingerprint may be retrieved from surface an individual has touched (which is part of their utility in forensics).	Biometric templates stored locally under control of the data subject. Informing data subjects.
Linkability	The ability to use the biometric to connect previously separate databases, and create detailed profiles on individuals.[262] Coupling biometric data to other personal data.	Decentralising databases. Limiting circumstances justifying linkability, requiring consent for linking databases.
Difficulty of proving system error	It may be difficult for an individual incorrectly identified by a biometric system to prove that a biometric system has made a mistake.	Accuracy testing and certification schemes, published false match and false reject error rates.
Genetic or health discrimination	Biometric images may contain additional data on physical characteristics, which	This data is not recorded or stored. Can be enforced through

[262] Article 29 WP, Opinion 3/2012, op. cit., 2012, p. 7.

	may be used to make decisions about or categorise the subject.	design of the scanning technology.
Cross over with behavioural or targeted marketing	Biometrics may produce data and techniques which could be used for other purposes, including targeted marketing.	The data is not recorded or stored. May be enforced through design of the scanning technology.
Identity theft/fraud	Theft or loss of biometric data may be far more detrimental for an individual than any other loss of personal information, as biometric data is unique and difficult or impossible to change by nature.[263]	Information security practices and standards. Some data protection and privacy risks associated with the storage of biometric templates can be mitigated by storing the template in a decentralised manner under user control, rather than in a centralised database. There is also work on revocable biometrics that distort the biometric template.
Unclear purpose of system	The purpose of a biometric system may be unclear to those subjected to it.	Transparency of purpose/purpose specification
Disproportionality	Biometric applications can violate the principle of proportionality	System design. Proportionality test in planning stages, privacy impact assessment.
Function creep	The purpose of a biometric system may shift from the original to other, additional purposes.	Design-based use restriction according to purpose binding principle. Purpose transparency.
Biometric information crossing public/private sector boundary	Biometric data might be transferred to law enforcement from the private sector.	Privacy policies, regulation.
Biometric system not in compliance with privacy laws	In addition to specific risks, a biometric system may be designed and operated in a manner that violates privacy laws of the EU and Member States.	Prior checking with DPA, Privacy impact assessment.
Re-use of biometrics by operator of biometric application	Once a biometric image (or signal) is recorded, it may potentially be used for other purposes.[264]	Prior checking with DPA. Consent required for further processing. Privacy-by-design to prevent additional use.
Re-use by third parties	The development of routine use of (for example) fingerprints for access control may encourage the re-use of these databases by third parties for their own purposes. This may include law enforcement agencies.[265]	IT security measures. Strong access controls.
Poor quality of captured data	Lower quality data can lead to more false matches and more false rejections. This can result in intrusive follow-up procedures or inconvenience.	Interoperability standards. Use of improved technologies. Accuracy testing.

[263] De Hert, Paul, Wim Schreurs and Evelien Brouwer, "Machine-readable identity documents with biometric data in the EU: Overview of the legal framework" *Keesing Journal of Documents & Identity*, Issue 27, 2007, pp. 23-26. http://www.vub.ac.be/LSTS/pub/Dehert/131.pdf

[264] Bolle et al, "Biometric perils", op. cit., 2002.

[265] Article 29 WP, Working Document, op. cit., 2003, p. 2.

Unintended functional scope	Biometric collection may collect other biological data and personal information from scanned biometrics. Individuals may be concerned about providing other medical information. Biometric data (and in particular raw images rather than derived templates) may contain more information than is necessary for identification or authentication. This information may frequently be related to ethnicity, gender or health and is likely to be sensitive personal data.	If captured, this data should be destroyed as soon as possible.[266] Ideally, this information would not be captured. Biometric templates derived from scans or measurements should be stored, rather than a raw image of the scan.
Tampering with stored biometrics	Biometric templates stored in a system may be altered, which could allow for inaccurate identification, or false rejection.	Information security measures.
Unintended impacts upon anonymity	Legitimate anonymity or pseudonyms (such as aliases) could be violated by strong biometric identifiers.	Establish procedures for anticipating and managing this.
Stigma/association with criminality	Biometrics (particularly fingerprints) may have associations with the criminal justice system which may discomfort or stigmatise individuals.	Public education and awareness.
Obtrusive equipment	Intrusive measuring technologies may elicit strong negative reactions from individuals to be subjected to them.	Sensitive technology design. Cover technologies (which carry own risks).
Desensitisation to data protection risks	The Article 29 Working Party expressed concern that the routine use of biometric technologies may have implications for desensitising members of society to associated data protection risks.[267]	Sensitisation of organisations using biometrics and of affected data subjects.

Table 13 Biometric privacy risks

More positively, as a potential security measure, biometric recognition technologies can be used to increase the security of personal data held in databases (for example, acting as an encryption key or restricting access to authorised users), and therefore potentially contribute to privacy protecting measures.[268]

5.3.5.3 Applicable legislation and standards

There is no specific provision (or exemption) for biometrics in Directive 95/46/EC, therefore applications processing biometric data must follow the general provisions of the Directive. The General Data Protection Regulation includes the processing of any biometric data under Article 9, Section 1.[269]

The Article 29 WP considers that Directive 95/46/EC applies to biometric systems, and that similarly so should national implementations of the Directive. The Working Party has

[266] Article 29 WP, Working Document, 2003, p.8.
[267] Article 29 WP, Working Document, 2003, p.2.
[268] Prabhakar, Saul, Sharath Pankanti and Anil K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy*, March/April 2003, pp. 33-44.
[269] European Commission, Proposal for a Regulation, op. cit., 2012.

produced guidance to assist the harmonised and effective national interpretation of the Directive in relation to biometrics.[270] Measures of biometric information are, in most cases personal data, and can almost always be considered "information relating to a natural person" by their very nature.[271] The implication is that systems are only legal in the EU if processing of biometric data is conducted in compliance with Directive 95/46/EC. This includes an evaluation of the proportionality and legitimacy of the processing, and taking into account the risks to fundamental rights and freedoms. It requires assessing whether the intended purposes of the system could be achieved in a less intrusive way.

Some Member States have specific references to the regulation of biometrics in their national legislation.[272]

Country	Specific legislation	Details
Norway	Act of 14 April 2000 No.31 Relating to the processing of personal data (Personal Data Act)[273]	Article 12: clear means of identification may only be used in the processing when there is an objective need for certain identification and the method is necessary to achieve such identification.
Slovenia	Personal Data Protection Act (ZVOP-1) 15 July 2004[274]	Defines biometrics in Article 6 (21). Has a specific chapter (3) on biometrics applicable to processing in both public and private sectors.
Italy	Personal Data Protection Code – Legislative Decree No.196/2003.[275]	Section 37, notification of processing of biometrics to supervisory authority. Section 55, data processing by the police and prior communication to the authority.
Luxembourg	Act of 2002 relating to the protection of individuals in relation to the processing of personal data (2002 Act)[276]	Article 14, prior authorisation by supervisory authority before biometric processing can take place.
Slovakia	Act No. 428/2002 Coll. On protection of personal data, as amended by Act No. 602/2003 coll., Act No. 576/2004 coll. and the Act No. 90/2005 coll.[277]	Regulation of biometric data within the regulation of sensitive data.
Czech Republic	Act No.101/2000 Coll., of	Article 4, defines biometric data as sensitive data.

[270] Article 29 WP, Working Document, 2003, p. 3.
[271] Article 29 WP, Working Document, 2003, p. 5.
[272] Iglezakis, Ioannis, "EU data protection legislation and case-law with regard to biometric application" SSRN, 18 June 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2281108
[273] Norwegian Parliament, Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act), 14 April 2000. http://www.ub.uio.no/ujur/ulovdata/lov-20000414-031-eng.pdf
[274] English translation available at http://ec.europa.eu/justice/policies/privacy/docs/implementation/personal_data_protection_act_rs_2004.pdf
[275] President of the Republic of Italy, Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2427932
[276] Chambre des Députés, Texte coordonné de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel modifiée par la loi du 31 juillet 2006, la loi du 22 décembre 2006, la loi du 27 juillet 2007. http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002mod_fr.pdf#pagemode=none
[277] National Council of the Slovak Republic, Act No. 428/2002 Coll. on Protection of Personal Data, as amended by the Act No. 602/2003 Coll., Act No. 576/2004 Coll. and the Act No. 90/2005 Coll. http://www.dataprotection.gov.sk/buxus/docs/act_428.pdf

	April 4, 200 on the Protection of Personal Data and on Amendments to Some Acts.[278]	
Estonia	Personal Data Protection Act, 1 January 2008	Section 4(2) defines biometric data as sensitive data.

Table 14 Examples of national laws regulating biometrics

Legislation regulates the use of biometric systems at the EU level. The Biometric Passport Regulation[279] requires compulsory enrolment of all EU citizens applying for a new passport or passport renewal. The e-Passports of Schengen Member States must include a chip containing a facial scan of the passport holder and two of his or her fingerprints from 2009 onwards.[280] Regulation 444/2009/EC of the European Parliament and of the Council of 28 May 2009 amending Council Regulation 2252/2004/EC on standards for security features and biometrics in passports and travel documents issued by Member States, contains security standards as an annex to the Regulation. In terms of biometrics, these standards refer in turn to Part 1 (machine-readable passports) of ICAO document 9303. Non-EU citizens and third country nationals are also affected by EU use of biometric matching systems (primarily fingerprints) in the European Union Visa Information System (VIS).[281]

The Biometrics Institute, an international body for biometrics vendors and users has developed a set of Privacy Guidelines in order to

> Provide a universal guide for suppliers, end users, managers and purchasers of biometric systems. It is the public's assurance that biometric managers have followed best practice privacy principles when designing, implementing and managing biometric based projects.[282]

The key principles of the Guidelines are: respect for client privacy, proportionality, informed consent, truth and accuracy in business operations, protection of biometric data collected, complaints and enquiries, purpose, anti-discrimination, accountability, informed sharing of biometric data, the provision of advance warning of surveillance, limitations on the transmission of data beyond national borders, the protection of employee biometric data, the creation and maintenance of a culture of privacy, limiting the extent of personal data passed around systems, privacy logs, and subject access.

There are several biometric standards and certification initiatives in domains other than privacy and data protection. Examples include the International Civil Aviation Authority standards on biometric passports, and the standardisation initiatives under Joint Technical Committee 1 (JTC 1) of ISO/IEC subcommittee SC37 "Biometrics". ISO/IEC 19794-2 relates

[278] Parliament of the Czech Republic, Personal Data Protection Act, Act no. 101/2000 Coll., of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts, 2000. http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&lang=en

[279] European Commission, 2252/2004/EC of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *OJ L* 385, Brussels, 29 Dec 2004, p. 1–6.

[280] Aus, Jonathan P., "Decision making under Pressure: The Negotiation of the Biometric Passports Regulation in the Council, ARENA Centre for European Studies, Working Paper 11, Sept 2006.

[281] European Commission, "Visa Information System". http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/

[282] Biometrics Institute, Privacy Guidelines, Revised Draft, Jan 2012. http://www.biometricsinstitute.org/data/Privacy/BiometricsInstitute_BIOMETRICS_GUIDELINES_Revised_Subject_to_Approval.pdf

to interoperability amongst different biometric systems. More specifically, ISO/IEC 19794-2 specifies a concept and data format for fingerprints that is generic and can be used in a range of automated fingerprint recognition applications.[283] The European Committee for Standardisation (CEN) published a report on conformance and interoperability which made several interoperability recommendations in areas such as sensors, data quality, spoofing prevention, security, interfaces, data exchange formats, scalability, reliability, accessibility, and environmental conditions.[284]

5.3.5.4 Certification-related good practices

There are several reports, projects and initiatives which provide guidance on the elements that should be included within a privacy certification scheme for biometric systems. Good practices relate to ensuring an informed data subject, including a clear delineated purpose, with personal data adequate, relevant and not excessive in relation to that purpose.

The Article 29 Data Protection Working Party recommends that industry develops biometric systems that implement their recommendations on compliance with Directive 95/46/EC in co-ordination with data protection authorities, to promote biometric systems that are constructed in a data protection friendly manner, minimise social risks and prevent the misuse of biometric data.[285] The Working Party also highlights the importance of ensuring that biometric systems implement all appropriate technical and organisational security measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure and access.[286]

The BioVision report on privacy issues suggests that a code of conduct for biometrics could be developed by the European Commission with industry recognition into a quality assurance seal.[287]

The 2008 JRC report recommends EU-wide standardisation and certification of the process surrounding the use of biometric systems.[288] This would include enrolment processes, data quality control, usability and operator training, would allow for the enrolled individual to be made aware of the purposes and use of the biometric application, and the opportunity to view and verify that the identity data collected is correct. Standards would also include the presence of acceptable fall-back options if biometric enrolment was not possible. The report also recommends EU-wide procedures for un-enrolment and data modification, with strictly authorised, supervised and transparent intermediaries. Finally, when an application ends or expires, the associated biometric data must be deleted.

---

[283] International Organization for Standardization, "Abstract, ISO/IEC 19794-2:2011 Information Technology – Biometric Data Interchange formats".
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50864
[284] Wolf, Andreas, *Technical Report: A consensus on conformance and interoperability mechanisms, both for applications and sensors, in order to reach security evaluated interoperable solutions between the European Union Member States*, CEN, Focus Group on Biometrics, Brussels, 29 March 2009.
[285] Article 29 WP, Working Document on Biometrics, op. cit., 2003, p.10.
[286] Ibid. p. 9.
[287] Albrecht, Astrid and Martin Walsh, *BIOVISION: Report on legal and privacy issues*, BioVision Deliverable 7.3 and 7.5, 28 Aug 2003. p.6. http://www.biteproject.org/documents/biovision-privacy-issues.pdf
[288] Goldstein et al, Large-scale biometrics, op. cit., 2008, p. ix.

The CEN conformance and interoperability report also made recommendations on privacy and data protection, and on health, societal, cultural and ethical aspects.[289] In relation to privacy and data protection, the report recommends the development of guidelines for privacy-friendly systems that can be approved by data protection authorities.

Whilst not an ISO standard, the ISO/IEC TR24714-1 technical report relates to the design and implementation of biometric technologies with respect to the legal and societal constraints on the use of biometric data; accessibility for the widest population; and health and safety, addressing the concerns of users regarding direct potential hazards and the possibility of the misuse of inferred data from biometric information.[290] ISO TR24714-1 recommends that the following principles should be maintained:

- Transparency and access rights of data subjects
- Consent and limitation of purpose
- Preference for opt-in and limitation of collection, as well as period of retention
- Adherence to performance criteria
- Data protection, secure audit, and responsible data transfer between different jurisdictions
- Information on automated decisions
- Accountability
- Appropriate accuracy of biometric data, which should be kept anonymous whenever possible.

The Future of Identity in the Information Society (FIDIS) project produced an analysis of approaches that would move biometrics from a "privacy invasive technology" to a "privacy enhancing technology".[291] The categorisation depends upon the extent to which a technology is obligatory or voluntary, the choice of biometric, the purpose of authentication or verification, the degree of personal control, the extent to which a biometric is combined with other security methods, the potential for function creep, data quality, the existence of a right to object to biometric processing, and the ease of linkability. This report set out a series of decisions at planning, design and testing stages to facilitate this.[292] The BioPrivacy Application Impact Framework (see table below) adopts a similar approach to FIDIS, with ten categories which determine if a biometric application is likely to have lower or higher impact upon privacy.[293] Guidance such as this could be included in a progressive best practice certification approach.

Question	Lower risk to privacy	Higher risk to privacy
Are users aware of the system's operation?	Overt	Covert
Is the system optional or mandatory?	Optional	Mandatory
Is the system used for identification or verification?	Verification	Identification
Is the system deployed for a	Fixed period	Indefinite

[289] Wolf, op. cit., *Technical report*, op. cit., 2009.
[290] ISO/IEC, Technical Report 24714-1:2008 Information Technology – biometrics – Jurisdictional and societal considerations for commercial applications–part 1 General Guidance. http://www.iso.org/iso/catalogue_detail?csnumber=38824
[291] Sprokkereef, Annemarie and Bert-Jaap Koops, *D3.16: Biometrics: PET or PIT?* FIDIS, 20 Aug 2009. http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables2/fidis-WP3-del3.16-biometrics-PET-or-PIT.PDF
[292] Ibid.
[293] International Biometric Group, BioPrivacy Application Impact Framework, http://www.bioprivacy.org/bioprivacy_text.htm

fixed period of time?		
Is the deployment public or private sector?	Private sector	Public sector
In what capacity is the user interacting with the system?	Individual, consumer	Employee, Citizen
Who owns the biometric information?	Enrollee	Institution
Where is the biometric data stored?	Personal storage	Database storage
What type of biometric technology is being deployed?	Behavioural	Physiological
Does the system utilise biometric templates, biometric images, or both?	Templates	Images

Table 15 BioPrivacy Application Impact Framework

Certification processes for some elements of biometric technologies already exist. In 2013, Morpho, a biometric technology developer, received certification under the Common Criteria scheme for detection of spoofed fingerprints in a biometric fingerprint reader.[294] The Common Criteria scheme is an international standard for information technology security.[295]

The CEN technical report examines potential certification options for biometrics, and states that Common Criteria may be a potential blueprint for a biometrics certification scheme, with other inspiration coming from the ISO SC37 Standards 19795-4 (Biometric Performance Testing and Reporting – Interoperability performance testing) and 290120-1 (Machine readable test data for biometric testing and reporting).[296] The BioTesting Europe project (a Supporting Activity under Preparatory Actions for Security Research) conducted a consultation on the European need for biometrics testing and prepared a road-map for biometrics testing and certification capabilities. This activity focused primarily on the reliability, accessibility and interoperability functions of biometric systems and components, rather than upon privacy issues. The project identified that operators and suppliers were conducting testing in an ad-hoc manner.[297]

5.3.5.5 Need for privacy certification

Biometric systems are a powerful technology of surveillance, and therefore suitable targets for privacy protecting policy responses. Such systems have the inherent purpose of distinguishing (and discriminating) between different individuals. Biometric systems have a strong potential to violate rights to privacy and anonymity. In addition, biometric systems often allow for automated tracking, tracing or profiling of persons and can have an increased impact upon privacy.[298] In regard to biometric data, the Article 29 WP states that "This kind

[294] SAFRAN Morpho, "Morpho, Worlds First Company to Receive Common Criteria Certification for Fake Finger Detection", Press Release, Paris, 2 July 2013.
[295] Common Criteria was analysed in Deliverable 2.4 of the Privacy Seals Study.
[296] Wolf, *Technical report,* op. cit., 2009, p. 45.
[297] Mansfield, Tony, "BioTesting Europe: Addressing European needs for testing and assurance of biometric systems", BioTesting Europe, Presentation to Biometrics Consortium Conference, Baltimore, 13 Sept 2007. http://www.biometrics.org/bc2007/presentations/Thu_Sep_13/Session_III/13_Mansfield_STATUS.pdf
[298] Article 29 WP, Opinion 3/2012, op. cit., 2012, p. 3.

of data is of a special nature as it relates to behavioural and physiological characteristics of an individual and may allow his or her unique identification."[299]

Several reports and projects identify a need for particular policy attention to biometrics and a potential specific role for privacy certification. The Article 29 WP supports the development of codes of conduct supporting the proper implementation of data protection principles in biometric systems.[300] A report on large scale biometric applications for the Joint Research Centre linked privacy certification with trust:

> Standards, testing and certification are not only needed to address issues of interoperability, conformity, performance and security, but are also important to build up trust in general. Especially, because privacy is a concern of each individual, trust in any system is essential for its successful implementation.[301]

The BioVision project report on biometric privacy issues argued that the development of a code of conduct including privacy aspects would enable the biometrics industry to "meet the needs of the more vulnerable sections of society, i.e. the consumer and end-user" and also provide a competitive advantage in a global market.[302]

The CEN Technical report on conformance and interoperability measures for European biometric systems advocated a certification approach to privacy and data protection issues in biometrics, again primarily in terms related to ensuring public acceptance:

> To promote public acceptance and to ensure compliance of biometric installations with privacy and data protection laws within each EU Member State, it is recommended to develop guidelines for privacy-friendly systems which could be certified by the data protection authorities of the Member States. These data protection authorities should always participate in the teams involved in the development of conformance projects, tools and infrastructures.[303]

This report also identifies user perception of biometric systems as pivotal to their acceptance.[304] There is a potential that certification measures could improve the perception of biometric systems. The CEN technical report suggests that:

> Certifications for compliance to privacy and data protection principles are a desirable goal. As an initial step, recognition of compliance by data protection officers of EU Member State governments as well as by non-governmental organizations dealing with data protection and consumer protection should be obtained. This would already improve the acceptance of biometric technology. Better acceptance will lead to more user cooperation, which in turn will lead to better performance of biometric systems.[305]

These reports indicate that public opposition to biometric systems and associated technologies may be a potential barrier to the adoption of biometric systems for travel, border control, security and other functions desirable to governments and being developed in support of

[299] Article 29 WP, Working Document on Biometrics, op. cit., 2003, p. 2.
[300] Ibid., p.10
[301] Goldstein et al, Large-scale biometrics, op. cit., 2008, p. 75.
[302] Albrecht and Walsh, BIOVISION, op. cit., 2003, p.6.
[303] Wolf, *Technical report*, op. cit., 2009, p. 41.
[304] Wolf, *Technical report*, op. cit., 2009, p. 43.
[305] Wolf, *Technical report*, op. cit., 2009, p. 45.

European and Member State policy objectives. A lack of trust in biometrics may also limit the development of a European market in consumer-facing biometric technologies. Privacy certification therefore could play a role in assuaging public distrust and privacy concerns in relation to biometric applications. Privacy certification at a European level may be particularly beneficial in relation to cross-border sharing of data within the region. If European citizens are expected to interact with biometric technologies and share sensitive personal data with them, then they have a right to expect those technologies and systems to operate in a manner that is both in compliance with the law, and embody best practices standards for privacy protection. As biometric systems are increasingly cross-border, an EU wide privacy and data protection certification scheme with applicability to biometric systems could be an important counterbalance. .

5.3.5.6 Potential barriers to certification

In Task 2 of this Study, we identified a number of key challenges for EU-wide certification schemes. Many of these challenges are relevant to any attempt to establish and maintain a certification scheme for privacy and data protection in biometric applications.[306] Reports looking at biometric certification have also raised similar issues. The CEN technical report states:

> One should take into account the fact that any certification consumes significant resources; therefore any certification scheme requirements will have impact on prices. Thus, the EU should on one hand try to harmonize European schemes internationally, while, on the other hand, balancing financial, logistical and research support which might all be appropriate to reach the required results as quickly as possible.[307]

There are also some specific issues applicable to biometrics in particular. We can identify the rapid pace of technological development in IT in general, and in biometrics in particular as a potential barrier to certification. Co-ordination issues that have limited efforts to establish biometric security certification will also impact attempts to establish biometric privacy certification given that similar actors are likely to be involved. Biometrics is a relatively mature technology, i.e., there are several active applications. However, it is also a rapidly developing area with the potential for technological development and progress over the lifespan of any certification scheme. A certification scheme must therefore find a way to address potential future developments. Similarly, the range of different technologies and applications that include some form of biometric is wide and diverse (ranging from a biometric security gate at an airport operated by a government worker, to a biometric sensor replacing a password to turn on your own personal laptop computer). This creates complexity for a seal scheme, and means that what is being certified may become increasingly unclear to the end user.

One question biometric certification must address is if a public facing certification scheme is meaningful for mandatory technologies such as those used in European biometric passports. These implementations are often mandated through legislation which might supersede

[306] Rodrigues, Rowena, David Barnard-Wills, David Wright, Luca Remotti, Tonia Damvakeraki, Paul De Hert & Vagelis Papakonstantinou, *Task 2: Comparison with other EU certification schemes, D2.4, Final report*, EU Privacy Seals Study, European Commission Joint Research Centre, Institute for Protection and Security of the Citizen, 2013.
[307] Wolf, *Technical report*, op. cit., 2009, p. 45.

additional certification measures. Secondly, while the display of certification may reassure users in these contexts that some additional standard has been reached, it does not allow the users to make any decisions or take different action in relation to the use of the biometric application.[308]

5.3.5.7 Scope and limitations of privacy certification

Based upon the preceding risks, existing mitigation measures and certification best practices, the following sections explore the potential scope and requirements of the application of a hypothetical EU privacy certification scheme for biometric systems.

In this we assume that the scheme is based on the identification of *least intrusive techniques* for biometric applications by a centralised specialist body. The techniques would be those that could achieve the legitimate purposes of biometric applications in the least intrusive and most privacy-protecting manner. Biometric applications which adopt these least intrusive techniques would be able to display a seal to signify this.[309] Display of the seal, for example on a biometric scanner or identity document should signify that if there were several measures which could have been taken, that the one selected is the most privacy-friendly measure for achieving the specified purpose. Techniques are understood as being broader than technologies and including the use of the technology for a particular purpose in a particular context and taking into account the organisational processes that surround the biometric technology. This approach would recognise the privacy invasive potential of biometrics and be linked to the principles of proportionality and specification of purpose embedded in data protection law.

The moment of enrolment in a biometric system may be particularly important for certification processes (if public facing); this is the point at which an individual has to decide to trust the system sufficiently to enrol. Biometric data may be difficult or impossible to revoke from the system, and future privacy and security risks will result from this moment of decision.[310] This may make this an appropriate point to display or provide details of the certification.

5.3.5.8 Target of certification

Biometric matching systems offer several potential options for the target of certification. Firstly, one could certify particular technologies, particular implementations of systems, or the institutional processes surrounding an implementation. Biometrics can be broadly grouped into three categories of application: commercial, governmental and forensic. The groups likely have different tolerances for false matches and false rejection errors, and may have

[308] Response to questions from the Biometric Institute (http://www.biometricsinstitute.org)

[309] This hypothetical certification scheme draws direct inspiration from the Best Available Techniques of the Integrated Pollution prevention and control (IPPC) certification scheme. The essence of IPPC is that industrial and agricultural operators in particularly polluting industries should use the best options available to achieve a reduction in pollution and a high level of protection of the environment taken as a whole. IPPC achieves this by requiring the operators to acquire permits based upon the use of the best available techniques (known as BAT), together with a consideration of the local environmental conditions, the technical characteristics of the specific installation and its location. See European Commission DG Environment, "The IPPC Directive: Summary of Directive 2008/1EC concerning integrated pollution prevention and control (The IPPC Directive)", 30 Nov 2012. http://ec.europa.eu/environment/air/pollutants/stationary/ippc/summary.htm

[310] Goldstein et al, Large-scale biometrics, op. cit., 2008, p. 76.

different requirements or issues relating to certification. However, an EU privacy scheme with applicability to biometrics should ideally be able to encompass these differences. The BioTesting Europe project suggests that testing and certification (of non-privacy elements) of biometric systems would not replace the testing of these systems by their operators (during installation and as part of knowing their own systems).[311] The context for privacy issues is different however, as the certification regime would presumably be aimed primarily at reassuring or informing the subjects whose privacy or personal data is affected by the biometric systems rather than the operators of those systems.

Certifying particular technologies and implementations are the approaches to certification adopted for security, accuracy and interoperability certification in biometrics. These issues are amenable to the isolated testing of technologies and components. For example, a test dataset could be used on a sensor to determine if its false-reject rate was as advertised. These approaches are not appropriate for privacy certification because of the relatively complexity of privacy-related issues. The exact same biometric technology or product could be applied in ways that are either privacy invasive or privacy friendly. The JRC report suggests the question "What is the purpose of the system and what kind of personal data are strictly needed to serve that purpose?" is central in data protection and privacy issues associated with biometrics. The absence of an answer to this question inhibits attempts to analyse the security and privacy elements of a biometric scheme.[312] Questions of the proportionality of measures relate to the clear identification of purpose.

The PIAF project (a Privacy Impact Assessment Framework for data protection and privacy rights) recommended that independent and accountable privacy impact assessments be conducted for all biometric projects that produce publicly accessible reports.[313] Article 33 of the proposed General Data Protection Regulation provides details of Data Protection Impact Assessments which would appear to be required in the context of most forms of biometric processing, based upon the identification of biometric data as included within special categories of personal data (Article 9 (1)), and therefore as carrying special risk.[314] One option for EU privacy certification of the institutional process and technological implementation of biometric systems might be to certify that such a privacy impact assessment was conducted properly.

Another suitable approach to privacy certification for biometrics would be to adopt a certification model parallel to that used in the Integrated Pollution Prevention and Control (IPPC) Certification. In this scheme, industrial and agricultural activities with a high pollution potential are required to acquire a certificate. Part of the requirements for this certificate is the use of Best Available Techniques (BAT) for pollution reduction in the certified activity. The European IPPC Bureau produces reference documents setting out best available techniques, which are updated in line with technological advances. This model might be suitable for meeting the requirement under Directive 95/46/EC that data processing applications make use of the *least intrusive technique* to achieve a given legitimate stated purpose. This case study reflects upon the applicability of the latter approach. However, product certification and

[311] Mansfield, BioTesting Europe, op. cit., 2007.
[312] Goldstein et al, Large-scale biometrics, op. cit., 2008, p. 74.
[313] De Hert, Paul, Dariusz Kloza and David Wright, *Recommendations for a privacy impact assessment framework for the European Union, PIAF Deliverable D3*, Brussels, November 2012. http://www.piafproject.eu/ref/PIAF_D3_final.pdf
[314] European Commission, Proposal for a Regulation, op. cit., 2012.

privacy impact assessment could be important tools for determining the least invasive techniques in individual contexts, and provide evidence that a least intrusive approach has been adopted.

5.3.5.9 Beneficiaries

The primary beneficiary of biometric privacy certification schemes should be the data subject enrolled in a biometric application or whose personal data is processed. This orientation towards the data subject is necessary to achieve the benefits identified for certification in this domain (i.e., increase of public trust and acceptance of biometric systems) and focuses upon the party with the least effective power and influence over the construction and use of the biometric system. The certification scheme must therefore provide useful information to the individual and certify features that align with genuine public concerns. A system that identified least intrusive techniques for biometric applications would have particular benefits for the individual; they would be exposed to a reduced degree of privacy violation in many cases. Society would benefit as the general level of unnecessary privacy invasion would reduce.

The seal may have secondary beneficiaries such as the purchasers and implementers of biometric applications who can have increased confidence that their systems comply with appropriate standards. Reduced resistance to the use of a biometric system or increased uptake will be beneficial to such actors. Least intrusive techniques could be regularly published for relevant technologies and applications which would act as continually updated resources and guide to the best practices. The developers of biometric applications would gain information about what might be desirable privacy-protecting measures to incorporate into their technologies. Use of privacy-protecting biometric applications and their certification might increase the number of such applications on the market, making it easier for operators to select privacy-protecting biometric applications.

5.3.5.10 Harmonisation and common standards

Iglezakis describes decisions by data protection authorities on biometrics as "ambiguous and lack[ing] consistency".[315] This is based upon differing assessments of proportionality, for example between the French CNIL, and UK ICO in relation to the use of fingerprint biometrics in schools, and previously divergent assessments on the proportionality of voluntary iris scans for air passengers between the Greek DPA, and the Dutch and British DPAs.

The use of biometrics for European passports is now mandatory following Regulation 2252/2004/EC. The introduction and operation of EU-wide biometric programmes, for example in travel and identity documents, creates significant problems of scale and interoperability, but also means that privacy certification schemes for these systems must be relevant across the EU.

A 'least invasive techniques' approach requires the development of common standards that show the least invasive techniques for specific applications. An independent organisation with technological and social scientific expertise, in collaboration with appropriate industry

[315] Iglezakis, "EU data protection legislation", op. cit., 2003.

representatives and expert groups could take charge of this. There is an existing research base on what makes biometric technologies more or less invasive, and any standards developed could incorporate existing work on privacy-by-design, security-by-design and privacy impact assessment frameworks.

5.3.5.11 Policy requirements

There are not many examples of existing privacy certification schemes directed at government administered systems. If a certification scheme for biometric systems with a focus upon passports, visas and other travel documents is developed, then its structure would need to take into account the role of Member State governments in the procurement, administration and operation of biometric identification systems. Least invasive techniques would provide guidance to Member State governments in the design of national and international biometric systems, and would increase the availability of privacy-protecting biometric technologies for governments to draw upon.

The setting up and operation of an independent body providing assessments of least intrusive techniques for biometric technologies would require policy support. It would also be important to identify the key stakeholders who could contribute to and advise this body. Furthermore, this body would require a sustainable source of funding.

5.3.5.12 Regulatory requirements

The IPPC certification upon which this approach is modelled includes a regulatory component which identifies particularly polluting industrial and agricultural practices, and requires that sites and organisations engaging in these practices acquire IPPC certification from their national competent body. If a privacy certification scheme follows this model, similar regulation could be an important component, and would need both European and harmonised national components. However, even without the regulatory pressure for such certification, then a method to demonstrate that a biometric application has been developed using industry-standard and internationally recognised best practice might still be appealing to developers and operators, but would lack regulatory force. Enforcement measures related to the certification may require regulatory support; alternatively, the enforcement mechanism could draw inspiration from the Green Dot packaging waste scheme by using trademark infringement law to challenge unauthorised use of the visual identity of the ‘least intrusive measures’ seal.

5.3.5.13 Technical requirements

Certification of least intrusive measures for biometric applications (and across a range of industries and technologies) requires a relatively heavy technical burden; the various measures must be evaluated on the basis of their intrusiveness. This requires technical knowledge and input from legal and social science perspectives. Additionally, as technologies develop, these standards should regularly be re-evaluated and updated. This might require the creation of a dedicated organisation to conduct and publish such evaluations.

Given that the privacy invasive nature of technologies cannot be determined from the technology alone, some element of these assessments must be conducted in situ and standards organisations must keep abreast of the social impacts of surveillance technologies. Further

research may be necessary to develop coherent and detailed accounts of least intrusive techniques.

5.3.5.14 Market requirements

Non-mandatory biometric certification schemes would need to offer benefits to the scheme participant in order to ensure take-up. For mandatory schemes, even those targeted at the most potentially intrusive uses of systems, a level of participant benefits may be appropriate to ensure good will, shared benefit, and reduce resistance to the implementation of the scheme. Procurement incentives are a likely source of benefits to participants if, for example, participation in the scheme offers a benefit in terms of easing the technology's involvement in the procurement processes of large organisations. This would require such organisations to make reference to the privacy certification scheme in their procurement policies. Governmental and European Union bodies would be appropriate places to start imbedding such incentives. Generally, the market would require evidence that the scheme would reduce public distrust for biometric technologies, and would ease their adoption. During the lifetime of the scheme, these benefits would need to be tracked and communicated to participants and potential participants.

5.3.5.15 Roles and actions of stakeholders

The following table identifies the roles and key actions of various stakeholders in the development of the hypothesised certification approach.

Stakeholder	Role	Action
Data protection authorities	Would still have a legal role in relation to the processing of biometric personal data, as set out in national data protection legislation.	Consultation with evaluation body, contribution to least invasive techniques.
Independent evaluation body	Responsible for developing, updating standards.	Determine, publish and update technical and process standards for the least intrusive techniques in biometric applications.
Technology developers	Responsible for the design of technologies to achieve current least invasive practices, engage in R&D to develop less invasive practices, and integrate these into biometric systems.	Develop least invasive techniques. Incorporate least invasive techniques into next generation of biometric technologies.
Biometrics industry	Responsible for aligning biometric applications with the requirements of certification.	Integrate least invasive techniques into technology by design. Develop biometric applications.
Independent cross-sector bodies	Cross-border, cross-sector experience and networks.	Contribute to least invasive techniques, promote scheme and share best practices.
The public	Beneficiaries of certification scheme and source of legitimacy.	Attribute trust to scheme or not.
Privacy advocacy groups	Source of advice and experience on invasive qualities of biometric technologies	Advise and consult on the development of least invasive techniques.

Table 16 Stakeholders, roles and actions

5.3.5.16 Responsibility and oversight mechanisms

The body responsible for developing least intrusive measures should be independent of the biometrics industry, although able to draw upon its expertise where possible. To the extent that such a measure should be generalised across technologies, this independence should continue. The body would, therefore, require institutional support at the EU level. The body may benefit from a close working relationship with data protection authorities or bodies such as the Article 29 Working Party (or the EDPB under the GDPR) and other international standards organisations.

An oversight mechanism would help determine that organisations claiming they are using least-invasive techniques in their biometric applications are actually doing so. The difficulty of this would be affected by how detailed the current standard for least invasive techniques are. Organisations may have to provide a report with evidence of how they are implementing the least invasive techniques in their application for certification. National data protection authorities would be suitable candidates for this oversight role, but may require some additional resources and sources of expertise.

5.3.5.17 Sustainability

The development and updating of a set of least intrusive techniques would require initial resources to set up, and further resources to ensure its sustainability and continued relevance. This would mean a continued source of funding and institutional support. Such a scheme would not be self-funding unless further legislation was passed to mandate a levy upon the technologies and practices that were identified as particularly privacy invasive and therefore in need of having least invasive techniques developed and identified. The frequency with which the least invasive techniques are to be updated should be calibrated against the expected rate of development and change in the technologies involved, but maintain a capacity for responses to unexpected developments and new technologies which may need to be reflected in the guidance.

5.3.5.18 Evaluation and conclusion

As a case study for EU privacy certification, biometric systems have a number of relevant characteristics. An EU privacy seal scheme based upon a least-invasive techniques approach presents a number of conclusions.

Firstly, biometric systems pose particular sets of privacy and data protection risks. Not all the relevant issues for biometrics are necessarily relevant for a wider privacy seal, which would have to operate at a greater level of abstraction. However, it suggests that attention to those technologies (such as biometrics) which have a significant surveillance potential could be a focus for certification schemes. In parallels with the IPPC certification, such a model could be applied across industries and technologies identified as particularly privacy invasive. These areas could have least-invasive techniques determined for them.

Secondly, ‘biometric systems’ encompasses a wide and varied range of technologies, from different manufacturers, across different applications and use-cases. Basing certification upon a developed set of improving standards for particular fields allows for variation across those

fields, while still upholding a common privacy-protecting principle compatible with data protection legislation.

Thirdly, biometric systems are complex and largely opaque to the individual end users whose biometric information is processed. A certification scheme based upon the best available techniques for preventing the invasion of privacy allows for some user confidence without the requirement that users fully understand all elements of the biometric processes. There is also an existing evidence base on what might constitute least intrusive techniques.

Existing certification initiatives for biometrics in relation to technological standards, interoperability and security constitute an environment into which EU-level privacy certification could potentially be integrated. An approach to biometric certification could therefore focus upon reducing the privacy intrusive elements of biometrics. However, not all privacy-invasive technologies have similar levels of certification in progress.

6 LESSONS LEARNED FROM THE CASE STUDIES

This section presents the lessons learned from the development and finalisation of the individual case studies.

6.1 DIFFERENCES IN CONTEXT

One of the key emergent messages from the case studies exercise is the differences in context in each of the case studies. Differences in context are relevant as an EU privacy seal scheme will inevitably encounter these. The preceding analysis shows that each of case studies has a different context; each is unique. Each has a different nature (though a few similarities may exist). There are also differences in: the design of the (underlying) technology, type, features, implementation, use across sectors, benefits, investment, profitability, national priorities, impact, public perception and acceptance of the technology or service.

Some of the risks of the case studies are common (heightened surveillance, identification, breaches of personal data); others are more specific to each case (e.g. risks inherent in the placement of CCTV cameras and unauthorised filming, non-consent based capture of biometrics, profiling of domestic energy usage by smart meters, unauthorised interception of personal data stored in cloud services). Some risks are relative to how, and by whom, the technology underlying each case study is implemented, and the measures that are available and used to mitigate privacy and data protection risks. Privacy and data protection sensitivities differ for each case study, as does the potential for risk aggravation.

In relation to applicable legislation, the case studies demonstrate how complex each of their applicable regulatory frameworks are. Although all case studies generally process personal data and therefore fall within the scope of the Directive 95/46/EC, some of the legal frameworks are more settled as the technology has been in existence for some time (e.g. CCTV); in other cases such as cloud computing the regulatory frameworks are developing or underdeveloped (cloud transfers). Some fields such as biometrics or smart metering already benefit from sector-specific EU legislation that ought to be taken into account while elaborating upon privacy protecting policy options. Furthermore, processing may be undertaken by public or private bodies, a factor that must also be considered when attempting practices (particularly when processing refers to the ‘hard core’ of public administration such

as passport issuing). Finally, there are national differences in regulatory efforts that must be taken into account.

In the case of standards too, there are differences in whether these exist, their levels of development, and their prevalence. Good practices also vary. All the case studies have some form of good practice. Some are certification related, others not so much and are of a more general nature. The good practices identified range from EU guidelines, to regulatory and industry codes of practice and privacy by design measures.

Given this variety in the context, regulatory environment, applicable legislation and best practice, privacy certification in relation to each of the case studies might serve different needs. In essence, privacy certification is a potential solution for different privacy problems in each policy area. For CCTV, it might mean more effective control, reduction in the regulatory burden, making design and implementation of the technology more privacy friendly, boosting the visibility of effects. For cloud services (a frequently evolving environment) it might generate traceability, provide assurance on the processes and the rights of data subjects and processors in respect to cloud processors and sub-processors, or help clarify the different elements of the responsibility chain. For smart metering, it might help optimise trust (specifically due to public opposition and negative opinions in regard to an increasingly mandated technology). For biometric systems, it might help address issues of interoperability, conformity, security, meet needs of vulnerable sections and give its users a competitive advantage. In all cases, we can identify potential for EU privacy certification to create trust, transparency, drive up and incentivise privacy and data protection standards and further support privacy and data protection compliance.

6.2 POTENTIAL BARRIERS

The following table summarises the list of the potential barriers for each case study based on our research findings:

List of barriers	CCTV	Cloud services	Smart metering	Biometric systems
National considerations and distinctions in policy, regulation and implementation	●	●	●	
Resource impacts (increase in prices etc.)		●		●
Rapid pace of technological development in general and specific to case study	●	●		●
Co-ordination issues				●
Differences in cultural attitudes and threat perceptions relating to sector across EU Member States	●		●	●
Existence of other threats in conjunction with privacy, data protection threats	●		●	
Resistance and mistrust of the scheme/current role of regulators and attitudes of potential certified entities	●		●	
Lack of added value	●			
Lack of regulatory support and a legal compulsion to certify	●			
Competition and conflict with other existing standards	●	●		
Identifying the data processor responsible for a			●	

particular installation				
Absence of sectoral legislation at EU level	●	●		
A lack of harmonisation of national regulations		●		●
The failure of the European DPAs to endorse the scheme.		●		
The failure of a common, agreed vision on sector related personal data and privacy protection (between regulators and industry)		●	●	
The lack of embeddedness of the seal in the institutional setting of privacy governance		●		
Applicability of certification schemes to technologies to which the data subject has no meaningful choice			●	●

Table 17 Comparative presentation of potential barriers

6.3 TARGET OF CERTIFICATION

The following table outlines the potential targets of certification identified in each case study:

	Potential targets
CCTV	Technology and its use, system, system installers and operators, owners
Cloud services	The specific cloud computing service
Smart metering	Organisational practices and processes surrounding the implementation and use of smart grid technologies.
Biometric systems	Technologies, particular implementations of systems, or the institutional processes surrounding an implementation

Table 18 Targets of certification

The CCTV case study deliberately does not pin down a single target of certification and uses a broader approach. Adopting a singular, restrictive approach does not seem in the best interests of maximising privacy and data protection for this sector. The other case studies do specify certain targets. Based on our research into existing privacy seals, certification schemes in other fields, we identified the specific contexts of those case studies that are the most appropriate targets for privacy certification and protecting the interests of data subjects.

6.4 POLICY, REGULATORY, TECHNICAL AND MARKET REQUIREMENTS

In understanding the requirements generated by each case study, our approach was driven by the particular context of those cases.

6.4.1 Policy requirements

The following table summarises the policy requirements identified by each case study as essential for EU privacy requirements:

Policy requirements	CCTV	Cloud services	Smart metering	Biometric systems
Appropriate and consistent EU policies	●	●	●	●
Incentivising privacy, data protection compliant organisations, products and services	●			
Policy guidance/policy	●	●	●	●

recommendations				
Integration of resources to operationalise the scheme (institutionalisation and co-ordination)	●	●	●	●
Setting out of core scheme objectives and priorities for the scheme	●	●	●	
Mutual recognition efforts	●	●		
Communication and information dissemination	●	●	●	●

Table 19 Policy requirements summary

Four policy requirements (appropriate and consistent EU policies, policy guidance and policy recommendations, integration of resources and the need for communication and information dissemination) apply across all four case studies. We could assume that these policy requirements would apply across a larger range of relevant policy domains.

6.4.2 Regulatory requirements

In all the above four cases, we would need an overarching harmonised legislation that forms the basis of the EU certification and its criteria. The GDPR could provide this basis. However, there might also be need for additional regulatory measures specifically dealing with open issues that are not specified in the Regulation. The CCTV case highlighted the need to embed certification in the regulatory process either through direct legal requirement or through soft law approaches such as provisions in codes of practice. We must also note the findings of the biometrics case study which highlights that even without the regulatory pressure for such certification, then a method to demonstrate that a biometric application has been developed using industry-standard and internationally recognised best practice might still be appealing to developers and operators, but would lack regulatory force. Enforcement measures related to the certification may require regulatory support; alternatively, the enforcement mechanism could draw inspiration from the Green Dot packaging waste scheme by using trademark infringement law to challenge unauthorised use of the visual identity of the 'least intrusive measures' seal.

6.4.3 Technical requirements

Each of the case studies differs in their coverage of technical requirements. The CCTV case study specifies or covers the following elements: operation and administration of the scheme, scheme criteria and requirements, conditions for award of certification, certification process, review of the scheme, validity of certification, termination and revocation of certification and renewal of certification. The cloud study specifies a very similar list. The smart meters case study suggests that the technical requirements of an industry-developed and regulator-approved standard are relatively limited and that the standard requirements could later be incorporated into technical designs for smart metering to facilitate privacy and security by design, data limitation, etc. The biometrics case study recognises that the certification of least intrusive measures for biometric applications (and across a range of industries and technologies) would mean a relatively heavy technical burden and require technical knowledge, and input from legal and social science perspectives. It also calls for the establishment of a dedicated organisation to conduct and publish biometric certification evaluations.

6.4.4 Market requirements

The following table summarises the market requirements identified by each case study as essential for EU privacy requirements:

Market requirements	CCTV	Cloud services	Smart metering	Biometric systems
Market demand and support for good quality, privacy compliant products and services	●		●	
Procurement incentives	●			●
Critical mass		●		
Market research		●		
Competitive advantage			●	
Mechanisms to prevent free-riding			●	
Provision of market benefits to scheme participants				●

Table 20 Market requirements

6.5 ROLES AND ACTIONS OF STAKEHOLDERS

Each of the case studies shows the importance of various stakeholders who would play a role in an EU privacy seal scheme. While the roles advanced might be specific to the case study, overall we find several commonalities. All the four case studies lead us to conclude that, whatever the final form of the EU privacy seal scheme, the relevant stakeholders will need to collaborate and there will be some overlap in their roles. For this reason, it is important to gain as much support from the core stakeholders (i.e. those directly involved in the implementation of the Scheme and those affected by the implementation of the scheme[316]) for the success of the EU privacy seal scheme. Based on our research we find there is a lot of scepticism about an EU privacy seal scheme (based on some stakeholders' experiences with past EC trust mark initiatives and the commercial seals marketplace). Effective action to bring stakeholders on board and to gain their confidence is highly essential. Given that an EU privacy seal scheme may cut cross several sectors, the range of associated stakeholders will be broad. Some of these actions include: consultation and engagement, pilots, regular reviews, communication, promotion and awareness-raising activities.

6.6 SUSTAINABILITY

An EU privacy seal scheme would have to be sustainable. Sustainability will mean adequate resources at the EU and national level (financial, human, organisational and technical) that support its continued existence.

The key factors identified in the case studies that will help contribute to the sustainability of an EU privacy scheme throughout its life cycle are: wide acceptance and recognition of the scheme across the EU, mutual recognition, public-private collaborations and technical assistance, long term policy commitment exclusion of competing schemes, review of the scheme at regular intervals and embedded flexibility to adapt to changing technologies, privacy and data protection expectations.

[316] Each of the case studies identified a relevant set of stakeholders.

7 CONCLUSIONS

Current state of affairs – gaps and shortcomings

Having mapped the field of privacy and non-privacy certification in the EU in the reports of Tasks 1 and 2 respectively, this report attempted to elaborate upon the challenges and scope of an EU privacy seal scheme with the help of four case studies – CCTV, cloud computing services, smart metering and biometric systems. Despite the evident conceptual merits of an EU-wide scheme, this objective remains (at time of writing) elusive: no truly EU-wide privacy seal scheme is in operation or has been initiated to date. This probably constitutes a missed opportunity, particularly given the numerous shortcomings identified in relation to existing privacy seal schemes. The list of these shortcomings is long and important. As far as the data protection purposes are concerned, there are shortcomings, *inter alia*, in the guaranteed level of data protection, user awareness and trust, enforcement and regulatory oversight, and in harmonisation and common standards. Each one of these issues alone poses serious threats to personal data protection – their cumulative effect may explain why contemporary schemes continue to be piecemeal, duplicitous, fragmented efforts that for most of their part, have no formal recognition, and enjoy limited public acceptance and, less enthusiastic use.

Urgent priorities

An EU privacy seal scheme could address most (and, if properly designed and implemented, all) of these issues. The priorities for such a scheme would attempt to resolve the shortcomings of existing efforts. The scheme would need to guarantee an appropriate level of privacy and personal data protection for individuals. It would need to implement a standardised approach within the EU that would help reinforce the internal market dimension. Such a scheme would also need to demonstrate flexibility and adaptability over the different processing sectors it purports to regulate, while at the same time remaining specific to their needs and sustainable over its life cycle. It would also need to enhance transparency and accountability.

Building on the gaps in existing privacy seal schemes, and the analysis of the requirements and issues relating to privacy seals in the areas of CCTV cloud computing, smart meters, and biometrics, the following sections summarise the core findings of this report and examine the challenges and dilemmas for an EU privacy seal scheme as well as key planning requirements.

7.1 CHALLENGES AND DILEMMAS

While the priorities for an effective EU privacy seal scheme may be more or less self-evident, it is the challenges and constraints, that the scheme needs to overcome, that will ultimately decide upon its success or failure. Important challenges need to be addressed to develop the scheme's full potential; not all of these are within the reach of the potential designers and operators.

The dynamics of technological progress

One major challenge for an EU privacy seal scheme comes from the dynamism and fluidity of the technologies it purports to regulate. As has been repeatedly demonstrated over the past

few decades, personal data processing is intrinsically connected to technological progress. In fact, all recent information technology developments have proven relevant, in one way or another, to personal data processing, whether referring to business models (for instance, Internet social networks or search engines) or technologies per se (e.g., data mining, data matching, profiling). The case studies demonstrate this; all are the result of technological developments that made the relevant processing possible, alongside social and economic demands that have driven their uptake and use. In addition, the relevant technologies are far from settled. Within this environment, data protection law (or, for the same purposes, any regulation) inevitably struggles to keep up. A privacy certification scheme would face substantial difficulties while attempting to regulate sectors and fields where technological progress may make rules and standards irrelevant within a short period of time. Frequent updates and re-assessment, and a permanent monitoring and enforcement mechanism, appear therefore an indispensable part of an effective EU privacy seals scheme. In addition, a properly designed privacy seals scheme may be able to drive information processing practices in a particular desired normative direction, rather than simply provide increased information on the *status quo*.

The significance of a flexible EU privacy seals scheme

Similar to fluid technologies, an EU privacy seal scheme would have to regulate unsettled sectors. The case studies demonstrate this: CCTV surveillance is a well-known type of personal data processing, and regulators and societies have established practices towards it (at least until new technological developments such as face recognition pose new, unknown problems). Biometrics, however, is a type of personal data processing that is relatively new, marginally used (for instance, in passports), and only indirectly regulated in existing legislation. Somewhere in the middle lie the other two case studies, smart metering (where dedicated legislation may be found but currently only limited use across the EU, although this will change over the next few years) and cloud computing (with which practically everybody is engaged but often at a standalone level and with limited awareness of its data protection risks). All these cases show that the public threat perception may differ substantially from the actual privacy and data protection risks. Furthermore, data processing roles and actions vary in the different case studies: in CCTV surveillance, data processing is mostly performed by the public sector and private sector for security purposes (and widely used for domestic purposes); in smart metering, data processing is performed by private parties and data subjects may be anything from individuals to large private or public organisations; biometrics may find as many uses (and, respectively, actors); cloud computing may involve "private purposes" use (individuals keeping their data in servers overseas) to systematic, outsourced personal data processing in third-country jurisdictions.

Given this, an EU privacy seals scheme would have to tread carefully and differentiate, with great attention to detail; in some sectors, a lightweight approach might be possible, whilst in others a specified, detailed scheme seems necessary to gain appreciable benefits. In addition, the ability of privacy certification to engender trust might be limited given that certain sectors present risks that go beyond privacy and data protection. It may therefore be necessary to encourage the use of other privacy and data protection enhancing measures such as privacy impact assessments, privacy by design or privacy enhancing technologies in combination with privacy certification.

The complexities of the regulatory environments

The third challenge, beyond the control lying outside an EU privacy seal scheme control refers to the substantially different regulatory environments in the data processing sectors it would otherwise have to regulate. As evidenced in the case studies, certain fields of personal data processing benefit from additional and specific established rules (for instance, CCTV) while others have not yet attracted the legislators' attention. Certain fields have EU legislation regulating their operation (smart metering, certain cases of biometrics), while others are only found at an evaluation level (reporting on the difficulties of their regulation, as is the case with cloud computing). To further complicate things, even EU regulation may come in different forms and statuses (Regulations as opposed to Directives, a choice that affects harmonisation levels). An EU privacy seal would have to pay attention to such difference. In certain cases, it would have to conform to already established EU rules. In other cases, it may fall upon its drafters to attempt to formulate the first rules for the respective field. Secondary legislation, or even *soft law*, is also important. National laws developed by individual Member States set a precedent within their respective jurisdictions. In cases where industry codes of practice or even privacy certification schemes of some kind are already in place, their existence should not be ignored. The same applies to certification schemes that are not directly related to privacy issues. Their use and experience could prove valuable for data protection purposes (such as security and integrity of systems). All of the above form the complex regulatory environment that a prospective EU privacy seal scheme would have to take into account.

7.2 NEED FOR CAREFUL PLANNING AND EXECUTION

The above challenges (fluid technologies, unsettled sectors and varying regulatory environments) constitute issues not directly controlled or controllable by the designers of an EU privacy seal scheme. In order to address these challenges as best as possible, mitigation measures would need to include, among others, flexible rules, frequent updates and reviews, and a permanent monitoring mechanism. Nevertheless, not all challenges for an EU privacy seal scheme lie outside the control of its designers. In fact, the opposite is the case: an EU privacy seal scheme would have to be carefully planned and executed to overcome shortcomings identified in existing implementations and to develop its own full potential.

Need to overcome scepticism

An EU privacy seal scheme would, first and foremost, have to overcome scepticism expressed about its *raison d'être*. Such scepticism was evident in the case study analyses; its roots could lie in the gaps and shortcomings of existing schemes that might have caused some harm to the idea of privacy certification, the uncertainty regarding the benefits of a hypothetical scheme and the acknowledgement of the important difficulties that an effective scheme would have to overcome. The critical contribution that an EU privacy seal scheme could make to overturn such scepticism would be its added value. The scheme would have to prove the added value for privacy and data protection in order to justify its existence. Within a regulatory environment where a multitude of data protection rules and dedicated (data protection) authorities purport to protect the individual right to data protection (already elevated at the EU constitutional level), an EU privacy seal scheme will have to prove that it can make a difference to the everyday life of data subjects, data controllers, and preferably to both.

Added value

The added value of the scheme would lie in its contribution to specificity, clarity, accountability and transparency. These are important priorities for an EU privacy seal scheme, whose adequate execution constitutes at the same time, a crucial challenge for its survival. Through enhancing, in a practical and identifiable manner, data controllers' accountability, by providing them with concrete and specific guidance on their processing practices, and data subjects' trust, by means of making processing processes transparent, an EU privacy seal scheme would succeed in its data protection purposes. To accomplish this, critical questions need to be answered concerning the target of certification; redress mechanism; the renewal process; the enforcement methods, etc. The answers to these questions, in the actual organisation of an EU privacy seals scheme, will ultimately determine its usefulness and relevance in contemporary dynamic personal data processing environments.

Addressing sustainability issues

Another important challenge for an EU privacy seal scheme refers to its sustainability. As demonstrated in all case studies, an effective EU privacy seal scheme would require considerable resources to set up, be maintained and kept relevant. Such costs could be covered by fees paid by participants, who will presumably recognise the competitive advantage afforded by carrying the relevant seal and be willing to pay for it. However, this is probably an expectation for the future, when the scheme has proven its value and strength in the market. Until such time, the issue of cost will, presumably, remain unresolved. In certain cases, as is the case for biometrics processing, costs could be covered by imposing a levy on particularly invasive technologies. However, such mandatory payments are probably not applicable in all personal data processing fields. Mandatory participation in an EU scheme, once released and officially ratified, could be one solution. However, this would create yet another burden in an already overstretched market. In any event, all of the above illustrate that sustainability of the scheme is a crucial factor that needs careful planning and weighing of the options at hand.

Creation of an adequate, supportive regulatory framework

Yet another challenge for an EU privacy seals scheme refers to the creation of an adequate regulatory framework to support it. For the time being, Directive 95/46/EC is still in effect, but does not appear to provide a suitable legislative framework against which to build a strong privacy certification system. This is also illustrated by the identified shortcomings of current privacy seals schemes. The General Data Protection Regulation could assist the privacy seals effort in a two-fold manner: first, unlike a directive, it will be applicable directly in all Member States, eliminating local interpretations and varying approaches. And, second, by expressly referring to them in a dedicated Article, it will grant privacy seals the legal power to expand, by means of secondary legislation, implementing measures, etc. Depending therefore on its ultimate wording, the General Data Protection Regulation could be the decisive factor for the initiation and success of a truly European privacy seals scheme.

What next?

The appropriate model for such an EU privacy seals scheme is yet to be decided. The General Data Protection Regulation, released by the Commission in January 2012, adopted a neutral viewpoint as to the scheme's organisational particulars. However, the Draft European

Parliament Legislative Resolution on GDPR provides a significant amount of detail with regard to its preferred model. Whatever the ultimate wording of the Regulation, a formal, legislatively endorsed privacy seals scheme constitutes a mostly untested attempt, in and out of the EU, to protect personal data and privacy. Careful consideration and planning therefore need to be undertaken in devising and implementing such a, scheme particularly given the findings and recommendations of the first three tasks of the Study. The next and final task of the Study (task 4) will determine how best to encourage the development of the EU-wide privacy seals scheme and examine the key options that will support the General Data Protection Regulation to this effect. It will identify the challenges, assess their benefits and provide some guidance and recommendations on how to implement these options.

8 REFERENCES

Anderson, Ross, and Shailendra Fuloria, "Who controls the off switch?" http://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf

Agustina, J.R., and Gemma Galdon Clavell, "The impact of CCTV on fundamental rights and crime prevention strategies: The case of the Catalan Control Commission of Video surveillance Devices", *Computer Law & Security Review*, Vol. 27, 2011, pp. 168-174.

Albrecht, Astrid and Martin Walsh, *BIOVISION: Report on legal and privacy issues*, BioVision Deliverable 7.3 and 7.5, 28 Aug 2003. p.6 http://www.biteproject.org/documents/biovision-privacy-issues.pdf

Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 11750/02/EN, WP 89, 11 Feb 2004. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf

Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 20 June 2007, 01248/07/EN, WP 136.

Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, WP 173, 13 July 2010.

Article 29 Data Protection Working Party, Opinion 12/2011 on smart metering, WP183, Brussels, 4 April 2011.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, 01037/12/EN WP 196 1 July 2012.

Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, Brussels, 27 April 2012.

Article 29 Data Protection Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force, 00678/13/EN, WP205, 22 April 2013.

Article 29 Data Protection Working Party, "Working Document on Biometrics", WP80, Brussels, 1 August 2003.

Aus, Jonathan P., "Decision making under Pressure: The Negotiation of the Biometric Passports Regulation in the Council, ARENA Centre for European Studies, Working Paper 11, Sept 2006.

Aventura Technologies, "Camera Tutorial".
http://www.aventuracctv.com/PDF/Aventura_Camera_Tutorial.pdf

Better Business Bureau, "ADT Security Services, Inc." http://www.bbb.org/south-east-florida/business-reviews/burglar-alarms-and-monitoring-systems/adt-security-services-in-boca-raton-fl-30001337#sealclick.

Biometrics Institute, Privacy Guidelines, Revised Draft, January 2012. http://www.biometricsinstitute.org/data/Privacy/BiometricsInstitute_BIOMETRICS_GUIDELINES_Revised_Subject_to_Approval.pdf

Bock, Kirsten, "EuroPriSe Trust Certification: An approach to strengthen user confidence through privacy certification", *Datenschutz und Datensicherheit*, Vol. 1, 2008.

Bolle, Ruud M., Jonathan H. Connell & Nalini K. Ratha, "Biometric Perils and Patches", *Pattern Recognition*, Vol. 35, 2002, pp. 2727-2738.

BSI, "CCTV". http://shop.bsigroup.com/Browse-By-Subject/Security/Electronic-Security-Systems/CCTV/

BSI, *BS 7958:2009 Closed circuit television (CCTV), Management and operation, Code of practice*, BSI, London, 30 Sept 2009.

BSI, *Installation and remote monitoring of detector-activated CCTV systems, Code of practice*, BSI, London, 31 July 2010.

Buckinghamshire County Council (UK), *Privacy Impact Assessment on the UTMC CCTV and ANPR System: Summary Report*.
http://democracy.buckscc.gov.uk/documents/s20018/PT14.11%20PIA%20Report.pdf

CCTV National Standards Forum. http://www.cnsf.co.uk/

CENELAC, "*European Standard EN 50132-1:2010 Alarm systems - CCTV surveillance systems for use in security applications",* 2010.
http://www.cenelec.eu/dyn/www/f?p=104:110:730415270979609::::FSP_PROJECT,FSP_LANG_ID:2485,25

CEN, CENELEC, ETSI, *Smart Grid Information Security*, November 2012. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_security.pdf

Chambre des Députés, Texte coordonné de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel modifiée par la loi du 31 juillet 2006, la loi du 22 décembre 2006, la loi du 27 juillet 2007, Luxembourg.
http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002mod_fr.pdf#pagemode=none

Chen, D., Y. Chang, R. Yan, J. Yang, "Tools for protecting the privacy of specific individuals in video", *EURASIP Journal on Applied Signal Processing*, Vol. 2007, Issue 1, 2007, pp. 107-107.

Cloud Security Alliance, "Privacy Level Agreement Working Group". https://cloudsecurityalliance.org/research/pla/

Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V3*.0. Cloud Security Alliance, 14 Nov 2011.
https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

Commission nationale de l'information et des libertés (CNIL), "Videosurveillance". http://www.cnil.fr/les-themes/videosurveillance/

Commission nationale de l'information et des libertés (CNIL), *Vidéosurveillance / vidéoprotection: les bonnes pratiques pour des systèmes plus respectueux de la vie privée*, Press communication, June 2012.

Consumer Centre Denmark, E-Commerce Trustmarks in Europe - an overview and comparison of Trustmarks in the European Union, Iceland and Norway, *Report*, 18 March 2010.

Consumer Focus, "Consumer Information: Smart meters – what are they and how can I find out more". http://www.consumerfocus.org.uk/get-advice/energy/smart-meters-what-are-they-and-how-can-i-find-out-more/privacy-and-security-issues

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12 and 13, Rome, 4 Nov 1950. http://www.echr.coe.int/Documents/Convention_ENG.pdf

Council of Europe Parliamentary Assembly, Video Surveillance in Public Areas, Resolution 1604 (2008). http://assembly.coe.int/ASP/Doc/XrefViewPDF.asp?FileID=17633&Language=en

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Explanatory Report. http://conventions.coe.int/Treaty/en/Reports/Html/108.htm

Council of the European Union, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No 108, Strasbourg, 28 Jan 1981.

Council of the European Union, Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJ L* 350, 30 Dec 2008, pp 60-71.

Daon, *European Union – Biometric Matching System*, White paper, 2008. http://daon.com/content/european-unions-biometric-matching-system

De Hert, Paul, Dariusz Kloza and David Wright, *Recommendations for a privacy impact assessment framework for the European Union, PIAF Deliverable D3*, Brussels, November 2012. http://www.piafproject.eu/ref/PIAF_D3_final.pdf

De Hert, Paul, Wim Schreurs and Evelien Brouwer, "Machine-readable identity documents with biometric data in the EU: Overview of the legal framework" *Keesing Journal of Documents & Identity*, Issue 27, 2007, pp. 23-26. http://www.vub.ac.be/LSTS/pub/Dehert/131.pdf

Department of Energy and Climate Change, *Smart Metering Implementation Programme: Data Access and Privacy: Government response to consultation*, London, Dec 2012. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf

Department of Homeland Security, *CCTV: Developing Privacy Best Practices*, Report on the DHS Privacy Office Public Workshop, 17-18 Dec 2007. http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf

Donbavand, Barry, *Sedgemoor District Council CCTV Impact Assessment S.4 ICO COP*, 28 Feb 2013 http://www.sedgemoor.gov.uk/CHttpHandler.ashx?id=12244&p=0

Doward, Jamie, "Energy smart meters are a threat to privacy, says watchdog", *The Observer*, 1 July 2012. http://www.guardian.co.uk/environment/2012/jul/01/household-energy-trackers-threat-privacy

ECORYS, *Security Regulation, Conformity Assessment & Certification Final Report – Volume I: Main Report*, European Commission, DG Enterprise & Industry, Brussels, October 2011.

EDPS, Opinion of the European Data Protection Supervisor on the Commission's Communication on Unleashing the potential of Cloud Computing in Europe, Brussels, 16 Nov 2012. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

ENISA, *Critical Cloud Computing, A CIIP perspective on cloud computing services, Version 1.0*, ENISA, Dec 2012.

ENISA, *ENISA Briefing: Behavioural Biometrics*, Jan 2010.

ENISA, *Security certification practice in the EU, Information Security Management Systems – A case study, Report*, Oct 2013.

ENISA, *Cloud Computing: Benefits, risks and recommendations for information security*, ENISA, 2009.

Energy UK, "Energy UK's Privacy Commitments for Smart Metering: Version 1.0". http://www.energy-uk.org.uk/publication/finish/37-smart-meters/448-era-privacy-commitments-for-smart-metering.html

EFUS, Charter for a democratic use of video-surveillance, 28 May 2010. http://www.cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Charta/CCTV_Charter_EN.pdf

European Commission, Directorate-General Justice, Freedom and Security, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments*, Final Report, 20 Jan 2010.
http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

European Commission Enterprise and Industry Directorate-General, *Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability*, Brussels, 12 March 2009. http://www.cen.eu/cen/Sectors/Sectors/Measurement/Documents/M441.pdf

European Commission DG Environment, "The IPPC Directive: Summary of Directive 2008/1EC concerning integrated pollution prevention and control (The IPPC Directive)", 30 Nov 2012. http://ec.europa.eu/environment/air/pollutants/stationary/ippc/summary.htm

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25 Jan 2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

European Commission, Communication from the Commission to the European Parliament, the Council, the 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, Brussels, 4 Nov 2010. http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

European Commission, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529 final, Brussels, 27 Sept 2012.

European Commission, Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems, *OJ L* 73/9, Brussels, 13 March 2012.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:EN:PDF

European Commission, 2252/2004/EC of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *OJ L* 385, 29 Dec 2004, pp. 1-6.

European Committee for Electrotechnical Standardization (CENELEC), EN 50132-7 Alarm systems - CCTV surveillance systems for use in security applications Part 7: Application guidelines, ICS 13.320, June 1996.

European Consumer Centres Network (ECC-Net), "Can I trust the trustmark?" *Trustmarks Report 2013*, October 2013.

European Data Protection Supervisor (EDPS), *The EDPS Video-surveillance Guidelines*, Brussels, 17 March 2010.
https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD),A7-0402/2013, 21 Nov 2013.

European Parliament and the Council, Directive 95/46/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, *OJ L* 281, 23 Nov 1995, pp. 0031-0050.

European Parliament and the Council, Directive 2006/114/EC of 12 December 2006 concerning misleading and comparative advertising, *OJ L* 376, pp. 21-27.
European Parliament and the Council, Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), OJ L 149, 11.6.2005, p. 22.

European Parliament and the Council, Regulation 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *OJ L* 8, 12 Jan 2001, pp. 1-22.

European Parliament and the Council, Directive 2009/72/EC of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, *OJ L* 211/55, 14 Aug 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:0093:EN:PDF

European Parliament, the Council and the Commission, Charter of Fundamental Rights of the European Union, *Official Journal of the European Union*, C 83/391, 30 March 2010.

Expert Group 2, *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety and Consumer Protection: Recommendation to the European Commission, V1.0*, 5 Dec 2011.

Fitzgerald, Michael, "Finding and fixing a Home's Power Hogs", *The New York Times,* 27 July 2008. http://www.nytimes.com/2008/07/27/technology/27proto.html

Foley, Mark F. "Data Privacy and Security Issues for Advanced Metering Systems (Part 2)", *Smart Grid News*, 1 Jul 2008. http://www.smartgridnews.com/artman/publish/industry/Data_Privacy_and_Security_Issues_for_Advanced_Metering_Systems_Part_2.html

Garante per la Protezione dei Dati Personali, *Cloud Computing. How to protect your data without falling from a cloud*, Rome, June 2012.

Gellman, Robert, "TRUSTe fails to justify its role as privacy arbiter", *Privacy Law and Policy Reporter*, Vol. 7, No. 6, Dec 2000.
http://www.austlii.edu.au/au/journals/PLPR/2000/53.html.

Gill, Martin & Angela Spriggs, *Home Office Research Study 292: Assessing the Impact of CCTV*, Home Office Research, Development and Statistics Directorate, Feb 2005.

Goldstein, James, Rina Angeletti, Manfred Holzbach, Daniel Konrad, Max Snijder & Pawel Rotter, *Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats*. European Commission Joint Research Centre, Seville, Oct 2008. http://www.a-sit.at/pdfs/biometrics_report.pdf

Goold, Benjamin, "CCTV and Human Rights" in European Forum for Urban Security (ed.), *Citizens, Cities and Video Surveillance, Towards a democratic and responsible use of CCTV*, June 2010, pp. 27-36.

Goold, B., *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*, Oxford University Press, Oxford, 2004.

Hampapur, Arun, Sharathchandra Pankanti, Andrew William Senior, "System and practice for surveillance privacy-protection certification and registration", US8494159 B2, Application No. US 12/062,978, 23 July 2013. http://www.google.com/patents/US8494159

Hargreaves, Tom, Michael Nye and Jacquelin Burgess, "Making energy visible: a qualitative field study of how householders interact with feedback from smart energy monitors", *Energy Policy*, Vol. 38, No.10, 1 Oct 2010, pp. 6111-6119.

Hier, S. and K. Walby, "Privacy Pragmatism and Streetscape Video Surveillance in Canada," *International Sociology*, Vol. 26, No. 6, 2011, pp. 844–861.

Home Office, *Surveillance Camera Code of Practice Pursuant to Section 29 of the Protection of Freedoms Act 2012.*
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

Iglezakis, Ioannis, "EU data protection legislation and case-law with regard to biometric application" SSRN, 18 June 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2281108

Information Commissioner's Office, *CCTV Code of Practice*, 2008.
http://www.ico.org.uk/Global/faqs/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx

Information Commissioner's Office, Guidance on the Use of Cloud Computing, Version: 1.1, 2 Oct 2012.
http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

Information and Privacy Commissioner, Ontario, Canada and Future of Privacy Forum, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, Nov 2009. http://www.ipc.on.ca/images/Resources/pbd-smartpriv-smartgrid.pdf

International Organization for Standardization, "Abstract, ISO/IEC 19794-2:2011 Information Technology – Biometric Data Interchange formats". http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50864

ISO/IEC, Technical Report 24714-1:2008 Information Technology – biometrics – Jurisdictional and societal considerations for commercial applications – part 1 General Guidance. http://www.iso.org/iso/catalogue_detail?csnumber=38824

Jaruwek Marek, Martin John, and Florian Kerschbaum, "Plug in Privacy for Smart Metering Billing" in S. Fischer-Hübner and N. Hopper (eds.), *Privacy Enhancing Technologies: 11th International Symposium*, 2011. http://link.springer.com/chapter/10.1007/978-3-642-22263-4_11#page-2

Kalogridis, G., C. Efthymiou, S.Z. Denic, T.A. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards undetectable load signatures", First IEEE International Conference on Smart Grid Communications, Gathersburg, 2010.

Katz, Hagai, "Access Denied". http://www.magal-s3.com/contentManagment/uploadedFiles/In_the_Press/Airports_World_-Access_denied_AW6.pdf

LaRose, Robert, and Nora Rifon, "Your privacy is Assured of Being Disturbed: Websites With and Without Privacy Seals", *New Media & Society*, Vol. 8, No. 6, 2006.

Lim, Laurent, "The legal framework of video surveillance in Europe", in European Forum for Urban Security (ed.), *Citizens, Cities and Video Surveillance: Towards a democratic and responsible use of CCTV*, June 2010, pp.81-98.

Lisovich, Michael, A., Stephen B. Wicker, "Privacy concerns in upcoming residential and commercial demand-response systems" *IEEE Proceedings on Power Systems,* Vol.1, No.1, March 2008.

Lockstep Consulting, *PIA Report: Advanced Metering Infrastructure (AMI), Version 1.2*, Department of Primary Industries, Victoria, Canada. August 2011.

Mansfield, Tony, "BioTesting Europe: Addressing European needs for testing and assurance of biometric systems", BioTesting Europe, Presentation to Biometrics Consortium Conference, Baltimore, 13 Sept 2007.
http://www.biometrics.org/bc2007/presentations/Thu_Sep_13/Session_III/13_Mansfield_STATUS.pdf

Mathieson, S.A., "UK gov's smart meter dream unplugged: a 'Colossal waste of cash': Everything you need to know about the kit that'll know everything about you", *The Register*, 19 July 2013. http://www.theregister.co.uk/2013/07/19/feature_uk_gov_power_meter_plan/

McDaniel, P. and S. McLaughlin, "Security and Privacy challenges in the smart grid", *Security and Privacy, IEEE*, Vol. 7, No.3, 1 May 2009.

Mell, Peter and Tim Grance, *The NIST Definition of Cloud Computing, Version 15*. National Institute of Standards and Technology, Information Technology Laboratory, 10 July 2009. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

Metering.com, "Smart Meters to not be compulsory in Netherlands", 14 April 2009. http://www.metering.com/smart-meters-not-to-be-compulsory-in-netherlands/

McKenna, Eoghan, Ian Richardson and Murray Thomson, "Smart meter data: Balancing consumer privacy concerns with legitimate applications", *Energy Policy*, Vol.41, 1 Feb 2012. pp. 807-814.

Moores, Trevor, "Do Consumers Understand the Role of Privacy Seals in E-commerce?" *Communications of the ACM*, Vol. 48, No. 3, March 2005, pp. 86-91.

Murrill, Brandon, J., Edward C. Liu and Richard M. Thompson II, *Smart Meter Data: Privacy and Security*, Congressional Research Service, 3 Feb 2012.

National Council of the Slovak Republic, Act No. 428/2002 Coll. on Protection of Personal Data, as amended by the Act No. 602/2003 Coll., Act No. 576/2004 Coll. and the Act No. 90/2005 Coll. http://www.dataprotection.gov.sk/buxus/docs/act_428.pdf

Navigator, *Smart Metering – Data Access and Privacy: Public Attitudes Research*, Department of Energy & Climate Change, Dec 2012.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43045/7227-sm-data-access-privacy-public-att.pdf

Neustaedter, C., S. Greenberg, M. Boyle, "Blur filtration fails to preserve privacy for homebased video conferencing", *ACM Transactions on Computer Human Interactions*, Volume 13, Number 1, March 2006, pp. 1-36.

Norris, Clive, *A Review of the Increased Use of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe*, Civil Liberties, Justice and Home Affairs Committee (LIBE), European Parliament, April 2009.

Norwegian Parliament, Act of 14 April 2000 No. 31 relating to the processing of personal data (Personal Data Act), 14 April 2000. http://www.ub.uio.no/ujur/ulovdata/lov-20000414-031-eng.pdf

NSAI, "CCTV Certification". http://www.nsai.ie/Our-Services/Certification/Product-Certification/Product-Certificaton-for-Security-Systems/IS-EN-5013---CCTV-Certification.aspx

Office of the Privacy Commissioner of Canada, "Fact Sheets: Cloud Computing" October 2011. https://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_02_e.asp

Parliament of the Czech Republic, Personal Data Protection Act, Act no. 101/2000 Coll., of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts, 2000. http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&lang=en

Pearson, Siani, "Data Protection in the Cloud" Cloud Security Alliance. https://chapters.cloudsecurityalliance.org/uk/2012/12/13/data-protection-in-the-cloud/

Ponemon Institute, *Perceptions about Privacy on the Smart Grid*, Nov 2010.

Prabhakar, Saul, Sharath Pankanti and Anil K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy*, March/April 2003, pp.33-44.

President of the Republic of Italy, Personal Data Protection Code, Legislative Decree no. 196 of 30 June 2003. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2427932

Privacy International, "Response to the European Commission's Communication on the 'Comprehensive Approach on Personal Data Protection in the European Union", January 2011. http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/ pi_en.pdf

Regalado, Antonio, "Rage against the Smart Meter" *MIT Technology Review*, 26 April 2012. https://www.technologyreview.es/printer_friendly_article.aspx?id=40018

Renner, Stephan, Mihaela Albu, Henk van Elburg, Christoph Heinemann, Artur Lazicki, Lauri Penttinen, Francisco Puente, and Hanne Saele. *European Smart Metering Landscape Report: SmartRegions Deliverable 2.1*, Vienna, February 2011. http://www.piio.pl/dok/European_Smart_Metering_Landscape_Report.pdf

Rial, Alfredo, and George Danezis, "Privacy-Preserving smart metering", WPES 11 Proceedings of the 10th Annual ACM workshop on Privacy in the Electronic Society, ACM, New York, 2011.

Richards, Patsy, and Mike Fell, "Smart Meters", *House of Commons Library Note*, 20 June 2013

Rodrigues, Rowena, David Wright and Kush Wadhwa, "Developing a privacy seal scheme (that works)" *International Data Privacy Law*, Vol. 3, Issue 2, 2013.

Rodrigues, Rowena, David Barnard-Wills, David Wright, Paul De Hert and Vagelis Papakonstantinou, *Inventory and Analysis of Privacy Certification Schemes: Final Report Study Deliverable 1.4*, Publications Office of the European Union, Luxembourg, 2013.

Rodrigues, Rowena, David Barnard-Wills, David Wright, Luca Remotti, Tonia Damvakeraki, Paul De Hert & Vagelis Papakonstantinou, *Task 2: Comparison with other EU certification schemes, D2.4, Final report*, EU Privacy Seals Study, European Commission Joint Research Centre, Institute for Protection and Security of the Citizen, 2013.

SAFRAN Morpho, "Morpho, Worlds First Company to Receive Common Criteria Certification for Fake Finger Detection", Press Release, Paris, 2 July 2013.

Samani, Raj, "Addressing security and privacy issues with smart meters", *Grid Insights*, 11 Dec 2012. http://gridinsights.energycentral.com/detail.cfm/detail.cfm/Addressing-security-and-privacy-issues-with-smart-meters?id=71

Senior, Andrew, "Privacy protection in a Video Surveillance System", in Andrew Senior (ed.), *Protecting Privacy in Video Surveillance*, Springer, New York, 2009.

Smart Grid Interoperability Panel – Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, NIST, August 2010. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

Smartmeters, "Smart Meter Privacy and Security", 30 Sept 2013. http://www.smartmeters.vic.gov.au/privacy

Sprokkereef, Annemarie, and Bert-Jaap Koops, *D3.16: Biometrics: PET or PIT?* FIDIS, 20 Aug 2009. http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables2/fidis-WP3-del3.16-biometrics-PET-or-PIT.PDF

Task Force Smart Grids, Expert Group 2, *Regulatory Recommendations for Data Safety, Data Handling and Data Protection*, 16 Feb 2011. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf

The Economist, *Privacy uncovered; Can private life exist in the Digital Age? A report from the Economist Intelligence Unit*, 2013.

The Future of Privacy Forum and the Information and Privacy Commissioner, Ontario, Canada, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, Toronto, Nov 2009. http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf

TRUSTe, "ADT LLC", 11 Jan 2013. http://privacy.truste.com/privacy-seal/ADT-LLC/validation?rid=9e4c2a3a-1a6d-4bb8-baac-d33720fdc07f

Urbaneye, *On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts*, Final report, Office for Official Publications of the European Communities, Luxembourg, HPSE-CT-2001-00094. http://cordis.europa.eu/documents/documentlibrary/100123891EN6.pdf

Webster, C. William R., "CCTV Policy in the UK: Reconsidering the Evidence Base", *Surveillance & Society*, Vol. 6, No. 1, 2009, pp. 10-22.

Wissner, Mathias, "The Smart Grid – A saucerful of secrets?" *Applied Energy*, No. 88, 2011, pp. 2509-2518.

Wolf, Andreas, *Technical Report: A consensus on conformance and interoperability mechanisms, both for applications and sensors, in order to reach security evaluated interoperable solutions between the European Union Member States*, CEN, Focus Group on Biometrics, Brussels, 29 March 2009.

Wright, David (ed.), *Surveillance, fighting crime and violence*, Deliverable D1.1. A report of the IRISS consortium to the European Commission, December 2012. http://irissproject.eu/wp-content/uploads/2012/02/IRISS_D1_MASTER_DOCUMENT_17Dec20121.pdf.

Wright, David and Paul De Hert, "Introduction to Privacy Impact Assessment," in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, 2012, pp. 3-32.

European Commission
EUR 26699 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: EU Privacy seals project

Authors: Paul De Hert, Vagelis Papakonstantinou, Rowena Rodrigues, David Barnard-Wills, David Wright, Luca Remotti, Tonia Damvakeraki

2014 – 137 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-38672-5

doi:10.2788/85717

Abstract

The objective of this report is focus on the challenges of implementing an effective EU privacy seal and its possible scope. It returns the focus to privacy and data protection, and presents further groundwork to feed into Task 4 of the Study (Proposals and evaluation of options for an EU-wide privacy seals scheme). Where relevant, research results and analyses of Tasks 1 and 2 are used.

First, the report assesses the gaps in current privacy seal sector. Next, it highlights the advantages of, priorities for and possible scope of an EU privacy seal scheme. Eventually, four case studies (CCTV systems, cloud services, smart metering systems and biometric systems) illustrate the possible scope of an EU privacy seal scheme and demonstrate whether an EU privacy seals scheme would bring any added value to privacy and data protection.

LB-NA-26699-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

doi:10.2788/85717

ISBN 978-92-79-38672-5

Publications Office